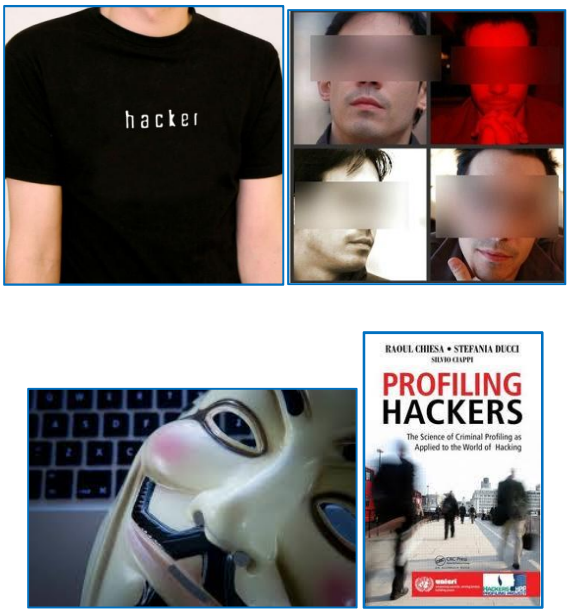
Hacking revealed



De hacker geanalyseerd: de successen, de geschiedenis, de hack zelf.

Kunnen we het zien gebeuren? Kunnen we een hack voorkomen?

Referenties

Auteur:	ing. T.L.P. Heinsbroek C|CISO, CISSP, CISA
Organisatie:	**SeKuRiGo**[1], http://www.sekurigo.nl
Datum:	17 februari 2013
Licentie:	Attribution-Share Alike 3.0 

[1] **SeKuRiGo** is een onafhankelijke organisatie die zich richt op het grensvlak van organisatie en IT en is gespecialiseerd in information security management, identity and accessmanagement en IT-audit.

Inhoudsopgave

Voorwoord

Hacking lijkt het nieuws nogal te domineren de laatste tijd. Comodo, Stuxnet, Diginotar, Anonymous, Luzsec, Duqu, de KPN hack, de geïnfecteerde websites weeronline.nl en nu.nl, de Flashack-botnet en Flame, ze waren allemaal in het nieuws. De vraag is nu: is hacking echt zo dominant op het moment? Of krijgen deze hacks domweg heel veel media-aandacht? Laten we het zo zeggen: is hacking een nieuw fenomeen of is hacking van alle tijden?

In deze whitepaper toon ik aan dat hacking niet nieuw is. Dat we wel dat idee krijgen komt vooral door de media-aandacht en door de openheid van organisaties die te maken kregen met cyberaanvallen. Ik zal ingaan op de verschillende type hackers en hun diverse redenen en doelen om te doen wat ze doen. Daarnaast leg ik uit wat het verschil is tussen hackers (professionals en overheid), crackers, wannabees en scriptkiddies en ik geef inzage in technieken zoals social engineering, het installeren van Trojaanse Paarden, backdoors en zero-day-exploits met gebruik van maintenance hooks (trapdoors), poortscanning en enumeratie.

Verder zal ik informatie geven uit wetenschappelijk onderzoek van de United Nations Interregional Crime and Justice Research Institute (UNCRI) waaruit blijkt dat hacken van alle tijden is en zich in de afgelopen jaren heeft ontwikkeld. Daarnaast presenteer ik het zogeheten Hackers Profiling Model dat hackers identificeert op basis van hun modus operandi. Met dit model kunnen organisaties de hacker achter de hack identificeren.

Het feit dat hacking niet nieuw is, wil niet zeggen dat het niet dominant is. Hacking heeft tenslotte een keerzijde: veel websites zijn nog steeds kwetsbaar voor hacking en zijn niet goed beschermd tegen gevoeligheden zoals SQL-injectie. Om die reden ga ik dieper in op de hack zelf en last but not least leg ik uit hoe je een aanval kunt identificeren en analyseren door preventieve, detectieve, correctieve en compenserende maatregelen te nemen.

Hacken: een introductie

Hackers, crackers, phreakers en scriptkiddies

Hackers zijn er in vele soorten en maten en die hebben diverse redenen om te doen wat ze doen. Er zijn grofweg vier groepen hackers die ik hier zal typeren.

Een *hacker* ziet zichzelf als iemand die wil leren hoe computersystemen en beveiliging werken. Zijn doel is om kennis te verzamelen over die zaken. Zijn doel is niet om schade aan te richten. Een hacker wil dus vooral leren. Hij of zij gebruikt deze kennis ter evaluatie van computerbeveiliging. Een hacker voert veiligheidstests uit om te zien of de software kwetsbaar is voor (onbekende) exploits en of er backdoors en trapdoors zijn geïnstalleerd. Als een hacker fouten in de code of gevoeligheden in de software vindt, dan is hij bereid om zijn bevindingen te delen met de eigenaar van de software.

Een *ethische hacker* is een hacker die hacks uitvoert op aanvraag: iemand vraagt de hacker om tests uit te voeren. Daarbij is hij gebonden aan de randvoorwaarden die vooraf in een contract tussen de hacker en de organisatie (of sponsor) zijn vastgesteld.

Behalve hackers zijn er ook de zogenoemde *crackers*. Crackers zijn criminelen en dus strafbaar. Hun motieven zijn niet zo nobel: naamsbekendheid (UseNet, dark-hacker scene, IRC-kanalen), persoonlijk gewin en wraakzucht zijn hun drijfveren. Het zijn de crackers die de meeste ravage aanrichten. Ze zijn gespecialiseerd in schade aanrichten, informatie stelen, softwarebeveiliging deactiveren, toegang krijgen tot afgeschermde 'security areas' en het programmeren van virussen. In de wereld van hackers worden de hackers ook wel 'white hats' genoemd en crackers 'black hats'.[2]

Phreakers zijn degenen die op zoek gaan naar de verste uithoeken van telefoonnetwerken en maken gebruik van technologie om frequenties te manipuleren. Hun doel is om gratis te kunnen bellen naar elk werelddeel en soms ook om in te breken in belangrijke centra. Tegenwoordig zijn phreakers vooral gericht op mobiele telefoons, draadloze technologieën en VoIP (Voice over Internet Protocol).

Onderaan de lijst vinden we de zogenoemde 'want to be lamer' en *scriptkiddies*. Dit zijn hackers die niet veel kennis hebben en die gebruik maken van tools die publiekelijk te verkrijgen zijn, vaak te vinden op internet. Zij zijn volledig afhankelijk van deze tools en doen met hun acties dus geen kennis op van de onderliggende infrastructuur van netwerken. Ze pikken hun doelwit willekeurig uit met gebruik van Usenet en/of IRC-

[2] Deze benamingen komen voort uit oude zwart-wit Westerns (films) waarin de good guys een witte hoed op hadden en de bad guys een zwarte hoed droegen.

kanalen. Soms voeren scriptkiddies aanvallen uit op een specifieke Microsoft OS-omgeving vanuit een UNIX OS-omgeving. Voorbeelden hiervan zijn: website defacing, Ping of Death, Distributed Denial of Services (DDoS) en LOIC (Low Orbit Ion Canon). Allemaal op basis van tools, zonder kennis.

Terwijl de cracker zich focust op 'hacking on demand' en op georganiseerde misdaad, focust de ethische hacker zich vooral op onderzoek (beveiliging), op het vinden van zero-day-exploits en op het verkopen van zijn bevindingen aan de eigenaar of leverancier.

Bovenaan de lijst vinden we de professionele hackers: de cyber-warrior, de industriële spion, de geheim agent en de militaire hacker. Vaak aangestuurd door woede, spionage en ook door overheidsinstanties is hun doel om internet infrastructuren in andere landen of van private bedrijven aan te vallen. Daarvoor maken ze gebruik van hackingtools en technieken om toegang te krijgen tot gevoelige informatie of om industriële faciliteiten te verstoren, maar ook voor crimineel gedrag.

Vier generaties

De *eerste generatie* hackers (jaren 70) werd geïnspireerd door een zucht naar kennis. Ze wilden vooral uitvinden hoe computers werken. Dit was in die tijd nog kersverse technologie en de enige manier om daar meer over te weten was door letterlijk een kijkje te nemen in de hardware en de software.

De *tweede generatie* hackers (1980-1984) werd gedreven door nieuwsgierigheid. Ze wilden uitvinden hoe besturingssystemen en netwerkcomponenten nu echt werkten. De enige manier om hier achter te komen was door ze te hacken. Eind jaren '80 wordt hacking echt een trend.

De *derde generatie* hackers (jaren 90) werd vooral gedreven door een kwade drang voor hacken: een mix van verslaving, nieuwsgierigheid, nieuwe dingen leren, het hacken van IT-systemen en netwerken en informatie uitwisselen met het ondergrondse circuit. Gedurende deze periode zagen nieuwe concepten zoals hackers magazines, e-zines en elektronische bulletinboards het licht.

De *vierde generatie* hackers (2000 to nu) wordt vooral gedreven door boosheid en door geld. We zien regelmatig personen die weinig knowhow hebben maar die denken dat het 'cool' is om hacker te zijn. Deze hackers zijn nauwelijks geïnteresseerd in de geschiedenis van hacken en phreaking en ook niet in de cultuur en de ethiek. Dit is ook de generatie waarbij hacking politiek wordt (cyber-hacktivism, occupybeweging) evenals crimineel (cybercrimiminaliteit).

Computercriminaliteit: drijfveren

Het aantal computergebruikers, websites en internetgebruikers stijgt nog elke dag en daarmee stijgt ook het aantal potentiële slachtoffers en aanvalsvectoren dagelijks. Dankzij breedbandinternet blijven krachtige hackingtools en technieken vaak onopgemerkt: ze verstoppen zichzelf in het normale internetverkeer. Dit stimuleert de hacker. Een andere stimulans is geld verdienen, soms heel veel geld. Er wordt wel gezegd dat sommige 'bonnetherders' meer geld verdienen in één dag dan normale werknemers in een maand.

