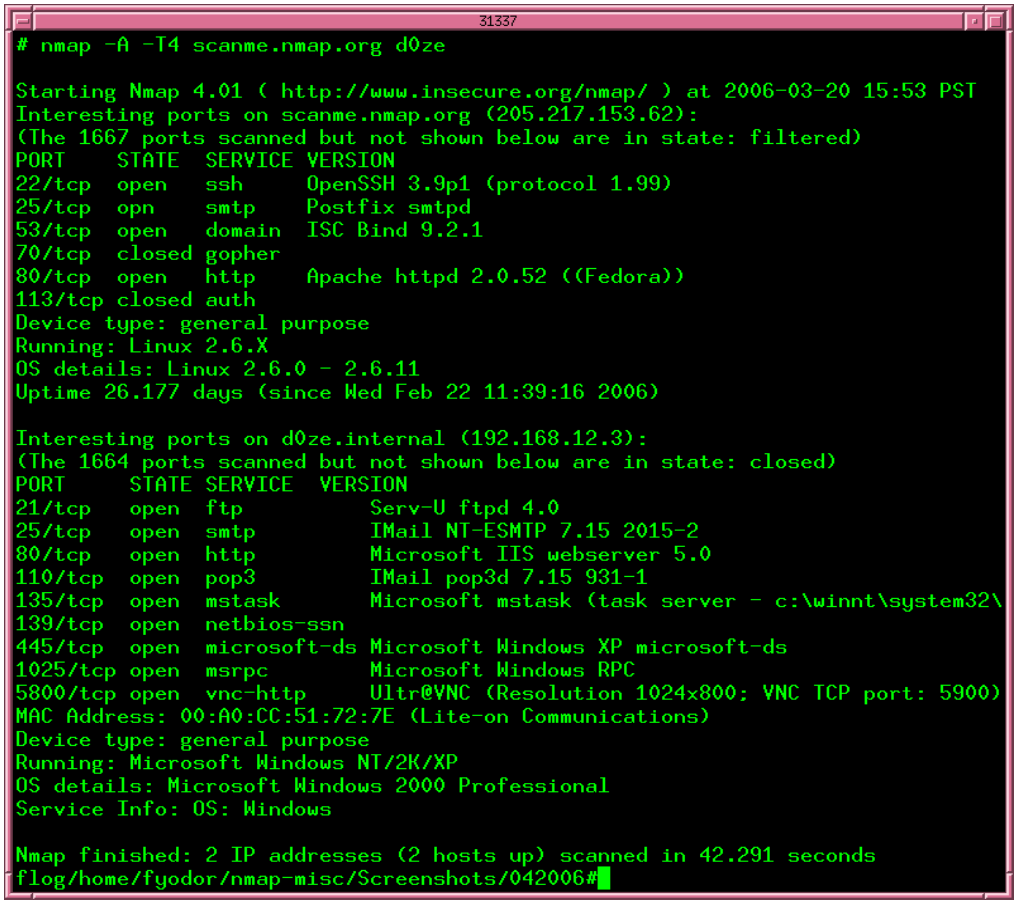
Port scanning: poging tot inbraak in een geautomatiseerd systeem?



Scriptie in het kader van de studie Rechtsgeleerdheid
Universiteit van Amsterdam

mr. drs. J. Timmer
Winterswijk, september 2006

Afstudeercommissie:
mr. drs. C.F. Mulder
mr. drs. M.M. Dolman

Voorwoord

"Sendai needs only a little bit of information about the targets right now. Most importantly, he wants to know what operating system they are running so that he can tailor his rootkit appropriately. For this purpose, he obtains the latest Nmap Security Scanner. Sendai considers what options to use. Certainly he will need ***-sS -F****, which specifies a stealth SYN TCP scan of about a thousand common ports. The* ***-P0*** *option ensures that the hosts will be scanned even if they do not respond to Nmap ping probes, which by default include an ICMP echo request message as well as a TCP ACK packet sent to port 80. Of course* ***-O*** *will be specified to provide OS detection. The* ***-T4*** *option speeds things up, and* ***-v*** *activates verbose mode for some additional useful output. Then there is the issue of decoys. This Nmap option causes the scan (including OS detection) to be spoofed so that it appears to come from many machines. A target administrator who notices the scan will not know which machine is the actual perpetrator and which are innocent decoys. Decoys should be accessible on the Internet for believability purposes. Sendai asks Nmap to find some good decoys by testing 250 IP addresses at random…"*

(Fyodor, 'Return on investment' in R. Russell e.a., *Stealing the network, How to own a continent*, Rockland, Syngress Publishing, Inc., 2004)

Voor velen is het zoeken naar een geschikt onderwerp voor een scriptie niet makkelijk. Voor u ligt echter een scriptie waarvan het onderwerp voor mij al jarenlang vast stond. Vanwege het feit dat een studie Informatica aan een universiteit destijds niet binnen de mogelijkheden lag, heb ik, na mijn studie Bestuurskunde gekozen voor de studie Nederlands recht. De interesse voor informatica en ICT en met name het onderwerp hacking is echter sinds de middelbare school nooit weg geweest en zie hier het resultaat: een perfecte combinatie tussen ICT en strafrecht.

Hiervoor wil ik mijn voormalig teamleider, mr. W. van Horen, alsnog hartelijk danken. Nadat ik namelijk na enkele jaren fiscaal recht te hebben gestudeerd tot de ontdekking kwam dat dit "not my cup of tea" was, heb ik met hem in goed overleg besloten te switchen naar Nederlands recht. Dit bood mij de mogelijkheid vakken te volgen die in de lijn lagen van mijn interesses en papers te schrijven over onderwerpen die gerelateerd waren aan hacking, cybercrime en netwerk- en informatiebeveiliging.

Een van de echte hackers die ik sinds lange tijd bewonder is de auteur van Nmap (Network Mapper). Nmap, geschreven door Fyodor, biedt systeembeheerders de mogelijkheid hun netwerk te scannen op zwakke plekken. De tool is om deze reden ook zeer geliefd onder hackers om, na een scan van een netwerk, te bepalen waar zij hun aanval kunnen inzetten om een geautomatiseerd systeem binnen te dringen. Toen ik voor het eerst met Nmap in aanraking kwam, kwam bij mij reeds de gedachte op of deze verkenning van een netwerk met Nmap een voorbode is voor een daadwerkelijke poging tot

inbraak in een geautomatiseerd systeem. Het onderwerp voor mijn scriptie was geboren!

Tijdens het schrijven van de scriptie kwam ik tot de ontdekking dat verhandelingen over de pogingsleer in het strafrecht volop te vinden waren maar dat een combinatie tussen de pogingsleer en computervredebreuk een compleet onontgonnen terrein was. Ik ben me er daarom van bewust dat de inhoud van de scriptie voor sommigen vragen kan doen oproepen voor wat betreft de technische aspecten en de daarbij gebezigde begrippen en afkortingen. Daarom wil ik u nu reeds attenderen op de bijlagen met begrippen en afkortingen die de inhoud van deze scriptie wellicht kunnen verduidelijken.

Ik wil in de eerste plaats mijn begeleider, mr. drs. C.F. Mulder, bedanken voor zijn uitstekende begeleiding. Hij heeft mij vanaf het moment dat ik het onderwerp van mijn scriptie aan hem kenbaar maakte, gesteund bij mijn keuze voor dit onderwerp, ondanks dat voor hem het technische aspect van de scriptie redelijk onbekend was. De korte terugkoppelingen via de e-mail en de korte persoonlijke besprekingen gaven mij een grote mate van vrijheid om in Winterswijk aan de scriptie te werken met daarnaast toch het gevoel van begeleiding op grote afstand vanuit Amsterdam.

Voorts ben ik de FIOD-ECD erkentelijk voor de studiefaciliteiten die ik heb gekregen en die mij hiertoe in staat gesteld hebben deze opleiding af te ronden. Tenslotte wil ik vooral het thuisfront bedanken voor hun steun en het geduld als zij mij weer eens een heel weekend moesten missen vanwege allerlei studieverplichtingen.

Winterswijk, september 2006

drs. Jaap Timmer

Inhoudsopgave

1 Inleiding

1.1 Achtergrond en aanleiding

The judge rejected that claim, as well as an argument that the port scan, and a throughput test Moulton allegedly aimed at the VC3 system, threatened public health and safety. "The tests run by Plaintiff Moulton did not grant him access to Defendant's network", wrote the judge. "The public data stored on Defendant's network was never in jeopardy."[1]

Het opzettelijk wederrechtelijk binnendringen in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, is in Nederland strafbaar gesteld in artikel 138a lid 1-3 van het Wetboek van Strafrecht (WvSr). De omschrijving van het delict computervredebreuk in artikel 138a lid 1-3 WvSr betreft echter een voltooid delict waarbij tevens nog als voorwaarde gesteld wordt dat bij het 'wederrechtelijk binnendringen' er enige beveiliging bij doorbroken is of de toegang is verworven door een technische ingreep. De voorafgaande fase, die voor een hacker cruciaal is om een succesvolle aanval te kunnen uitvoeren, is echter tot nu toe niet strafbaar gesteld. Zowel niet op nationaal als internationaal niveau.

Het bovenstaande oordeel uit 2000 van de rechter van het Federal Court of Georgia in de Verenigde Staten dat het uitvoeren van een port scan niet strafbaar is aangezien de veiligheid en openbare orde hiermee niet in gevaar komt betreft deze voorafgaande fase. Port scans worden door hackers vaak toegepast om vast te stellen welke TCP- en UDP-poorten op externe systemen luisteren en zijn in deze fase een mogelijke indicatie dat er een gerichte aanval op een geautomatiseerd systeem, het doelsysteem, op handen is.

Voordat een geautomatiseerd systeem kan worden gehackt, moeten drie essentiële stappen genomen worden door de hacker. Ten eerste dient de hacker een profiel vast te stellen (footprinting) van het gebruik van de doelsystemen. Bij een delict als diefstal zullen dieven niet gewoon een bank binnen gaan en vragen om geld. Ze zullen eerst alle mogelijke moeite doen om informatie over de bank te vergaren: routes en aflevertijden van het geld, vluchtwegen, kortom alles wat maar van belang kan zijn om de overval succesvol te laten verlopen.

Succesvolle hackers volgen dezelfde methode. Ze moeten een massa informatie verzamelen om een doelgerichte, chirurgische aanval te kunnen uitvoeren. Ze proberen dan ook zoveel mogelijk te weten te komen van de beveiligingsaspecten van een organisatie. Uiteindelijk bezitten ze een uniek profiel van de aanwezigheid van een organisatie op Internet, externe toegang en intranet / extranet.[2]

Als het opstellen van een profiel vergelijkbaar is met het doorzoeken van een gebouw door een inbreker die op zoek is naar informatie kan scannen, de tweede stap, worden vergeleken met het op

1 Zie <http://www.securityfocus.com/print/news/126>

2 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 10

alle muren kloppen om alle deuren en ramen te vinden die open staan. Port scans stellen vast welke systemen luisteren naar inkomend netwerkverkeer (actieve systemen) en via Internet bereikbaar zijn.[3]

Als de indringer met behulp van technieken en tools voor port scanning erachter is gekomen welke doelsystemen en services actief zijn, zal deze zijn aanval richten op de bekende zwakke plekken van de actieve services. Dit proces wordt enumeratie genoemd en gebeurt veelal door zogenaamde vulnarability scanners.

Het belangrijkste verschil tussen enumeratie en het hierboven genoemde footprinting en scanning zit in de mate waarin in een systeem wordt binnengedrongen. Bij enumeratie is er sprake van actieve verbindingen met systemen en gerichte queries. Als zodanig kunnen ze gelogd of anderszins geregistreerd worden.[4]

Omdat vrijwel alle firewalls alarm slaan als er een port scan wordt uitgevoerd op een doelsysteem kunnen ook deze port scans gelogd worden in de firewall-logs. In veel gevallen betreft het slechts een enkele scan of soms een actieve verbinding van de computer met een Domain Name System-server (DNS-server) die door de firewall geregistreerd wordt. Indien echter in de firewall-logs meerdere port scans van één IP-adres, het bronadres, worden vermeld op specifieke poorten van het doelsysteem kan mogelijk worden gesproken van een gerichte verkenning van het doelsysteem op luisterende TCP- en UDP-poorten. Een port scan is hiermee de eerste zichtbare aanwijzing op het doelsysteem dat er een gerichte aanval op handen is.

De vergelijking die McClure, Scambray en Kurtz maken ten aanzien van scanning[5], het op alle muren kloppen om alle deuren en ramen te vinden die open staan, maakt het mogelijk een vergelijking te maken tussen een poging tot een normale inbraak of een poging tot een ander delict en een poging tot inbraak in een geautomatiseerd systeem. Het leerstuk van de poging heeft een aantal facetten, die zich in vragende vorm aldus laten omschrijven:[6]

- Had de dader het voornemen om een misdrijf te plegen?
- Heeft dit voornemen zich geopenbaard?
- Is het openbaren van het voornemen geschied door een begin van uitvoering van het misdrijf? (uitvoeringshandeling – voorbereidingshandeling)
- Is de uitvoering alleen niet voltooid ten gevolge van omstandigheden van de wil van de dader onafhankelijk (al dan niet vrijwillige terugtred)

In dit onderzoek wil ik nagaan of port scanning op dit moment strafbaar is en, indien dit niet het geval is, of dit in de toekomst strafbaar gesteld dient te worden, zowel op nationaal als internationaal niveau.

3 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 36
4 Ibid, p. 70
5 Ibid, p. 36
6 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, editie 2004, p. 552

Hiervoor dient eerst vastgesteld te worden welke nationale en internationale wetgeving op dit moment relevant is ten aanzien van computervredebreuk. Vervolgens zal ik deze wetgeving relateren aan het leerstuk van de poging aan de hand van bovengenoemde facetten om te kijken of er sprake kan zijn van een strafbare poging tot inbraak in een geautomatiseerd systeem indien er sprake is van port scanning. Omdat er op het Internet dagelijks grote hoeveelheden scans, doch met verschillende frequenties en intenties, plaatsvinden, zal vastgesteld moeten worden van welk niveau en vooral met welke intentie er sprake moet zijn van port scanning voor er van een gerichte poging tot inbraak sprake is. Deze intentie zou kunnen blijken uit de frequentie van de port scans op een doelsysteem en de specifiek gescande poorten.

Om een goede vergelijking te kunnen maken tussen de uitvoerings- en voorbereidingshandelingen die bij een normale poging tot inbraak of bij een poging tot een ander delict worden gepleegd en de uitvoerings- en voorbereidingshandelingen die door een hacker gepleegd moeten worden om een inbraak in een geautomatiseerd systeem te plegen, zal ik de voorafgaande fases aan een inbraak in een geautomatiseerd systeem beschrijven om een goede vergelijking te kunnen maken tussen een poging tot een ‘gewone’ inbraak en een poging tot inbraak in een geautomatiseerd systeem.

1.2 Probleemstelling en onderzoeksvragen

De probleemstelling die als leidraad voor mijn onderzoek zal fungeren luidt:

Is port scanning op dit moment strafbaar op nationaal en internationaal niveau en is het wenselijk dit in de toekomst strafbaar te stellen op nationaal en internationaal niveau ter beveiliging van geautomatiseerde systemen?

Om een antwoord op deze probleemstelling te vinden, is het onderzoek opgedeeld in een aantal onderzoeksvragen:

1. Welke wetgeving is op dit moment relevant voor computervredebreuk op nationaal en internationaal niveau?
2. Is port scanning naar zijn uiterlijke verschijningsvorm te beschouwen als een poging tot inbraak in een geautomatiseerd systeem?
3. Van welk niveau en met welke intentie moet er sprake zijn van port scanning voor er van een gerichte poging tot inbraak sprake is?
4. Moet port scanning strafbaar worden gesteld op nationaal en internationaal niveau ter beveiliging van geautomatiseerde systemen en is dit juridisch en technisch haalbaar?

In het volgende hoofdstuk zal ik ter verduidelijking eerst een beschrijving geven van footprinting, port scanning en enumeratie, de gebruikte technieken en de samenhang met de uiterlijke kenmerken van

een normale inbraak. In hoofdstuk drie komt onderzoeksvraag een, de huidige nationale en internationale wetgeving, aan de orde. Om te kunnen bepalen of een port scan gekwalificeerd zou kunnen worden als een poging tot inbraak in een geautomatiseerd systeem zal ik in hoofdstuk vier de pogingsleer uit het Wetboek van Strafrecht en de relevante geldende jurisprudentie ten aanzien van de pogingsleer relateren aan port scanning en hiermee onderzoeksvragen twee en drie bespreken. Onderzoeksvraag vier, de juridische en technische haalbaarheid van strafbaarstelling van port scanning bespreek ik tezamen met de conclusies en tevens zal ik hierin enkele aanbevelingen doen.

2 Footprinting, port scanning en enumeratie

2.1 Inleiding

Voordat een goede vergelijking tussen een poging tot een normale inbraak en een poging tot een inbraak in een geautomatiseerd systeem mogelijk is, dienen de voorafgaande fases beschreven te worden om te kijken welke uitvoerings- en voorbereidingshandelingen voor een hacker noodzakelijk zijn om een gerichte aanval te kunnen uitvoeren. De nadruk zal hierbij liggen op de port scan aangezien deze handeling de eerste zichtbare aanwijzing is op het doelsysteem dat er mogelijk een inbraak op handen is en hieruit in eerste instantie de intentie van de hacker zou kunnen blijken door de frequentie, ruchtbaarheid en decoys van port scans. Ik ga in dit hoofdstuk niet expliciet in op de technieken en tools voor footprinting en enumeratie doch bespreek de handelingen in deze fases wel omdat deze in combinatie met port scanning van belang zijn om de intentie van de hacker te bepalen.

2.2 Footprinting

Door systematisch een profiel van het karakteristieke gebruik van de doelsystemen vast te stellen, krijgen hackers een volledig beeld van de beveiligingssituatie van het doelsysteem. Via een combinatie van hulpmiddelen en technieken kunnen ze een onbekende grootheid nemen, bijvoorbeeld de Internetverbinding van www.marktplaats.nl, en die reduceren tot een specifieke reeks domeinnamen, netwerkblokken en individuele IP-adressen van systemen die direct met het Internet verbonden zijn. Alle technieken zijn erop gericht informatie te verkrijgen die betrekking heeft op de volgende omgevingen: Internet, intranet, externe toegang en extranet.[7]

Het vaststellen van een profiel is noodzakelijk voor een hacker om zich er systematisch van te verzekeren dat alle informatie met betrekking tot de genoemde omgevingen geïdentificeerd worden. Technieken die gebruikt kunnen worden zijn onder andere het uitvoeren van whois-queries en het downloaden van DNS-zoneoverdrachten om een lijst op te stellen van de netwerken met bijbehorende individuele IP-adressen. Deze technieken verstrekken hackers waardevolle informatie, zoals namen, telefoonnummers, IP-adresgroepen, DNS-servers, mailservers en e-mailadressen.

Indien een IP-adres voorkomt in een DNS-zoneoverdracht betekent dit niet meteen dat het systeem bereikbaar is via Internet. Elk doelsysteem zal getest moeten worden om te zien of het actief is en op welke poorten het luistert. Hiervoor kan een port scanner gebruikt worden die de TCP/IP-stack van systemen controleert op poorten die in de LISTEN-toestand staan. Voor port scanning zijn verschillende scantechnieken ontwikkeld; ieder met een verschillende vorm en volledigheid van de verbinding met het doelsysteem. Deze verschillende vormen en volledigheid van de verbinding dienen er ten eerste voor om de actieve poorten te bepalen en ten tweede om het risico van ontdekking te beperken. De verschillende scantechnieken en de volledigheid van de verbinding met het doelsysteem worden in de hieronder volgende paragraaf besproken.

7 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 10

2.3 Port scanning

Het begin van de verkenning van een doelsysteem en een van de meest essentiële stappen om een netwerk in kaart te brengen, is het uitvoeren van een automatische ping-sweep op een groep IP-adressen en netwerkblokken om vast te stellen welke individuele systemen actief zijn. Het ping-commando wordt traditioneel gebruikt om ICMP ECHO-pakketten (type 8) naar een doelsysteem te sturen om te zien of er een ICMP ECHO_REPLY (type 0) teruggestuurd wordt, wat aangeeft dat het doelsysteem actief is.

Als ICMP-verkeer geblokkeerd wordt door een firewall is port scanning een alternatieve methode om actieve hosts te identificeren. Door te scannen op algemene poorten op elk potentieel IP-adres kan worden vastgesteld welke systemen actief zijn als er open of luisterende poorten op het doelsysteem geïdentificeerd kunnen worden.

Port scanning is het proces waarbij verbinding wordt gemaakt met TCP- en UDP-poorten op het doelsysteem om vast te stellen welke services er actief zijn en zich in een LISTEN-toestand bevinden. Het identificeren van luisterende poorten is heel belangrijk om vast te stellen wat voor besturingssysteem en toepassingen er gebruikt worden. Actieve services die luisteren, kunnen een onbevoegde gebruiker toelaten tot systemen die onjuist geconfigureerd zijn of een softwareversie hebben met bekende zwakke plekken op het gebied van beveiliging. De belangrijkste doelstellingen van een port scan op een doelsysteem zijn:[8]

- Identificeren van zowel de TCP- als UDP-services die op het doelsysteem worden uitgevoerd;
- Identificeren van het type besturingssysteem van het doelsysteem en
- Identificeren van specifieke toepassingen of versies van een bepaalde service.

Voordat ik een van de meest gebruikte hulpmiddelen voor port scanning met daarin verschillende mogelijkheden om een verbinding tot stand te brengen om het risico op ontdekking te verkleinen zal bespreken, zal ik eerst de de wijze waarop de verbinding tot stand komt tussen een client en een server schetsen alsmede de verschillende port scantechnieken.

Als een client, bijvoorbeeld een webbrowser, verbinding wil maken met een server, de site waarop een webserver draait, verstuurt de client een SYN-pakket richting de server. De server antwoordt hierop met een SYN/ACK-pakket die hij verstuurt richting de client. De client antwoordt hierop weer richting de server met een ACK-pakket. Indien deze ‘three-way-handshake’ voor een TCP-verbinding zonder onderbrekingen wordt afgelegd is er een verbinding tot stand gekomen tussen de client en de server. Port scanners en port scantechnieken maken gebruik van deze ‘three-way-handshake’ om luisterende poorten en actieve services te ontdekken. De port scantechnieken die kunnen worden onderscheiden

8 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 44

zijn:[9]

- TCP-verbindingsscan. Dit type scan maakt een verbinding met de doelpoort en voert een volledige drievoudige handshake uit (SYN, SYN/ACK en ACK). Dit type scan kan gemakkelijk door het doelsysteem ontdekt worden.
- TCP SYN-scan. Deze techniek wordt half-open scanning genoemd omdat er geen volledige verbinding wordt gemaakt. In plaats daarvan wordt er een SYN-pakket naar de doelpoort verstuurd. Als een SYN/ACK van de doelpoort ontvangen wordt, kunnen we concluderen dat de poort de status LISTENING heeft. Als een RST/ACK wordt ontvangen, geeft dit gewoonlijk aan dat de poort niet luistert. Een RST/ACK wordt verzonden door het systeem dat de port scan uitvoert zodat er nooit een volledige verbinding tot stand komt. Deze techniek heeft het voordeel minder snel opgemerkt te worden dan een volledige TCP-verbinding en wordt mogelijk niet door het doelsysteem geregistreerd.
- TCP FIN-scan. Bij deze techniek wordt een FIN-pakket naar de doelpoort gestuurd. Volgens RFC 793 (http://www.ietf.org/rfc/rfc0793.txt) moet het doelsysteem voor alle gesloten poorten een RST terugsturen.
- TCP Xmas Tree-scan. Bij deze techniek wordt een FIN-, URG- en PUSH-pakket naar de doelpoort gestuurd. Volgens RFC 793 moet het doelsysteem voor alle gesloten poorten een RST terugsturen.
- TCP Null-scan. Bij deze techniek worden alle pakketten verstuurd. Volgens RFC 793 moet het doelsysteem voor alle gesloten poorten een RST terugsturen.
- TCP ACK-scan. Deze techniek wordt gebruikt om firewall-regelsets te analyseren. De scan kan van nut zijn bij het bepalen of de firewall een eenvoudig pakketfilter is dat alleen tot stand gekomen verbindingen toelaat of een firewall met geavanceerde pakketfiltering.
- TCP Windows-scan. Bij deze techniek kunnen op sommige systemen zowel open als gefilterde / niet-gefilterde poorten ontdekt worden aan de hand van een afwijkende wijze waarop de TCP-venstergrootte wordt aangeduid.
- TCP RPC-scan. Deze techniek is specifiek voor UNIX-systemen en wordt gebruikt om RPC-poorten (Remote Procedure Call) en hun bijbehorende programma en versienummer te ontdekken en te identificeren.
- UDP-scan. Deze techniek stuurt een UDP-pakket naar de doelpoort. Als de doelpoort antwoordt met het bericht 'ICMP Port Unreachable', is de poort gesloten en andersom. Aangezien UDP bekend staat als een verbindingloos protocol is de nauwkeurigheid en betrouwbaarheid niet altijd even groot.