Een technische drijfveer voor computercriminaliteit is de publieke beschikbaarheid van tools en technieken. In het ondergrondse circuit en op de zwarte markt wordt flink gehandeld en kun je persoonsgegevens en IP-adressen van gehackte slachtoffers kopen evenals zero-day-exploits, botnets, gebruiksklare aanvallen en creditcardnummers. Omdat hacking zo populair is (pochen, persoonlijk gewin, 'cool') is het heel eenvoudig om jongeren te rekruteren en groepen te creëren om die vervolgens om te vormen tot crackers en criminelen. De laatste drijfveer voor hacken is het feit dat de pakkans zo klein is. Dit maakt het nog aantrekkelijker om adepten te werven.

Hackers Profiling Project

In 2004 begon een team van onderzoekers aan het zogeheten Hackers Profiling Project (HPP): een theoretische verzameling van bewijzen en observaties in het ondergrondse IT-beveiligingscircuit. Dit project resulteerde in een classificatiedatabase die werd vergeleken werd met het originele theoretische model waarin profielen van hackers werden gedefinieerd.

Eerste model

De onderzoekers stelden een model op en combineerden dit model met bestaande bewijzen zoals veroordelingen en met feitelijke observaties uit de echte hackerswereld. Het eerste model, dat puur theoretisch was, werd gepubliceerd met als doel de bewustwording te vergroten. In dezelfde periode werd ook het boek[3] gepubliceerd.

<table>
<tr><th>Profiel</th><th>Status</th><th colspan="2">Invloed</th><th colspan="2">Doelwit</th></tr>
<tr><td>Want to be lamer</td><td rowspan="2">Amateur</td><td colspan="2">Geen</td><td colspan="2">Eindgebruiker</td></tr>
<tr><td>Scriptkiddie</td><td colspan="2">Laag</td><td>MKB</td><td>Specifieke beveiligingslekken</td></tr>
<tr><td>Cracker</td><td rowspan="3">Hobbyist</td><td>Medium</td><td>Hoog</td><td colspan="2">Bedrijven (corporate)</td></tr>
<tr><td>Ethische Hacker</td><td colspan="2">Medium</td><td>Leverancier</td><td>Technologie</td></tr>
<tr><td>Stille, paranoïde, kundige hacker</td><td>Medium</td><td>Hoog</td><td colspan="2">Leveranciers, technologie, bedrijven</td></tr>
<tr><td>Cyber-Warrior</td><td rowspan="4">Professional</td><td colspan="2">Hoog</td><td>"Symbool" ondernemingen</td><td>Eindgebruiker</td></tr>
<tr><td>Industriële Spion</td><td colspan="2">Hoog</td><td>Bedrijven</td><td>Ondernemingen</td></tr>
<tr><td rowspan="2">Overheidsagent (spion)</td><td colspan="2" rowspan="2">Hoog</td><td>Overheid / regering</td><td>Verdachte terroristen</td></tr>
<tr><td>Strategische ondernemingen</td><td>Individu</td></tr>
<tr><td>Militaire Hacker</td><td colspan="2">Hoog</td><td>Overheid / regering</td><td>Strategische ondernemingen</td></tr>
</table>

[3] Profiling Hackers: the Science of Criminal Profiling as applied to the World of Hacking, ISBN 978-1-4200-8693-5-9000.

Tweede model

In 2005 en 2007 werden fikse veranderingen waargenomen in het ondergrondse hackingircuit. Verandering qua stemmingen, nieuwe spelers en actoren en een toename van betrokkenheid bij georganiseerde criminaliteit en informatieoorlogsvoering. Deze observaties werden meegenomen in onderstaande tweede model, dat meer is dan enkel theoretisch. Met dit model werd het mogelijk om hacks te profileren en methoden te definiëren op basis van het ervaringsniveau en technologieniveau van de hacker zelf.

Profiel	**Dader ID**	**Alleen/Groep**	**Motivatie/Doel**
Wanna be lamer	9-16 jaar, "Ik wil graag een hacker zijn, maar kan het (nog) niet"	Groep	Het is stoer, in de mode en cool => om op te scheppen
Scriptkiddie	10-18 jaar De script boy	Groep, Handelt alleen	Om boosheid (op de wereld) te uiten en veel media-aandacht te krijgen
Cracker	17-30 jaar De vernieler, tactiek van de verschoeide aarde	Alleen	Kracht en kennis demonstreren / veel media-aandacht trekken
Ethische Hacker	15-50 jaar De 'ethische' hackerswereld	Alleen Groep voor de fun	Nieuwsgierigheid, om te leren en altruïsme
Stille, paranoïde, slimme hacker	16-40 jaar De zeer gespecialiseerde en paranoïde hacker	Alleen	Nieuwsgierigheid, om te leren => egoïstische doelen
Cyber-Warrior	18-50 jaar De soldaat, hacken voor geld	Alleen	Om geld te verdienen (winst te maken)
Industriële Spion	22-45 jaar Industriële spionage	Alleen	Om geld te verdienen (winst te maken)
Overheidsagent	25-45 jaar CIA, Mossad, FBI, etc.	Alleen/Groep	Spionage / contraspionage, weerbaarheidtesten en activity monitoring
Militaire Hacker	25-45 jaar	Alleen/Groep	Monitoren / crash testen / beheersen systemen

Hacks en hackers: een geschiedenis

Nu we een idee hebben gekregen van de hackerswereld en iets meer weten over de mens achter het masker, is de volgende vraag: is hacking een nieuw fenomeen of krijgt hacking domweg meer media-aandacht?

Beroemde hacks

Volgens een recent artikel[4] in een Nederlands computertijdschrift (CHIP) is hacking niet nieuw. Het artikel stelt dat de allereerste hack al uitgevoerd werd in 1184 voor Christus toen het beroemde Paard van Troje werd achtergelaten op het strand. Zo zijn er meer historische hacks geweest. Denk daarbij aan het kraken van de Enigmacode en aan de recentere cyberaanvallen. Hieronder een historisch overzicht van beroemde hacks.

Datum	Naam	Hack
1184 (v. Chr.)	Paard van Troje	Een Grieks aanvalsleger verstopt in een groot houten paard dat achtergelaten werd op het strand. Tegenwoordig synoniem voor malware (code).
1939	Enigma	Een internationaal team van cryptologen kraakt de Duitse Enigmacode.
1961	Space War	Steve Russell programmeert de eerste computer game, Space War, op een onderzoekscomputer op MIT University (Massachusetts, VS).
1971	Blue Box	John T. Draper slaagt erin om het AT&T voice response dialing-systeem te bedienen met een simpel fluitsignaal. Hierna wordt het Blue Box-programma ontwikkeld waarmee gratis telefoongesprekken gevoerd kunnen worden.
1984	Btx-hack	De Computer Chaos Club (CCC) steelt €135.000 door in the breken in de beveiliging van het Bildschirmtextsysteem. Een dag laten geven ze het geld terug.
1988	Morris-worm	Robert Tappan Morris codeert het eerste computerwormprogramma op 23-jarige leeftijd.
1993	Green Building	Studenten aan de MIT University maken een enorme decibelmeter in hun studentenflat op de campus.
1999	DeCSS	Jon Lech Johansen, een 15-jarige (!) Noor kraakt de cryptografische code van Dvd's.
2000	I Love You	Deze computerworm, ingepakt als 'I love you'-bericht gaat de hele wereld over en veroorzaakt miljoenen schade.
2007	Estonia	Cyberaanvallen gelanceerd op de overheid, het parlement, banksystemen en de media in Estland.
2010	Stuxnet	Een computerworm speciaal ontwikkeld om industriële IT-infrastructuren aan te vallen. De worm had als doelwit Iranese kerncentrales en industriële software voor het verrijken van uranium.

[4]CHIP magazine, 2012, editie 91, uit het artikel 'Historic Hackers', door Manuel Köppl en Peter Marinus.