Een van de meest gebruikte port scanners is nmap. Nmap (http://www.insecure.org/nmap),

9 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 45

geschreven door Fyodor, biedt alle bovengenoemde essentiële TCP- en UDP-scanmogelijkheden[10] en scantechnieken. Daardoor is het mogelijk om met nmap een compleet netwerk te scannen. De uitkomst van een TCP SYN-scan op een van mijn PC's in mijn eigen netwerk is hieronder weergegeven:

```
antietam:/home/alphaw0lf # nmap -sS 192.168.0.2

Starting nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2006-07-06 10:57 MST
Interesting ports on vicksburg (192.168.0.2):
(The 1665 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE
135/tcp  open  msrpc
1025/tcp open  NFS-or-IIS
5679/tcp open  activesync
MAC Address: 00:04:76:90:D1:59 (3 Com)

Nmap finished: 1 IP address (1 host up) scanned in 1.657 seconds
antietam:/home/alphaw0lf #
```

Nmap identificeert drie poorten die open staan en rapporteert hier meteen het protocol en de actieve service bij. De belangrijkste reden echter voor de populariteit van nmap is de mogelijkheid vele opties mee te kunnen geven bij een port scan waarvan de belangrijkste zijn de mogelijkheid om het doelsysteem te kunnen scannen zonder ping zodat de scan minder luidruchtig is, de mogelijkheid om een scan uit te voeren met 'decoys' en de 'sneaky' scan. Decoys dienen om een doelsysteem te overspoelen met overbodige informatie. Het principe van deze optie is dat gelijktijdig met een echte scan decoy-scans worden verstuurd. Dit wordt gedaan door het bronadres van echte servers te vervalsen en deze valse scans met de echte port scan te mengen. Het doelsysteem zal dan zowel aan de valse adressen als aan de werkelijke port scan antwoorden. Bovendien zit het doelsysteem met het probleem om alle scans te moeten opsporen om vast te stellen welke echt zijn en welke vals. Het decoy-systeem moet hierbij wel actief zijn anders kunnen de scans op het doelsysteem een vloedgolf aan SYN-pakketten veroorzaken.[11] Nmap kan ook de optie meegegeven worden om de scan 'sneaky' uit te voeren waarbij de timing policy dusdanig wordt ingesteld dat de scan gedurende een langere periode wordt uitgevoerd op bepaalde tijdstippen om het risico van ontdekking te verkleinen.

2.4 Enumeratie

Nu de indringer er met behulp van de technieken uit de voorgaande paragrafen achter is gekomen welke systemen en services actief zijn, zal deze zijn aanval richten op het ontdekken van bekende zwakke plekken van de actieve services. Dit proces wordt enumeratie genoemd.

Het belangrijkste verschil tussen de eerste twee fases en enumeratie zit in de mate waarin in een

10 Zie voor een uitleg en overzicht van de opties die aan Nmap meegegeven kunnen worden Bijlage 3.
11 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 50

systeem wordt binnengedrongen. Bij enumeratie is er sprake van actieve verbindingen met doelsystemen en gerichte queries. Als zodanig kunnen ze gelogd of anderszins geregistreerd worden. Enumeratie wordt meestal gebruikt om namen te verzamelen van gebruikersaccounts om bijvoorbeeld hiermee wachtwoorden te raden, om informatie te verzamelen over verkeerd geconfigureerde bronnen, bijvoorbeeld onbeveiligde bestandsshares, of om te zoeken naar oudere softwareversies met bekende beveiligingsproblemen zoals webservers met mogelijkheden voor een buffer-overflow.[12]

Enumeratietechnieken zijn vaak besturingssysteemspecifiek en dus sterk afhankelijk van de informatie die tijdens een port scan is achterhaald. Voor enumeratie bestaan vele tools en technieken per besturingssysteem die ik hier niet zal bespreken maar de relatie tussen port scanning en enumeratie is zeer hecht. Met een port scan worden doelsystemen gevonden met poorten die open zijn en waarop actieve services draaien. Met enumeratie wordt vervolgens gekeken of die actieve services verouderde versies betreffen met reeds bekende zwakke plekken die kunnen worden benut om toegang te krijgen tot een geautomatiseerd systeem.

2.5 Samenvatting en conclusie

Naast tijd is informatie het krachtigste wapen van een kwaadwillende computerhacker. Het aantal toepassingen en tools over de diverse besturingssystemen om informatie te vergaren over de doelsystemen is vrijwel oneindig en groeit iedere dag.

Er bestaan veel verschillende manieren waarop hackers een netwerk kunnen verkennen of een profiel van een netwerk kunnen vaststellen. Veel van deze informatie is gewoon online te verkrijgen en is bovendien veelal gratis. Met behulp van een aantal eenvoudige queries zijn snel namen, telefoonnummers, IP-adresgroepen, DNS-servers, mailservers en e-mailadressen van de doelsystemen te achterhalen.

Nadat het netwerk verkend is, kunnen vele technieken en tools aangewend worden voor ping-sweeps en port scans om doelsystemen te identificeren die actief zijn en luisterende poorten hebben. Ook het besturingssysteem dat wordt gebruikt, wordt veelal vastgesteld middels een port scan. Nmap biedt vele mogelijkheden om deze port scans zo omzichtig mogelijk te kunnen uitvoeren middels ‘sneaky’ scans en het uitvoeren van scans zonder dat daarbij het doelsysteem gepingd wordt. Nmap biedt bovendien de mogelijkheid een port scan uit te voeren door daarbij het doelsysteem te overspoelen met informatie en zodoende de port scan te vermengen met valse scans om het risico van ontdekking te minimaliseren.

Nadat met een port scan doelsystemen gevonden zijn met open poorten en waarop actieve services draaien wordt vervolgens gekeken of die actieve services verouderde versies betreffen met reeds bekende zwakke plekken die kunnen worden benut om toegang te krijgen tot een geautomatiseerd systeem. Vervolgens zal een hacker die zwakke plek uitbuiten om toegang te krijgen tot het doelsysteem.

12 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 70

3 Wetgeving en jurisprudentie

3.1 Inleiding

In dit hoofdstuk zal ik de eerste onderzoeksvraag bespreken en hiervoor de belangrijkste huidige nationale en internationale wetgeving ten aanzien van computercriminaliteit op een rij zetten. Hierbij zal ik tevens de toekomstige wetgeving betrekken naar aanleiding van het wetsvoorstel Computercriminaliteit II van maart 2005.[13] Dit wetsvoorstel is ingevoerd vanwege de nieuwe ontwikkelingen in de informatietechnologie. De behandeling heeft geruime tijd stilgelegen omdat de regeling van de strafrechtelijke aansprakelijkheid van tussenpersonen in strijd was met Europese regelgeving.

Om het op 23 november 2001 tot stand gekomen Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, het Cyber Crime Verdrag[14] te kunnen ratificeren, zijn enkele noodzakelijke wetswijzigingen door middel van de tweede nota van wijziging in het wetsvoorstel Computercriminaliteit II ondergebracht. Een voorstel tot goedkeuring van het Cyber Crime Verdrag[15] is op 15 maart 2005 bij de Tweede Kamer ingediend.

Het voorstel is op 27 september 2005 aangenomen door de Tweede Kamer. De Eerste Kamercommissie voor Justitie heeft op 14 maart 2006 het eindverslag uitgebracht. De plenaire behandeling vindt plaats op 30 mei 2006 en wordt gezamenlijk behandeld met het wetsvoorstel Goedkeuring Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken.[16] Op het moment van schrijven is het wetsvoorstel Computercriminaliteit II zo juist in werking getreden per 1 september 2006.[17]

In dit onderzoek zal ik met name kijken naar de nationale en internationale artikelen die voor de strafbaarstelling van port scanning van belang kunnen zijn. Omdat de doelstelling van dit onderzoek is om te kijken of port scanning geclassificeerd zou kunnen worden als een poging tot inbraak in een geautomatiseerd systeem zal ik naar díe artikelen kijken die bepaalde voorbereidings- en uitvoeringshandelingen strafbaar stellen. Voor een goed begrip van de samenhang tussen de verschillende artikelen die betrekking hebben op de strafbaarstelling van het aantasten van (een) geautomatiseerd syste(e)m(en) is het echter noodzakelijk alle betreffende artikelen in hun onderlinge samenhang te analyseren.

Bij een analyse van deze bepalingen mag, vanwege het feit dat vele van de te analyseren strafbepalingen een opzet- en schuldvariant kennen, een goed begrip van de algemene leerstukken opzet, schuld en wederrechtelijkheid niet ontbreken. In de paragrafen 3.2 en 3.3 zal ik daarom

13 TK 2004 – 2005, 26 671, nr 7 - 9

14 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, Trb. 2002, nr. 18

15 TK 2004 – 2005, 30 036

16 TK 2004 – 2005, 30 036

17 Besluit van 4 juli 2006 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 1 juni 2006, houdende wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met de nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II) (Stb. 300), Stb. 301

aandacht besteden aan deze leerstukken.

3.2 Opzet en schuld

Wettelijke bestanddelen waarmee de intentie waarmee een strafbaar feit is begaan tot uitdrukking wordt gebracht, worden 'schuldvormen' genoemd. De wettelijke schuldvormen omvatten opzet en schuld. Deze laatste soort schuld, veelal omschreven als onachtzaamheid, is in relatie tot de schuldvormen te beschouwen als schuld in enge zin. De schuldvormen omvatten dus opzet en schuld in enge zin: in het Latijn 'dolus' en 'culpa'.[18] In de hierna te analyseren delictsomschrijvingen komt altijd één van deze schuldvormen voor. Sommige van de misdrijven hebben een doleuze én culpoze variant.

De betekenissen van opzet en schuld kennen een aantal gradaties.[19] Het opzet (de dolus betekent in zijn meest zuivere vorm: willens en wetens, met volledig bewustzijn. Dat wil zeggen handelen overeenkomstig plan, toeleg of voornemen. Willen is daarbij uitgesprokener dan alleen denken, veronderstellen, hopen en wensen. Weten betekent begrijpen, beseffen, het bewustzijn hebben van iets. De volgende gradatie is zekerheids- of noodzakelijkheidsbewustzijn. Wanneer slechts de mogelijkheid van een bepaald gevolg aanwezig is, is er sprake van mogelijkheidsbewustzijn. Mogelijkheidsbewustzijn kan zich op twee manieren voordoen. De eerste mogelijkheid is dat de dader het eventuele gevolg voor lief of op de koop toe neemt. Deze geesteshouding wordt 'voorwaardelijk opzet' genoemd en wordt tot de sfeer van het opzet gerekend. De tweede mogelijkheid is dat de dader een (te) optimistische inschatting van de situatie maakt. Hij gaat er van uit, ondanks het risico, zijn handeling tot een goed gevolg te kunnen brengen. Deze geestestoestand wordt 'bewuste schuld' genoemd en valt onder de schuldvorm culpa. Culpa betekent in zijn zuiverste vorm: grove onachtzaamheid, roekeloosheid, onnadenkendheid. Bij deze vorm heeft de dader niet nagedacht waar hij wel had moeten nadenken. Er wordt dan ook gesproken van 'onbewuste schuld'.
Het vaststellen van de psychische gesteldheid die op het moment van de daad in relatie tot die daad aanwezig moet zijn geweest vergt een rechterlijke interpretatie. De psychische gesteldheden opzet en schuld laten zich wel mede afleiden uit de sociale werkelijkheid, dat wil zeggen uit de feitelijke omstandigheden waaronder en uit de middelen waarmee het gewraakte gedrag plaats vond en uit hetgeen de menselijke ervaringsregels in deze omstandigheden plegen mee te brengen.[20] In de normatieve opvatting over de schuldvormen, worden de begrippen culpa en dolus daarom wel 'geobjectiveerd': opzet of schuld worden afgeleid uit de sociale werkelijkheid, dat wil zeggen uit de uiterlijke omstandigheden van het geval en uit wat een gemiddeld mens in die omstandigheden gewild zal hebben.[21]

De wet formuleert het opzetvereiste op verschillende wijzen. Het opzetvereiste komt onder meer

18 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 170
19 Ibid, pp. 181 - 191
20 Ibid, pp. 171 - 172
21 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent-arrest

op de volgende manieren in de wet tot uitdrukking. In de meeste delictsomschrijvingen wordt letterlijk het begrip 'opzettelijk' gebruikt. In andere omschrijvingen worden de woorden 'wetende dat' of 'kennis dragende dat' gebruikt.[22] Een andere methode die wordt toegepast is het gebruik van werkwoorden die uit hun aard opzet omvatten, zoals: 'opruien', 'zich verzetten', of 'binnendringen'. In een aantal bepalingen wordt het woord 'oogmerk' gebruikt, dat is een verbijzondering van het opzetvereiste. Het kan het opzetvereiste zelf representeren of kan naast het opzettelijk handelen worden geëist. Er is dan sprake van een bijkomend oogmerk. De wetgever probeert door middel van het woord oogmerk een verder weg gelegen doel van het handelen aan te wijzen, teneinde het opzetvereiste tot uitdrukking te brengen. Het oogmerk maakt de handeling opzettelijk. Hoe specifiek de term oogmerk moet worden uitgelegd, hangt af van de bedoeling van de wetgever en de wijze waarop deze het speciale oogmerk heeft verwoord. Het opzet moet gericht zijn op alle bestanddelen van de delictsomschrijving die, door het woord of een equivalent ervan, taalkundig worden beheerst.[23] In enkele delictsomschrijvingen is een bepaald bestanddeel onttrokken aan de opzeteis. Er wordt dan gesproken van een 'geobjectiveerd' bestanddeel.[24]

Voor wat betreft port scanning geldt dat de dader er in de regel op uit is om de zwakke plekken van een geautomatiseerd systeem te detecteren. Hij wil en weet dus dat een bepaald gevolg in zal treden ten gevolge van zijn gedragingen. Daarmee handelt hij in beginsel opzettelijk. Van onachtzaam / onnadenkend ofwel culpoos handelen zal niet snel sprake zijn daar er meerdere handelingen nodig zijn om een port scan uit te voeren en het te gebruiken programma dermate veel deskundigheid vereist dat een port scan niet eenvoudig en / of onachtzaam kan worden uitgevoerd. Daar de culpoze varianten van de te analyseren artikelen nauwelijks denkbaar zijn voor een port scan, zullen deze in de hiernavolgende analyses onbesproken blijven.

3.3 Wederrechtelijkheid

Als voorwaarden voor de strafbaarheid gelden in het algemeen: een menselijke gedraging, die een delictsomschrijving vervult, die wederrechtelijk is en aan schuld te wijten.[25] Wederrechtelijkheid is daarmee een stilzwijgend element van het strafbare feit. Het leerstuk van de wederrechtelijkheid betreft het normoverschrijdende karakter van de delictsomschrijving. In veel gevallen heeft de wetgever de term wederrechtelijkheid expliciet, hetzij woordelijk, hetzij door middel van een synoniem, als bestanddeel in de delictsomschrijving opgenomen. De reden hiervoor is dat anders gevallen onder de delictsomschrijvingen zouden kunnen vallen waarvoor deze niet bedoeld is.[26] Er bestaan verschillende opvattingen over de betekenis van het begrip wederrechtelijkheid als wettelijk bestanddeel. Enerzijds is er het eng wederrechtelijkheidsbegrip, dit wordt ook wel aangeduid met de term 'facetwederrechtelijkheid'. Het begrip 'wederrechtelijk' komt dan een eigen specifieke betekenis toe in overeenstemming met het doel en de strekking van de desbetreffende bepaling. Dit komt neer

22 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 192
23 Ibid, p. 177
24 Ibid, p. 196
25 Ibid, p. 119
26 Ibid, p. 123

op het toekennen van een beperkte, enge betekenis aan het begrip wederrechtelijkheid omdat het van het ruime scala wederrechtelijkheid in het algemeen slechts één bepaald facet vertegenwoordigt.[27] Tegenover de opvatting van de 'facetwederrechtelijkheid' staat een heel andere opvatting, één die de wederrechtelijkheid zeer ruim interpreteert. Wederrechtelijk heeft dan de betekenis van 'in strijd met het objectieve recht' en bewerkstelligt een grotere reikwijdte van de strafbaarheid.[28]

Het bestanddeel 'wederrechtelijkheid' heeft in ieder van de hieronder te bespreken artikelen een specifieke betekenis. Meestal betekent het zonder toestemming, zoals in de artikelen 138a en 350a WvSr. In artikel 138a WvSr staat het bestanddeel wederrechtelijk niet alleen woordelijk in de delictsomschrijving, maar wordt het tevens tot uitdrukking gebracht door het woord 'binnendringen'. In artikel 139c WvSr staat het woord 'wederrechtelijk' niet letterlijk in de delictomschrijving, maar wordt de vereiste wederrechtelijkheid tot uitdrukking gebracht door de woorden 'niet voor hem, mede voor hem of voor degene in wiens opdracht hij handelt' en betekent het zonder toestemming. In het artikel 139d WvSr is de betekenis van het bestanddeel wederrechtelijkheid 'in strijd met het in de artikelen 139a t/m c WvSr bepaalde'.

3.4 Nationale wetgeving

De Wet Computercriminaliteit II[29] is een combinatie van het wetsvoorstel Computercriminaliteit II uit 1999[30] en de aanpassingen die voortvloeien uit het Cyber Crime Verdrag.[31] In de Wet Computercriminaliteit II worden zowel wijzigingen doorgevoerd van bepalingen in het materiële strafrecht als in het formele strafrecht. De wijzigingen van het materiële strafrecht hebben betrekking op cyber crime in enge zin[32]. De wijzigingen van het formele strafrecht hebben vooral betrekking op bevoegdheden die worden toegekend aan de met opsporing en vervolging belaste organen, onder andere met het kunnen vorderen van gegevens bij verschillende organisaties. De wijzigingen in het formele strafrecht naar aanleiding van de Wet Computercriminaliteit II vallen buiten het bestek van dit onderzoek en zullen derhalve niet besproken worden.

27 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 125

28 Ibid, p. 125

29 Wet van 1 juni 2006 tot wijziging van het Wetboek van Strafrecht, het Wetboek van Strafvordering en enige andere wetten in verband met de nieuwe ontwikkelingen in de informatietechnologie (computercriminaliteit II), Stb. 300

30 TK 1999 – 2001, 26 671, nr 1 - 6

31 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, Trb. 2002, nr. 18, TK 2004 – 2005, 30 036 (R 1784), nr. 3 – 5

32 Kaspersen onderscheidt computercriminaliteit in enge en brede zin. Onder computercriminaliteit in enge zin verstaat Kaspersen de strafbare handelingen die zich richten op het verstoren of beïnvloeden van de werking van computersystemen of met die systemen onderhouden geautomatiseerde processen. Computercriminaliteit in brede zin betreft gedragingen waarbij IT een belangrijke rol bij de uitvoering speelt of die in een geautomatiseerde omgeving, zoals het Internet, worden begaan. Kaspersen duidt hierbij op een tweedeling tussen enerzijds misdrijven en overtredingen die rechtstreeks verband houden met het gebruik van computers en computerbestanden en daarvan niet los te denken zijn en anderzijds traditionele overtredingen die met behulp van computers worden begaan maar ook op een andere manier mogelijk zijn. (H.W.K. Kaspersen, 'Bestrijding van cybercrime en de noodzaak van internationale regelingen', *Justitiële Verkenningen*, 2004/8, p. 63)

3.4.1 Artikel 138a WvSr

Dit artikel betreft het binnendringen in een geautomatiseerd werk. Ook wel computerinbraak, computervredebreuk of hacken genoemd. Het artikel luidt:

1. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk wederrechtelijk binnendringt in een geautomatiseerd werk voor de opslag of verwerking van gegevens, of in een deel daarvan, indien hij
a. daarbij enige beveiliging doorbreekt of
b. de toegang verwerft door een technische ingreep, met behulp van valse signalen of een valse sleutel dan wel door het aannemen van een valse hoedanigheid.
2. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen in een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, overneemt en voor zichzelf of een ander vastlegt.
3. Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk gepleegd door tussenkomst van een openbaar telecommunicatienetwerk, indien de dader vervolgens
a. met het oogmerk zich wederrechtelijk te bevoordelen gebruik maakt van verwerkingscapaciteit van een geautomatiseerd werk;
b. door tussenkomst van het geautomatiseerd werk waarin hij is binnengedrongen de toegang verwerft tot het geautomatiseerd werk van een derde.

Voor strafbaarheid moet het opzet hier gericht zijn op de wederrechtelijkheid en de overige bestanddelen tot het woord ‘indien’. De woorden ‘binnendringen’ in het eerste lid en ‘doorbreekt’ en ‘de toegang verwerft’ onder a en b impliceren echter tevens opzet. Binnendringen moet worden opgevat als binnengaan tegen de verklaarde wil van de rechthebbende. Volgens de Memorie van Toelichting (MvT) wordt binnengaan binnendringen als een beveiliging wordt doorbroken.[33] Deze uitleg die de MvT geeft aan het begrip binnendringen, namelijk dat een beveiliging moet worden doorbroken, lijkt inherent tegenstrijdig met het bestaan van sub b van het eerste lid en maakt sub a feitelijk overbodig. Het woordje ‘of’ tussen sub a en b doet vermoeden dat het bij sub b niet om een vorm van beveiliging gaat. De wetgever heeft hiermee bepaalde vormen van binnendringen nader omschreven, naast het noemen van de beveiligingseis in het algemeen.

Volgens de MvT bij de Wet Computercriminaliteit I is om van ‘enige beveiliging’ te kunnen spreken, de aanwezigheid van een reële beveiliging voldoende. Het is niet nodig dat deze beveiliging ook adequaat is. Het gaat erom dat de beveiliging zodanig is, dat het voor de binnendringer duidelijk is dat hij een beveiligd systeem binnendringt en dat enige inspanningen nodig zijn om deze beveiliging te doorbreken.[34] Pas dan krijgt het binnengaan ook een wederrechtelijk karakter. Indien een gebruikersnaam en password nodig zijn om toegang te krijgen tot een systeem, is er in ieder geval sprake van enige beveiliging.
Onder technische ingreep wordt onder meer verstaan het binnendringen met een speciaal daarvoor geschreven programma. Bij valse signalen of valse sleutel zal gedacht moeten worden aan het

33 TK 1989 – 1990, 21 551, nr. 3, p. 15
34 TK 1989 – 1990, 21 551, nr. 3, p. 16

hanteren van een toegangsprocedure die de eigenlijke manier van binnenkomen omzeilt, bijvoorbeeld het aanbieden van een eigen PGP-sleutel op naam van een ander.
De leden 2 en 3 van het artikel geven criteria voor strafverzwarende omstandigheden. Strafverzwarend op grond van lid 2 is het overnemen en voor zichzelf of een ander vastleggen van gegevens die zijn opgeslagen in het geautomatiseerde werk waarin is binnengedrongen. Met overnemen en voor zichzelf vastleggen, wordt kopiëren bedoeld. Onvoldoende is bijvoorbeeld het oproepen van gegevens op het eigen beeldscherm. Kopiëren kan geschieden door de gegevens over te brengen naar een extern geheugen of over te schrijven of te printen. Dat het moet gaan om opgeslagen gegevens betekent dat het vastleggen van zogenoemde stromende gegevens (gegevens in transport) buiten de reikwijdte van dit lid valt.[35]
Op grond van lid 3 sub a is strafverzwarend 'diefstal van gebruik'. Hier wordt gedoeld op de situatie dat iemand na het hacken van een particuliere computer, gebruik maakt van diensten (systeemfuncties of aanwezige applicatieprogrammatuur) waarvoor elders gewoonlijk zou moeten worden betaald. Sub b is opgenomen, omdat geautomatiseerde werken die zijn aangesloten op een netwerk, toegang kunnen verschaffen tot andere geautomatiseerde werken. Niet is vereist dat bij die derde computer ook enige beveiliging wordt doorbroken.[36]

Artikel 138a WvSr en de Wet Computercriminaliteit II

Op grond van de Wet Computercriminaliteit II is artikel 138a lid 1 WvSr als volgt gewijzigd:

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel of
d. door het aannemen van een valse hoedanigheid.

De huidige redactie van het artikel formuleert de onderdelen a en b als voorwaarden voor strafbaarheid. In de voorgestelde versie zijn de onderdelen a t/m d voorbeelden van gevallen waarin sprake is van binnendringen. Er worden dus geen eisen meer gesteld aan het binnendringen. Hierdoor wordt ieder opzettelijk en wederrechtelijk binnendringen in een computersysteem strafbaar. De verwarring die met de huidige redactie van het artikel kan ontstaan met betrekking tot het begrip binnendringen, wordt hierdoor geëlimineerd. Door tussenvoegen van het woordje 'en' tussen de woorden opzettelijk en wederrechtelijk, vervalt de eis dat de dader weet dat zijn gedraging wederrechtelijk is. De woorden 'voor de opslag of verwerking van gegevens' na 'geautomatiseerd werk', zijn geschrapt omdat ze, gelet op de definitie van artikel 80sexies WvSr, een overbodige specificatie vormen.[37]

35 TK 1998 – 1999, 26 671, nr. 3, p. 28
36 R. Vrielink, *Autodialers, Phishing, Identity theft en Spyware,* Utrecht, Juli 2005, p. 32
37 TK 1998 – 1999, 26 671, nr. 3, p. 44

In de Wet Computercriminaliteit II is lid 2 van artikel 138a WvSr gewijzigd in:

Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie wordt gestraft computervredebreuk, indien de dader vervolgens gegevens die zijn opgeslagen, worden verwerkt of overgedragen door middel van een geautomatiseerd werk waarin hij zich wederrechtelijk bevindt, voor zichzelf of een ander overneemt, aftapt of opneemt.

De toevoegingen van het 'aftappen of opnemen' van gegevens die 'worden verwerkt of overgedragen' door middel van het geautomatiseerde werk waarin wederrechtelijk is binnengedrongen, geeft aan dat op grond van het tweede lid naast het overnemen van reeds bestaande in de computer opgeslagen gegevens ook strafbaar is het overnemen, aftappen of opnemen van gegevens die ten tijde van de computervredebreuk binnenkomen (de 'stromende' gegevens), zijn binnengekomen of binnen een computersysteem worden verwerkt.[38] De strafbaarheid is dus verruimd ten aanzien van de huidige redactie van het artikel. Waarom het aftappen en/of opnemen nog beperkt zou moeten blijven tot alleen binnenkomende en niet ook uitgaande gegevens onder de bepaling zouden kunnen vallen, is niet duidelijk.

3.4.2 Artikel 350a en b Wetboek van Strafrecht

De artikelen 350a en 350b WvSr beschermen het ongestoorde gebruik van computergegevens tegen ondermeer het onbevoegd veranderen of ontoegankelijk maken van die gegevens. Artikel 350a WvSr betreft de opzet variant, artikel 350b WvSr de schuldvariant. De voor dit onderzoek van belang zijnde variant, artikel 350a WvSr, luidt:

1. Hij die opzettelijk en wederrechtelijk gegevens die door middel van een geautomatiseerd werk zijn opgeslagen, worden verwerkt of overgedragen, verandert, wist, onbruikbaar of ontoegankelijk maakt, dan wel andere gegevens daaraan toevoegt, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.
2. Hij die het feit, bedoeld in het eerste lid, pleegt na door tussenkomst van een openbaar telecommunicatienetwerk, wederrechtelijk in een geautomatiseerd werk te zijn binnengedrongen en daar ernstige schade met betrekking tot die gegevens veroorzaakt, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.
3. Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.
4. Niet strafbaar is degene die het feit, bedoeld in het derde lid, pleegt met het oogmerk om schade als gevolg van deze gegevens te beperken.

Het artikel stelt twee soorten gedragingen strafbaar:

1. Het opzettelijk onbruikbaar maken, wissen, ontoegankelijk maken of veranderen van gegevens, en
2. Het opzettelijk ter beschikking stellen en verspreiden van gegevens die schade aan kunnen richten door zichzelf te vermenigvuldigen.

38 TK 1998 – 1999, 26 671, nr. 3, p. 28 en 44

Ad 1. Wederrechtelijk betekent in dit verband zonder toestemming. Het 'veranderen' omvat enige van de andere gedragingen; het gebeurt meestal door het wissen of toevoegen van gegevens. In zoverre is de opsomming wat aan de ruime kant. Bij ontoegankelijk maken van gegevens kan worden gedacht aan het wijzigen van een toegangscode. 'Onbruikbaar maken' voegt ook niet wezenlijk iets toe aan de opsomming. Dit zal niet veel anders kunnen geschieden dan door middel van veranderen, wissen of toevoegen. Geen vereiste voor strafbaarheid op grond van lid 1 is dat de veranderde, gewiste, ontoegankelijk of onbruikbaar gemaakte gegevens niet meer in de oude toestand kunnen worden hersteld. Van onherstelbare schade hoeft geen sprake te zijn.[39]
Onder lid 2 is strafverzwarend, wanneer iemand via een openbaar telecommunicatienetwerk wederrechtelijk in een geautomatiseerd werk is binnengedrongen en daar ernstige schade met betrekking tot die gegevens heeft veroorzaakt. Onder ernstige schade kan worden verstaan schade die niet of slechts met veel moeite en/of kosten kan worden hersteld en/of grote financiële gevolgen heeft. Onduidelijk is nog hoe ruim het begrip schade moet worden genomen: gaat het alleen om de directe schade aan gegevens of valt gevolgschade eveneens onder het begrip 'ernstige schade'.
Ad 2. Het doel van het derde lid is het strafbaar stellen van het verspreiden en ter beschikking stellen van computervirussen. Door de redactie van het lid te beperken tot gegevens die schade aanrichten door zichzelf te vermenigvuldigen (de zogenaamde wormen), vallen een aantal andere 'virusachtigen' niet onder de voorgestelde redactie. Men kan hierbij denken aan gegevens die bepaalde instructies toevoegen of systeemfuncties uitschakelen, waaronder Trojaanse paarden.[40] Niet duidelijk is waarom het lid beperkt is tot alleen dergelijke, zichzelf vermenigvuldigende virussen. Het is voor strafbaarheid op grond van dit lid niet noodzakelijk dat het virus ook daadwerkelijk schade heeft aangericht.
Lid 4 van artikel 350a betreft een specifieke rechtvaardigingsgrond. Gedacht kan hierbij worden aan systeembeheerders die anti-virussoftware verspreiden om handelingen zoals beschreven in het derde lid ongedaan te maken.

Artikel 350a en b Wetboek van Strafrecht en de Wet Computercriminaliteit II
Op grond van de Wet Computercriminaliteit II zijn de artikelen 350a en b WvSr als volgt gewijzigd:

1. In het eerste lid wordt na geautomatiseerd werk ingevoegd of door middel van telecommunicatie en vervallen de woorden dan wel andere gegevens daaraan toevoegt.
2. In het derde lid wordt de zinsnede die bedoeld zijn om schade aan te richten door zichzelf te vermenigvuldigen in een geautomatiseerd werk vervangen door: die zijn bestemd om schade aan te richten in een geautomatiseerd werk.

Ad 1. Door de toevoeging van de woorden 'of door middel van telecommunicatie', wordt volgens de MvT buiten twijfel gesteld dat strafbaarheid op grond van dit artikel ook bestaat bij vernieling van gegevens die door middel van computernetwerken worden overgedragen.[41]

39 R. Vrielink, *Autodialers, Phishing, Identity theft en Spyware,* Utrecht, Juli 2005, p. 34
40 Ibid, p. 35

41 TK 1998 – 1999, 26 671, nr. 3, pp. 39 - 40

Ad 2. Met deze wijziging wordt de beperking die is besproken bij artikel 350a lid 3 WvSr opgeheven. Door de nieuwe redactie van het lid vallen ook virusachtigen die anders dan door zichzelf te vermenigvuldigen, schade aanrichten in een geautomatiseerd werk onder de strafbepaling van dit artikel.

3.4.3 Artikel 161sexies Wetboek van Strafrecht

Het opzettelijk veroorzaken van stoornis in de werking van een geautomatiseerd werk is strafbaar gesteld in artikel 161sexies WvSr. Hiervoor dient één van de in het artikel genoemde gevolgen in te treden. Het beschermde belang van dit artikel is de ongestoorde automatische opslag, verwerking en overdracht van gegevens. Artikel 161sexies WvSr luidt:

Hij die opzettelijk enig geautomatiseerd werk voor opslag of verwerking van gegevens of enig werk voor telecommunicatie vernielt, beschadigt of onbruikbaar maakt, stoornis in de gang of in de werking van zodanig werk veroorzaakt, of een ten opzichte van zodanig werk genomen veiligheidsmaatregel verijdelt, wordt gestraft:
1°. met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie, indien daardoor wederrechtelijk verhindering of bemoeilijking van de opslag of verwerking van gegevens ten algemenen nutte of stoornis in een openbaar telecommunicatienetwerk of in de uitvoering van een openbare telecommunicatiedienst, ontstaat;
2°. met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie, indien daarvan gemeen gevaar voor goederen of voor de verlening van diensten te duchten is;
3°. met gevangenisstraf van ten hoogste negen jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is;
4°. met gevangenisstraf van ten hoogste vijftien jaren of geldboete van de vijfde categorie, indien daarvan levensgevaar voor een ander te duchten is en het feit iemands dood ten gevolge heeft.

De bestanddelen ‘vernielen en onbruikbaar maken’ zien op het onklaar maken van een voorwerp voor de bestemming waartoe het is ingericht. Beschadigen staat daar enigszins naast. Verijdelen betekent het ontnemen van de werking. Voorbeelden van veiligheidsmaatregelen zijn technische voorzieningen zoals firewalls of logische toegangsbeveiliging zoals gebruikersnaam en password. Eén van de gevolgen van sub 1 tot en met 4 moet zijn ingetreden. Onder sub 1 dient het te gaan om werken die iedereen ten dienste staan. Indien met computersystemen die binnen een organisatie worden gebruikt een openbare dienst wordt verleend, dan is dit ‘ten algemenen nutte’.[42]

Artikel 161sexies Wetboek van Strafrecht en de Wet Computercriminaliteit II

Op grond van de Wet Computercriminaliteit II is artikel 161sexies WvSr zo gewijzigd, dat onder aanduiding van de bestaande tekst als eerste lid, een nieuw lid is toegevoegd, luidende:

2. Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vijfde categorie wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in het eerste lid (onderdeel 1) wordt gepleegd,
a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of

42 TK 1998 – 1999, 26 671, nr. 3, p. 36

b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.

Op basis van bovenstaande tekst kunnen de volgende criteria worden onderscheiden voor de strafbaarstelling van een aantal voorbereidingshandelingen bij het opzettelijk veroorzaken van stoornis in de gang of werking van een computersysteem dat wordt gebruikt ten behoeve van de opslag of verwerking van gegevens ten algemenen nutte. Er moet sprake zijn van:[43]

1. Het oogmerk een stoornis te veroorzaken.
2. Een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen is voor het veroorzaken van een stoornis, of
3. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor de toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan.
4. Het ter beschikking stellen of het voorhanden hebben door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of verspreiden.

Cruciaal is het woord 'hoofdzakelijk'. Veel software die door black-hathackers is ontwikkeld en door dezen wordt gebruikt, is ook verplichte kost voor systeembeheerders voor het beveiligen van netwerken. Het zal aan de rechter zijn om middels jurisprudentie duidelijk te maken wat er met 'hoofdzakelijk' wordt bedoeld.[44]

3.4.4 Artikel 139c Wetboek van Strafrecht

De artikelen 139a t/m e WvSr stellen strafbaar het afluisteren van gesprekken en gegevens. Voor de moderne vormen van dit onderzoek is het afluisteren van gesprekken in een woning, in een besloten lokaal of erf als bedoeld in artikel 139a WvSr en 139b WvSr niet van belang. Hieronder zullen derhalve alleen de artikelen 139c, d en e WvSr geanalyseerd. Het aftappen en opnemen van gegevens door middel van een openbaar telecommunicatiewerk is strafbaar gesteld in artikel 139c WvSr en luidt:

1. Hij die door middel van een openbaar telecommunicatienetwerk, of door middel van daarop aangesloten randapparatuur overgedragen gegevens die niet voor hem, mede voor hem of voor degene in wiens opdracht hij handelt, zijn bestemd, opzettelijk met een technisch hulpmiddel aftapt of opneemt, wordt gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie.
2. Het eerste lid is niet van toepassing op het aftappen of opnemen:
1°. van door middel van een radio-ontvangapparaat ontvangen gegevens, tenzij om de ontvangst mogelijk te maken een bijzondere inspanning is geleverd of een niet toegestane ontvanginrichting is gebruikt.
2°. door of in opdracht van de gerechtigde tot een voor de telecommunicatie gebezigde aansluiting, behoudens in geval van kennelijk misbruik;
3°. ten behoeve van de goede werking van een openbaar telecommunicatienetwerk, ten behoeve van de strafvordering, dan wel ter uitvoering van de Wet op de inlichtingen- en veiligheidsdiensten.

43 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 131
44 A. Dasselaar, *Handboek digitale criminaliteit, Over daders, daden en opsporing*, Culemborg, Van Duuren Media, 2005, p. 214

Het moet in deze bepaling gaan om het onderscheppen en vastleggen van stromende gegevens. Dat blijkt ondermeer uit de MvT bij het wetsvoorstel Computercriminaliteit II:
"(…) een belangrijke uitzondering wordt gevormd door de artikelen 139a e.v. WvSr, die straf stellen op overtreding van de zogenaamde aftap- en opneemverboden: deze strafbepalingen zijn en blijven in dit voorstel gereserveerd voor het onderscheppen van gegevens in transport."[45]
Uit de MvT bij de Wet Computercriminaliteit I volgt dat met 'overdracht van gegevens' niet mede wordt bedoeld het gegevensverkeer op korte afstand, bijvoorbeeld tussen een computer en een daarop aangesloten beeldscherm.[46] Het tweede lid beschrijft een aantal uitzonderingsgevallen waarin het eerste lid niet van toepassing is. Deze zijn voor dit onderzoek niet relevant en zullen derhalve niet worden besproken.

Artikel 139c Wetboek van Strafrecht en de Wet Computercriminaliteit II
Op grond van de Wet Computercriminaliteit II is het eerste lid van artikel 139c WvSr als volgt komen te luiden:

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk met een technisch hulpmiddel gegevens aftapt of opneemt die niet voor hem bestemd zijn en die worden verwerkt of overgedragen door middel van telecommunicatie of door middel van een geautomatiseerd werk.

Het huidige artikel is alleen van toepassing op gegevens die door middel van een openbaar telecommunicatienetwerk of door middel van daarop aangesloten randapparatuur worden overgedragen. Door de nieuwe redactie wordt het artikel ook van toepassing op datacommunicatie in besloten netwerken, zoals bedrijfsnetwerken en gegevensoverdracht op korte afstand. Door toevoeging van het begrip 'verwerken', wordt het artikel ook van toepassing op gegevensverwerking door of binnen een computer. Onder de nieuwe versie vallen derhalve alle gegevensstromen.[47]

3.4.5 Artikel 139d Wetboek van Strafrecht

In artikel 139d WvSr wordt een specifiek soort voorbereiding tot het opnemen, aftappen en afluisteren strafbaar gesteld. Het artikel luidt:

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft hij die met het oogmerk dat daardoor een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk wederrechtelijk wordt afgeluisterd, afgetapt of opgenomen, een technisch hulpmiddel op een bepaalde plaats aanwezig doet zijn.

Wat onder 'aanwezig doen zijn' moet worden verstaan is niet geheel helder. Gaat het slechts om het plaatsen van een technisch hulpmiddel of wordt hieronder ook verstaan het laten voortduren van de

45 TK 1998 – 1999, 26 671, nr. 3, p. 28
46 TK 1989 – 1990, 21 551, nr. 3, p. 7
47 R. Vrielink, *Autodialers, Phishing, Identity theft en Spyware,* Utrecht, Juli 2005, p. 38

aanwezigheid van de apparatuur op een bepaalde. Oogmerk betekent hier: met de (persoonlijke) bedoeling en moet mede op de wederrechtelijkheid gericht zijn. Wederrechtelijk betekent in het verband van dit artikel in strijd met het in de artikelen 139a t/m c WvSr bepaalde. Uit de woorden 'dat daardoor (…) opgenomen' volgt dat degene die de apparatuur aanwezig doet zijn, niet de persoon hoeft te zijn die ermee wil afluisteren.[48]

Artikel 139d Wetboek van Strafrecht en de Wet Computercriminaliteit II

Op grond van de Wet Computercriminaliteit II zijn de volgende twee nieuwe leden aan artikel 139d WvSr toegevoegd:

2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138a, eerste lid, 138b of 139c wordt gepleegd,
a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.
3. Met gevangenisstraf van vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt indien zijn oogmerk gericht is op een misdrijf als bedoeld in artikel 138a, tweede of derde lid.

Deze leden bieden verruimde mogelijkheden voor strafbaarheid van bepaalde *voorbereidingshandelingen*. Daarbij gaat het om voorbereidingshandelingen met betrekking tot artikel 138a, eerste lid WvSr, het nieuw voorgestelde en hieronder te bespreken 138b WvSr en artikel 139c WvSr. Met het 'oogmerk' wordt niet het doel van handelen als omschreven in dit artikel maar het begaan van een misdrijf bedoeld in de artikelen 138a, eerste lid WvSr, 138b WvSr of 139c WvSr, aangewezen.
Op basis van bovenstaand artikel kunnen de volgende criteria worden onderscheiden voor de strafbaarstelling van een aantal voorbereidingshandelingen. Er moet sprake zijn van:[49]

1. Het oogmerk om te hacken, om de functie van een computer(systeem) te belemmeren of om gegevens af te tappen of op te nemen.
2. Een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen is om te hacken, een ernstige stoornis in een computersysteem te veroorzaken dan wel af te tappen of op te nemen, of
3. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan.
4. Ter beschikking stellen of voorhanden hebben door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of het verspreiden.

48 R. Vrielink, *Autodialers, Phishing, Identity theft en Spyware,* Utrecht, Juli 2005, p. 38
49 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 135

Een voorbeeld van een voorbereidende handeling kan zijn een website waarop bepaalde scripts zijn aangebracht, of het uitbuiten van kwetsbaarheden in browsers waardoor een Trojaans paard op de computer van een bezoeker kan worden geplaatst.

Het oogmerk is in dit artikel een belangrijk onderscheidend criterium om te bepalen of er sprake is van een strafbare voorbereidingshandeling. Het oogmerk om te hacken houdt bijvoorbeeld in dat iemand ook het doel heeft om het strafbare feit te plegen. Het beroepsmatig gebruikmaken van technische hulpmiddelen, door bijvoorbeeld informatiebeveiligers of systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, betekent niet direct dat er sprake is van een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. De toevoeging van het voorgestelde tweede en derde lid hebben betrekking op de strafbaarstelling van het in bezit hebben of de voorbereidingshandelingen op zich. Dit houdt in dat anders dan in het huidige recht het geval is, ook in het geval het hoofddelict niet volgt, een aantal specifieke voorbereidinghandelingen toch strafbaar wordt gesteld. Een voorbeeld van een voorbereidende handeling kan zijn een website waarop bepaalde scripts zijn aangebracht waardoor een Trojaans paard op de computer van een bezoeker kan worden geplaatst of het plaatsen van bots om een (d)Dos aanval te bewerkstelligen.[50] Zowel het in bezit hebben als het verspreiden wordt strafbaar gesteld. Het voordeel van de strafbaarstelling van deze specifieke voorbereidingshandelingen is dat niet aan de zware eis van de algemene voorbereidingsbepaling van artikel 46 WvSr hoeft te worden voldaan. Op basis van artikel 46 WvSr is een voorbereidingshandeling strafbaar als op het misdrijf een gevangenisstraf van acht jaar of meer is gesteld. Aangezien de strafmaat bij het overgrote deel van cyber crime is gesteld op een gevangenisstraf die onder de acht jaar ligt, kan een voorbereidingshandeling met betrekking tot cyber crime op grond van het huidige recht ook bijna niet worden strafbaar gesteld.[51]

3.4.6 Artikel 139e Wetboek van Strafrecht

Dit artikel stelt strafbaar het voorhanden hebben en bekendmaken van gegevens die door onrechtmatig aftappen of opnemen zijn verkregen. Het artikel luidt:

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de vierde categorie wordt gestraft:
1°. Hij die de beschikking heeft over een voorwerp waarop, naar hij weet of redelijkerwijs moet vermoeden, gegevens zijn vastgelegd die door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk zijn verkregen;
2°. Hij die gegevens die hij door wederrechtelijk afluisteren, aftappen of opnemen van een gesprek, telecommunicatie of andere gegevensoverdracht door een geautomatiseerd werk heeft verkregen of die, naar hij weet of redelijkerwijs moet vermoeden, ten gevolge van zulk afluisteren, aftappen of opnemen te zijner kennis zijn gekomen, opzettelijk aan een ander bekend maakt;
3°. Hij die een voorwerp als omschreven onder 1° opzettelijk ter beschikking stelt van een ander."

Onder 'voorwerp' vallen alle voorwerpen waarop elektronische gegevens worden bewaard,

50 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 135
51 Ibid, p. 136

bijvoorbeeld computers of diskettes, cd's, memory-sticks. Onder 'bekend maken' valt ook het ongericht openbaar maken. Bekendmaking kan in elke mogelijke vorm geschieden. Ter beschikking stellen: hieronder valt ook het aan een ander meedelen van de inhoud van het voorwerp.

3.4.7 Voorstel tot nieuw artikel 138b Wetboek van Strafrecht.

De Wet Computercriminaliteit II voert een nieuw artikel in dat betrekking heeft op het veroorzaken van een stoornis in de gang of werking van een geautomatiseerd systeem. Artikel 138b WvSr luidt:

Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft hij die opzettelijk en wederrechtelijk de toegang tot of het gebruik van een geautomatiseerd werk belemmert door daaraan gegevens aan te bieden of toe te zenden.

Invoering van het artikel wordt mede ingegeven door artikel 5 van het Cybercrime Verdrag en artikel 3 van het Kaderbesluit van de Raad van de EU inzake aanvallen op informatiesystemen. Doel van het nieuwe artikel is strafbaarstelling van de schending van de integriteit van computersystemen.
In de toelichting op de voorgestelde bepaling staat dat de term 'belemmeren' een adequate invulling geeft aan de in het Verdrag en Kaderbesluit gehanteerde termen. Het verdrag spreekt van 'serious hinder' en het Kaderbesluit van 'ernstig hinderen'.
Bij ernstige hinder kan volgens het aanpassingsvoorstel gedacht worden aan het in een zodanige vorm of omvang of frequentie toezenden van gegevens aan een computer(systeem), dat dit een significant nadelig effect heeft op de mogelijkheden voor de eigenaar of gebruiker om de computer te gebruiken of te communiceren met andere systemen. Gedacht kan worden aan (d)Dos-attack (distributed denial of service attacks), programma's (bijvoorbeeld virussen) die het gebruik van computersystemen onmogelijk maken of dit substantieel vertragen of programma's die grote hoeveelheden email versturen met als doel de communicatiefunctie van het systeem te verstoren. De werking van het systeem moet zodanig verstoord zijn dat het gebruik ervan of de communicatie met andere computersystemen voor enige tijd niet of nauwelijks mogelijk is of aanzienlijk vertraagd wordt. Voordeel van dit artikel is dat niet steeds uitgeweken hoeft te worden naar art. 161sexies WvSr, waarbij het steeds moet gaan om een systeem 'ten algemenen nutte'. Ook de belemmering van de privé-computer thuis en (d)Dos-attacks op computersystemen die niet het openbaar belang dienen zijn op grond van artikel 138b WvSr nu strafbaar.[52]

3.5 Internationale wetgeving

Op 23 november 2001 heeft de Raad van Europa het Cyber Crime Verdrag aangenomen.[53] Het doel van het verdrag is het harmoniseren van de opsporing en de wetgeving met betrekking tot cyber crime

52 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 129

53 Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken, Boedapest, 23 november 2001, Trb. 2002, nr. 18, TK 2004 – 2005, 30 036 (R 1784), nr. 3 – 5

binnen Europa en enkele landen daarbuiten zoals Canada, de Verenigde Staten en Japan. In hoofdlijnen omvat het verdrag twee onderwerpen:

- Bepalingen die politie, het Openbaar Ministerie en de rechters in acht moeten nemen bij de opsporing, vervolging en berechting van strafbare feiten.
- Bepalingen die aangeven welke gedragingen strafbaar zijn en welke straffen de rechter de dader op kan leggen. Deze bepalingen beogen de informatiesystemen zelf te beschermen.

In het verdrag wordt de term 'CIA-delicten' gehanteerd voor de bepalingen die de informatiesystemen beogen te beschermen.[54] Hieronder vallen delicten die de volgende aspecten van informatiesystemen in gevaar kunnen brengen:

- Confidentiality;
- Integrity en
- Availability.

De bepalingen die aan deze CIA-delicten gewijd zijn, zijn te vinden in de artikelen 2 tot en met 6 van het Cyber Crime Verdrag.[55]

3.5.1 Artikel 1 Cyber Crime Verdrag: definities

In artikel 1 van het Cyber Crime Verdrag worden eerst de definities weergegeven die gebruikt worden om aan te geven wat onder een 'computer system' en 'computer data' moet worden verstaan.

Artikel 1 van het Cyber Crime Verdrag luidt:

Computer sysytem means any device or a group of inter-connected or related devices, one or more which, pursuant to any program, performs automatic processing of data.

Computer data means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

3.5.2 Artikel 2 Cyber Crime Verdrag: illegal access

Artikel 2 van het Cyber Crime Verdrag heeft betrekking op het opzettelijk binnendringen in een deel van een computer, zonder dat de dader hiertoe gerechtigd is.

Artikel 2 van het Cyber Crime Verdrag luidt:

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A party

54 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 137
55 TK 1999-2000, 23530, nr. 40, p.3 en 4 en TK 2000 – 2001, 23530, nr. 45, p.6

may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Artikel 138a WvSr betreffende het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk is een uitwerking van bovenstaande bepaling.

3.5.3 Artikel 3 Cyber Crime Verdrag: illegal interception

Artikel 3 van het Cyber Crime Verdrag omvat het opzettelijk, met behulp van een technisch hulpmiddel, onrechtmatig onderscheppen van gegevensverkeer dat via telecommunicatie gaat naar of afkomstig is van een computersysteem.

Artikel 3 van het Cyber Crime Verdrag luidt:

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Artikel 3 van het Cyber Crime Verdrag komt overeen met de bepalingen in de artikelen 139c WvSr en heeft betrekking op het aftappen van netwerken die niet ter beschikking staan van het publiek (artikel 139c WvSr).

3.5.4 Artikel 4 Cyber Crime Verdrag: data interference

In artikel 4 van het Cyber Crime Verdrag is de strafbaarstelling van opzettelijke beschadiging, verwijdering, wijziging en / of vernietiging van geautomatiseerd opgeslagen gegevens geregeld.

Artikel 4 van het Cyber Crime Verdrag luidt:

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2. A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Deze bepaling komt overeen met artikel 350a die strafbaar stelt het opzettelijk onbruikbaar maken, wissen, wijzigen en veranderen van computergegevens.

3.5.5 Artikel 5 Cyber Crime Verdrag: system interference

Artikel 5 van het Cyber Crime Verdrag stelt het opzettelijk veroorzaken van stoornis in het functioneren van computersystemen strafbaar. De stoornis kan bijvoorbeeld veroorzaakt worden door het verwijderen, wijzigen, toevoegen of beschadigen van computergegevens.

Artikel 5 van het Cyber Crime Verdrag luidt:

Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing of computer data.

In de toelichting bij het Cyber Crime Verdrag wordt als voorbeeld genoemd het verzenden van email-bommen. Daarnaast kan gedacht worden aan Distributed Denial of Service-aanvallen ((d)Dos-attacks) of verspreiding van virussen.