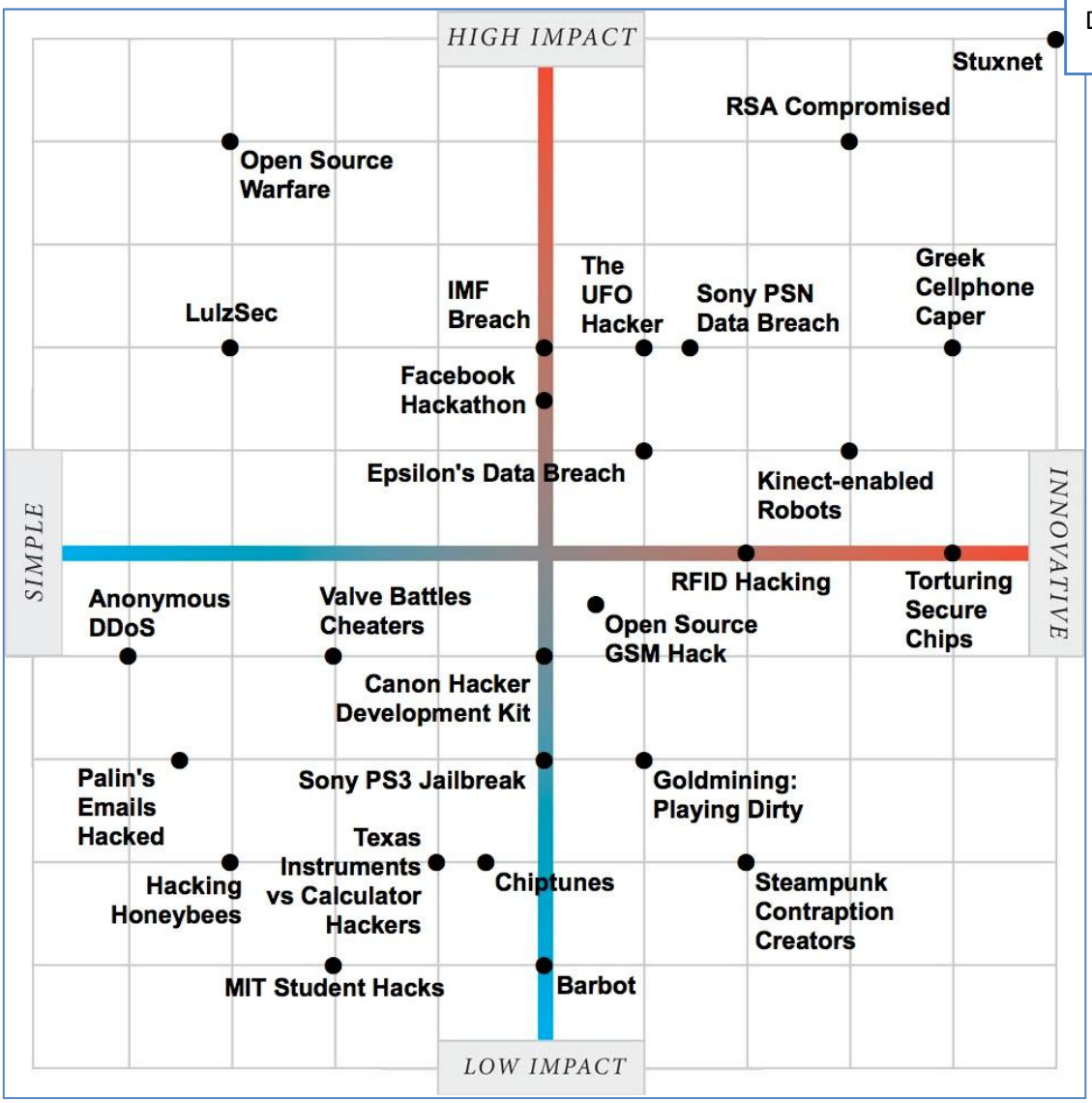
		Hoewel niemand uit de regering de verantwoordelijkheid opeiste voor Stuxnet, waren de frontlinies van IT-beveiliging er 100% van overtuigd dat een overheidsinstelling verantwoordelijk was voor het creëren van de worm, zoals bijvoorbeeld cryptologen van de Amerikaanse National Security Agency of een soortgelijke organisatie uit Israel of Groot Brittannië.
2010	Kinect	Fans van de Xbox 360 die geen zin hadden om te wachten op de officiële lancering van de nieuwe Kinect hardware, ontwikkelden zelf een programmeercode om de Kinect te simuleren.
2011	PSN-hack	Tijdens een aantal hacks op het Sony PlayStation Netwerk werden meer dan 1.000 creditcardgegevens van klanten buit gemaakt. Nadat het Playstationnetwerk een week uit de lucht was geweest gaf Sony het toe: "Er zijn gebruikersgegevens gecompromitteerd in verband met een illegale en ongeoorloofde inbraak op ons netwerk."
2011	DigiNotar	Op 29 augustus 2011 werd bekend dat er een frauduleus DigiNotar beveiligingscertificaat voor het Googledomein Google.com was uitgegeven aan iemand in Iran als gevolg van een hack. Dit voorval leidde tot het faillissement van DigiNotar
2011	Duqu	De nieuwe generatie Stuxnet. Deze superworm is waarschijnlijk het geesteskind van een veiligheidsdienst van een regering.
2012	Cyberoorlog	Volgens diverse IT-beveiligingsexperts zullen cyberaanvallen uitgevoerd door regeringen en overheidsinstanties zich ook gaan richten op energie- IT-infrastructuren.
2012	Flame	Ontwikkeld door professionele softwareprogrammeurs. Een geavanceerde architectuur en een scripttaal met de naam Lua die hackers de mogelijkheid biedt maatwerkmodules te creëren voor aanvallen. Flame bevat een SQLite database voor het verzamelen en opslaan van informatie.

"Hacking matrix"

Leuk zo'n historisch overzicht van beroemde hacks, maar een interessante vraag is nu: wat is de impact van zulke hacks? Heeft iedere hack evenveel grote en destructieve gevolgen of kunnen we onderscheid maken in niveaus en innovatief karakter? Het IEEE (Institute of Electrical and Electronics Engineers [5]) maakte de zogeheten "Hacking Matrix" [6] om de bovengenoemde hacks te rangschikken op niveau van impact en innovativiteit. Ze kozen de 25 grootste en beste verhalen (hacks) uit en beoordeelden die op basis van twee peilers: impact en innovatie. Het resultaat is een model waarin hacks in grofweg vier categorieën zijn opgedeeld:

[5] IEEE is een non-profitorganisatie en tevens 's werelds grootste professionele vereniging voor de vooruitgang van technologie.
[6] http://spectrum.ieee.org/static/hacker-matrix

Flame? / Duqu?



Hacking matrix

Beroemde hackers

Nu we meer weten over beroemde hacks en hun impact, is het tijd voor de hackers zelf. In zijn artikel 'The ten biggest legends of the hacker universe'[7] publiceerde Carlos Cabezas López een lijst van de personen achter de hacks. Zelf heb ik er nog twee (groepen) aan toegevoegd die niet mochten ontbreken: Anonymous and Lulzsec.

[7] The Ten Biggest Legends of the Hacker Universe, http://voices.yahoo.com/the-ten-biggest-legends-hacker-universe-369297.html

Naam	Hack
Kevin Mitnick	Staat wereldwijd bekend als de "beroemdste hacker" en voor het feit dat hij de eerste was die een gevangenisstraf uitzat voor het infiltreren in computersystemen. Hij begon al jong te experimenteren en gebruikte een methode die bekend staat als 'phone phreaking'. Hoewel Mitnick nooit werkzaam is geweest als programmeur is hij ervan overtuigd dat fikse schade kan worden aangericht met een telefoon en bellen. Tegenwoordig, na een lange gevangenisstraf, heeft hij afstand genomen van zijn oude hobby en werkt hij al beveilingsconsultant voor multinationals met zijn bedrijf "Mitnick Security."
Gary McKinnon	Deze 41-jarige Schot, ook wel bekend als Solo, is het brein achter wat wel de grootste hack in de geschiedenis van de informatica wordt genoemd. Doelwit was een militair systeem. De Schot maakte later (2001 en 2002) een lachertje van de beveiliging van NASA en het Pentagon. Momenteel zit McKinnon in de gevangenis en heeft hij geen toegang tot een computer met internet.
Vladimir Levin	Deze Russische biochemicus en wiskundige werd beschuldigd van het plegen van een van de grootste bankovervallen van alle tijden met behulp van een crackingtechniek. Levin slaagde erin om vanuit St. Petersburg via de Citibank in New York fondsen over te maken van ongeveer 10 miljoen dollar naar diverse rekeningen die hij overal ter wereld had geopend. Interpol arresteerde hem in 1995 op vliegveld Heathrow. Ondanks dat hij 10 miljoen dollar buit maakte, kreeg hij slechts drie jaar gevangenisstraf. Hij is inmiddels weer vrij.
Kevin Poulsen	Hij mag dan tegenwoordig een journalist zijn die samenwerkt met de autoriteiten om pedofielen op het internet te achterhalen, maar Poulsen heeft een duister verleden als cracker en phreaker. Hij is het meest berucht om het feit dat hij in 1990 het telefoonnetwerk in Los Angeles kraakte nadat een radiozender een Porsche uitloofde voor diegene die beller 102 zou zijn. Het spreekt voor zich wie de Porsche won: Poulsen.
Timothy Lloyd	In 1996 kreeg Omega, een informatie services bedrijf dat diensten levert aan NASA en aan de Amerikaanse Marine, te maken met een verlies van zo'n 10 miljoen dollar. Het was niemand minder dan Tim Lloyd, een voormalige werknemer die een paar weken ervoor was ontslagen, die hier achter zat. Lloyd liet voor zijn vertrek een virtuele informatiebom achter in de bedrijfssoftware die afging op 31 juli 1996.
Robert Morris	In 1988 krijgt Morris, zoon van een van de bedenkers van het computervirus, het voor elkaar om maar liefst 6.000 computers die verbonden zijn aan ArpaNet (voorloper van internet) te infecteren. Hij doet dit vanaf de befaamde MIT University in Massachusetts. Morris wordt vier jaar gevangenisstraf opgelegd die uiteindelijk wordt teruggebracht tot een taakstraf.
David Smith	Niet alle hackers kunnen zeggen dat ze het snelstverspreide computervirus wereldwijd hebben gemaakt. David Smith kan dat wel. In 1999 slaagde de bedenker van het Melissavirus erin om 100.000 e-mailaccounts te infecteren en te laten crashen. Smith was toen 30 jaar oud. Hij kreeg een straf opgelegd

	maar kwam op borgtocht vrij.
MafiaBoy	In februari 2000 kregen veel van de grote internetbedrijven in de VS, waaronder eBay, Yahoo en Amazon te maken met een totaalverlies van 1.7 miljard dollar als gevolg van een technisch probleem genaamd Denial of Service. Ze wisten toen nog niet dat de veroorzaker hiervan een 16-jarige Canadees was met de alias MafiaBoy? Daar kwamen ze echter vrij snel achter omdat het ventje het niet kon laten op school op te scheppen over zijn daad.
Richard Stallman	Deze New Yorker met een hippie-uitstraling is al sinds begin jaren '80, toen hij hacker was met als specialisme kunstmatige intelligentie, een van meest actieve, militante voorstanders van gratis software. Hij verzette zich flink tegen de privatisering van de software van laboratorium op MIT University en creëerde wat nu bekend staat als GNU evenals het concept CopyLeft. Populaire systemen zoals Linux maken gebruik van GNU en Stallman is momenteel een van de goeroes op het gebied van het democratiseren van software.
Masters of Deception (MoD)	MoD was een cybergang uit New York die hoogtij vierden begin jaren '90 met diverse aliassen als dekmantel. Hun grootste aanvallen betroffen het overnemen van het telefoonnetwerk en internetcentra (internet bestond nog maar net). MoC naam deel aan de historische "battles of the hackers" samen met andere groepen zoals de Legion of Doom (LoD) met als doel elkaar net zolang te vernietigen totdat de computer het niet meer aankonden.
Anonymous[8]	"Hello World. We are Anonymous. What you do or do not know about us is irrelevant. We have decided to write to you, the media, and all citizens of the free world to inform you of our intentions, potential targets, and our ongoing, active campaign for the freedom of information exchange, freedom of expression, and free use of the Internet." (Manifest Anonymous)
Lulzsec[9]	Lulz Security, vaak afgekort als LulzSec, was een hackersgroep die de verantwoordelijkheid opeiste voor diverse high profile aanvallen waaronder het compromitteren van gebruikersaccounts van Sony Pictures in 2011. Ook eiste de groep verantwoordelijkheid op voor het uit de lucht halen van de website van de CIA. Sommige beveiligingsexperts zeggen dat de acties van LulzSec hun ogen hebben geopend voor de gevaren van onveilige systemen en hergebruik van wachtwoorden. Lulzsec kreeg veel aandacht vanwege de prominente doelwitten en door hun sarcasme. Een van de oprichters van LulzSec is een computerbeveiligingsspecialist die online onder de naam Sabu werkte. De man die verdacht werd Sabu te zijn hielp justitie bij het achterhalen van de andere leden van de groep in ruil voor strafvermindering. Zeker vier medeplichtigen werden gearresteerd in maart 2012. Vlak daarvoor hadden de Britse autoriteiten ook twee tieners gearresteerd die verdacht werden lid te zijn van LulzSec: T-flow and Topiary.