Het artikel is deels opgenomen in artikel 161sexies WvSr. In artikel 5 van het Cyber Crime Verdrag is sprake van 'computersystemen' en heeft hier betrekking op alle computersystemen en niet alleen op 'computersystemen die gebruikt worden voor de gegevensverwerking ten algemenen nutte', zoals in artikel 161sexies WvSr. In de kamerstukken is aangegeven dat er een aanvullende bepaling zal moeten komen voor het veroorzaken van een stoornis in het functioneren van niet-openbare netwerken.[56]

3.5.6 Artikel 6 Cyber Crime Verdrag: misuse of devices

Artikel 6 van het Cyber Crime Verdrag stelt strafbaar het opzettelijk vervaardigen, beschikbaarstellen en verspreiden van:

1. Voorwerpen of programma's die geschikt zijn om delicten genoemd in de artikelen 2 – 5 te kunnen plegen en
2. Wachtwoorden en toegangscodes waardoor iemand in staat wordt gesteld zichzelf toegang te verschaffen tot (een deel van) een computersysteem. Met het gebruik van het wachtwoord moet iemand de bedoeling hebben om een van de delicten in de artikelen 2 – 5 te plegen.

Artikel 6 van het Cyber Crime Verdrag luidt:

1. Each party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, and without right:
a. the production, sale, procurement for use, import, distribution or otherwise making available of:

56 TK 2000 – 2001, 23530, nr. 45, p.6 en *Handleiding Cyber Crime, Van herkenning tot aangifte*, Govcert.nl (/KLPD), Den Haag, Augustus 2005, p. 138

a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 – 5;
a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5; and
b. the possession of an item referred to in paragraphs (a)(1) or (2) above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 – 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
2. This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this Article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorized testing or protection of a computer system.
3. Each Party may reserve the right not to apply paragraph 1 of this Article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 (a)(2).

Het bezit van een voorwerp of programma dat geschikt is om de delicten genoemd in de artikelen 2 – 5 van het Cyber Crime Verdrag te plegen en het bezit van wachtwoorden / toegangscodes (indien iemand de bedoeling heeft het te gebruiken om een van de delicten genoemd in de artikelen 2 – 5 van het Cyber Crime Verdrag te plegen) is ook strafbaar.

Artikel 6 van het Cyber Crime Verdrag betreft het misbruik van instrumenten en dergelijke. De verdragspartijen moeten strafbaar stellen het opzettelijk en wederrechtelijk (‘intentionally and without right’) vervaardigen, verkopen, verwerven, invoeren, verspreiden of anderszins ter beschikking stellen of voorhanden hebben van :

- een technisch hulpmiddel (daaronder begrepen een computerprogramma) dat hoofdzakelijk ontworpen is c.q. hoofdzakelijk geschikt gemaakt is tot het plegen van een van de strafbare feiten van de artikelen 2 tot en met 5 van het Cyber Crime Verdrag of van
- een computerwachtwoord, toegangscode of soortgelijk gegeven waardoor een computersysteem of deel daarvan kan worden binnengedrongen.

Eis voor strafbaarheid is volgens artikel 6 van het Cyber Crime Verdrag wel, dat een en ander plaatsvindt ‘met de bedoeling’ dat het desbetreffende object of gegeven wordt gebruikt met het doel om een strafbaar feit te plegen als bedoeld in de artikelen 2 tot en met 5 van het Cyber Crime Verdrag. Het gaat hier in feite om de strafbaarstelling van voorbereidingshandelingen in verband met de hier besproken computervredebreuk en het belemmeren van de werking van geautomatiseerde werken, evenals het in artikel 139c WvSr strafbaar gestelde aftappen van computergegevens. Deze materie wordt in het geldende strafrecht slechts ten dele afgedekt door bepalingen als artikel 350a lid 3 WvSr (wormen) en artikel 139d WvSr (voorhanden hebben of aanwezig doen zijn van een technisch hulpmiddel met het oogmerk communicatie af te tappen). In het conceptwetsvoorstel wordt getracht het voorschrift van artikel 6 Cyber Crime Verdrag volledig na te leven door het toevoegen van een nieuw tweede en derde lid aan artikel 139d WvSr.

De Nederlandse wetgever is tot op heden niet zo scheutig om voorbereidingshandelingen ‘als zodanig’ strafbaar te stellen. Met het voorgestelde tweede en derde lid van artikel 139d WvSr worden nieuwe

strafbare voorbereidingshandelingen aan ons strafrecht toegevoegd. Artikel 6 lid 2 van het Cyber Crime Verdrag vermeldt uitdrukkelijk dat het niet de bedoeling is om het gebruik van technische hulpmiddelen, wachtwoorden et cetera te goeder trouw, bijvoorbeeld om de eigen beveiliging te testen, onder het bereik van de strafwet te brengen. De minister is dit ongewenste effect tegen gegaan door de opzet-variant 'oogmerk' als bestanddeel op te nemen. Dat betekent dat iemand op grond van het tweede lid van artikel 139d WvSr pas strafbaar is als hij de onder a en b genoemde handelingen verricht met als naaste doel dat het delict hacking, een (d)Dos-aanval of het aftappen van gegevens wordt gepleegd. Het gebruik van de term 'oogmerk' sluit het toepassen van 'voorwaardelijk opzet' (het aanvaarden van de geenszins als denkbeeldig te verwaarlozen kans dat ...) volgens vaste jurisprudentie uit, en dat lijkt, gezien de potentieel nogal ruime strekking van deze bepaling, geen overbodige luxe.[57] Ik zal hier in het volgende hoofdstuk verder op ingaan als ik de frequentie en intentie van een port scan bespreek.

Wel ontstaan er problemen met betrekking tot het voorgestelde derde lid van artikel 139d WvSr. Aldaar worden de in het tweede lid genoemde gedragingen met een aanzienlijk hogere straf bedreigd indien het oogmerk van de dader gericht is op gekwalificeerde[58] hacking. Het gaat daarbij om de vormen van computervredebreuk die in het tweede en derde lid van artikel 138a WvSr strafbaar zijn gesteld. Daarvoor moet allereerst het gronddelict (de computervredebreuk van het eerste lid van artikel 138a WvSr) worden gepleegd en vervolgens gegevens gekopieerd (artikel 138a lid 2 WvSr) of door tussenkomst van een openbaar netwerk met het oogmerk van wederrechtelijke bevoordeling systeemtijd worden gebruikt dan wel worden binnengedrongen in een derde systeem (artikel 138a lid 3 WvSr). Dit betekent in de praktijk een vrijwel onmogelijke bewijslast voor het Openbaar Ministerie. Met betrekking tot het in het tweede lid van artikel 139d WvSr (nieuw) strafbaar gestelde zal moeilijk te bewijzen zijn dat men bijvoorbeeld een wachtwoord of utility voorhanden heeft met het oogmerk dat daarmee gehackt gaat worden. Dat wordt wellicht anders indien er daadwerkelijk een 'poging' is gevolgd, dus als er een gerichte port scan heeft plaats gevonden, kwetsbare plekken in het geautomatiseerde systeem zijn gevonden en vervolgens een poging tot inbraak middels een exploit is gevolgd. Artikel 139d lid 2 WvSr (nieuw) kan dan worden ingezet in plaats van de als zodanig zeer moeilijk bewijsbare poging tot computervredebreuk via artikel 45 WvSr.

3.6 Samenvatting en conclusie

In het Wetboek van Strafrecht is geen bepaling opgenomen die de portscan strafbaar stelt. Een portscan wordt gebruikt om te onderzoeken welke mogelijke onbeveiligde poorten er op een geautomatiseerd systeem zijn. Er wordt bij een portscan geen enkele verdere actie ondernomen. Er is aldus niet direct sprake van het binnendringen in een geautomatiseerd werk (art. 138a WvSr), gegevensaantasting (art. 350a en b WvSr), het veroorzaken van een stoornis in de werking van een

57 F.P.E. Wiemans, *Computervredebreuk nieuwe stijl en strafbare voorbereidingshandelingen*, JAVI, December 2004, nummer 6, p. 203

58 Ibid, p. 204

geautomatiseerd werk (art. 161sexies WvSr) of het aftappen en opnemen van gegevens (art. 139c en d WvSr).

Zowel de Wet Computercriminaliteit II als het Cyber Crime Verdrag besteedt geen specifieke aandacht aan een portscan. Wel worden er met het tweede en derde lid van artikel 139d WvSr nieuwe strafbare voorbereidingshandelingen aan het strafrecht toegevoegd. Daarbij worden de volgende criteria onderscheiden voor de strafbaarstelling van een aantal voorbereidingshandelingen. Er moet sprake zijn van:[59]

1. Het oogmerk om te hacken, om de functie van een computer(systeem) te belemmeren of om gegevens af te tappen of op te nemen.
2. Een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen is om te hacken, een ernstige stoornis in een computersysteem te veroorzaken dan wel af te tappen of op te nemen, of
3. Een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan.
4. Ter beschikking stellen of voorhanden hebben door bijvoorbeeld het vervaardigen, verkopen, verwerven, invoeren of het verspreiden.

Aangezien een portscan doorgaans met behulp van speciale programmatuur wordt uitgevoerd is het in de toekomst wellicht mogelijk om artikel 139d lid 2 (voorbereidingshandelingen) van toepassing te verklaren. Het zal echter van de omstandigheden van het geval afhangen of de portscan wordt gebruikt voor het plegen van een ander strafbaar feit (bijvoorbeeld hacken). Er kan dan sprake zijn van poging met betrekking tot het plegen van dat andere delict. Het is mogelijk dat de informatie die uit de portscan naar voren komt, gebruikt wordt om één van de andere vormen van cyber crime te plegen. Afhankelijk van welke gedraging volgt kan de dader strafbaar zijn. Indien de portscan kan worden gezien als een voornemen van de dader tot een ander strafbaar feit, het binnendringen in een geautomatiseerd werk (art. 138a WvSr), gegevensaantasting (art. 350a en b WvSr), het veroorzaken van stoornis in de werking van een geautomatiseerd werk (art. 161sexies WvSr) of het aftappen en opnemen van gegevens (art. 139c t/m d WvSr), dan zou strafbaarheid kunnen ontstaan op grond van poging. Het zal echter bijzonder lastig zijn om de opzet van de verdachte aan te tonen (het vereiste voornemen van de verdachte om het systeem binnen te dringen of andere strafbare handelingen te verrichten).

In het volgende hoofdstuk zal ik daarom de pogingsleer bespreken en relateren aan de port scan om te bepalen of een strafbaarstelling mogelijk en zinvol is op grond van de gewijzigde artikelen naar aanleiding van de Wet Computercriminaliteit II en het Cyber Crime Verdrag.

59 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 135

4 Port scanning gekoppeld aan de pogingsleer

4.1 Inleiding

In het vorige hoofdstuk is de relevante nationale en internationale wetgeving ten aanzien van computercriminaliteit op een rij gezet. Hieruit bleek dat er geen bepaling in de Wet Computercriminaliteit II of het Cyber Crime Verdrag is opgenomen ten aanzien van de port scan. Het zal van de omstandigheden van het geval afhangen of de port scan wordt gebruikt voor het plegen van een ander strafbaar feit, zoals het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk (art. 138a, lid 1 WvSr). Er kan dan sprake zijn van poging met betrekking tot het plegen van dat andere delict.

Om onderzoeksvragen twee en drie (is port scanning naar zijn uiterlijke verschijningsvorm te beschouwen als een poging tot inbraak in een geautomatiseerd systeem en van welk niveau en met welke intentie moet er sprake zijn van port scanning voor er van een gerichte poging tot inbraak sprake is) te beantwoorden, zal ik hierna de geldende pogingsleer met de daarbij behorende facetten presenteren en deze per facet relateren aan de handelingen die een hacker uitvoert om een geautomatiseerd systeem te verkennen door middel van een port scan. Tevens zal ik hierbij ingaan op relevante jurisprudentie en beoordelen of er een vergelijking getrokken kan worden tussen de facetten van de pogingsleer en de verschillende stadia en opties bij portscanning naar aanleiding van de verschillende leren die door de Hoge Raad zijn gehanteerd ten aanzien van de pogingsleer.

Ik zal bij onderzoeksvraag twee met name ingaan op de vraag of een port scan naar zijn uiterlijke verschijningsvorm is te beschouwen als een poging tot inbraak in een geautomatiseerd systeem (art. 138a, lid 1 WvSr) en niet verder ingaan op de in het vorige hoofdstuk behandelde andere strafartikelen aangezien deze bijna alle pas kunnen plaatsvinden nadat er daadwerkelijk is ingebroken in een geautomatiseerd systeem. Wel zal ik kort aandacht besteden aan de twee, door de Wet Computercriminaliteit II toegevoegde, nieuwe leden aan artikel 139d WvSr, omdat deze leden verruimde mogelijkheden bieden voor strafbaarheid van bepaalde voorbereidingshandelingen. Daarbij gaat het onder andere om voorbereidingshandelingen met betrekking tot art. 138a, lid 1 WvSr.
Bij de behandeling van de port scan zal ik gebruik maken van de man-pages[60] van de tool Nmap. Nmap (Network Mapper), geschreven door Fyodor, is de meest krachtige en flexibele port scanner die er op dit moment is en draait zowel onder UNIX / Linux als onder Windows. Nmap is bedoeld voor netwerkverkenning en security-audits. Het kan een doelsysteem of een compleet netwerk scannen waarbij het naast doelsystemen scant op randapparatuur en de poorten, services en applicaties die daarop draaien. Nmap gebruikt daarnaast een zeer verfijnde database met 'fingerprints' van bepaalde besturingssystemen (OS, operating systems) om te bepalen wat voor soort doelsysteem of randapparatuur het scant en om het OS daarvan te detecteren en kan zelfs bepaalde typen firewalls

60 Man-pages (manual pages) zijn toelichtingen die bij ieder UNIX / Linux programma / toepassing zijn op te roepen door in een shell-omgeving het commando 'man X' in te typen, waarbij X staat voor het desbetreffende programma; hier: 'man nmap'.

detecteren. Het spreekt voor zich dat deze tool niet alleen zeer populair is onder systeembeheerders maar ook bij vele hackers om zwakke plekken in de beveiliging van doelsystemen of netwerken te ontdekken. Nmap biedt enorm veel mogelijkheden voor het uitvoeren van port scans. Ik zal hier echter alleen díe opties in Nmap bespreken die voor de facetten bij de pogingsleer van belang zijn om van een eventuele poging tot een inbraak in een geautomatiseerd systeem te kunnen spreken.

4.2 Voorwaarden voor strafbare poging

Artikel 45, lid 1 WvSr luidt: 'Poging tot misdrijf is strafbaar wanneer het voornemen van de dader zich door een begin van uitvoering heeft geopenbaard'. Uit de wet zelf valt dus niet op te maken wat precies onder poging moet worden verstaan maar daarvoor is in de MvT uitdrukkelijk verwezen naar de dogmatiek en de opvattingen onder rechtsgeleerde schrijvers.[61]
In art. 45 WvSr wordt in feite volstaan met het noemen van een tweetal voorwaarden voor strafbaarheid van de poging, te weten dat er een voornemen van de dader moet zijn, hetwelk moet blijken uit een begin van uitvoering. Vervolgens wordt in art. 46b WvSr de poging alsnog straffeloos verklaard als die uitvoering waarmee een begin is gemaakt niet tot voltooiing van het misdrijf heeft geleid tengevolge van omstandigheden die van de wil van de dader zelf afhankelijk zijn: vrijwillige terugtred. Als de eenmaal begonnen uitvoering echter wordt gestuit door omstandigheden die uitsluitend buiten de eigen invloedssfeer van de dader zijn gelegen dan is de poging dus wèl strafbaar.[62]

Binnen de wettelijke voorwaarden voor de strafbare poging kunnen zich zeer uiteenlopende situaties voordoen. Aan de ene kant zijn er de situaties waarin de dader niet tot voltooiing van het voorgenomen misdrijf is gekomen, terwijl er van zijn kant wel al het mogelijke is gedaan om die voltooiing te bereiken: in deze situaties wordt gesproken van een 'voltooide' poging. Dit doet zich bijvoorbeeld voor als het slachtoffer extra sterk blijkt te zijn en de dader er een onmogelijke kluif aan heeft de betrokkene te beroven. Aan de andere kant doen zich situaties voor waarin al in een vroeg stadium van de uitvoering van het misdrijf een verhindering optreedt om dit te voltooien. In dat geval spreekt men van 'onvoltooide poging'. Hierbij kan men denken aan een oplettende buurman die een stel inbrekers betrapt die nog maar net begonnen zijn met de inbraak en daarom wegvluchten.

Er zijn twee belangrijke restricties aan de (mate van) strafbaarheid van de poging gesteld die beide zijn te herleiden tot het feit dat een niet voltooid delict als minder ernstig feit geldt dan een voltooid delict. In de eerste plaats is poging uitsluitend strafbaar als het om een voorgenomen misdrijf staat. Poging tot overtreding is niet strafbaar daar overtreding op zichzelf al een geringere graad van onrecht betreft zodat strafbaarstellen overtrokken zou zijn. In de tweede plaats kent art. 45 WvSr voor het geval van poging een verlaging van het op het desbetreffende misdrijf toepasselijke strafmaximum met een derde. Hieruit valt echter allerminst te concluderen dat poging een strafverlagende

61 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 303
62 Ibid, p. 303

omstandigheid zou zijn. Integendeel, poging tot misdrijf betekent een uitbreiding van strafbaarheid omdat zonder de regeling van de poging er helemaal geen sprake van een strafbaar feit zou zijn.[63]

4.2.1 Voornemen

De vraag die zich ten aanzien van het voornemen van de dader opwerpt is of het voornemen ook denkbaar is in de versie van voorwaardelijke opzet, nu in de term 'voornemen' een soortgelijk bewust willen en weten doorklinkt als in opzet het geval is.[64] Het verschil blijft natuurlijk dat van voornemen slechts wordt gesproken met betrekking tot situaties die niet tot een voltooid misdrijf hebben geleid, zodat het veel moeilijker is om het bewuste willen en weten te reconstrueren. Dit bleek uit het geval van een automobilist die inreed op een politieagent die zich nog net kon redden door tijdig opzij te springen. De Hoge Raad ging ermee akkoord dat hier poging tot doodslag op de agent werd aangenomen en derhalve dat het vereiste voornemen zich kon manifesteren als voorwaardelijke opzet.[65] Dit oordeel berustte op twee nauw met elkaar samenhangende veronderstellingen, namelijk dat als de agent niet tijdig opzij gesprongen was hij inderdaad doodgereden zou zijn en dat de automobilist toen hij doorreed deze eventuele dood van de agent ook voor lief heeft genomen. Een en ander betekent een anticipatie op een bepaald te verwachten causaal verloop op basis van een normatieve interpretatie van de handeling van de automobilist: gezien de omstandigheden wordt naar de ervaring leert door een dergelijk handelen het leven van een ander in gevaar gebracht terwijl in deze handeling qua teneur tevens de intentionaliteit ten aanzien van de dood van die ander kan worden gezien (normatief opzet).[66] Voornemen mag aldus worden gelijkgesteld met opzet. Dat wil dus zeggen dat evenals bij het voltooide delict hier het opzet moet zijn gericht op alle bestanddelen die in de delictsomschrijving van het gronddelict door het woord opzet of een vergelijkbare term taalkundig worden beheerst. Opzet kan zich ook hier in alle gradaties voordoen, inclusief het voorwaardelijk opzet, dat ook geobjectiveerd kan worden ingevuld.[67] Kent het gronddelict echter een zwaarder opzetvereiste, dan geldt dat vereiste ook voor de poger.[68]

Voornemen in relatie tot port scanning

In de Wet Computercriminaliteit II is artikel 138a lid 1 WvSr gewijzigd. Artikel 138a, lid WvSr luidt nu:

Met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie wordt, als schuldig aan computervredebreuk, gestraft hij die opzettelijk en wederrechtelijk binnendringt in een geautomatiseerd werk of in een deel daarvan. Van binnendringen is in ieder geval sprake indien de toegang tot het werk wordt verworven
a. door het doorbreken van een beveiliging,
b. door een technische ingreep,
c. met behulp van valse signalen of een valse sleutel of
d. door het aannemen van een valse hoedanigheid.

63 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, pp. 304 - 305
64 Ibid, p. 309
65 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent
66 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, pp. 309 - 310
67 Zie HR 17 december 1996, NJ 1997, 245 en HR 21 november 2000, NJ 2001, 160
68 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 318

De huidige redactie van het artikel formuleert de onderdelen a en b als voorwaarden voor strafbaarheid. In de voorgestelde versie zijn de onderdelen a t/m d voorbeelden van gevallen waarin sprake is van binnendringen. Er worden dus geen eisen meer gesteld aan het binnendringen. Hierdoor wordt ieder opzettelijk en wederrechtelijk binnendringen in een computersysteem strafbaar. De verwarring die met de huidige redactie van het artikel kan ontstaan met betrekking tot het begrip binnendringen, wordt hierdoor geëlimineerd. Door tussenvoegen van het woordje 'en' tussen de woorden opzettelijk en wederrechtelijk, vervalt de eis dat de dader weet dat zijn gedraging wederrechtelijk is.[69]

Waaruit is het voornemen van een hacker bij een port scan af te leiden als van voornemen slechts wordt gesproken met betrekking tot situaties die niet tot een voltooid misdrijf hebben geleid? Het bewuste willen en weten van een hacker bij een port scan kan mijns inziens worden onderkend door een aantal opties die aan Nmap kunnen worden meegegeven en in een router, een firewall of een Intrusion Detection System (IDS) gelogd kunnen worden.
Nmap biedt de mogelijkheid om de frequentie van scans in te stellen, bijvoorbeeld op een moment dat er weinig of geen systeem beheerders aanwezig zijn of dat de port scan wordt uitgevoerd met voldoende tijd tussen de verschillende scans om geen argwaan te wekken. Daarnaast biedt Nmap de mogelijkheid om 'sneaky' scans uit te voeren. Dit zijn scans die niet of slecht opgemerkt kunnen worden door firewalls of Intrusion Detection Systems (IDS's). Een hacker kan tevens een port scan met Nmap uitvoeren met verschillende decoys of een gespoofed IP-adres, waardoor de scan van een ander IP-adres afkomstig lijkt te zijn dan van het werkelijke IP-adres van de hacker of de te verzenden packets fragmenteren waardoor het wederom moeilijker wordt voor een firewall of IDS een port scan op te merken. Tenslotte, en dat is wellicht de meest zichtbare aanwijzing dat een hacker doelbewust op zoek is naar kwetsbare doelsystemen of netwerken, kan een hacker Nmap de optie meegeven specifiek te scannen op bepaalde poorten met bekende services waarvan bekend is dat er beveiligingslekken zijn ontdekt ten aanzien van die services.

<u>Specifieke port scans</u>
Nmap biedt de mogelijkheid om zeer specifiek te scannen op poorten met bekende services / protocollen, bijvoorbeeld op het FTP-protocol op poort 21, het Telnet-protocol op poort 23 of, de meest bekende, het HTTP-protocol op poort 80. Van deze services is bekend dat er met enige regelmaat door hackers zwakke plekken worden ontdekt die vervolgens uitgebuit kunnen worden om toegang te kunnen krijgen tot een geautomatiseerd systeem.
Port scans die worden uitgevoerd op specifieke poorten kunnen, in het geval er een firewall, router of IDS actief draait op het doelsysteem, worden gelogd en opgeslagen in log-files. Op deze wijze kan inzicht worden verkregen in de frequentie van de scan en op welke poorten de hacker specifiek zijn aandacht heeft gericht. Onderstaand is een voorbeeld weergegeven van een deel van de log-files in mijn router op 4 juni 2006:

Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:5000

69 TK 1998 – 1999, 26 671, nr. 3, p. 44

Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1720
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1030
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1029
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1028
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1027
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1026
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1025
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1024
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:1002
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:443
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:389
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:143
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:119
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:113
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:110
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:80
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:79
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:25
Sun Jun 04 18:55:10 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:23
Sun Jun 04 18:55:11 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:22
Sun Jun 04 18:55:11 2006 Unrecognized attempt blocked from 4.79.142.206:39647 to 62.195.X.X TCP:21[70]

Duidelijk zichtbaar is dat de hacker een aantal specifieke poorten in slechts enkele seconden heeft gescand. Port scans vinden op het Internet echter erg veel plaats maar daarbij is vaak sprake van een korte connectie tussen een geautomatiseerd systeem en het doelsysteem en wordt slechts een bepaalde service benaderd. Een voorbeeld hiervan is de korte verbinding die ontstaat tussen een geautomatiseerd systeem en een Domain Name System-Server (DNS-server). Wat tevens aan de log-file opvalt, is dat de hacker niet gescand heeft op de poorten 135 – 139 (Windows-protocollen) zodat deze vermoedelijk specifiek op zoek was naar doelsystemen waar geen Windows OS op draait.
De hacker heeft met deze port scan in totaal 22 poorten gescand met de meest bekende protocollen. Daarnaast heeft hij specifiek op poorten gescand boven poort 1024.[71] Dit zou kunnen betekenen dat de hacker op zoek was naar bijvoorbeeld Trojans als Back Orifice[72] of Subseven[73] om op afstand de controle van een doelsysteem over te nemen en als zodanig direct volledige toegang te hebben tot een doelsysteem. Dergelijke Trojans kunnen zich op het systeem van een argeloze computergebruiker installeren door bijvoorbeeld het openen van een emailbijlage. Indien het servergedeelte van een Trojan zich eenmaal geïnstalleerd heeft, luistert het, op door de maker van de Trojan vooraf bepaalde poorten, naar inkomende verzoeken van het clientgedeelte op de computer van de hacker om verbinding te leggen met het geïnfecteerde doelsysteem. De standaardpoorten voor dit soort programma's is algemeen bekend onder hackers en port scans worden dan ook vaak uitgevoerd op díe poorten waarvan bekend is dat er een servergedeelte van een Trojan actief kan luisteren naar inkomende verbindingen.

70 Om privacyredenen zijn de laatste twee cijfercombinaties van het IP-adres van het doelsysteem niet weergegeven.

71 De poorten van 0 – 1024 zijn 'officiële' toegewezen poorten door de Internet Assigned Numbers Authority (IANA) en kunnen op de meeste systemen alleen gebruikt worden door systeemprocessen of door programma's die door gepriviligieerde gebruikers (root) opgestart worden. De poorten 1025 – 65535 zijn vrij om door gebruikers toegewezen te worden om door andere applicaties gebruikt te worden.

72 Zie <http://www.bo2k.com>

73 Zie <http://www.hackpr.net/~sub7/support.shtml>

De informatie die een port scan oplevert kan ervoor zorgen dat een doelsysteem zijn kwetsbare plekken onthult. Jamieson beschouwt daarom een port scan als kwaadaardig als de hacker het voornemen heeft om met de port scan kwetsbare plekken in een doelsysteem te vinden.[74] Had de hacker met deze port scan het voornemen om een geslaagde poging tot inbraak in een geautomatiseerd systeem te plegen? Juist het aantonen van dit voornemen, en dus het aantonen van de opzet op alle bestanddelen in de delictsomschrijving van art. 138a, lid 1 WvSr, blijft problematisch omdat het gronddelict niet voltooid is. Gaat men echter uit van een normatief opzet-begrip zoals door de Hoge Raad gehanteerd in het Inrijden op agent-arrest[75] dan kan een en ander een anticipatie op een bepaald te verwachten causaal verloop betekenen op basis van een normatieve interpretatie van de specifieke port scan door de hacker: gezien de omstandigheden worden, naar de ervaring leert, door een specifieke port scan de kwetsbare plekken in een geautomatiseerd systeem onthuld en kan mijns inziens aan de handeling (de *specifieke* port scan) qua teneur tevens de intentionaliteit ten aanzien van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem worden gezien.

Sneaky scans

Hieronder is een deel van de man-pages van Nmap weergegeven die uitleg geven over 'sneaky' scans middels het uitvoeren van respectievelijk een Null scan, een FIN-scan of een Xmas-scan:

> Null scan (**-sN**)
> Does not set any bits (tcp flag header is 0)
> FIN scan (**-sF**)
> Sets just the TCP FIN bit.
> Xmas scan (**-sX**)
> Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree.
> These three scan types are exactly the same in behavior except for the TCP flags set in probe packets. If a RST packet is received, the port is considered closed, while no response means it is open|filtered. The port is marked filtered if an ICMP unreachable error (type 3, code 1, 2, 3, 9, 10, or 13) is received.
> *The key advantage to these scan types is that they can sneak through certain non-stateful firewalls and packet filtering routers. Another advantage is that these scan types are a little more stealthy than even a SYN scan. Don't count on this though -- most modern IDS products can be configured to detect them* (cursivering JT). The big downside is that not all systems follow RFC 793 to the letter. A number of systems send RST responses to the probes regardless of whether the port is open or not. This causes all of the ports to be labeled closed. Major operating systems that do this are Microsoft Windows, many Cisco devices, BSDI, and IBM OS/400. This scan does work against most UNIX-based systems though. Another downside of these scans is that they can't distinguish open ports from certain filtered ones, leaving you with the response open|filtered.[76]

Zoals de man-pages van Nmap al aangeven is het grote voordeel van deze scantypes dat deze scans door bepaalde non-stateful[77] firewalls en packet-filtering routers kunnen doordringen. Een ander voordeel is dat dit type scans nog meer 'stealthy' zijn dan een reeds stille SYN-scan hoewel bij de moderne IDS's ook dit type scans al wordt opgemerkt.

---

74 S. Jamieson, *The ethics and legality of port scanning*, GSEC Practical assignment, v2.1f, October 8, 2001, p. 2

75 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent

76 Zie <http://www.insecure.org/nmap/man/man-portscanning-techniques.html>

77 Een non-stateful firewall is een firewall die ieder netwerkpakketje afzonderlijk behandelt. Zo'n firewall weet niet of dit pakketje een onderdeel is van een bestaande connectie, een nieuwe verbinding probeert te leggen of een kwaadaardig los pakketje is. Moderne firewalls (stateful firewalls) zijn 'verbindingsbewust' en geven systeembeheerders een betere controle om het netwerkverkeer te analyeren.

Wat betekent het voor het voornemen van een hacker als dit type scans worden aangetroffen in routers, IDS's of firewall-logs? Hoewel Nmap door de auteur dan wellicht als security- en administratorstool wordt gekenmerkt, biedt het programma de mogelijkheid om een dergelijke 'sneaky' scan uit te voeren en om door bepaalde non-stateful firewalls en packet-filtering routers door te kunnen dringen. Systeembeheerders kunnen Nmap gebruiken om de veiligheid van hun systemen en / of netwerken te testen en ook dit type scans op hun systemen / netwerken los laten. Dergelijke scans zullen, vanwege de vereiste specialistische kennis om de resultaten van zo'n scan te kunnen analyseren, niet snel worden ingezet door niet-systeembeheerders. Hackers beschikken vaak over een nog grotere kennis dan systeembeheerders en hebben vaak al door middel van een eerdere Nmap-scan vastgesteld welk type firewall of router er op het doelsysteem draait, welke versie het betreft en of het een packet-filtering firewall of router betreft. Indien er daarna gericht wordt gescand door middel van een van bovenstaande scan-types kan dit een sterke indicatie zijn dat het voornemen van de hacker erop gericht is om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen. Gaat men ook hier weer uit van een normatief opzet-begrip zoals door de Hoge Raad gehanteerd in het Inrijden op agent-arrest[78] dan kan een en ander een anticipatie op een bepaald te verwachten causaal verloop betekenen op basis van een normatieve interpretatie van de opties die aan de port scan door de hacker zijn meegegeven: gezien de omstandigheden worden, naar de ervaring leert, door dergelijke port scans non-stateful firewalls en packet filtering routers omzeild en kan mijns inziens aan de handeling (de port scan met de opties die het mogelijk maken bepaalde typen routers, firewalls of IDS's te omzeilen) qua teneur tevens de intentionaliteit ten aanzien van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem worden gezien.

> Network obstructions such as firewalls can make mapping a network exceedingly difficult. It will not get any easier, as stifling casual reconnaissance is often a key goal of implementing the devices. Nevertheless, Nmap offers many features to help understand these complex networks, and to verify that filters are working as intended. *It even supports mechanisms for bypassing poorly implemented defenses* (cursivering JT). One of the best methods of understanding your network security posture is to try to defeat it. Place yourself in the mindset of an attacker, and deploy techniques from this section against your networks. Launch an FTP bounce scan, Idle scan, fragmentation attack, or try to tunnel through one of your own proxies.
>
> In addition to restricting network activity, companies are increasingly monitoring traffic with intrusion detection systems (IDS). All of the major IDSs ship with rules designed to detect Nmap scans *because scans are sometimes a precursor to attacks* (cursivering JT). Many of these products have recently morphed into intrusion prevention systems (IPS) that actively block traffic deemed malicious. Unfortunately for network administrators and IDS vendors, reliably detecting bad intentions by analyzing packet data is a tough problem. *Attackers with patience, skill, and the help of certain Nmap options can usually pass by IDSs undetected* (cursivering JT). Meanwhile, administrators must cope with large numbers of false positive results where innocent activity is misdiagnosed and alerted on or blocked.
>
> Occasionally people suggest that Nmap should not offer features for evading firewall rules or sneaking past IDSs. *They argue that these features are just as likely to be misused by attackers as used by administrators to enhance security* (cursivering JT). The problem with this logic is that these methods would still be used by attackers, who would just find other tools or patch the functionality into Nmap. Meanwhile, administrators would find it that much harder to do their jobs. Deploying only modern, patched FTP servers is a far more powerful defense than trying to prevent the distribution of tools implementing the FTP bounce attack. [79]

78 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent

79 Zie <http://www.insecure.org/nmap/man/man-bypass-firewalls.html>

De auteur van Nmap geeft in zijn man-pages aan dat netwerk obstructies zoals firewalls het scannen van een netwerk kunnen bemoeilijken. Daarom worden tegenwoordig veelal regels in IDS's ingebouwd om Nmap-scans (ook de 'sneaky' scans) door IDS's te kunnen detecteren omdat zij volgens de auteur vaak een voorbode van een aanval kunnen zijn. Een hacker met veel geduld en kennis kan echter, in combinatie met de opties die Nmap biedt, deze IDS's ongemerkt omzeilen.

Fragmented packet scans, decoy scans en spoofed source address scans

Uit de man-pages blijkt dat de volgende scantypes gebruikt kunnen worden voor het doorbreken van IDS's of firewall-regels: fragmented packet scans, decoy scans en spoofed source address scans.

> **-f** (fragment packets); **--mtu** (using the specified MTU)
> The **-f** option causes the requested scan (including ping scans) to use tiny fragmented IP packets. *The idea is to split up the TCP header over several packets to make it harder for packet filters, intrusion detection systems, and other annoyances to detect what you are doing* (cursivering JT). (…) Or you can specify your own offset size with the **--mtu** option. (…) Do a scan while a sniffer such as Ethereal is running to ensure that sent packets are fragmented. If your host OS is causing problems, try the **--send-eth** option to bypass the IP layer and send raw ethernet frames.
>
> **-D <decoy1 [,decoy2][,ME],...>** (Cloak a scan with decoys)
> Causes a decoy scan to be performed, which makes it appear to the remote host that the host(s) you specify as decoys are scanning the target network too. *Thus their IDS might report 5-10 port scans from unique IP addresses, but they won't know which IP was scanning them and which were innocent decoys. While this can be defeated through router path tracing, response-dropping, and other active mechanisms, it is generally an effective technique for hiding your IP address* (cursivering JT).
>
> Separate each decoy host with commas, and you can optionally use ME as one of the decoys to represent the position for your real IP address. *If you put ME in the 6th position or later, some common port scan detectors (such as Solar Designer's excellent scanlogd) are unlikely to show your IP address at all* (cursivering JT). If you don't use ME, nmap will put you in a random position.
>
> Note that the hosts you use as decoys should be up or you might accidentally SYN flood your targets. Also it will be pretty easy to determine which host is scanning if only one is actually up on the network. *You might want to use IP addresses instead of names (so the decoy networks don't see you in their nameserver logs)* (cursivering JT).
>
> (…)
>
> **-S <IP_Address>** (Spoof source address)
> In some circumstances, Nmap may not be able to determine your source address (Nmap will tell you if this is the case). In this situation, use **-S** with the IP address of the interface you wish to send packets through.
>
> *Another possible use of this flag is to spoof the scan to make the targets think that someone else is scanning them. Imagine a company being repeatedly port scanned by a competitor!* (cursivering JT). The **-e** option would generally be required for this sort of usage, and **-P0** would normally be advisable as well.[80]

Door middel van het sturen van gefragmenteerde IP-packets kan de TCP-header over verschillende packets verdeeld worden om het voor firewalls, IDS's of andere *vervelende* hindernissen moeilijker te maken om een port scan te detecteren. Door de auteur wordt aangeraden het programma Ethereal[81] mee te laten draaien om de persoon die de port scan uitvoert zich ervan te laten verzekeren dat de verzonden packets gefragmenteerd zijn. De optie –D kan gebruikt worden voor het scannen met verschillende decoys. Op die manier lijkt het of de port scan van 5 tot 10 unieke IP-adressen afkomstig

80 Zie <http://www.insecure.org/nmap/man/man-bypass-firewalls.html>
81 Zie <http://www.wireshark.org>

is zodat een systeembeheerder moeilijk kan achterhalen van welk IP-adres de port scan daadwerkelijk afkomstig was en welke slechts onschuldige decoys waren. Door de auteur wordt tevens aangeraden om bij een dergelijke scan het IP-adres te gebruiken in plaats van de computernaam om deze computernaam ook niet te laten opduiken in de nameserver-logs van de netwerk-decoys. Als Nmap niet in staat is om het IP-adres van de hacker te gebruiken bij een port scan kan de optie –S gebruikt worden. Hiermee wordt het IP-adres van de machine van de hacker gespoofed zodat het lijkt of iemand anders de scan uitvoert. Het verschil met de optie –D is dat de port scan hier wordt uitgevoerd zonder decoys, dus direct vanaf de machine van de hacker maar met een gespoofed IP-adres. In de firewall-logs van het doelsysteem zal dus slechts een gespoofed IP-adres gelogd worden in tegenstelling tot de meerdere IP-adressen die bij een decoy-scan gelogd worden.

Het probleem met dergelijke scans is dat deze vrijwel niet door een firewall of IDS opgemerkt kunnen worden. Pas na een grondige analyse van de firewall-logs of IDS-logs kan er vastgesteld worden dat er port scans worden uitgevoerd met gefragmenteerde packets. Decoy-scans en spoofed source address scans kunnen, zoals de auteur van Nmap al aangeeft, door router path tracing, response-dropping en andere actieve mechanismes gedetecteerd worden. De vraag die hierbij natuurlijk opkomt is: wat is de reden voor een dergelijke scan en waarom wil een hacker onopgemerkt blijven?
Het detecteren van dergelijke scantypes kan naar mijn mening een zeer sterke indicatie zijn dat het voornemen van de hacker erop gericht is om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen. Uitgaande van een normatief opzet-begrip zoals door de Hoge Raad gehanteerd in het Inrijden op agent-arrest[82] dan kan een en ander een anticipatie op een bepaald te verwachten causaal verloop betekenen op basis van een normatieve interpretatie van de opties die aan de port scan door de hacker zijn meegegeven: gezien de omstandigheden wordt het, naar de ervaring leert, voor IDS's en packet filters moeilijker om dergelijke typen port scans te detecteren en kan mijns inziens wederom aan deze handeling (de port scan met de opties die het mogelijk maken bepaalde typen packet filters en IDS's te omzeilen) qua teneur tevens de intentionaliteit ten aanzien van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem worden gezien.

4.2.2 Openbaren

Het voornemen van de dader moet zich door een begin van uitvoering hebben geopenbaard. De vraag is wat onder 'openbaren' moet worden verstaan. 'Openbaren' in art. 45 WvSr kan niet betekenen 'algemeen bekend maken'. Het zou te ver gaan om voor strafbaarheid van een poging te eisen dat een dader zijn voornemen algemeen bekend maakt. Immers de dader zal steeds trachten zijn daad aldus te stellen dat de kans op ontdekking zo gering mogelijk is. Openbaren moet hier daarom veeleer worden geduid als 'doen kennen' of 'uiten'. Het ziet op een naar buiten gerichte gedraging die opgemerkt kan worden: 'openbaren' in tegenstelling tot 'geheel in het verborgene'.[83] Het arrest van 24 oktober 1978 (Cito-arrest) kijkt voor wat betreft het openbaren naar de 'uiterlijke verschijningsvorm'

82 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent

83 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 553

van de gedraging. Uit die uiterlijke verschijningsvorm moet af te leiden zijn dat de gedraging moet worden beschouwd als te zijn gericht op de voltooiing van het misdrijf.

Openbaren in relatie tot port scanning

In de voorgaande paragraaf is beschreven welke opties Nmap een hacker biedt om zijn voornemen te verbergen. Het feit dat Nmap over de mogelijkheden beschikt om 'sneaky' scans uit te voeren, decoys in te bouwen en IP-adressen te spoofen, zorgt ervoor dat een hacker zijn voornemen zo veel mogelijk kan maskeren. Een hacker die zijn opzet heeft gericht op het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem, zal zijn voornemen niet algemeen bekend maken. Hij zal zijn handelingen dus zo veel mogelijk maskeren middels de reeds genoemde scantypes. Een port scan blijft echter wel een naar buiten gerichte gedraging die opgemerkt kan worden; het blijft niet 'geheel in het verborgene'. De port scan kan opgemerkt worden door een analyse van de log-files die in een router, firewall of IDS worden opgeslagen. Uit die uiterlijke verschijningsvorm (de log-files die de port scan hebben opgeslagen) moet dan wel af te leiden zijn dat de gedraging, in casu de port scan, moet worden beschouwd als te zijn gericht op de voltooiing van het misdrijf, het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem.

Aangezien een gewone port scan niet veel kennis vereist, kan deze ook door zogenaamde scriptkiddies[84] uitgevoerd worden die slechts complete netwerk ranges scannen en de resultaten niet verder kunnen interpreteren. Dit betekent mijns inziens dat het voornemen van een hacker tot het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem zich kan openbaren door een begin van uitvoering van een port scan indien, en slechts indien, die voldoet aan een van de in de vorige paragraaf genoemde scantypes.

4.2.3 Begin van uitvoering

Wat onder begin van uitvoering moet worden verstaan is door de Memorie van Toelichting (MvT) destijds helemaal overgelaten aan de rechtspraak en aan de wetenschap. Niettemin vormt daarbij het uitgangspunt in ons recht dat men niemand slechts op grond van zijn gedachten gevangen kan zetten. Dit alles laat onverlet de vraag waar precies de grens moet worden getrokken tussen de niet strafbare voorfase van de voorbereidingshandelingen, die wel reeds een bepaald voornemen verraden en de strafbare fase van de uitvoeringshandelingen.[85] Het ligt voor de hand te erkennen dat in voorbereidingshandelingen zo veel onzekerheid is gelegen dat deze in het belang van de rechtszekerheid dienen te blijven.

Het is uitermate moeilijk om voor de rijk geschakeerde werkelijkheid een enigszins sluitende formule te vinden voor wat onder het begrip uitvoeringshandeling moet worden gevat. Twee verschillende opvattingen hebben zich hieromtrent afgetekend, respectievelijk onder de naam van de subjectieve

84 Scriptkiddies gebruiken de tools die door echte hackers zijn ontwikkeld en leggen zelf weinig tot geen creativiteit aan de dag. Zo zijn veel virussen die door echte hackers zijn geschreven door scriptkiddies verspreid.

85 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 311

leer en de objectieve leer. In termen van de wettelijke omschrijving van art. 45 WvSr gaat men er in de subjectieve leer vanuit dat er begin van uitvoering moet zijn van het voornemen. Uitgangspunt is de kenbare misdadige gezindheid van de dader, de gevaarlijkheid, die in hem steekt. De objectieve gevaarlijkheid van de daad is in beginsel van geen belang. In zijn uiterste vorm komen we in deze leer gevaarlijk dicht in de buurt van een 'Gesinnungsstrafrecht'. Daarom wordt deze leer in zijn meest extreme vorm hier te lande ook niet aangehangen.[86] De objectieve leer is de leer die in ons land door de Hoge Raad wordt gehuldigd. Deze leer gaat uit van het objectieve gevaar van de daad voor de rechtsorde en laat pas als uitvoeringshandeling toe datgene wat als daadwerkelijke uitvoering van het misdrijf zelf en dus als objectieve inbreuk op de rechtsorde is te beschouwen. Hierbij wordt onderscheid gemaakt tussen delicten met een materiële en die met een formele omschrijving. Voor elk geven ze een andere definitie van het begin van uitvoering. Bij materieel geformuleerde delicten (gevolgdelicten) is er sprake van begin van uitvoering als de dader een zodanige handeling heeft verricht dat zonder zijn nader ingrijpen het delict zou zijn voltooid.[87] Bij formeel geformuleerde delicten (gedragsdelicten) is er begin van uitvoering als de dader begonnen is met de in de delictsomschrijving neergelegde handeling.[88]

Aangenomen moet worden dat art. 45 WvSr niet bedoelt iedere uiting van het voornemen tot misdrijf strafbaar te stellen maar pas die uiting waarin een begin van uitvoering van het misdrijf zelf kan worden gezien. Doch men kan toch een subjectieve opvatting over de uitvoeringshandeling voorstaan, namelijk op grond van een bepaalde kwade bedoeling die er duidelijk uit spreekt.[89]

Jurisprudentie

Voor de bepaling door de rechter van de grens tussen voorbereiding en uitvoering biedt de wettelijke delictsomschrijving een zeer belangrijke grondslag. Hoe preciezer de delictshandeling in de formele omschrijving is getypeerd hoe minder ruimte er voor begin van uitvoering zal overblijven. Bij de materieel omschreven delicten echter is het niet de handeling zelf maar het door de handeling teweeggebrachte gevolg dat wordt getypeerd.[90] Volgens Kelk ligt het sterk voor de hand dat ook met betrekking tot uitvoeringshandelingen enigszins normatieve interpretaties kunnen worden ontleend aan de concrete omstandigheden en wat ervaringsregels ons leren.[91]

De Hoge Raad heeft in het algemeen steeds de objectieve leer gehanteerd.[92] Steeds echter moet er om van uitvoering te kunnen spreken in ieder geval een zodanige gedraging zijn geweest, dat op het moment van de verhindering de voltooiing waarschijnlijk was.[93] In het Eindhovense

86 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 319

87 Formeel omschreven delicten zijn delicten waarbij sprake is van een duidelijk getypeerde delictshandeling. Materieel omschreven delicten worden getypeerd door een bepaald ongewenst gevolg.

88 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, pp. 119 - 120

89 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 311

90 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 312

91 Ibid, p. 313

92 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 320

93 Th.J.B. Buiting *In het voetspoor van Pompe, Strafbare poging*, diss. Utrecht, 1965, p. 134 in: C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 303

brandstichtingarrest[94] is door de Hoge Raad aanvankelijk zeer objectief geoordeeld. Hierbij was door de daders alles in gereedheid gebracht om in een huis een gaspistool te laten afgaan dat gericht was op in benzine gedrenkte lappen om verzekeringspenningen op te strijken. Hiervoor hoefden zij alleen nog maar aan het touwtje te trekken dat verbonden was aan de trekker van het gaspistool. Vanwege het feit dat de sterke benzinegeur zich verspreidde werden de buurtbewoners gealarmeerd waardoor de daders de aftocht bliezen. De Hoge Raad zag in deze feiten nog geen begin van uitvoering, hoewel over het doel toch weinig te raden overblijft. Als criterium voor uitvoering werd door de Hoge Raad de theorie van Simons gehanteerd, zodat van uitvoering pas sprake zou zijn geweest als er een daad was verricht, welke 'naar de regelen van de ervaring, zonder enig nader ingrijpen van de dader zelf tot brandstichting leidt'.[95] Hierbij kan bijvoorbeeld gedacht worden aan het breken van het touwtje als er aan getrokken zou worden. Een nog objectievere benadering lijkt nauwelijks mogelijk en hiermee werd het gebied tussen strafbare uitvoering en straffeloze uitvoering wel erg klein.