[8] http://www.indybay.org/newsitems/2010/12/09/18666107.php, http://nl.wikipedia.org/wiki/Anonymous_(groep)
[9] http://nl.wikipedia.org/wiki/LulzSec

De hack zelf: soorten, doel en methode

We weten nu meer over hackers, hacking, phreaking en cracking en van de impact die zij kunnen veroorzaken met in sommige gevallen vernietigende consequenties. Nu is het tijd om wat dieper te graven en te kijken naar de hack zelf: de type hacks, de doelen en de methodes.

We maken onderscheid tussen twee soorten hacks: de 'normale' hack en de zogeheten ethische hack. Een normale hack is bij wet verboden en dus strafbaar, een ethische hack echter is een hack op aanvraag: de aanvrager en de hacker werken op basis van een vooraf wederzijds overeengekomen contract.

Het belangrijkste doel van een hack is toegang krijgen tot IT-systemen, gevoelige informatie en andere bronnen. Om dit te bereiken probeert de hacker administratorrechten of toegangsrechten voor de root te krijgen. Heeft hij zulke rechten dan heeft hij volledige controle over het systeem of netwerk en kan hij zijn sporen wissen, backdoors creëren en op zoek gaan naar een volgend slachtoffer.

Doelen en methodes

In het algemeen zijn er twee doelstellingen voor hacken. De eerste doelstelling is om een botnet te creëren en daarmee SPAM-runs en DDoS-aanvallen uit te voeren. De tweede doelstelling is om in te breken in een systeem om gevoelige informatie te kunnen stelen en te ontrekken via normale IT-communicatiekanalen of geconverteerde netwerkkanalen.

Botnet

Een *botnet* bestaat uit een grote groep geïnfecteerde computers. Het *botnetvirus* verstopt zich op de PC van het slachtoffer en doet zijn best om ongezien te blijven. Het botnetvirus kan onjuiste of vervalste resultaten meegeven aan antivirussoftware door deze software te laten denken dat computer niet geïnfecteerd is. Daarnaast is het botnetvirus in staat om nieuwe virussen te creëren. Na een succesvolle infectie met een botnetvirus wordt de computer van het slachtoffer onderdeel van de botnet en wordt dan een zombiecomputer of *bot* genoemd. Bots en botnets zijn een veelvoorkomende vorm van internetcriminaliteit en een krachtige tool voor hackers. Botnets kunnen relatief klein zijn en slechts een paar honderd zombiecomputers bevatten, maar sommige botnets bestaan uit maar liefst honderdduizenden bots of zelfs meer.

- SPAM is een collectieve benaming voor ongewenste (e-mail-)berichten en voor ongevraagde junkmailadvertenties op websites. SPAM verschilt van de andere vormen van commerciële communicatie omdat het bericht verzonden wordt naar een groep die veel groter is dan de potentiële doelgroep. Kenmerken van SPAM berichten zijn:

- Verzonden in grote aantallen. Tot wel (honderd-)duizend geadresseerden gelijktijdig.
- Een commercieel doel. Een SPAM bericht bevat normaal gesproken een verwijzing naar een product of (commerciële) website.
- Verzonden of gepost zonder toestemming of zonder medeweten van de eigenaar of zonder voorafgaande goedkeuring van de ontvanger.

Het idee achter een SPAM bericht is om het slachtoffer te verleiden naar een nepwebsite te gaan waarna een zogeheten dropper malware installeert op de PC van het slachtoffer of om mensen te over te halen een bijlage te openen die vervolgens kwaadaardige software installeert.

- DDoS: Denial-of-Service-aanvallen (DoS) en Distributed Denial-of-Service-aanvallen (DDos) zijn pogingen om computerservices uit te schakelen of te verstoren voor de beoogde gebruikers. Het verschil tussen een Dos en een DDos-aanval is dat laatstgenoemde meerdere aanvallen tegelijkertijd uitvoert op meerdere computers, meestal een botnet. Soms zitten er ook meerder hackers (een groep) achter die deze attacks coördineren (zoals Anonymous). Het motief is en blijft: het uitschakelen of verstoren van services voor de beoogde gebruikers.

  De meestvoorkomende netwerkgebaseerde Denial-of-Service-hacks zijn in te delen in twee categorieën: zogeheten *malformed packet attacks* en *packet floods*:

  - *Malformed packets attacks*: deze aanvallen bestaan meestal uit een of twee 'packets' die op een onverwachte manier zijn geformatteerd. Als de software deze fouten slecht verwerkt is de kans groot dat het systeem crasht na het ontvangen van zo'n packet.
  - *Packet Floods*: de aanvallen sturen een stortvloed van verkeer naar een systeem op het netwerk met als gevolg dat het systeem overspoelt raakt en niet meer correct kan reageren naar legitieme gebruikers. Hackers hebben diverse technieken ontwikkeld om zulke stortvloeden te creëren. De meest populaire zijn de zogeheten SYN-flood, 'directed broadcast attacks' en gedistribueerde Denial-of-Service-tools.

Data exfiltreren

In computertechnologie verwijst *exfiltratie* naar het ongeautoriseerd vrijgeven van gegevens uit een computersysteem. Dit is inclusief het kopiëren van gegevens via verborgen datacommunicatiekanalen of het kopiëren van data naar onbevoegde media.

Organisaties proberen hun infrastructuur zo te bouwen dat gevoelige gegevens beschermd zijn en dat mensen met verkeerde bedoelingen worden geweerd. Maar als het hackers toch lukt om in te breken in de IT-infrastructuur dan zijn er heel wat mogelijke manieren om gevoelige gegevens op te halen, zelfs versleutelde gegevens. Methodes van exfiltratie zijn:

- Informatie verzenden via bestaande protocollen zoals DNS (Domain Name Services) en HTTP (Hyper Text Transfer Protocol). Om te voorkomen dat de gevoelige gegevens worden tegengehouden door Data Leakage Prevention oplossingen (DLP) versleuteld de hacker versleuteld de gevoelige informatie met zijn 'public key' en verzend de gegevens via diensten zoals Dropbox, Facebook, Twitter of blogcomments. Deze diensten worden vaak niet gefilterd door controlemechanismes van de organisatie.
- Een andere methode van exfiltratie is printen. Versleutelde data worden verzonden naar en bedrijfsprinter. Zulke printjes eindigen vaak simpelweg in de prullenbak en niet in de papierversnipperaar. De documenten worden achterhaald met ouderwets vuilnissnuffelen (Dumpster diving). Daarna is het eenvoudig: OCR'en en decoderen en de buit is binnen.
- Naast printers bieden ook faxapparaten dezelfde mogelijkheden.
- De laatste methode voor het exfiltreren van data is door gebruik te maken van het VoIP-netwerk. VoIP-netwerken zijn gewoonlijk toegankelijk via het lokale netwerk. Gevoelige informatie wordt geconverteerd van binair naar een audio-formaat en dan verzonden via het VoIP-netwerk.

Ethisch hacken

Ethisch hacken is het bekijken van de IT-infrastructuur van een organisatie door de ogen van een hacker. Het doel is om de sterkte van de beveiliging van het doelwit te testen. Ethisch hacken gebeurt meestal op basis van vooraf overeengekomen afspraken over hoe om te gaan met de gevonden kwetsbaarheden. Dit kan variëren van slechts een rapportage tot aan het daadwerkelijk exploiteren of oplossen van het lek.

Trouwens: een hacker die contact opneemt met uw bedrijf met de mededeling dat hij een ethische hack heeft uitgevoerd en lekken in de beveiliging heeft ontdekt waarover hij graag met u wenst te praten is geen ethische hacker, maar een criminele en is strafbaar volgens artikel 138ab van het Nederlandse wetboek van Strafrecht.

Er zijn diverse manieren om een ethische hack uit te voeren. De bekendste drie zijn:

- Whitebox testen: de hacker ontvangt vooraf informatie over het doelsysteem
- Blackbox testen: de hacker ontvangt vooraf geen informatie over het doelsysteem
- Greybox testen: een combinatie van de twee bovenstaande methodes.

Het is belangrijk om vooraf solide afspraken te maken met de hacker en die afspraken vast te leggen in een wettelijk contract voordat er getest wordt. Een dergelijke overeenkomst moet op zijn minst het volgende bevatten:

- Vastgelegde en ondertekende afspraken over doel, tijden, contacten, waarschuwingen en verantwoordelijkheden.
- Vastgestelde en ondertekende afstandsverklaringen en autorisatiedocumenten.
- Vastgelegde en ondertekende afspraken over archivering, vernietiging en bewaartermijn van de observaties.

Let op: wanneer je een ethische hacker inhuurt om een veiligheidstest uit te voeren op uw IT-omgeving, dan kunnen er dingen misgaan: servers die uit de lucht zijn, netwerkcomponenten kunnen uitschakelen en gevoelige informatie kan verloren gaan of gewijzigd worden. Het is dus heel belangrijk om een businesscontinuïteitsplan te hebben of op zijn minst een complete en gesteste back-up te hebben die bewaard wordt op een veilige plaats. Dit alles voorafgaand aan iedere penetratietest

Social Engineering

Social engineering[10] is eerder een psychologische aanvalsvector dan een technische. Het is de mensgerichte manier van inbreken in bedrijfs- en persoonlijke computers om zo informatie te verkrijgen. Social engineering is een methode om de zwakste schakel (namelijk de mens) te verleiden iets te doen of om gevoelige informatie af te staan zonder dat dat nodig of noodzakelijk is. Elk bedrijf, ook al is het in het bezit van een goed authenticatieproces, een firewall, VPN's of netwerkmonitoringsoftware, kan het slachtoffer worden van een bekwame social engineer. Waar hacken vooral steunt op technische vaardigheden, steunt social engineering vooral op de techniek van het overtuigen: de social engineer probeert zijn slachtoffer over te halen informatie te geven waarmee hij kan inbreken in het systeem. In de meeste gevallen gebeurt dat niet face-to-face. Ze kennen elkaar niet. Social engineering maakt gebruik van het menselijke besluitvormingsproces dat bekend staat als 'coginitive biases'. Vaak zijn dat denkfouten of redeneerfouten. Social engineers gebruiken verschillende technieken, een overzicht:

- *Pre-texting*: een vals scenario creëren waar een beoogd slachtoffer zich in kan vinden en zich comfortabel genoeg voelt om informatie te geven. Deze techniek behelst meer dan simpel liegen. In sommige gevallen is een gezaghebbende en eerlijk klinkende stem voldoende, maar meestal doet de social engineer zich voor als een bekende (iemand die het slachtoffer vertrouwd) zodat men denkt dat het OK is om de gevraagde informatie te geven.