Dit duurde tot het Poging tot gasmoordarrest.[96] Hierbij was door een vrouw en haar buitenechtelijke vriend het plan opgevat om de man van de vrouw te vermoorden in twee fasen: eerst zou de vriend de man in zijn slaap met een hamer op het hoofd bewusteloos slaan en vervolgens zou de man met zijn hoofd in een gasoven worden gelegd en de gaskraan worden opengedraaid zodat hij door verstikking om het leven zou komen. Het pakte echter anders uit doordat de man zich in zijn slaap omdraaide op het moment dat de vriend met de hamer sloeg en de slag afschampte zodat hij wakker werd waardoor het plan niet tot uitvoering kwam. Indien de Hoge Raad net zo extreem zou hebben geoordeeld als in het Eindhovense brandstichtingarrest, dan zou wellicht nog niet tot strafbare poging zijn geconcludeerd omdat de realisering van het plan in de eerste fase was blijven steken. Het verschil tussen de eerste fase van het Eindhovense brandstichtingarrest (het brandklaar maken van het huis) en die van de Poging tot het gasmoordarrest (het bewusteloos slaan van de echtgenoot) was gelegen in het feit dat de eerste fase van de brandstichting op zichzelf nog geen strafbaar feit opleverde in tegenstelling tot de eerste fase van de moord. Daarin was op zijn minst sprake van zware mishandeling. De Hoge Raad was dan ook van mening dat er een begin van uitvoering van het misdrijf als geheel kon worden aangenomen, en dus met het voorgenomen in twee fasen aantasten van het slachtoffer, doordat de dader een begin had gemaakt met de eerste fase.
Uit de literatuur en rechtspraak met betrekking tot het onderscheid 'voorbereidingshandeling – uitvoeringshandeling' kan worden geconcludeerd dat er van een duidelijke en eenvormige opvatting geen sprake is. Uit de literatuur spreekt verdeeldheid: van uiterst 'objectieve' tot uiterst 'subjectieve' leren met alle tussenliggende varianten. De rechtspraak is ook niet eenduidig: van 'objectieve' uitspraken als HR 19 maart 1934, NJ 1934, 450 'Eindhovense brandstichtingarrest' tot meer subjectieve uitspraken als HR 19 november 1917, NJ 1918, 11 (het vastbinden van een uit te voeren koe aan een boom nabij de grens is een uitvoeringshandeling).[97]

94 HR 19 maart 1934, NJ 1934, 450, Eindhovense brandstichting
95 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 314
96 HR 29 mei 1951, NJ 1951, 480, Poging tot gasmoord
97 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 553

Inmiddels is de Hoge Raad overgegaan tot het gebruik van een ander criterium, te weten dat van de uiterlijke verschijningsvorm van de uitvoeringshandeling. Het criterium van de uiterlijke verschijningsvorm is in wezen gerelateerd aan de indruk die een goede waarnemer, die de gemiddelde burger geacht wordt te zijn, ter plaatse zou hebben gekregen omtrent de verwerkelijking van een bepaald misdrijf.[98] Gedragingen zijn als een begin van uitvoering van het voorgenomen misdrijf aan te merken als zij naar haar uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf. Dit criterium werd voor het eerst gebruikt in het Cito-arrest.[99] Hierbij was sprake van twee gedeeltelijk gemaskerde mannen die aanbelden met schietklare vuurwapens en een lege weekendtas in de hand bij het uitzendbureau Cito te Amsterdam vlak nadat daar een grote hoeveelheid contant geld was gebracht door een geldauto ten behoeve van de wekelijkse uitbetaling. Na het aanbellen werd de deur echter niet opgedaan maar werden de mannen door gewaarschuwde politiemannen overmeesterd. De Hoge Raad was hier de indruk toegedaan dat een begin was gemaakt met de uitvoering van de voorgenomen overval daar deze gedragingen 'naar hun uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf'.
In een daaropvolgende zaak, het Grenswisselkantoorarrest[100], werd het criterium van de uiterlijke verschijningsvorm zoals gehanteerd in het Cito-arrest weer sterk in objectieve sfeer toegepast. Twee mannen waren na een langdurige voorbereiding 's-ochtends voor het openingsuur van het grenswisselkantoor in een gestolen auto die was voorzien van valse kentekenplaten, nabij dat grenswisselkantoor op een parkeerplaats gaan staan. Terwijl zij de motor lieten draaien wachtten zij met een pruik op het hoofd de komst van de bankemployé af om deze bij het openen van het kantoor te grijpen. In hun auto hadden zij een dubbelloops jachtgeweer liggen en een imitatie vuistvuurwapen evenals handboeien, touw en tape om de bankemployé te knevelen. Toen deze arriveerde kreeg hij echter argwaan omdat hij de auto al een dag eerder had zien staan en waarschuwde de politie in plaats van het kantoor te openen. Toen de politie bij het grenswisselkantoor aankwam sloegen de mannen op de vlucht en na een achtervolging werden de mannen tot stoppen gedwongen. De Hoge Raad achtte echter nog geen begin van uitvoering aanwezig, als iemand, die het voornemen heeft opgevat in een bank het misdrijf van art. 317 WvSr (afpersing) te plegen, zich met een auto naar die bank heeft begeven 'doch – om welke reden dan ook – die auto niet heeft verlaten, noch – in of vanuit die auto – een gedraging heeft verricht welke naar haar uiterlijke verschijningsvorm moet worden beschouwd als te zijn gericht op de voltooiing van dat voorgenomen misdrijf'. Dit criterium bestrijkt zowel de kwestie 'uitvoeringshandeling – voorbereidingshandeling' als de kwestie van het 'openbaren' en brengt beide kwesties met elkaar in verband.[101]

Samenvattend kan worden gesteld dat, laverend tussen subjectieve theorieën, waarbij de relatie met de delictsomschrijving van het gronddelict kan dreigen verloren te gaan en objectieve theorieën, waarbij soms de strafbare poging dreigt te worden beperkt tot het enge stadium waarin de vervulling

98 Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 316
99 HR 24 oktober 1978, NJ 1979, 52, Uitzendbureau Cito
100 HR 8 september 1987, NJ 1988, 612, Grenswisselkantoor
101 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 553

van de gehele delictsomschrijving voor de dader zelf onherroepelijk is geworden, heeft de Hoge Raad in de loop van zijn rechtspraak over het algemeen een gematigd objectief standpunt ingenomen. In de huidige rechtspraak van de Hoge Raad wordt herhaaldelijk de formulering gebezigd, dat de gedragingen zijn aan te merken als uitvoeringshandelingen indien zij naar hun uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf.[102]

Begin van uitvoering in relatie tot port scanning

Zowel de Wet Computercriminaliteit II als het Cyber Crime Verdrag besteedt geen aandacht aan de port scan. In het rapport 'Handleiding Cyber Crime, Van herkenning tot aangifte' van het Govcert.nl (/KLPD)[103] wordt gesteld dat een port scan doorgaans niet met behulp van speciale programmatuur wordt uitgevoerd en dat het daardoor lastig is om het nieuwe artikel 139d, lid 2 WvSr (voorbereidingshandelingen) van toepassing te verklaren. Gezien het bovenstaande lijkt mij deze conclusie te voorbarig aangezien er naast Nmap nog vele andere goede en speciale port scanners bestaan en deze allen met het specifieke doel kunnen worden ingezet om de poorten van een systeem te scannen.[104]

In artikel 139d WvSr is de voorbereidingshandeling – het plaatsen van aftap- en afluisterapparatuur – strafbaar gesteld. In de Wet Computercriminaliteit II is in het eerste lid van art. 139d WvSr de strafmaat voor deze specifieke voorbereidingshandeling verhoogd van ten hoogste een half jaar naar een jaar. Daarnaast wordt in lijn met art. 6 van het Cyber Crime Verdrag een nieuw tweede en derde lid bij art. 139d WvSr voorgesteld. Deze luiden:

2. Met dezelfde straf wordt gestraft hij die, met het oogmerk dat daarmee een misdrijf als bedoeld in artikel 138a, eerste lid, 138b of 139c wordt gepleegd,
a. een technisch hulpmiddel dat hoofdzakelijk geschikt gemaakt of ontworpen is tot het plegen van een zodanig misdrijf, vervaardigt, verkoopt, verwerft, invoert, verspreidt of anderszins ter beschikking stelt of voorhanden heeft, of
b. een computerwachtwoord, toegangscode of daarmee vergelijkbaar gegeven waardoor toegang kan worden verkregen tot een geautomatiseerd werk of een deel daarvan, verkoopt, verwerft, verspreidt of anderszins ter beschikking stelt of voorhanden heeft.
3. Met gevangenisstraf van vier jaren of geldboete van de vierde categorie wordt gestraft hij die het in het tweede lid bedoelde feit pleegt indien zijn oogmerk gericht is op een misdrijf als bedoeld in artikel 138a, tweede of derde lid.

Deze leden bieden verruimde mogelijkheden voor strafbaarheid van bepaalde voorbereidingshandelingen. Daarbij gaat het om voorbereidingshandelingen met betrekking tot art. 138a, eerste lid WvSr, het nieuw voorgestelde art. 138b WvSr en art. 139c WvSr. Met het 'oogmerk' wordt niet het doel van handelen als omschreven in dit artikel maar het begaan van een misdrijf bedoeld in de artikelen 138a, eerste lid WvSr, 138b WvSr of 139c WvSr, aangewezen.

---

102 Ibid, p. 558

103 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 95

104 Enkele voorbeelden van andere goede port scanners zijn: NetScanToolsPro (http://www.netscantools.com), Superscan (http://www.foundstone.com) en Netcat (http://www.atstake.com/research/tools/network_utilities)

Het oogmerk is in dit artikel een belangrijk onderscheidend criterium om te bepalen of er sprake is van een strafbare voorbereidingshandeling. Het oogmerk om te hacken houdt bijvoorbeeld in dat iemand ook het doel heeft om het strafbare feit te plegen. Het beroepsmatig gebruikmaken van technische hulpmiddelen, door bijvoorbeeld informatiebeveiligers of systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, betekent niet direct dat er sprake is van een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. De toevoeging van het voorgestelde tweede en derde lid hebben betrekking op de strafbaarstelling van het in bezit hebben of de voorbereidingshandelingen op zich. Dit houdt in dat, anders dan in het huidige recht het geval is, ook in het geval het hoofddelict niet volgt, een aantal specifieke voorbereidinghandelingen toch strafbaar wordt gesteld. Zowel het in bezit hebben als het verspreiden wordt strafbaar gesteld. Het voordeel van de strafbaarstelling van deze specifieke voorbereidingshandelingen is dat niet aan de zware eis van de algemene voorbereidingsbepaling van art. 46 WvSr hoeft te worden voldaan.

Het zal duidelijk zijn dat deze strafbaarstelling van voorbereidingshandelingen met betrekking tot deze delicten een breuk met de traditie van de objectieve pogingsleer betekent, aangezien deze leer uitgaat van het objectieve gevaar van de daad voor de rechtsorde en pas als uitvoeringshandeling toelaat datgene wat als daadwerkelijke uitvoering van het misdrijf zelf en dus als objectieve inbreuk op de rechtsorde is te beschouwen. Gezien de vage omschrijving van wat strafbare voorbereiding is, zal al snel aan het vereiste niveau van verdenking zijn voldaan.[105]
Vanwege de delictsomschrijving in art. 139d WvSr is de cruciale vraag of een port scanner een technisch hulpmiddel is dat hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van een zodanig misdrijf als bedoeld in art. 138a, eerste lid, 138b of 139c WvSr. Zoals gezegd is het beroepsmatig voorhanden hebben van technische hulpmiddelen door systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, niet meteen een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. Het is mijns inziens niet onredelijk om ook voor art. 139d WvSr de eis van kennelijke bestemming, die bij art. 46 WvSr gehanteerd wordt, te gebruiken. Aan deze term moet een objectieve, beperkte strekking worden toegekend. De gemiddelde rechtsgenoot moet uit de combinatie van zaken overduidelijk kunnen afleiden dat er een crimineel doel is.[106] In dit geval kan uit het slechts voorhanden hebben van een port scanner niet direct worden afgeleid dat deze een crimineel doel dient / zal dienen. Hierin is zo veel onzekerheid gelegen dat deze in het belang van de rechtszekerheid straffeloos dienen te blijven.

Volgens de MvT wordt poging gestraft ‘om den misdadigen wil, het opzet des daders te treffen, zoodra deze eene zoo gevaarlijke rigting heeft aangenomen, dat daarvan objectief blijkt door het begin van

105 . Kelk geeft hiervoor het volgende voorbeeld: wie een stalen T-balk in zijn schuur heeft liggen, stelt zichzelf bloot aan de kans afgeluisterd te worden, aangezien zo’n balk als stormram op een auto *kan* worden gemonteerd, waarmee vervolgens een pui *kan* worden geforceerd in: C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 333; met de aantekening dat het voorbeeld van Kelk een artikel 46 WvSr-voorbereidingshandeling betreft in tegenstelling tot de specifieke strafbaarstelling van voorbereiding in artikel 139d, lid 2 WvSr.

106 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 327

uitvoering van een bepaald misdrijf'.[107] In de literatuur zijn met betrekking tot de vraag wanneer sprake is van een begin van uitvoering twee opvattingen ontwikkeld. In de subjectieve leer zou als uitgangspunt de kenbare misdadige gezindheid van de hacker worden genomen. De objectieve gevaarlijkheid van de daad is in beginsel van geen belang. De objectieve leer is echter de leer die in ons land door de Hoge Raad wordt gehuldigd. Deze leer gaat uit van het objectieve gevaar van de daad voor de rechtsorde en laat pas als uitvoeringshandeling toe datgene wat als daadwerkelijke uitvoering van het misdrijf zelf en dus als objectieve inbreuk op de rechtsorde is te beschouwen.

Artikel 138a, eerste lid WvSr betreft een formeel delict, een delict waarbij sprake is van een duidelijk getypeerde delictshandeling. Dit in tegenstelling tot een materieel omschreven delict dat in de eerste plaats wordt getypeerd door een bepaald ongewenst gevolg. In art. 138a, eerste lid WvSr is duidelijk omschreven aan welke handelingen een persoon dient te voldoen voordat er sprake is van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem. Bij formeel geformuleerde delicten (gedragsdelicten) is er begin van uitvoering als de dader begonnen is met de in de delictsomschrijving neergelegde handeling. De objectieve leer laat pas als uitvoeringshandeling toe datgene wat als daadwerkelijke uitvoering van het misdrijf zelf en dus als objectieve inbreuk op de rechtsorde is te beschouwen. Aangezien art. 138a, eerste lid WvSr een formeel delict is en de hacker met een port scan, zelfs met een van de in de vorige paragraaf genoemde typen port scans, nog niet is begonnen met de handelingen zoals omschreven in art. 138a, eerste lid WvSr is hij volgens de objectieve leer niet strafbaar want hij dringt nog niet opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen door middel van het doorbreken van een beveiliging ofwel door een technische ingreep dan wel met behulp van valse signalen of een valse sleutel of door het aannemen van een valse hoedanigheid.

Volgens de subjectieve leer, die de gevaarlijke gezindheid van de dader centraal stelt en als uitvoeringshandeling beschouwt datgene wat als uitvoering van deze gezindheid is op te vatten, zou een hacker die een port scan uitvoert strafbaar zijn. De objectieve gevaarlijkheid van de daad is hierbij in beginsel van geen belang. De port scan wordt door deze leer gezien als uitvoering van zijn gevaarlijke gezindheid, namelijk het voornemen om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen. Door de aandacht vooral te richten op de misdadige bedoeling en de indruk die dat maakt op het rechtsgevoel wordt de strafbaarheid vergaand tot de voorbereidingsfase uitgerekt. Dit zou dan ook betekenen dat een scriptkiddie die een port scan uitvoert binnen de subjectieve leer strafbaar zou zijn hetgeen mijns inziens als onwenselijk moet worden beschouwd gezien het feit dat deze met de resultaten van de port scan, vanwege zijn ontoereikende kennis, daarna nooit daadwerkelijk opzettelijk en wederrechtelijk het gescande geautomatiseerde systeem zou kunnen binnendringen.

Als het uitvoeren van specifieke typen port scans op een geautomatiseerd systeem niet als uitvoeringshandeling valt te kwalificeren binnen de objectieve leer en daardoor niet strafbaar is, hoe zit

107 Ibid, p. 319

het dan met de uiterlijke verschijningsvorm hiervan in geval van een aantal doelgerichte 'sneaky' port scans met decoys op poorten waar services op draaien met net bekend geworden beveiligingslekken over een bepaalde periode waarin de kans op ontdekking kleiner is, bijvoorbeeld 's-nachts als er geen systeembeheerder aanwezig is? Zijn deze handelingen wellicht aan te merken als een begin van uitvoering van het voorgenomen misdrijf, daar zij naar haar uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf?
In het Cito-arrest[108] is bepaald dat gedragingen als een begin van uitvoering van het voorgenomen misdrijf aan te merken zijn als zij naar haar uiterlijke verschijningsvorm moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf. Dit criterium bestrijkt zowel de kwestie 'uitvoeringshandeling – voorbereidingshandeling' als de kwestie van het 'openbaren' en brengt beide kwesties met elkaar in verband.[109]
De feiten op basis waarvan de vragen naar uitvoerings- of voorbereidingshandelingen en het al dan niet geopenbaard zijn van het voornemen tot het opzettelijke en wederrechtelijk binnendringen in een geautomatiseerd systeem middels een port scan moeten worden beantwoord, laten zich ten aanzien van een port scan zoals hierboven omschreven, als volgt omschrijven:

1. De hacker zal de beschikking moeten verkrijgen over een port scanner om te kunnen scannen naar online systemen;
2. Vervolgens zal hij een directe verbinding moeten maken met een van de ontdekte doelsystemen door een port scan uit te voeren op dit doelsysteem;
3. Het uitvoeren van een 'sneaky' port scan met decoys op dit ontdekte doelsysteem waarvan hij door de eerste port scan inmiddels weet welke poorten er luisteren naar inkomende verbindingen en hierbij de optie meegeven om het OS te bepalen en bij de output van de port scan de optie meegeven om zo veel mogelijk informatie te verkrijgen om de versies van de services te bepalen;
4. Daarna moet de hacker de optie meegeven specifiek te scannen op díe luisterende poorten waarvan hij inmiddels weet dat er services op draaien die een verouderde versie betreffen en waarvan bekend is geworden dat er beveiligingslekken ten aanzien van die versies zijn ontdekt;
5. De hacker zal de port scan moeten uitvoeren op tijdstippen dat het risico op ontdekking zo klein mogelijk is, bijvoorbeeld 's-nachts als er weinig of geen systeembeheerders aanwezig zijn of de port scan over een lange tijd uitvoeren zodat de port scan geen argwaan wekt.

Op grond van bovenstaande feiten / handelingen zijn naar mijn mening als voorbereidingshandelingen voor een voorgenomen opzettelijke en wederrechtelijke inbraak in een geautomatiseerd systeem te noemen:

108 HR 24 oktober 1978, NJ 1979, 52, Uitzendbureau Cito

109 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 553

1. Het verkrijgen van de beschikking over een port scanner om te kunnen scannen naar online systemen en
2. Het maken van een directe verbinding met een van de ontdekte doelsystemen door een port scan uit te voeren op dit doelsysteem.

Deze voorfase van voorbereidingshandelingen, die wel reeds een bepaald voornemen zouden kunnen verraden, maar daarnaast nog zo veel onzekerheid herbergen omtrent de daadwerkelijke intentie van een hacker dienen in het belang van de rechtszekerheid straffeloos te blijven. Dergelijke port scans worden ook uitgevoerd door nieuwsgierige scriptkiddies die niet de kennis hebben om met de resultaten verdere uitvoeringshandelingen te plegen.
Indien echter de eerste port scan wordt gevolgd door de hieropvolgende fasen waarbij:

1. Sneaky port scans met decoys door de hacker worden uitgevoerd op dit ontdekte doelsysteem waarvan hij inmiddels door de eerste scan weet welke poorten er luisteren naar inkomende verbindingen en hierbij door de hacker de optie meegegeven wordt om het OS te bepalen en bij de output van de port scan de optie meegegeven wordt om zo veel mogelijk informatie te verkrijgen om de versies van de services te bepalen en
2. Daarna door de hacker de optie meegegeven wordt specifiek te scannen op díe luisterende poorten waarvan hij inmiddels weet dat er services op draaien die een verouderde versie betreffen en waarvan bekend is geworden dat er beveiligingslekken ten aanzien van die versies zijn ontdekt en
3. De port scan door de hacker wordt uitgevoerd op tijdstippen dat het risico op ontdekking zo klein mogelijk is, bijvoorbeeld ’s-nachts als er weinig of geen systeembeheerders aanwezig zijn of de port scan over een lange tijd uitgevoerd wordt zodat de port scan geen argwaan wekt,

zijn deze naar mijn mening, gezien de uiterlijke verschijningsvorm waaruit de intentie van de hacker blijkt, zeker als uitvoeringshandelingen te kwalificeren.

Het criterium van de uiterlijke verschijningsvorm is in wezen gerelateerd aan de indruk die een goede waarnemer, die de gemiddelde burger geacht wordt te zijn, ter plaatse zou hebben gekregen omtrent de verwerkelijking van een bepaald misdrijf. De uiterlijke verschijningsvorm van een dergelijke port scan is echter dermate gecompliceerd dat een goede analyse alleen door systeembeheerders kan worden uitgevoerd en niet door een gemiddelde burger kan worden beoordeeld. De beoordeling van de feiten en het juridisch kwalificeren ervan vindt echter niet in het luchtledige plaats, maar geschiedt vanuit opvattingen die men heeft over het ‘behoren’. In casu gaat het daarbij om opvattingen aangaande de vraag of bepaalde gedragingen straffeloos mogen blijven. Die vraag kan natuurlijk

slechts aan de orde komen voor zover wettelijke bepalingen ruimte laten voor dergelijke normatieve oordelen. De bepalingen met betrekking tot de poging laten een dergelijke ruimte.[110]

Als bovenstaande laatste drie fasen zich voltrekken, blijkt hieruit naar mijn mening daadwerkelijk de bedoeling tot het uitvoeren van een opzettelijke en wederrechtelijke inbraak in een geautomatiseerd systeem. Dan pas zijn er gedragingen die rechtstreeks zijn gericht op de voltooiing van het misdrijf en is er een begin van uitvoering en dient dat niet straffeloos te blijven. Het lijkt ook niet in strijd met, integendeel in de lijn van de opvattingen van de Hoge Raad, om de rek die in de bepaling van art. 45 WvSr met betrekking tot het begin van uitvoering ongetwijfeld aanwezig is, te gebruiken om te voorkomen dat iemand straffeloos blijft van wie door zijn daden ondubbelzinnig vaststaat, dat hij, als het van hem had afgehangen, het misdrijf zou hebben voltooid.[111]

De tweede vraag die beantwoord moet worden is: heeft het voornemen van de hacker zich geopenbaard? Zoals reeds vermeld kan een port scan opgemerkt worden door een analyse van de log-files die in een router, firewall of IDS worden opgeslagen. Uit die uiterlijke verschijningsvorm (de log-files die de port scan hebben opgeslagen) moet dan wel af te leiden zijn dat de gedraging, de port scan, moet worden beschouwd als te zijn gericht op de voltooiing van het misdrijf, het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem.
Als een handeling van een hacker na analyse van de log-files door een systeembeheerder als verdacht wordt ervaren, dan is die handeling blijkbaar geschikt om een verdenking op te wekken. Anders gezegd: de uiterlijke verschijningsvorm van zo een handeling is blijkbaar dusdanig dat zij is te beschouwen als te zijn gericht op de voltooiing van het misdrijf. Als vervolgens zou blijken dat de handeling (die door de systeembeheerder conform het bovenstaande terecht als ‘verdacht’ werd ingeschat) om ‘onschuldige redenen’ is verricht, houdt dat niet in dat er aan de uiterlijke verschijningsvorm van de handeling (en daarmee aan het openbaren) iets mankeert, waardoor er geen sprake zou kunnen zijn van poging tot een misdrijf. Neen, dan mankeert er integendeel iets aan het innerlijk, echter niet van de handeling, maar van de hacker die de handeling stelde. Het ontbreekt de steller van de handeling, de hacker, in zo een geval aan het voornemen om een misdrijf te plegen en daarom is er geen sprake van een poging tot misdrijf.[112]
In casu is het voornemen om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen naar mijn mening naar zijn uiterlijke verschijningsvorm niet kwestieus. Blijft de vraag of in het bovenstaande geval de uiterlijke verschijningsvorm van de handelingen van de hacker dusdanig zijn dat zij moeten worden beschouwd als te zijn gericht op de voltooiing van het misdrijf en derhalve of er sprake is van openbaren van het voornemen. In de visie van de Hoge Raad bij het Grenswisselkantoor-arrest[113] is hierbij de toetssteen: moet het onbegrijpelijk worden geacht als een waarnemer (in casu een systeembeheerder) de gedraging beschouwt als te zijn gericht op de

110 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 554

111 Ibid, p. 555

112 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 556

113 HR 8 september 1987, NJ 1988, 612, Grenswisselkantoor

voltooiing van een misdrijf? Hoewel een dergelijke beoordeling op zich weer een subjectieve inschatting van een systeembeheerder impliceert, concludeer ik dat het niet onbegrijpelijk zou zijn als een systeembeheerder de laatste drie uitvoeringshandelingen van een hacker als verdacht inschat en dat de openbaring van deze uitvoeringshandelingen naar hun uiterlijke verschijningsvorm kunnen worden beschouwd als te zijn gericht op voltooiing van het misdrijf.

De belangrijke beperking die aan de reikwijdte van het Cito-criterium van de uiterlijke verschijningsvorm is gegeven door de Hoge Raad in het Grenswisselkantoor-arrest, doet zich naar mijn mening ook ten aanzien van de port scan voor. De Hoge Raad achtte hier nog geen begin van uitvoering aanwezig, als iemand, die het voornemen heeft opgevat in een bank het misdrijf van art. 317 WvSr (afpersing) te plegen, zich met een auto naar die bank heeft begeven 'doch – om welke reden dan ook – die auto niet heeft verlaten, noch – in of vanuit die auto – een gedraging heeft verricht welke naar haar uiterlijke verschijningsvorm moet worden beschouwd als te zijn gericht op de voltooiing van dat voorgenomen misdrijf'. Wat deze twee arresten, in onderling verband beschouwd, nu precies betekenen voor een port scan is niet duidelijk. Het criterium van de uiterlijke verschijningsvorm biedt weinig houvast. Per delict zal moeten worden vastgesteld wat de karakteristieke handelingen zijn die voldoende zijn voor een begin van uitvoering.[114] Indien een hacker slechts de eerste twee handelingen verricht (het verkrijgen van de beschikking over een port scanner en het maken van een directe verbinding met een van de ontdekte doelsystemen door het uitvoeren van een port scan) kunnen deze naar mijn mening naar hun uiterlijke verschijningsvorm ook niet worden beschouwd als te zijn gericht op de voltooiing van dat voorgenomen misdrijf. Om een vergelijking met het Grenswisselkantoor-arrest te maken: de hacker heeft de auto erheen gereden maar deze nog niet verlaten. Slechts de drie daarop volgende uitvoeringshandelingen zijn mijns inziens naar hun uiterlijke verschijningsvorm te kwalificeren als karakteristieke handelingen om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen en als zodanig te zijn gericht op de voltooiing van het misdrijf.