[10] The Hacker News, mei 2011 - editie 02 - Social Engineering Editie

- *Diversion theft*: het doel hiervan is om goederen om te leiden naar een andere locatie. De social engineer haalt de beheerder of het transportpersoneel over om de chauffeur te instrueren de goederen naar een ander adres te transporteren.
- *Phishing:* een populaire frauduleuze e-mailtechniek met als doel persoonlijke informatie te verkrijgen. Een e-mail wordt verzonden van wat lijkt een betrouwbare organisatie te zijn en het bericht bevalt meestal een soort waarschuwing dat het consequenties heeft als de ontvanger zijn gegevens niet afstaat. Phishing gaat soms ook samen met websites die lijken op de website van een legitieme organisatie, maar dat niet zijn, om slachtoffers te overtuigen dat het OK is om financiële of persoonlijke details af te verschaffen.
- *IVR of phone phishing*: het idee is hetzelfde als bij phishing maar in dit geval worden beoogde slachtoffers gevraagd, via een e-mail of brief van een gefungeerde autoriteit, om hen terug te bellen. Deze methode van phishing wordt ook wel 'vishing' genoemd.
- *Baiting:* een techniek zoals die van het 'echte' Trojaanse Paard die fysieke apparaten (opslagmedia) gebruikt en die gokt op de nieuwsgierigheid en hebzucht van het slachtoffer. De social engineer laat een media-apparaat, zoals een USB-stick of CD-rom met een legitiem uitziende label dat de nieuwsgierigheid wekt, achter op een plek waar het zeker gevonden. Doel is dat de vinder het apparaat gaat inlezen. Doet hij dat, dan wordt er malware geïnstalleerd waarmee de social engineer volledig toegang heeft tot de PC of het interne netwerk van het slachtoffer.
- *Quid pro quo*: ofwel: "ik geef wat, jij geeft wat". De social engineer biedt zijn beoogde slachtoffer iets aan (geld, cadeau) in ruil voor wachtwoorden of andere persoonlijke informatie.

Social engineers zijn niet enkel technisch, ze weten ook goed hoe ze gebruik (of misbruik) kunnen maken van menselijke zwaktes zoals gevoeligheid voor autoriteit, inleven in de 'problemen' van een ander, empathie, gevoeligheid voor charme, iets willen beteken voor een ander en de gevoeligheid voor druk en urgentie.

Het aanvalsplan en de fasering van de social engineer is bijna gelijk aan die van een technische hack. Een groot deel van de tijd zit hem in de eerste fase: de voorbereiding en het vertrouwen winnen van het potentiële slachtoffer. De volgende fase is om een strategie of aanvalsplan te bepalen.

De belangrijkste maatregel tegen social engineering is het creëren van een overkoepelend 'security awareness'-programma. Train je gebruikers op regelmatige basis en test de effectiviteit van het plan door weerbaarheidtests uit te voeren zoals een penetratietest, het gebruiken van mystery guests en met online testprogramma's.

Fases van een hack (hoe het werkt)

Nu we meer weten over de methodes, types en doelen van een hack en inzicht hebben gekregen in welke technieken hackers toepassen, is het tijd om specifiek naar de hack zelf te kijken in detail. Hacks zijn meestal opgebouwd in fasen. Deze fasen, acht in totaal, worden in dit hoofdstuk beschreven.

Footprinten

Het doel van footprinten is om algemene informatie te verkrijgen over het doelwit via publieke informatie op websites, in telefoongidsen, de Gouden Gids of via de Kamer van Koophandel. Bruikbare informatie voor de hacker zijn naam- en adresgegevens van werknemers, telefoonnummers, functienamen en organisatieschema's. Deze informatie zal worden gebruikt voor de hack zelf of in een aanvalsplan van een social engineer.

Doel: zoveel mogelijk te weten komen over het potentiële doelwit bijvoorbeeld adres- en naamgegevens. Het verzamelen van informatie is essentieel voorafgaand aan de aanvalsoperatie. Belangrijk is om niets over het hoofd te zien.

Techniek: zoekopdrachten in publieke zoekmachines en websites (Pipl, Google, Facebook), Whois queries en DNS zone transfers.

Tools: Usenet, Sam Spade, UNIX clients, ARIN database.

Een speciale focus tijdens de footprintingfase legt de hacker op specifieke ICT-informatie, de namen van (IT-)managers, en informatie over systemen, netwerken en applicaties. Daarvoor gebruiken hackers vaak communicatiekanalen zoals Usenet en IRC maar ook geautomatiseerde tools zoals Whois, Netcraft en Google.

De footprintingfase neemt soms wel tot 80% in beslag van de totale tijd die nodig is om een hack uit te voeren. Hoe meer tijd de hacker besteedt aan footprinten, hoe meer gedetailleerde informatie hij heeft om vast te stellen waar de zwakke plekken zitten en hoe groter zijn kans is op succes.

Scannen

Scannen is het zoeken en vaststellen van hosts, het scannen voor open poorten en het vaststellen van services en de bijbehorende softwareversies. De informatie uit de footprintingfase wordt gebruikt bij het scannen.

Doel: beoordelen van grote hoeveelheden doelwitten en identificeren van 'listening services' om de beste methode van toegang te achterhalen.

Techniek: Ping sweep, TCP en UDP poortscans

Tools: Nmap, scan.exe, fping, bindview, webtrends, ws_ping propack

Er zijn vier type scans:

1. IP-scan: systematisch een reeks IP-addressen scannen.
2. Poortscan: een verbinding opzetten met een applicatie die een specifieke poort afluistert.
3. Fingerprinting: vaststellen welke softwareversie de geïdentificeerde hosts draaien.
4. Bannerinfo: sommige applicaties geven informatie weg in zogeheten bannerinformatie.

Enumeratie

Enumeratie wordt ingezet als stap om meer en gedetailleerde informatie te achterhalen over gebruikersaccounts, netwerkshares en servicest. Enumeratie is de eerste 'aanval' op het doelnetwerk. Tijdens deze fase verzamelt de hacker gedetailleerde informatie over het doelwit (systemen en netwerken) en hun reactie op de scans.

Doelstelling: achterhalen gebruikersaccounts, onbeveiligde netwerkshares en andere IT resources.

Technieken : Lijsten van de gebruikersaccounts, lijsten van bestandsshares, identificeren van toepassingen en hun reacties.

Tools: DumpACL, NULL sessions, Onsight Admin, Show MOUNT, NAT, Banner grabbing met Telnet of netcat, rpcinfo, and het gebruik van standard ingebouwde Windows programma's (Windows 9x and later), zoals nbtstat, netstat en net nadat de command prompt verkregen is.

Toegang verkrijgen

Tijdens deze fase is het doel om daadwerkelijk toegang te krijgen tot IT resources, accounts en/of informatie. Dit kan alleen succesvol zijn als de juiste toegangsrechten zijn verkregen. Hiervoor kunnen ook social engineeringtechnieken of exploits worden gebruikt. Het doel van de hacker is om admin- of rootrechten te verkrijgen. Met deze rechten kan hij rootkits of Trojaanse Paarden installeren om zo de toegang tot het systeem te blijven behouden. Trojaanse Paarden vertrouwen op bedrog: ze verleiden de gebruiker of systeembeheerder het programma 'starten' omdat ze zogenaamd van pas komen, maar hun daadwerkelijke doel is om het systeem, of de machine aan te vallen. Als een hacker eenmaal superuser rechten heeft, kan hij deze behouden met rootkits. Rootkits verijdelen de pogingen die een systeembeheerder doet om de aanval te detecteren.

Doel: in deze fase heeft de hacker genoeg gegevens om op basis van kennis een poging te doen in te breken in het systeem.

Techniek: password eavesdropping, file share brute force, password file grab, buffer overflows

Tools: TCPdump, l0phtcrack, NAT, Legion, tftp, pwdump, ttdb, IIShack

Privilige escalation

Het doel van escalating privileges is gelijk aan de vorige fase: volledige toegang verkrijgen tot IT reosurces, accounts en informatie, maar ditmaal gaat de hacker op zoek naar volledige controle over een systeem of netwerk met als ultiem doel het overnemen van de gehele IT-infrastructuur.

Doel: volledige controle over het systeem. Als de hacker daarin slaagt, heeft hij de IT-infrastrcutuur geheel in beheer.

Techniek: kraken van wachtwoorden, exploits.

Tools: crack, l0phtcrack, rdist, getadmin en sechole.

Pilfering

Het doel van de pilferingfase is om toegang te krijgen tot vertrouwde systemen en gevoelige informatie. Deze fase combineert de uitkomsten van de vorige fases met de nieuwe informatie gevonden op overgenomen beveiligde systemen en de beveiligide locaties van gevoelige informatie.

Doel: identificeren van mechanismen om toegang te verkrijgen tot beveiligde systemen en gevoelige informatie.

Techniek: evaluate trust, zoeken naar clear-text-wachtwoorden.

Tools: rhosts, LSA secrets, user data, configuratiebestanden, register.

Sporen uitwissen

Een hacker wil niet enkel toegang tot een systeem, maar wil de controle over zijn doelwit ook graag in stand houden. Daarvoor dient hij zijn sporen te kunnen wissen. Dat doet hij in de meeste gevallen door het logsysteem te manipuleren.

Doel: trapdoors creëren op diverse plekken van het systeem om zo te garanderen dat de eerder verworven toegangsrechten makkelijk opnieuw te gebruiken zijn op elk gewenst moment.

Techniek: malafide gebruikersaccounts aanmaken, batch jobs inplannen, opstartbestanden infecteren, remote access services inzetten, monitoringmechanismes installeren en applicaties vervangen door Trojaanse Paarden.

Tools: 'members of the wheel', administratie, CRON, AT, rc, opstartmap, registersleutels, netcat, remote.exe, VNC, keystroke loggers, add account, mailaliassen, login, fpnwclnt.dll

Om niet ontdekt te worden, gebruikt de hacker verborgen datacommunicatie kanalen en manipuleert of verbergt hij zijn reguliere datacommunicatie. Ook omzeilt hij bestaande beveiligingsmaatregelen. De hacker manipuleert de log door deze volledig uit te zetten, fictieve logregels toe te voegen, of door de logniveaus aan te passen.

Backdoors creëren

Als een hacker eenmaal toegang heeft verworven tot een systeem wil hij kunnen garanderen dat hij "onopgemerkt" terug kan komen. Daarvoor installeert hij een backdoor of rootkit. Een backdoor is een programmaatje dat de bestaande veiligheidscontroles op een systeem omzeilt waardoor de hacker toegang heeft tot een computer zonder wachtwoord en zonder gelogd te worden.

Doel: mechanismes identificeren om toegang te krijgen tot beveiligde systemen en gevoelige informatie.

Techniek: evaluate trust, zoeken naar clear-text passwords.

Tools: rhosts, LSA secrets, user data, configuratiebestanden, register.

Preventie: een hack voorkomen

Misschien wel de meeste waardevolle informatie over hacken is informatie over preventie. Ofwel: hoe wordt je niet gehackt? Waaraan herken je een hack? Daarover gaat dit hoofdstuk: over algemene en specifieke maatregelen tegen hacking.

Algemene beveiligingsmaatregelen

Beveiligingsmaatregelen zijn er in diverse soorten en maten en dienen geïmplementeerd te worden in overeenstemming met hun doelstelling. Er zijn vijf soorten beveiligingsmaatregelen:

- Directieve: maatregelen om gewenste gebeurtenissen te veroorzaken of aan te moedigen. Directieve maatregelen zijn breed van aard en toepasbaar in alle situaties.
- Preventieve: het detecteren van problemen voordat ze zich voordoen. Proberen om potentiële problemen vooraf te voorspellen en noodzakelijke aanpassingen doen.
- Detectieve: fouten, nalatigheden en kwaadaardige acties opsporen en rapporteren.
- Correctieve: de impact van een dreiging minimaliseren: problemen die worden opgemerkt door detectieve maatregelen oplossen, de oorzaak van het probleem identificeren en fouten als gevolg van een probleem corrigeren.
- Compenserende: maatregelen die niet effectief zijn compenseren. Compenseren maatregelen die helpen het beheersdoel te bereiken en tevens kosteneffectief zijn, kunnen als adequaat beschouwd worden.

Soort	Voorbeelden
Directief	• Organisatiestructuur • Beleidsplannen • Procedures • Managementrichtlijnen • Begeleidende verklaringen/teksten • Handreikingen • Functieomschrijvingen
Preventief	• Tijdig blokkeren van accounts • Zones met beperkte toegang, kluizen en nachtelijk toezicht • Planningen, doelen, budgetten en vergelijking van budget vs. actual • Procedurele handleidingen • Onderzoeken verleden nieuwe werknemers • Alleen gekwalificeerd personeel aannemen • Scheiden van taken (afschrikfactor) • Beheren van fysieke faciliteiten • Goed ontworpen documenten gebruiken (fouten voorkomen) • Zorg voor passende procedures voor de autorisatie van transacties • Volledig geprogrammeerde editcontroles

	• Gebruiken van toegangscontrolesoftware zodat alleen geautoriseerd personeel toegang heeft tot gevoelige gegevens • Gebruik encryptiesoftware om ongeloorloofde vrijgave van data te voorkomen
Detectief	• Voer analyses uit op openstaande vorderingen debiteuren • Opstellen van inspectieprocedures voor inkomende goederen • Zorg ervoor dat personeelszaken het aannemen van personeel en het vastellen en wijzigingen van salarisschalen autoriseert • Zorg voor bestaande managementgoedkeuringen, dubbele controles, systeemtoegangcontroles en supervisie-evaluatie • Implementeer een werkordersysteem voor het bijhouden van onderhoudskosten • Gebruik vooraf genummerde controles • Laat alle werknemers verplicht een jaarlijkse vakantie nemen • Voer periodieke audits uit • Hash totals • Controlepunten in productiejobs • Echocontrols in datacommunicatie • Foutmeldingen op tapelabels • Dubbelchecken van berekeningen • Periodieke performancerapportages • Rapportages aangaande achterstallige betalingen • Evalueren van activity logs om pogingen tot ongeautoriseerde toegang te kunnen detecteren
Correctief	• Uitwijkplannen opstellen • Back-up en herstelprocedures • Rerunprocedures • Foutdetectie en reruns • Audit trails • Verschillenrapportages • Foutstatistieken
Compenserend	• Afgestemde batchcontroles • Transactielogs • Redelijkheids testen • Onafhankelijke reviews en audit trails, zoals console logs, library logs en account datum controles • Volgordecontroles en controlecijfers • Bewaren en opslaan van sourcedocumentatie

Een hack identificeren

Identificeren richt zich op ontdekken van een hacker, bij voorkeur nog voordat de hack plaatsvindt. Het identificatieproces bevat twee subprocessen: auditing en security monitoring. Auditing focust op het vinden van kwetsbaarheden, beveiligingslekken en ineffectieve instellingen. Security monitoring heeft tot doel afwijkingen te detecteren.

Auditing

Vulnerability scanners zijn tools voor real-time controles, ofwel auditing. De resultaten van de scans kunnen worden gebruikt als input voor de oplossingsrichting en voor het proces patch management[11]. Vulnerability scanners kunnen zowel netwerk-based als host-based zijn.

Wachtwoordcontroletools hebben als doel om wachtwoorden die in gebruik zijn te toetsen aan de eisen van het beleid. Het komt nogal eens voor dat voorschriften niet gehandhaafd worden en ook niet periodiek gecontroleerd worden. Vooral voor gebruikerswachtwoorden geldt dat het lastig is een goede balans te vinden tussen gebruiksgemak en veiligheid. Momenteel zijn gebruikerswachtwoorden van 10 tekens acceptabel. Voor beheerderwachtwoorden geldt een minimum van 14 tekens. Nog beter is echter om two-factor authenticatie toe te passen voor administrators.

Integriteitscontroles zijn er om wijzigingen in bestanden te ontdekken. De checksum-waarden uit deze bestanden worden periodiek vergeleken met eerdere waarden.

Security monitoring

Security monitoring heeft als doel afwijkingen te detecteren door (real-time) gebeurtenissen te analyseren. Het is te goed om hierbij rekening te houden met de events uit de fysieke beveilingsomgeving zoals inbraakalarmen, videobeelden (CCTV), personeelsverkeer, ongeautoriseerde toegang, infrarooddetectie enzovoort. Veel organisaties nemen deze events niet mee in security monitoring. De oorzaak hievan is de traditionele scheiding tussen IT en fysieke beveiliging.

Security monitoring kan ook door het toepassen van IDS of IPS-systemen. De kracht van deze systemen is dat ze alle gebeurtenissen en incidenten registreren. Er is echter ook een nadeel: ze generen zoveel data dat analyse enkel mogelijk is met filters en rapportagetools. Een veelgebruikte tool hiervoor is SIEM (Security Information & Event Management). Let op: een SIEM oplossing kan ook weer een doelwit zijn voor hackers.

[11] Een patch is een programmaatje waarmee bestaande bugs en fouten in de software worden verholpen. Patches kunnen preventief (problemen voorkomen), adaptief (omgevingsveranderingen), correctief (probleemoplossing) en perfectief (wijzigingen in de specificaties) zijn.

Specifieke maatregelen: een top 10

Behalve algemene beveiligingsmaatregelen om hacks te voorkomen, zijn er ook meer specifieke maatregelen te implementeren. Een top 10:

1. Incidentopvolging

Werkelijk effectieve procedures met betrekking tot incidentopvolging dienen multidisciplinair te zijn en niet enkel te focussen op IT. In plaats daarvan is het goed om rollen, verantwoordelijkheden en communicatieafspraken te documenteren en vast te leggen met alle afdelingen (HRM, Juridisch, PR etc.). Wijs iemand aan als het aanspreekpunt van het CSIRT (Computer Security Incident Response Team). Dat team komt bij elkaar wanneer zich een incident voordoet. Een CSIRT doet er goed aan periodieke oefeningen te doen om te testen of alle teamleden effectief hun rol vervullen.

2. Netwerk design

Om netwerkmapping en poortscans te voorkomen dienen systeembeheerders alle onnodige systemen te verwijderen en alle ongebruikte poorten te blokkeren of af te sluiten. Dat geldt ook voor onnodige protocollen en services. Alleen die services die een zakelijk doel vervullen, dienen actief te zijn. Een beveiligingsbeheerder dient periodiek de systemen te scannen.

3. Netwerkscanning

Systeembeheerders dienen ongebruikte netwerkpoorten af te sluiten. Om kwetsbaarheden weg te nemen dienen tijdige systeempatches te worden doorgevoerd. Organisaties doen er goed aan een gedocumenteerd wijzigingsproces in te stellen dat aangeeft hoe systeempatches up-to-date gehouden dienen te worden.

Deze procedure bevat ook het uitvoeren van periodieke 'vulnerability scans' op het netwerk om zo kwetsbaarheden te detecteren voordat een hacker dat doet. Wordt er een kwetsbaarheid ontdekt dan dient deze tijdig verholpen te worden door een patch aan te brengen.

Wanneer u een traditioneel telefoonnetwerk gebruikt dan is het aan te bevelen om maatregelen te nemen tegen 'war dialing'. De beste bescherming daartegen is het toepassen van modemrichtlijnen die het gebruik van modems verbiedt wanneer er geen zakelijk doel is. Voer daarnaast zelf war-dialing-tests uit op het netwerk om niet-geregistreerde modems te detecteren, een ongeautoriseerd modem dient gelokaliseerd en gedeactiveerd of verwijderd te worden.