4.2.5 Vrijwillige terugtred

Vrijwillige terugtred is uitsluitend relevant als aan de ene kant de uitvoeringsfase is begonnen en aan de andere kant het misdrijf nog kan worden voltooid. Is dit laatste onmogelijk geworden dan kan de vrijwillige terugtred niet meer aan de orde komen. Omdat het delict dan niet wordt voltooid, blijft het echter onzeker of de dader – ook als er niets was misgegaan buiten zijn invloedssfeer – het delict wel zou hebben voltooid en niet in een later stadium zelf tot inkeer zou zijn gekomen. In art. 46b WvSr wordt daarom met zoveel woorden van de verdachte zelf gevergd dat hij aannemelijk maakt dat de uitvoering niet is voltooid ten gevolge van omstandigheden van zijn wil afhankelijk.[115] Voor een goed begrip moet erop worden gewezen dat deze uitsluitingsgrond pas 'geactiveerd' kan worden als er bij poging een begin van uitvoering en bij voorbereiding inderdaad sprake van voorbereiding is. Als iemand ophoudt met zijn misdadige plan in de voorbereidingsfase bij poging, dan is hij straffeloos

114 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 322
115 Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 319

omdat er nog geen begin van uitvoering is. Ziet hij van zijn plannen af zonder aan voorbereiding te zijn toegekomen, dan geldt art. 46b WvSr evenmin. Wil vrijwillig terugtreden dus in aanmerking komen dan moet er een begin van uitvoering (art. 45 WvSr) of voorbereiding (art. 46 WvSr) zijn. In verband met het vrijwillig terugtreden is het onderscheid tussen de voltooide poging en onvoltooide poging van groot belang. Dit ligt voor de hand als men bedenkt dat van een voltooide poging sprake is als de dader alles gedaan heeft dat in zijn vermogen ligt zonder dat het gewenste resultaat is bereikt. Er is dan geen plaats meer voor vrijwillige terugtred. Voor vrijwillig terugtreden is, zolang het maar om een 'cause interne' gaat, het motief niet relevant. Het mag heel edel zijn maar het kan ook de angst voor ontdekking of angst voor straf zijn.[116]
Voldoende voor vrijwillige terugtred is dat de dader op grond van zijn autonome wil heeft meegewerkt aan de niet voltooiing van het misdrijf. Er kan dus ook sprake zijn van een combinatie van vrijwillige en onvrijwillige factoren die tot straffeloosheid leidt. De dader moet hoe dan ook een actief aandeel hebben gehad in de verhindering van het misdrijf dat hij tevoren nastreefde. In ieder geval is het duidelijk dat als de dader eenmaal door de politie is betrapt, het niet meer mogelijk zal zijn om vrijwillig terug te treden. Een autonome wil zal evenmin worden aangenomen als iemand zijn handelingen staakt uit vrees voor ontdekking mits bij voortzetting van de uitvoering ontdekking waarschijnlijk is.[117]
Beslissend voor een vrijwillige terugtred is dus de vraag of deze het gevolg is geweest van een spontane besluitvorming en niet plaatsvond uitsluitend onder invloed van uitwendige prikkels waarbij – volgens sommige schrijvers – zelfs aan een vermeende betrapping moet worden gedacht.

Vrijwillige terugtred in relatie tot port scanning
Het onderscheid tussen de voltooide en onvoltooide poging is, in verband met het vrijwillig terugtreden, van groot belang. Bij een voltooide poging tot het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem kan men denken aan de situatie dat een hacker alle poorten gescand heeft en daarna gecontroleerd heeft of er op een doelsysteem onbeveiligde poorten open staan die services draaien met bekende beveiligingslekken maar daarbij tot de ontdekking komt dat het systeem te goed beveiligd is om hem relevante informatie te verschaffen voor een te ondernemen inbraak in het systeem en daarom zijn aanval afbreekt. Voor een onvoltooide poging kan bijvoorbeeld de volgende situatie worden geschetst: een hacker merkt tijdens een port scan dat een systeembeheerder zijn port scan ontdekt en verbreekt, uit vrees voor ontdekking, de verbinding tussen zijn computer en het doelsysteem. De hacker kan de uitvoering van het misdrijf dan niet meer voltooien al zou hij het nog zo graag willen.

In het eerste geval van de voltooide poging kan niet gesproken worden van vrijwillige terugtred. De poging tot het binnendringen in het geautomatiseerde systeem wordt om externe redenen afgebroken. De vrijwillige terugtred is niet het gevolg van een spontane beslissing van de hacker maar vanwege uitwendige prikkels die het hem onmogelijk maken het doelsysteem verder te verkennen. Ook in het tweede geval, de onvoltooide poging, zal geen sprake zijn van vrijwillige terugtred aangezien er geen

116 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, pp. 334 - 335
117 C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001, p. 320

autonome wil zal worden aangenomen als de hacker zijn poging staakt uit vrees voor ontdekking mits bij voortzetting van de uitvoering ontdekking waarschijnlijk is.

4.3 Samenvatting en conclusie

Een van de moeilijkste problemen van strategische en ethische aard is om te bepalen op welk moment er ingegrepen dient te worden bij misdrijven als een voorgenomen inbraak in een geautomatiseerd systeem. Naarmate men de risico's verkleint door in een vroeg stadium actie te ondernemen, neemt in het schemerige grensgebied tussen voorbereidings- en uitvoeringshandelingen de mogelijkheid toe dat de strafrechter later zal oordelen dat er geen begin van uitvoering is geweest en dus zelfs geen strafbare poging is geweest.

De voorwaarden voor strafbaarheid van de poging, te weten dat er een voornemen van de dader moet zijn, wat moet blijken uit een begin van uitvoering, kunnen worden onderkend door een aantal opties die aan een port scanner zoals Nmap kunnen worden meegegeven en in een router, een firewall of een Intrusion Detection System (IDS) gelogd kunnen worden. In Nmap kunnen door een hacker opties meegegeven worden voor een bepaald type port scan: de specifieke port scan gericht op bepaalde poorten om te bepalen of er verouderde versies op draaien die gevoelig zijn voor exploits, de 'sneaky' scan om routers, firewalls of IDS's te omzeilen en fragmented packet scans, decoy scans en spoofed source address scans om de herkomst van de port scan zo veel mogelijk te verbergen. Het voornemen van een hacker tot het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem kan zich openbaren door een begin van uitvoering van een port scan indien, en slechts indien, die voldoet aan een van de hierboven genoemde scantypes.

Van voornemen wordt echter slechts gesproken in geval van situaties die niet tot een voltooid misdrijf hebben geleid, zodat het veel moeilijker is om het bewuste willen en weten te reconstrueren. In het geval van een poging tot inbraak in een geautomatiseerd systeem kan men zich de vraag stellen of de hacker met deze port scan het voornemen had om een geslaagde poging tot inbraak in een geautomatiseerd systeem te plegen. Indien men uitgaat van een normatief opzet-begrip zoals door de Hoge Raad gehanteerd in het Inrijden op agent-arrest[118] dan kan een en ander een anticipatie op een bepaald te verwachten causaal verloop betekenen op basis van een normatieve interpretatie van een bepaald specifiek type port scan door de hacker: gezien de omstandigheden worden, naar de ervaring leert, door een specifiek type port scan de kwetsbare plekken in een geautomatiseerd systeem onthuld en kan mijns inziens aan de handeling (de specifieke port scan gericht op bepaalde poorten om te bepalen of er verouderde versies op draaien die gevoelig zijn voor exploits, de 'sneaky' scan om routers, firewalls of IDS's te omzeilen en fragmented packet scans, decoy scans en spoofed source address scans om de herkomst van de port scan zo veel mogelijk te verbergen) qua teneur tevens de intentionaliteit ten aanzien van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem worden gezien.

118 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent

Dergelijke port scans kunnen echter pas uitgevoerd worden als de hacker ervoor zorgt dat hij de beschikking verkrijgt over een port scanner om te kunnen scannen naar online systemen en vervolgens ook een directe verbinding maakt met het doelsysteem door een port scan uit te voeren op dit doelsysteem. Deze fase van voorbereidingshandelingen, die wel reeds een bepaald voornemen zouden kunnen verraden, maar daarnaast nog zo veel onzekerheid herbergen omtrent de daadwerkelijke intentie van een hacker dienen in het belang van de rechtszekerheid straffeloos te blijven. Indien echter de eerste port scan wordt gevolgd door de hieropvolgende fasen waarbij:

1. Sneaky port scans met decoys door de hacker worden uitgevoerd op dit ontdekte doelsysteem waarvan hij inmiddels door de eerste scan weet welke poorten er luisteren naar inkomende verbindingen en hierbij door de hacker de optie meegegeven wordt om het OS te bepalen en bij de output van de port scan de optie meegegeven wordt om zo veel mogelijk informatie te verkrijgen om de versies van de services te bepalen en
2. Daarna door de hacker de optie meegegeven wordt specifiek te scannen op díe luisterende poorten waarvan hij inmiddels weet dat er services op draaien die een verouderde versie betreffen en waarvan bekend is geworden dat er beveiligingslekken ten aanzien van die versies zijn ontdekt en
3. De port scan door de hacker wordt uitgevoerd op tijdstippen dat het risico op ontdekking zo klein mogelijk is, bijvoorbeeld ’s-nachts als er weinig of geen systeembeheerders aanwezig zijn of de port scan over een lange tijd uitgevoerd wordt zodat de port scan geen argwaan wekt,

zijn deze naar mijn mening, gezien de uiterlijke verschijningsvorm waaruit de intentie van de hacker blijkt, zeker als uitvoeringshandelingen te kwalificeren.

Indien een hacker slechts de eerste twee handelingen verricht (het verkrijgen van de beschikking over een port scanner en het maken van een directe verbinding met een van de ontdekte doelsystemen door het uitvoeren van een port scan) kunnen deze naar hun uiterlijke verschijningsvorm ook niet worden beschouwd als te zijn gericht op de voltooiing van dat voorgenomen misdrijf. Slechts de drie daarop volgende uitvoeringshandelingen zijn mijns inziens naar hun uiterlijke verschijningsvorm te kwalificeren als karakteristieke handelingen om opzettelijk en wederrechtelijk een geautomatiseerd systeem binnen te dringen en als zodanig te zijn gericht op de voltooiing van het misdrijf.

De nieuw toegevoegde leden twee en drie aan artikel 139d WvSr bieden verruimde mogelijkheden voor strafbaarheid van bepaalde voorbereidingshandelingen. Vanwege de delictsomschrijving in art. 139d WvSr is de cruciale vraag of een port scanner een technisch hulpmiddel is dat hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van een zodanig misdrijf als bedoeld in art. 138a, eerste lid, 138b of 139c WvSr. Het beroepsmatig voorhanden hebben van technische hulpmiddelen door systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet,

betreft niet meteen een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. Aan de eis van kennelijke bestemming, die bij art. 46 WvSr gehanteerd wordt, te gebruiken moet een objectieve, beperkte strekking worden toegekend. De gemiddelde rechtsgenoot moet uit de combinatie van zaken overduidelijk kunnen afleiden dat er een crimineel doel is.[119] In dit geval kan uit het slechts voorhanden hebben van een port scanner niet direct worden afgeleid dat deze een crimineel doel dient / zal dienen. Hierin is zo veel onzekerheid gelegen dat deze in het belang van de rechtszekerheid straffeloos dienen te blijven.

119 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 327

5 Conclusies en aanbevelingen

5.1 Conclusies

Een port scanner is een van de meest gebruikte tools van de tegenwoordige hacker. Waarom dit zo is heb ik met het voorgaande willen verduidelijken: port scanners detecteren automatisch de kwetsbaarheden van een doelsysteem of netwerk, ze zijn snel, veelzijdig en betrouwbaar. Nog belangrijker is dat ze gratis verkrijgbaar zijn op het internet. Port scanners worden daarom op dit moment door vele hackers en ICT-security professionals gezien als de meest gevaarlijke tool in de gereedschapskist van een hacker.[120] McClure, Scambray en Kurtz[121] vergelijken de port scan met het op alle muren kloppen om alle deuren en ramen te vinden die open staan. De voorgaande hoofdstukken overziend, kom ik tot de conclusie dat een port scanner niet alleen een tool is waarmee op de deuren en ramen geklopt kan worden om te zien of die open staan maar dat een port scanner gezien kan worden als een breekijzer waarmee op de deuren en ramen geklopt wordt om te kijken of die open zijn en, indien dit zo is, om deze tussen het raam en het kozijn te plaatsen om de sterkte van het hout te bepalen en een eerste poging te doen om deze open te breken.

Als een port scanner op dit moment gezien wordt als de meest gevaarlijke tool in de handen van een vaardige hacker is het opmerkelijk dat zowel in de nationale als de internationale wetgeving ten aanzien van computercriminaliteit geen bepaling is opgenomen ten aanzien van de port scan. Het hangt van de omstandigheden van het geval af of de port scan wordt gebruikt voor het plegen van een ander strafbaar feit, zoals het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd werk (art. 138a, lid 1 WvSr). Er kan dan sprake zijn van poging met betrekking tot het plegen van dat andere delict. Indien de port scan kan worden gezien als een voornemen van de dader tot het binnendringen in de computer, het vernielen van een geautomatiseerd werk, het vernielen van gegevens of afluisteren, dan kan strafbaarheid ontstaan op grond van poging. Volgens het Govcert (/KLPD) is het bijzonder lastig om de opzet van de verdachte aan te tonen (het vereiste voornemen van de hacker om het systeem binnen te dringen).[122]

Indien echter bepaalde typen port scans met een normatief opzetbegrip geïnterpreteerd worden aan de hand van het Inrijden op agent-arrest[123] is het naar mijn mening echter zeer wel mogelijk de intentie van de hacker te bepalen. Aan de handeling, een specifiek type port scan, kan qua opzet de intentionaliteit ten aanzien van het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem worden gezien. De scantypes die hiervoor in aanmerking komen zijn specifiek gericht op bepaalde poorten om te bepalen of er verouderde versies op draaien die gevoelig zijn voor exploits, ‘sneaky’ scans om routers, firewalls of IDS’s te omzeilen of fragmented packet

120 A. Vincent, M. Taber & Anonymous, *Maximum security: a hacker’s guide to protecting your internet site and network*, Lawrence, Angel722 Inc. Computer Publishing, 2000, p. 135

121 McClure, Scambray en Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003, p. 36

122 Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005, p. 94

123 HR 6 februari 1951, NJ 1951, 475, Inrijden op agent

scans, decoy scans en spoofed source address scans om de herkomst van de port scan zo veel mogelijk te verbergen.

Dergelijke port scans kunnen echter pas uitgevoerd worden als de hacker ervoor zorgt dat hij de beschikking verkrijgt over een port scanner om te kunnen scannen naar online systemen en vervolgens ook een directe verbinding maakt met het doelsysteem door een port scan uit te voeren op dit doelsysteem. Deze fase van voorbereidingshandelingen, die wel reeds een bepaald voornemen zouden kunnen verraden, maar daarnaast nog zo veel onzekerheid herbergen omtrent de daadwerkelijke intentie van een hacker dienen in het belang van de rechtszekerheid straffeloos te blijven. Indien echter de eerste port scan wordt gevolgd door hieropvolgende fasen waarbij:

1. Sneaky port scans met decoys door de hacker worden uitgevoerd op dit ontdekte doelsysteem waarvan hij inmiddels door de eerste scan weet welke poorten er luisteren naar inkomende verbindingen en hierbij door de hacker de optie meegegeven wordt om het OS te bepalen en bij de output van de port scan de optie meegegeven wordt om zo veel mogelijk informatie te verkrijgen om de versies van de services te bepalen en
2. Daarna door de hacker de optie meegegeven wordt specifiek te scannen op díe luisterende poorten waarvan hij inmiddels weet dat er services op draaien die een verouderde versie betreffen en waarvan bekend is geworden dat er beveiligingslekken ten aanzien van die versies zijn ontdekt en
3. De port scan door de hacker wordt uitgevoerd op tijdstippen dat het risico op ontdekking zo klein mogelijk is, bijvoorbeeld 's-nachts als er weinig of geen systeembeheerders aanwezig zijn of de port scan over een lange tijd uitgevoerd wordt zodat de port scan geen argwaan wekt,

zijn deze naar mijn mening, gezien de uiterlijke verschijningsvorm waaruit de intentie van de hacker blijkt, zeker als uitvoeringshandelingen te kwalificeren.

Het criterium van de uiterlijke verschijningsvorm is in wezen gerelateerd aan de indruk die een goede waarnemer, die de gemiddelde burger geacht wordt te zijn, ter plaatse zou hebben gekregen omtrent de verwerkelijking van een bepaald misdrijf. De uiterlijke verschijningsvorm van een dergelijke port scan is echter dermate gecompliceerd dat een goede analyse alleen door systeembeheerders kan worden uitgevoerd en niet door een gemiddelde burger kan worden beoordeeld. De beoordeling van de feiten en het juridisch kwalificeren ervan vindt echter niet in het luchtledige plaats, maar geschiedt vanuit opvattingen die men heeft over het 'behoren'. In casu gaat het daarbij om opvattingen aangaande de vraag of bepaalde gedragingen straffeloos mogen blijven. Die vraag kan natuurlijk slechts aan de orde komen voor zover wettelijke bepalingen ruimte laten voor dergelijke normatieve oordelen. De bepalingen met betrekking tot de poging laten een dergelijke ruimte.[124]

124 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 554

Als bovenstaande laatste drie fasen zich voltrekken, blijkt hieruit naar mijn mening daadwerkelijk de bedoeling tot het uitvoeren van een opzettelijke en wederrechtelijke inbraak in een geautomatiseerd systeem. Dan pas zijn er gedragingen die rechtstreeks zijn gericht op de voltooiing van het misdrijf en is er een begin van uitvoering en dient dat niet straffeloos te blijven. Het lijkt ook niet in strijd met, integendeel in de lijn van de opvattingen van de Hoge Raad, om de rek die in de bepaling van art. 45 WvSr met betrekking tot het begin van uitvoering ongetwijfeld aanwezig is, te gebruiken om te voorkomen dat iemand straffeloos blijft van wie door zijn daden ondubbelzinnig vaststaat, dat hij, als het van hem had afgehangen, het misdrijf zou hebben voltooid.[125]

De nieuw toegevoegde leden twee en drie aan artikel 139d WvSr bieden verruimde mogelijkheden voor strafbaarheid van bepaalde voorbereidingshandelingen. In dit onderzoek is met name van belang het voorhanden hebben van een technisch hulpmiddel dat hoofdzakelijk geschikt is gemaakt of ontworpen tot het plegen van een misdrijf met het oogmerk dat daarmee een misdrijf als bedoeld in art. 138a, eerste lid WvSr wordt gepleegd. Vanwege de delictsomschrijving in art. 139d WvSr is de cruciale vraag of een port scanner een technisch hulpmiddel is dat hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van een zodanig misdrijf als bedoeld in art. 138a, eerste lid WvSr, 138b WvSr of 139c WvSr. Het beroepsmatig voorhanden hebben van technische hulpmiddelen door systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, betreft niet meteen een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. Aan de eis van kennelijke bestemming, die bij art. 46 WvSr gehanteerd wordt, te gebruiken moet een objectieve, beperkte strekking worden toegekend. De gemiddelde rechtsgenoot moet uit de combinatie van zaken overduidelijk kunnen afleiden dat er een crimineel doel is.[126] In dit geval kan uit het slechts voorhanden hebben van een port scanner niet direct worden afgeleid dat deze een crimineel doel dient / zal dienen. Hierin is zo veel onzekerheid gelegen dat deze in het belang van de rechtszekerheid straffeloos dienen te blijven.

5.2 Aanbevelingen

De opvatting van de Hoge Raad om de rek die in de bepaling van art. 45 WvSr met betrekking tot het begin van uitvoering ongetwijfeld aanwezig is, te gebruiken om te voorkomen dat iemand straffeloos blijft van wie door zijn daden ondubbelzinnig vaststaat, dat hij, als het van hem had afgehangen, het misdrijf zou hebben voltooid,[127] zou tot een bevestigend antwoord leiden op het laatste deel van de laatste onderzoeksvraag: moet port scanning strafbaar worden gesteld op nationaal en internationaal niveau ter beveiliging van geautomatiseerde systemen en is dit juridisch en technisch haalbaar?

Tot dusver zijn de delicten genoemd in artikel 138a WvSr, 139d, lid 2 WvSr en artikel 6 van het Cyber Crime Verdrag slechts strafbaar via de deelnemingsvormen van uitlokken, medeplegen en

125 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 555

126 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 327

127 Hoge Raad, 8 september 1987, 1908, NJ 1988, 612, Grenswisselkantoor in: M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht / strafprocesrecht met annotaties*, Deventer, Kluwer, editie 2004, p. 555

medeplichtigheid in de gevallen dat het hoofddelict of een poging daartoe ook daadwerkelijk wordt gepleegd. Govcert (/KLPD) stelt in haar rapportage 'Handleiding Cyber Crime, Van herkenning tot aangifte'[128] dat het Wetboek van Strafrecht dient te worden aangevuld met een bepaling dat ook wanneer het hoofddelict niet volgt, er toch sprake is van strafbaarheid. Deze mening deel ik niet ten aanzien van de port scan. Gezien het feit dat een port scan op zoveel verschillende mogelijkheden kan plaatsvinden door de vele opties die er aan meegegeven kunnen worden, is het naar mijn mening niet logisch dit in een apart strafartikel te doen. Een aparte strafbaarstelling zou betekenen dat elk type port scan tot in details omschreven moet worden en strafbaar gesteld moet worden. Door de vele opties die port scanners bieden zou het voor een hacker makkelijker zijn om díe opties aan de port scan mee te geven om aan de delictsomschrijving te ontkomen en straffeloos te blijven.

Een aparte strafbaarstelling van port scanning is naar mijn mening juridisch wel mogelijk doch stuit op grote technisch-specifieke problemen door de vele verschillende gedaanten die een port scan kan aannemen. De techniek sluit een goede en alles omvattende strafbaarstelling van port scanning uit, zeker gezien het feit dat er iedere dag weer nieuwe technieken worden ontwikkeld. De mogelijkheden voor port scanning worden daardoor ook weer groter en verfijnder waardoor een delictsomschrijving binnen de kortste keren weer ontoereikend is doordat het nieuwe type port scan niet meer onder deze delictsomschrijving valt.

Als een port scan zich kenmerkt door een van de drie uitvoeringshandelingen zoals hierboven omschreven, kan deze worden beschouwd als een poging tot het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem. Ik zou ervoor pleiten om de strafbaarstelling van een dergelijke port scan te baseren op art. 138a WvSr jo. art. 45 WvSr. Hoewel de uiterlijke verschijningsvorm van een dergelijke port scan dermate gecompliceerd is dat een goede analyse alleen door systeembeheerders kan worden uitgevoerd en niet door een gemiddelde burger kan worden beoordeeld, zou door een systeembeheerder aangifte kunnen worden gedaan indien deze port scan naar zijn mening als verdacht kan worden bestempeld. Als een handeling van een hacker na analyse van de log-files door een systeembeheerder als verdacht wordt ervaren, dan is die handeling blijkbaar geschikt om een verdenking op te wekken. Anders gezegd: de uiterlijke verschijningsvorm van zo een handeling is blijkbaar dusdanig dat zij is te beschouwen als te zijn gericht op de voltooiing van het misdrijf en dient als zodanig niet straffeloos te blijven.

De kamerstukken met betrekking tot het Cyber Crime Verdrag geven aan dat er een bepaling moet komen dat iemand niet strafbaar is als bijvoorbeeld hackingtools worden gebruikt om de beveiliging van een computersysteem te testen.[129] Ook deze mening deel ik niet ten aanzien van de port scan. Vanwege de delictsomschrijving in art. 139d WvSr is de cruciale vraag of een port scanner een technisch hulpmiddel is dat hoofdzakelijk geschikt is gemaakt of ontworpen is tot het plegen van een zodanig misdrijf als bedoeld in art. 138a, eerste lid, 138b of 139c WvSr. Het beroepsmatig voorhanden

128 *Handleiding Cyber Crime, Van herkenning tot aangifte*, Govcert.nl (/KLPD), Den Haag, Augustus 2005, p. 141

129 TK 2000 – 2001, 23530, nr. 45, p. 6 in: *Handleiding Cyber Crime, Van herkenning tot aangifte*, Govcert.nl (/KLPD), Den Haag, Augustus 2005, p. 141

hebben van technische hulpmiddelen door systeembeheerders, die ook voor het plegen van een strafbaar feit (kunnen) worden ingezet, betreft niet meteen een strafbare voorbereidingshandeling. In dit geval zal er namelijk geen sprake zijn van het oogmerk om een strafbaar feit te plegen. Aan de eis van kennelijke bestemming, die bij art. 46 WvSr gehanteerd wordt, te gebruiken moet een objectieve, beperkte strekking worden toegekend. De gemiddelde rechtsgenoot moet uit de combinatie van zaken overduidelijk kunnen afleiden dat er een crimineel doel is.[130] Uit het slechts voorhanden hebben van een port scanner kan niet direct worden afgeleid dat deze een crimineel doel dient / zal dienen. Hierin is zo veel onzekerheid gelegen dat deze in het belang van de rechtszekerheid straffeloos dienen te blijven. Een bepaling dat iemand niet strafbaar is als bijvoorbeeld hackingtools worden gebruikt om de beveiliging van een computersysteem te testen is naar mijn mening dan ook niet nodig. Door dergelijke voorbereidingshandelingen niet apart strafbaar te stellen ontloopt men de problemen die zouden kunnen ontstaan bij deze voorbereidingshandelingen tussen hackers en systeembeheerders voor wat betreft het opzetvereiste.

Afrondende woorden

Er wordt wel eens gezegd dat het recht achter de techniek aanloopt. Het bovenstaande onderzoek overziend lijkt de wetgeving voor een poging tot het opzettelijk en wederrechtelijk binnendringen in een geautomatiseerd systeem door middel van een specifieke port scan over het algemeen toereikend. Specifieke wetgeving ten aanzien van port scanning is overbodig en juist door de snelle technische ontwikkelingen onmogelijk bij te houden. Juist deze snelle technische ontwikkelingen zorgen er echter voor dat men constant op de hoede moet zijn en niet eeuwig op de huidige wetgeving moet vertrouwen. Aanpassing kan nodig zijn in de toekomst aangezien te veel vertrouwen in onze huidige beveiliging fataal kan zijn, getuige deze afsluitende woorden van hacker FX:

"It wasn't that difficult. Not nearly as hard as I expected. In fact, it actually was pretty easy. You just had to think about it. That's all. It seems that many security people think that by putting routers and firewalls and intrusion detection systems (IDSs) in place that they made their network secure. But that's not necessarily the case. All it takes is some small misconfiguration somewhere in their network or on a server somewhere to provide enough of a crack to let someone through…"

(Ido Dubrawski, 'Hide and seek' in R. Russell e.a., *Stealing the network, How to own the box*, Rockland, Syngress Publishing, Inc., 2003)

130 C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst en commentaar*, Deventer, Kluwer, 2004, p. 327

Bijlage 1 Lijst van begrippen en afkortingen

- ACK: Acknowledgement field significant (zie verder: TCP)

- Black hat hacker: Een black hat hacker, ook wel een cracker genoemd, is een kwaadaardige of criminele hacker. De naam komt van het tegenovergestelde: white hat hackers. Een black hat hacker is een hacker die zijn kennis van kwetsbaarheden en exploits voor zich zelf houdt in plaats van deze bekend te maken onder het publiek zodat fabrikanten en makers van software die kwetsbaarheden kunnen herstellen.