Manieren om succesvol footprinten te voorkomen: gebruik algemene zakelijke domeinen zoals een algemeen telefoonnummer (088). Dit voorkomt dat zakelijke telefoonnummers publiek worden en aan een bepaalde regio worden gekoppeld. Gebruik fictieve mailadressen en monitor berichten die

binnenkomen op die accounts. Check uw bedrijf op publieke websites zoals Pipl, Google, Facebook etc. Vindt u informatie, probeer dan uit te zoeken of die informatie noodzakelijk is en of het gebruikt kan worden voor mapping. Tot slot: publiceer geen lijst van ICT-infrastructuurcomponenten in online vacatures.

Zorg ervoor dat de "externe" netwerkcomponenten zo geconfigureerd zijn dat ze geen informatie afgeven (antwoorden) op IP- of poortscans. Analyseer en documenteer gebruikte en ongebruikte protocollen en services op de firewalls. Controleer regelmatig de huidige instellingen van de netwerkcomponenten en vergelijk de resultaten met de vorige keer. Installeer Intrusion Prevention Systems (IPS) / Intrusion Detection Systems (IDS) en analyseer de logs. Lokaliseer bedrijfskritische applicaties en zoek uit hoe deze applicaties reageren op externe scans. Controleer regelmatig "externe" netwerkcomponenten en voer zelf scans uit of probeer een 'net cat'-verbinding in te stellen naar de poorten. Vergeet niet dat uw IT-personeel niet alle scans en tools zullen opmerken omdat deze 'verstopt'worden in het reguliere datacommunicatie of netwerkverkeer of omdat een hacker 's deze nachts uitgevoerd.

4. Netwerkcommunicatie

De beste manier om zogeheten 'sniffing attacks' te voorkomen is om de te verzenden data te versleutelen. Verstuur geen wachtwoorden in leesbare tekst en elimineer de 'boadcast nature' van ethernet netwerken. Gebruik bij voorkeur switches in plaats van hubs.

Implementeer ook maatregelen tegen IP-spoofing. Systemen dienen geen IP-adressen te gebruiken voor authenticatie. Functies die alleen steunen op authenticatie op basis van IP-adressen dienen te worden vervangen of uitgeschakeld. Voorkom dat de systeembeheerder onveilige UNIX ***R***-commando's gebruikt. ***R***-commando's maken gebruik van alleen IP-adressen voor de authenticatie zonder wachtwoord. Implementeer anti-spooffilters op Demilitarized Zones (DMZ), deze verwijderen alle verkeer die van buiten de organisatie komt maar zich voordoet alsof het van binnenuit komt.

5. Ongewenste overname Netwerkverbinding

Vermijd het gebruik van onveilige protocollen en toepassingen voor gevoelige sessies zoals ***r***-login en Telnet. Gebruik in plaats daarvan SSH (secure shell), SSH biedt krachtige authenticatie en encryptie en kan worden geconfigureerd voor SCP (Secure Filetransfer Capability) ter vervanging van het FTP ptotocol (File Transfer Protocol).

6. Denial-of-Service

De beste bescherming tegen Denial-of-Service-aanvallen is het implementeren van solide kwetsbaarheden - en patchmanagementprocessen. Leveranciers updaten hun syteem regelmatig met patches om nieuwe soorten denial-of-service-aanvallen te kunnen voorkomen.

Een adequaat patchmanagementproces voorkomt veel problemen met kwetsbaarheden van software. De tijd tussen het ontdekken van een zwakte (vulnerability) en de beschikbaarheid van exploits waarmee de zwakte kan worden misbruikt wordt korter en korter. Dus patch, patch en patch.

7. Stack-Based Buffer overflow

Een goede bescherming tegen buffer overflow-aanvallen (bufferoverloop) is geod geschreven softwarecode zodat die niet gebruikt kan worden om de zogeheten stacks te manipuleren. Hackers kunnen in een slecht geschreven programma de buffer laten overlopen en de controle over het programma overnemen. Programma's dienen input van gebruikers te valideren om er zeker van te zijn dat de invoer past binnen de toegewezen geheugenstructuren. Elke variabele moet worden gecheckt om te garanderen dat de toegewezen buffers in staat zijn de data te verwerken. Daarnaast dienen security administrators en systeembeheerders het aantal SUID-programma's op gebruikerssystemen nauwkeurig te controleren en liefst te minimaliseren. Installeer enkel SUID-programma's die noodzakelijk zijn. Veel buffer overflow-aanvallen kunnen worden voorkomen door systemen zo te configureren dat ze geen code uitvoeren vanuit de stack.

De top 10 risico's voor webapplicaties in 2010

Webapplicaties: neem (internet facing) webapplicaties pas in productie nadat ze getest zijn. Zorg ervoor dat de webapplicaties ontwikkeld zijn met officiële software. De ontwikkelaar moet kunnen garanderen dat de applicatie in ieder geval is getest op de 10 grootste veiligheidsrisico's volgens OWASP (Open Web Application Security Project)[12]. Deze top 10 is (overgenomen van OWASP in het Engels):

1. *SQL-injection*
2. *Cross-site scripting (XSS)*
3. *Broken authentication en session management*
4. *Insecure direct object references*
5. *Cross-site request forgery (CSRF)*
6. *Security misconfiguration*
7. *Insecure cryptographic storage*
8. *Failure to restrict URL access*
9. *Insufficient transport layer protection*
10. *Invalidated redirects en forwards.*

Stel passende accountrichtlijnen op: gebruik wachtwoorden of beter nog, vereis sterke wachtwoorden en maak gebruik van krachtige authenticatiemethodes zoals tokens, smartcards, of biometrische identificatie voor remote access. Versleutel gevoelige informatie. Gebruik lockout-procedures voor accounts en limiteer het aantal inlogpogingen op alle IT-omgevingen. Dus niet enkel op de productieomgeving. Log alle 'failed account' en mislukte inlogpogingen in een logsysteem en bekijk deze logs dagelijks. Pas het beleid waar nodig aan.

Datavalidatie- en wijzigingsprocedures

Datavalidatie zorgt ervoor dat een applicatie goed beveiligd is tegen allerlei soorten invoerdata, of die data nou afkomstig is van de gebruikers, de infrastructuur, externe partijen of een database.

- *Sequentie check: controlenummers worden genummerd op volgorde. Als een controlenummer niet aan die volgorde voldoet of er dubbelen zijn worden deze afgewezen of genoteerd in een rapport van uitzonderingen. Een voorbeeld: facturen zijn altijd op volgorde genummerd. Stel dat de eerste factuur nummer 12001 heeft en de laatste 15045, dan wordt iedere factuur met een nummer dat hoger is dan 15045 afgewezen als ongeldig factuurnummer.*

[12] https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- *Limit check: een limiet stellen aan bijvoorbeeld bedragen of prijzen. Data die boven die vooraf bepaalde limiet uitkomen worden niet geaccepteerd. Voorbeeld: looncheques mogen niet meer bedragen dan €4.000. Data met een bedrag hoger dan €4.000 worden afgewezen ter verdere verificatie/autorisatie.*
- *Range check: gegevens moeten vallen binnen een vooraf bepaalde waardereeks. Voorbeeld: productcodes vallen altijd binnen een reeks van 100 tot 250.*
- *Validiteits check: geprogrammeerde controle van de validiteit van data volgens vooraf bepaalde criteria. Voorbeeld: een payrollrecord bevat een veld voor burgerlijke staat en de twee statuscodes die voldoen (valide zijn) zijn G (gehuwd) en A (Alleenstaand).*
- *Aanneembaarheidscontroles: invoergegevens worden gematcht met voorafgestelde aannemelijke limieten of aantallen. Voorbeeld: een widgetfabrikant ontvangt normaal gesproken nooit orders groter dan 20 widgets per keer. Komt er een order binnen voor meer dan 20 widgets dan moet het computerprogramma zo zijn ingesteld dat hij de order uitprint met een waarschuwing dat de order niet aannemelijk is en dus misschien onbetrouwbaar.*
- *Table lookups: invoergegevens die voldoen aan vooraf bepaalde criteria worden gehandhaafd in een geautomatiseerde tabel met mogelijke waarden.*
- *Existence checks: gegevens zijn correct ingevoerd en voldoen aan de vooraf bepaalde criteria. Voorbeeld: een valide transactiecode moet worden ingevoerd in het veld 'transactiecode'.*
- *Gegevensinvoerverificatie: een tweede persoon herhaalt een eerder, door een andere persoon, uitgevoerd invoerproces op een computer die de invoergegevens van beiden met elkaar vergelijkt.*
- *Check digit: een numerieke waarde, wiskundig berekend, wordt toegevoegd aan de data om er zeker van te zijn dat de oorspronkelijke data niet zijn gewijzigd of niet correct zijn, maar valide. Deze controle is nuttig bij het detecteren van transposities en transcriptiefouten. Voorbeeld: een controlecijfer is toegevoegd aan een bankrekeningnummer zodat deze gecontroleerd kan worden op correctheid (nauwkeurigheid) voor gebruik.*
- *Volledigheidscontroles: een veld moet altijd data bevatten en mag dus niet leeg zijn of nullen bevatten.*
- *Duplicaatcontrole: nieuwe transacties worden gematcht met eerdere input om er zeker van te zijn dat ze niet al eerder ingevoerd zijn.*
- *Logische relatiecontroles: als een bepaalde voorwaarde 'waar' is dan kan het zijn dat ook andere voorwaarden of datainvoergegevenrelaties 'waar' moeten zijn om valide invoer te garanderen. Voorbeeld: de indiensttredingdatum van een werknemer moet minimaal 16 jaar na zijn geboortedatum zijn.*