- (d)Dos: Distributed Denial of Service. Een aanval op een computer of netwerk waarbij met een aantal computers, vaak vanaf vele plaatsen op de wereld bestuurd vanaf een centraal punt, zoveel verbindingsverzoeken naar de server van een of meer sites verstuurd worden, dat de service ervan tijdelijk niet beschikbaar is, of de server zelfs crasht. Bij deze aanval wordt aan de server telkens een verzoek tot verbinding gedaan, en op het moment dat de server deze verbinding openstelt wordt door de aanvrager geen bevestiging of ander verkeer meer gestuurd. Omdat een server gedurende een bepaalde periode (time-out) wacht op deze bevestiging, kunnen op deze manier in korte tijd (te) veel verbindingen worden opengezet, waardoor de server geen dienst meer levert. Een herstart van het serverproces kan dan noodzakelijk zijn. Bij een andere vorm van (d)DoS attack wordt zeer veel netwerkverkeer naar een site of netwerk gegenereerd, waardoor veel bandbreedte van verbindingen wordt gebruikt, of verbindingen zelfs verzadigd raken.

- DNS: Domain Name System. Het Domain Name System is het systeem en protocol dat op het Internet gebruikt wordt om domeinnamen naar IP-adressen te vertalen en vice versa. Een DNS-Server of Domain Name Server is op deze technologie gebaseerd, en maakt deze vertalingen, zodat niet alle computers bij nummer hoeven te worden onthouden, maar aan de hand van een naam. Ook het omgekeerde: reverse DNS, het omzetten van een nummer in de bijbehorende naam is mogelijk. Een clientprogramma voor een internetdienst kan via aanroepen in een programmabibliotheek een Domain Name Server vragen om de vertaling uit te voeren. Een webbrowser doet dit elke keer automatisch wanneer een adres wordt ingetypt of een hyperlink wordt gevolgd.

- Exploits: Een klein stukje code / een programma dat wordt gebruikt om een kwetsbaarheid in software te activeren waardoor een aanvaller gebruikt toegang kan verkrijgen tot een geautomatiseerd systeem.

- FIN: No more data from sender (zie verder: TCP)

- Firewall: Firewall is letterlijk vertaald in het Nederlands "brandmuur". Dit soort muren (in gebouwen toegepast) dient om te voorkomen dat een brand aan de ene kant van de muur overslaat naar de andere kant. Op dezelfde manier heeft een firewall in een computernetwerk tot doel te voorkomen dat ongewenst verkeer van de ene netwerkzone terecht komt in een andere, teneinde de veiligheid in de laatstgenoemde te verhogen. Het beschermde netwerk is vaak een intranet of intern netwerk, en dit wordt beschermd tegen het internet. Het ongewenste verkeer bestaat bijvoorbeeld uit aanvallen van hackers en crackers (krakers), computervirussen, spyware, spam en denial of service attacks.

- Geautomatiseerd werk: Een inrichting die bestemd is om langs elektronische weg gegevens op te slaan en te verwerken (art. 80sexies WvSr). Met het begrip geautomatiseerd werk wordt een genusaanduiding gegenereerd waaronder niet alleen computers in de meer gangbare betekenis, maar ook netwerken van computers en geautomatiseerde inrichtingen voor telecommunicatie, zoals telefoon en fax en dergelijke begrippen worden geacht.

- Gegevens: Iedere weergave van feiten, begrippen of instructies, al dan niet op overeengekomen wijze, geschikt voor overdracht, interpretatie of verwerking door personen of geautomatiseerde werken (art. 80quinquis WvSr). Het begrip gegeven omvat een zeer omvangrijk en verscheiden terrein: niet alleen gegevens die in geautomatiseerde werken zijn opgeslagen of worden opgeslagen teneinde de mens te voorzien van informatie, maar ook de programmatuur ten behoeve van de besturing van dergelijke werken ongeacht hun al dan niet auteursrechtelijke bescherming. Met de keuze voor de aanduiding gegevens heeft de wetgever tot uitdrukking willen brengen dat het begrip ‘gegevens’ onderscheiden moet worden van het begrip ‘goed’ zoals gebruikt in de artikelen 310 en 321 WvSr.

- Hacker: In het dagelijkse spraakgebruik en in de lekenpers is een hacker meestal iemand die inbreekt in computersystemen. In bepaalde technisch georiënteerde subculturen is een hacker een persoon die geniet van de intellectuele uitdaging om op een creatieve, onorthodoxe manier aan technische beperkingen te ontsnappen; bijvoorbeeld een goede programmeur, hoewel een hacker niet per se iets met computers hoeft te doen. In deze subculturen wordt het gebruik van de woorden *hacker* en *hacken* door en voor computerinbrekers als misbruik van de term gezien; zij worden *crackers* of krakers genoemd. In het bijzonder wordt het woord *hacker* gebruikt in volgende betekenissen:

Iemand die een programmeertaal of -omgeving zo goed kent dat hij zonder zichtbare moeite een programma kan schrijven, iemand die een technologie bedenkt, ontwerpt, uitwerkt, implementeert, test, en verbetert, iemand die onconventionele maar adequate oplossingen bedenkt tegen lekken, fouten en problemen van andere aard met behulp van beschikbare middelen of iemand die tracht om via andere dan de officiële wegen een computersysteem binnen te dringen ten einde een beveiligingsprobleem te kunnen aantonen en mogelijk verhelpen. Hackers hebben ook normen, de zogenaamde hackersethiek. Deze is terug te vinden in de indeling "black-hat/grey-hat/white-hat hackers". Ook is het zo dat een hacker in de wereld van de hackers status kan verwerven door zijn of haar kennis te delen met anderen. Dit doet men door open-source software te schrijven.

- Host: In de specificaties van het IP-protocol betekent host elk apparaat dat een volledige tweewegcommunicatie kan uitvoeren met een ander apparaat op het internet. Elke host heeft een eigen IP-adres. Als via een modem verbinding wordt gemaakt met de Internet Service Provider of ISP, dan krijgt men gedurende die periode een IP-adres en geldt het systeem als host.

- IDS: Intrusion Detection System. Het doel van een IDS is om op verschillende plekken in een computernetwerk een analyse te kunnen maken van het type verkeer dat zich op dat moment door dat deel van het netwerk verplaatst. Dit met als doel om in staat te zijn in een vroegtijdig stadium worm-uitbraken, hackpogingen en ander kwaadaardig verkeer te kunnen detecteren.

- ICMP: Internet Control Message Protocol/ Het ICMP is een van de kernprotocollen voor de Internet Protocol suite. Het wordt voornamelijk gebruikt door computers, die door middel van een netwerk zijn verbonden, om foutmeldingen te versturen, bijvoorbeeld dat een bepaalde service niet beschikbaar is of dat een bepaalde host of router niet bereikt kan worden. ICMP verschilt van TCP en UDP in die zin dat het niet direct wordt gebruikt door netwerkapplicaties. Een uitzondering is de ping-tool die ICMP Echo request-berichten verstuurt en ICMP Echo Response-berichten ontvangt om te bepalen of een host te bereiken is en hoe lang netwerkpakketjes er over doen om die host te bereiken.

- Internet: Een internet is een netwerk van computernetwerken. Een computernetwerk is over het algemeen alleen beschikbaar binnen een organisatie of gebouw, een beperking die opgeheven wordt door een internet. Om een internet goed te laten werken is het nodig om afspraken te maken over protocollen. Een bijna universeel gebruikt protocol is het zogenaamde Internetprotocol (IP). Computers in verschillende computernetwerken kunnen dankzij die afspraken met elkaar communiceren. In het dagelijkse spraakgebruik

is internet vaak een synoniem voor het World Wide Web, maar dat is slechts één van de vele diensten die kunnen worden gebruikt via het Internet. Andere bekende diensten zijn e-mail, FTP en usenet.

- Intranet: Een intranet is een privaat netwerk binnen een organisatie. Het kan bestaan uit verschillende aan elkaar gekoppelde LAN's. Voor de gebruiker is het net een private versie van Internet. De meeste intranetten zijn via een gateway gekoppeld aan het wereldwijde Internet. Het primaire doel van een intranet is het elektronisch delen van informatie binnen een organisatie. Tevens kan het gebruikt worden voor teleconferenties en om het elektronisch samenwerken in groepen te faciliteren en stimuleren.

- IP: Internet Protocol. Een IP-adres is een adres waarmee een NIC (network interface card of controller) van een host op het internet uniek geadresseerd kan worden binnen het TCP/IP-model. Of in meer eenvoudige woorden: elke computer heeft een nummer waarmee deze zichtbaar is voor alle andere computers op het internet. Men kan dit vergelijken met telefoonnummers. Om het mogelijk te maken dat computers elkaar kunnen vinden en identificeren hebben deze hun eigen nummer nodig. Deze nummers zijn de "IP-adressen”.

- Linux: Linux is de algemeen gebruikte naam van een familie op Unix geënte besturingssystemen. Linux is vrije software en wordt onder de GPL verspreid: alle onderliggende broncode is door het publiek vrij te verkrijgen, vrij gebruiken, wijzigen, kopiëren en verspreiden. Dergelijke systemen, Linuxdistributies, zijn zowel gratis te verkrijgen als bij meerdere bedrijven te koop, dat laatste vaak met extra's zoals ondersteuning, handleidingen en extra (soms "niet-vrije") software.

- MTU: Maximum Transmission Unit. In computernetwerken refereert de term MTU aan de grootte (in bytes) van het grootste pakket dat over een bepaalde laag van een communicatieprotocol (zoals TCP/IP) kan worden verzonden. MTU parameters worden vaak gebruikt in combinatie met een communicatie-interface (NIC of seriële poort). Een hogere MTU geeft een betere bandbreedte efficiency. Grote netwerkpakketjes kunnen echter de communicatie-interface verstoppen of de interface voor enige tijd vertragen.

- MvT: Memorie van Toelichting. De MvT is de uitleg bij een wetsvoorstel. Deze toelichting wordt geschreven door de minister die het wetsvoorstel maakt. In de MvT geeft deze aan waarom het onderwerp dat in de desbetreffende wet is gelegen wettelijk moet worden geregeld. Tevens wordt in de MvT ieder artikel van de desbetreffende wet door middel van commentaar uiteen gezet. Een voorstel van wet wordt door de regering gezamenlijk

met de MvT en het advies van de Raad van State ingediend bij de Tweede Kamer.

- Netwerk: Een computernetwerk is een systeem voor communicatie tussen twee of meer computers. Er zijn zowel computernetwerken waarbij de computers communiceren via fysieke elektrische kabels of glasvezelkabels, als draadloze netwerken. In de topologieën van netwerken worden fysieke en logische topologieën onderscheiden. Globaal spreekt men van een Local Area Network (LAN) waarop computers binnen één gebouw of complex aangesloten worden en een Wide Area Network (WAN) om verbinding te leggen over grotere afstanden.

- OS: Operating System. Een besturingssysteem is het programma (meestal een geheel van samenwerkende programma's) dat bij het opstarten van de computer als eerste in het geheugen geladen wordt, en de functionaliteiten aanbiedt om andere programma's uit te voeren. Het besturingssysteem zorgt voor het opstarten en beëindigen van andere programma's, het regelt de toegang tot de harde schijf, het scherm, de invoer van gegevens, enzovoort. De andere programma's die gestart kunnen worden heten applicaties.

- Ping: Ping is een hulpprogramma voor computernetwerken, dat wordt gebruikt om de reactietijd in milliseconden tussen twee computers in een netwerk te meten. Hoe lager deze waarde is, hoe sneller je een reactie van de andere computer terugkrijgt. Ping maakt gebruik van het TCP/IP-protocol (bijvoorbeeld het Internet).

- PSH: Push function (zie verder: TCP)

- Router: Een router (uitspraak: *roeter* in het Engels of *rauter* in het Amerikaans-Engels) is een apparaat of software op een computer, dat twee of meer verschillende computernetwerken aan elkaar verbindt, bijvoorbeeld internet en een bedrijfsnetwerk. Een router kan gezien worden als een schakelapparaat voor datapakketten, dat actief is op OSI laag 3.

- RST: Reset the connection (zie verder: TCP)

- Server: Een server is een computer of een programma dat diensten verleent aan andere programma's. In de eerste betekenis wordt met server de fysieke computer aangeduid waarop een programma draait dat deze diensten verleent.

- Shell: Een shell is een computerprogramma waarmee een gebruiker commando's kan geven aan zijn computer. Het is van belang om hierbij onderscheid te maken tussen de terminalemulator en de shell zelf. Het doorgeven van de invoer en uitvoer van de grafische interface naar de shell gebeurt door middel van de terminalemulator. Bekende terminalemulators zijn XTerm en ATerm. De shell is een stuk software dat invoer van de gebruiker verwerkt en uitvoer terug geeft. Al deze communicatie tussen de gebruiker en de shell gebeurt via de terminalemulator. In Windows is er geen scheiding tussen de terminalemulator en de shell. Onder de meeste Microsoft Windowsversies kunnen zowel de terminalemulator als de bijbehorende shell worden benaderd door het programma *cmd* of *command* te starten. Deze shell is ongeveer gelijk aan de shell in DOS die COMMAND.COM heet. Onder UNIX is die scheiding er wel. Bekende shells onder UNIX zijn sh, csh, ksh en bash.

- Spoofing: Internet Protocol Spoofing of IP-spoofing is een techniek om ongeautoriseerde toegang te verkrijgen tot een computer via diens IP-stack. De techniek is gebaseerd op het vervalsen van de identiteit van een andere computer en is bijzonder effectief als de gefingeerde identiteit die is van een entiteit die de aangevallen computer vertrouwt. IP-spoofing maakt gebruik van het twee dingen om een succesvolle aanval op te zetten: Een aangevallen computer herkent de herkomst van TCP/IP-pakketten enkel en alleen aan het IP-adres dat in de IP-header vermeldt staat; deze header bestaat uit platte tekst die simpelweg aangepast kan worden. Wanneer een bericht in stukken verzonden wordt over een Internetverbinding, wordt de volgorde van de stukken bijgehouden in een teller in de TCP-header van ieder pakket. De manier waarop de teller voor ieder pakket en voor iedere boodschap wordt verhoogd, maakt dat het volgende nummer dat een computer in een pakket verwacht te ontvangen met een zekere nauwkeurigheid voorspelbaar is. Bij een IP-spoofing-aanval maakt de aanvaller van deze twee zaken gebruik om te proberen zijn slachtoffer te laten geloven dat hij een andere (vertrouwde) computer is dan hij eigenlijk is.

- SYN: Synchronize sequence numbers (zie verder: TCP)

- TCP: Transmission Control protocol. TCP is een protocol dat veel gebruikt wordt op het Internet. De afkorting staat voor Transmission Control Protocol en het is een connectie-georiënteerd protocol. TCP werkt boven het IP en is connectie-georiënteerd. Dit in tegenstelling tot stateless protocollen zoals UDP. TCP heeft als kenmerken dat het gegevens in streams kan versturen, waarbij er garantie is dat de gegevens aankomen zoals ze verstuurd worden, en eventuele zendfouten, zowel in de gegevens zelf als in de volgorde van de gegevens kunnen worden opgevangen. Hierdoor hoeft een

clientapplicatie die TCP als transmissieprotocol gebruikt geen rekening te houden met de onderliggende netwerkarchitectuur en eventuele zendfouten.
Connectie-georiënteerd betekent dat, voordat data kan worden verzonden, een betrouwbare verbinding moet worden verkregen en bevestigd. TCP level data transmissies, het verkrijgen van verbinding en het verbreken van verbinding worden verzorgd door specifieke controle parameters die het hele proces bestrijken. Deze controlebits zijn als volgt gerangschikt:
- URG: Urgent Pointer field sifnificant
- ACK: Acknowledgement field significant
- PSH: Push function
- RST: Reset the connection
- SYN: Synchronize sequence numbers
- FIN: No more data from sender

- TCP/IP: Transmission Control protocol/Internet Protocol. TCP/IP is een verzamelnaam voor de reeks netwerkprotocollen die voor een grote meerderheid van de netwerkcommunicatie tussen computers instaan. Het internet is het grootste en meeste bekende TCP/IP-netwerk. De naam TCP/IP is een samentrekking van de twee bekendste en protocollen die deel uit maken van de TCP/IP-protocol*stack* (stapel): het internetprotocol (IP) en het Transmission Control Protocol. TCP/IP wordt uitgesproken als "TCP over IP".

- UDP: User Datagram Protocol. UDP is de afkorting van User Datagram Protocol. UDP is een van de basisprotocollen van het Internet en opereert op hetzelfde niveau als TCP. Vergeleken met TCP is UDP minder betrouwbaar, maar dankzij een lagere overhead (zoals handshaking en verificatie) ook sneller. Zo biedt UDP geen garantie dat de gegevens werkelijk aankomen, het kan zijn dat er pakketjes niet aankomen bij de bestemming, zonder dat daarvan melding gemaakt wordt. Een aantal protocollen dat via UDP werkt en dus een laag hoger ligt op de TCP/IP-stack zorgt zelf voor verificatie van de aangekomen pakketten, dus voor de betrouwbaarheid wordt soms in een hogere laag gezorgd. UDP wordt veel gebruikt bij toepassingen waar het snel overdragen van de gegevens en een korte reactietijd zeer belangrijk is, en het minder erg is dat er gegevens verloren kunnen gaan, zoals bij videoconferencing, DNS of het online spelen van actievolle spellen, zoals first person shooters.

- UNIX: Unix (of UNIX) is een familie van besturingssystemen met *multitasking*- en *multiuser*-mogelijkheden voor zeer uiteenlopende typen computers, ontwikkeld door verscheidene fabrikanten en groepen. De eerste versie van Unix werd ontworpen bij Bell Labs in 1969, door (onder anderen) Ken Thompson en Dennis Ritchie. Unix wordt

gekenmerkt door de centrale rol van het bestandssysteem, dat niet alleen gebruikt wordt om bestanden op schijven en andere fysieke media aan te spreken, maar ook randapparatuur en in sommige varianten ook netwerkverbindingen. Om met het bestandssysteem te werken maakt Unix van oudsher gebruik van een groot aantal kleine, niet-interactieve programma's, die allemaal één zeer specifieke taak verrichten, en die via de *shell* gecombineerd kunnen worden tot grotere programma's.

- URG: Urgent Pointer field sifnificant (zie verder: TCP)

- White hat hacker: Een veelgenoemd verschil tussen hackers en crackers is dat hackers hun handelingen vaak verrichten als uiting van constructieve creativiteit ('voor de kunst van het bouwen') of als goedbedoelde handelingen (zoeken naar veiligheidslekken om deze later te kunnen dichten. Hackers zelf noemen degenen die uit criminele oogmerken een systeem 'kraken' *krakers* of *crackers* of *black-hat hackers*. Zelf noemen ze zich *white-hat hackers*, analoog aan cowboyfilms waarin de 'kwaden' zwarte hoeden droegen en de 'goeden' witte hoeden, ofschoon hackers zichzelf niet als zodanig benoemen. Ook zijn er *grey-hat hackers*, een kruising tussen crackers en hackers.

Bijlage 2 Literatuurlijst

- M. Bosch en S.A.M. Stolwijk, *Arresten strafrecht/strafprocesrecht met annotaties*, editie 2004, Kluwer, Deventer, 2004

- C.P.M. Cleiren en J.F. Nijboer, *Strafrecht, tekst & commentaar*, *vijfde druk*, Kluwer, Deventer, 2004

- A. Dasselaar, *Handboek digitale criminaliteit. Over daders, daden en opsporing*, Van Duuren Media Culemborg, 2005

- J.C. Foster & V. Liu, *Writing security tools and exploits*, Rockland, Syngress Publishing, Inc., 2006

- R.E. van Esch, *Recht en elektronische handel*, tweede druk, Deventer, Kluwer, 2002

- H. Franken e.a., *Recht en computer*, vijfde druk, Deventer, Kluwer, 2004

- Govcert.nl (/KLPD), *Handleiding Cyber Crime, Van herkenning tot aangifte*, Den Haag, Augustus 2005

- S. Jamieson, *The ethics and legality of port scanning*, GSEC Practical Assignment, v1.2f, October 8, 2001

- H.W.K. Kaspersen, 'Bestrijding van cybercrime en de noodzaak van internationale regelingen', *Justitiële Verkenningen*, 2004/8

- C. Kelk, *Studieboek Materieel Strafrecht*, Deventer, Gouda Quint, 2001

- J. Koziol e.a., *The Shellcoder's Handbook: Discovering and Exploiting Security Holes*, Indianapolis, Wiley Publishing, Inc., 2004

- S. McClure, J. Scambray & G. Kurtz, *Hacking exposed*, 4e editie, Nijmegen, Academic Services, 2003

- K.D. Mitnick & W.L. Simon, *The art of intrusion, The real stories behind the exploits of hackers, intruders & deceivers*, Indianapolis, Wiley Publishing, Inc., 2005

- R. Russell e.a., *Stealing the network, How to own the box*, Rockland, Syngress Publishing, Inc., 2003

- R. Russell e.a., *Stealing the network, How to own a continent*, Rockland, Syngress Publishing, Inc., 2004

- A. Vincent, M. Taber & Anonymous, *Maximum security: A hacker's guide to protecting your internet site and network,* Lawrence, Angel722 Inc. Computer Publishing, 2000

- R. Vrielink, *Autodialers, Phishing, Identity theft en Spyware,* Utrecht, Juli 2005

- F.P.E. Wiemans, *Computervredebreuk nieuwe stijl en strafbare voorbereidingshandelingen*, JAVI, december 2004

Online bronnen

- http://www.atstake.com/research/tools/network_utilities
- http://www.blackhat.com
- http://www.compulegal.demon.nl/files/compcrime.htm
- http://www.foundstone.com
- http://www.ietf.org/rfc/rfc0793.txt
- http://www.insecure.org
- http://www.insecure.org/nmap/man/man-portscanning-techniques.html
- http://www.insecure.org/nmap/man/man-bypassing-firewalls.html
- http://www.iusmentis.com/beveiliging/hacken/computercriminaliteit/
- http://www.nessus.org
- http://www.netkwesties.nl/editie41/artikel6.html
- http://www.netscantools.com
- http://www.sans.org/reading_room/whitepapers/legal
- http://www.securityfocus.com/print/news/126
- http://slashdot.org
- http://www.snort.org
- http://www.wetboek-online.nl

- http://www.wikipedia.org
- http://www.wodc.nl/onderzoeken

Bijlage 3 Nmap-opties

NAME

nmap - Network exploration tool and security / port scanner

SYNOPSIS

nmap [*Scan Type*...] [*Options*] {*target specification*}

DESCRIPTION

Nmap (lqNetwork Mapperrq) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the lqinteresting ports tablerq. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (**-sO**), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

A typical Nmap scan is shown in Example 13.1, lqA representative Nmap scanrq. The only Nmap arguments used in this example are **-A**, to enable OS and version detection, **-T4** for faster execution, and then the two target hostnames. Example 13.1. A representative Nmap scan.sp

```
# nmap -A -T4 scanme.nmap.org playground

Starting nmap ( http://www.insecure.org/nmap/ )
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1663 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.4.7 - 2.6.11, Linux 2.6.0 - 2.6.11
Uptime 33.908 days (since Thu Jul 21 03:38:03 2005)

Interesting ports on playground.nmap.org (192.168.0.40):
(The 1659 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE       VERSION
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
389/tcp  open  ldap?
445/tcp  open  microsoft-ds  Microsoft Windows XP microsoft-ds
1002/tcp open  windows-icfw?
1025/tcp open  msrpc         Microsoft Windows RPC
1720/tcp open  H.323/Q.931   CompTek AquaGateKeeper
5800/tcp open  vnc-http      RealVNC 4.0 (Resolution 400x250; VNC TCP
port: 5900)
5900/tcp open  vnc           VNC (protocol 3.8)
MAC Address: 00:A0:CC:63:85:4B (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows XP Pro RC1+ through final release
Service Info: OSs: Windows, Windows XP

Nmap finished: 2 IP addresses (2 hosts up) scanned in 88.392 seconds
```

The newest version of Nmap can be obtained from *http://www.insecure.org/nmap/*. The newest version of the man page is available from *http://www.insecure.org/nmap/man/*.

OPTIONS SUMMARY

This options summary is printed when Nmap is run with no arguments, and the latest version is always available at *http://www.insecure.org/nmap/data/nmap.usage.txt*. It helps people remember the most common options, but is no substitute for the in-depth documentation in the rest of this manual. Some obscure options aren't even included here.

```
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
```

```
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -P0: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idlescan
  -sO: IP protocol scan
  -b <ftp relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast - Scan only the ports listed in the nmap-services file)
  -r: Scan ports consecutively - don't randomize
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in milliseconds, unless you append 's'
  (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T[0-5]: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <time>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>:
Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe
retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use twice for more effect)
  -d[level]: Set or increase debugging level (Up to 9 is meaningful)
```

```
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to
HTML
  --webxml: Reference stylesheet from Insecure.Org for more portable
XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enables OS detection and Version detection
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sP 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -P0 -p 80
```