<u>Controleprocedures voor gegevensbestanden</u>

- *Voor en na controles: computerdata in een bestand voorafgaand aan en nadat een transactie heeft plaatsgevonden kunnen worden geregistreerd en gerapporteerd.*
- *Foutrapportages en foutafhandeling: controleprocedures die garanderen dat alle foutrapportages naar behoren worden afgehandeld en dat correcties tijdig doorgevoerd worden.*
- *Bewaren van brondocumentatie: brondocumentatie dient lang genoeg bewaard te worden om terughalen, reconstructie en verificatie van data mogelijk te maken.*
- *Intern en extern labelen: interne en externe labelling van verwisselbare opslagmedia is noodzakelijk om er zeker van te zijn dat de juiste gegevens worden geladen voor verwerking.*
- *Versie-update: voor foutloze verwerking is het belangrijk dat de juiste versie van een bestand wordt gebruikt en dat het het juiste bestand is.*
- *Veiligheid databestanden: controles op de veiligheid van databestanden voorkomen ongeautoriseerde toegang door ongeautoriseerde gebruikers die misschien wel toegang hebben tot een applicatie om gegevensbestanden te wijzigen.*
- *Een-op-een controles: individuele documenten moeten overeenkomen met een gedetailleerde uitdraai van de door de computer behandelde documenten.*
- *Vooraf ingevulde invoer: bepaalde informatievelden zijn vooraf ingevuld op lege invoerformulieren om zo het aantal invoerfouten te reduceren.*
- *Autorisatie updaten en onderhouden bestanden: voor het updaten en onderhouden van bestanden is een passende autorisatie nodig om te garanderen dat opgeslagen gegevens zijn gewaarborgd, juist en up-to-date zijn.*
- *Pariteitcontrole (ook wel Vertical Redundancy check genoemd): een bit (pariteitsbit) toe voegen aan elk teken tijdens verzending om ervoor te zorgen dat pariteit altijd oneven of even is. Bij veel fouten (bijvoorbeeld impulsruis tijdens hoge overdrachtsnelheden) is deze methode 50% betrouwbaar.*

- *Cyclische redundantiecontrole (CRC): controleert pakketverzonden data. De broncomputer genereert de CRC en stuurt die mee met de data. De ontvangende machine berekent de CRC en vergelijkt deze met de meegezonden CRC. Als ze gelijk zijn is het pakket data foutvrij. Met deze methode kunnen meerdere fouten worden gedetecteerd. In het algemeen kan CRC alle single-bit en dubble-bit-fouten herkennen.*
- *Echo check: lijnfouten detecteren door data terug te zenden naar de afzender (het apparaat) om deze te vergelijken met het oorspronkelijke bericht.*

Data-integriteit in online transaction processing systemen (ACID)

- *Atomair: atomair betekent dat elke transactie een regel 'alles of niets' volgt. Als een deel van de transactie mislukt, dan mislukt de hele transactie. Vanuit het oogpunt van de gebruiker is een transactie of helemaal compleet (als in: alle relevante databasetabellen zijn geüpdatet) of helemaal niet. Na een fout of interruptie worden alle wijzigingen tenietgedaan.*
- *Consistent: alle integriteitsregels van de database blijven gehandhaafd tijdens iedere transactie. De database gaat dus van de ene geldige staat naar de andere geldige staat. Is dus consistent.*
- *Geïsoleerd (Isolated): transacties worden geïsoleerd van elkaar uitgevoerd. Elke transactie heeft alleen toegang tot data die onderdeel uitmaken van een geldige en dus consistente database.*
- *Duurzaam: als een transactie eenmaal met goed gevolg is afgerond dan blijven de doorgevoerde veranderingen in de database bestaan, ook in geval van hardware- of softwarestoringen.*

---

8. Gekraakte wachtwoorden

De beste afweer tegen het kraken van wachtwoorden is het minimaliseren van blootstelling van versleutelde wachtwoordbestanden. Een sterk wachtwoordbeleid is cruciaal voor het beschermen van een veilig netwerk. Het wachtwoordbeleid vereist dat wachtwoorden uit minimaal tien karakters bestaan. Gebruikers moeten zich bewust zijn van de gevaren ontrent zwakke wachtwoorden en getraind worden in het bedenken en gebruiken van moeilijk te kraken wachtwoorden die wel te onthouden zijn.

Probeer te voorkomen dat de systeembeheerder dagelijks werkt met zijn admin of root-account. Zorg ervoor dat de beheerder voor taken die geen administratorrechten vereisen een gewoon gebruikersaccount gebruikt. Hernoem de standaard admin- of rootaccount (waar mogelijk) en block standaard gastaccounts. Kies voor een gepast wachtwoordenbeleid waarin een minimumlengte voor wachtwoorden is opgenomen evenals een wachtwoordgeschiedenis en welke voorvoegsels er niet gebruikt mogen worden (bv. 123, abc etc.). Bepaal de instellingen voor accountvergrendeling en implementeer deze niet alleen op productieniveau maar ook op de ontwikkel, de test- en de acceptatieomgevingen. Stel het logniveau vast en evalueer dit regelmatig. Pas de beleidsinstellingen waar nodig aan.

De accountmaatregelen voor systeembeheerders en administrators kunnen afwijken van die voor normale gebruikers. Zorg voor krachtige verificatieprocedures. Log alle 'failed account' en mislukte inlogpogingen in een logsysteem en bekijk deze logs dagelijks. Pas het beleid waar nodig aan.

---

9. Backdoors

De beste bescherming tegen backdoorprogramma's is de kennis van de systeembeheerder. Hij/zij moet weten welke processen er allemaal draaien op de machines. Vooral op die systemen die gevoelige en of belangrijke informatie opslaan of die hoogwaardige transacties uitvoeren. Als een proces plotseling runt als super user die naar een port luistert, dan moet de beheerder op onderzoek uitgaan.

Een centrale SYSLOGserver wordt gebruikt om – op bepaalde tijden - data over te brengen vanuit het lokale (systeem) logbestand. Gebruik APPEND-only-commando. Neem integriteitmaatregelen en voer loganalyses uit op regelmatige basis, inclusief automatische berichtgeving aan de administrator/manager.

10. Trojaanse Paarden en rootkits

De beste sleutel om bescherming te bieden tegen Trojaanse Paarden is bewustwording en kennis bij de gebruiker (user awareness). Gebruikers dienen de risico's die gepaard gaan met het downloaden en uitvoeren van onbetrouwbare software of progamma's te kennen. Dat geldt vanzelfsprekend ook voor het uitvoeren van .exe bestanden in mailbijlages van onbetrouwbare bronnen en voor het bezoeken van malafide websites. Computers moeten voorzien zijn van effectieve anti-virussoftware die up-to-date is. Voor bescherming tegen rootkits dienen systeembeheerders integriteitscontroleprogrammatuur te gebruiken voor kritische systeembestanden. Helaas kunnen kernel-level rootkits niet worden gedetecteerd met integriteitscontrolesoftware omdat de 'integrity checker' afhankelijk is van de onderliggende kernel. Als de kernel de boel om de tuin leidt worden de resultaten niet zichtbaar in de rootkitinstallatie.

Scan uw systeem regelmatig voor Trojaanse Paarden, rootkits en backdoors met zowel interne als externe (commerciële) scanners. Liefst zelfs met meerdere soorten en types scanners. Een voorbeeld: maak onderscheid tussen scanners voor de "buitenste" schil van de (interne) netwerklaag, de DMZ, de (applicatie-)servers en de werkstations. Gebruik integriteitscontrolesoftware. De beste bescherming tegen kernel-level root kits is een monolithische kernel die geen laadbare kernelmodules ondersteunt. Beheerders en administrators dienen op gevoelige systemen (Firewall, internet webservers, DNS-servers, mail servers etc.) de built uit te voeren met complete kernels zonder ondersteuning voor laadbare kernelmodules. Met deze configuratie verhindert het systeem eventuele hackers om toegang te krijgen tot root-level en de kernel real-time te patchen.

Nawoord

In deze white paper heb ik gesteld dat hacking weliswaar dominant in het nieuws is de laatste tijd, maar dat hacking van alle tijden is en waarschijnlijk nooit meer zal verdwijnen. Hacking zal eerder in intensiteit toenemen omdat de crackers (dus niet de hackers) vrij gemakkelijk veel geld kunnen verdienen met hun botnets, SPAM, ransom ware, drive-by-download infecties en aanvallen op websites en webapplicaties. Daarnaast blijft het aantal webgebruikers nog dagelijks groeien en daarmee ook het aantal potentiële slachtoffers.

Ik heb in mijn verhaal hacking, hacks en hackers ontmaskerd. Wie zijn het, wat doen ze, welke types zijn er en hoe gaat het eigenlijk in zijn werk. Een hack is opgebouwd uit fases. Op het moment dat je dit allemaal weet, begint de preventie.

Het kunnen identificeren en analyseren van een aanval (een hack) vormt het begin van preventie. De informatie in deze white paper helpt u bij het beschermen van uw bedrijf tegen hackers en hacks door gebruik te maken van preventieve, detectieve, correctieve, compenserende en specifieke beveiligingsmaatregelen.

Bibliografie

Bronnen:	1. ir. Kees Hogewoning, ing. Gerrit Th. Lith, ing. Marco G.M. van der Kraan, Erwin A.J. Verburg en anderen 2007, "Internet Security, securing internet connected networks", uitgegeven door NGN (www.ngn.nl) en Vanveen informatica (http://www.vanveen.nl). ISBN 978-90-71501-16-6. 2. Information Security Management Handbook, Fifth Edition, door Harold F. Tipton en Micki Kraus, 2004, uitgever: Auerbach publications, ISBN 0-8493-1997-8; 3. Govert 2011 presentatie "Auditing the Hacker's mind: the Hacker's Profile Project 2.0", Raoul Chiesa, Senior Adviseur Cybercrime at Emerging Crime Unit (ECU), United Nations Interregional Crime and Justice Research Institute (UNICRI). 4. Profiling Hackers: the Science of Criminal Profiling as applied to the World of Hacking, ISBN 978-1-4200-8693-5-9000. 5. Hacking Exposed, Network Security Secrets & Solutions, 2004, door Stuart McClure, Joel Scambray en George Kurtz, uitgegeven door Osborne/McCraw-Hill, ISBN 0-07-212127-0 6. CHIP magazine, 2012, nummer 91, artikel 'Historical hackers', door Manuel Köppl and Peter Marinus. 7. The Ten Biggest Legends of the Hacker Universe, http://voices.yahoo.com/the-ten-biggest-legends-hacker-universe-369297.html , door Carlos Cabezas López. 8. The Hacker News, mei 2011 - editie 02 - Social Engineering Edition.
Referenties (Websites):	1. National Cyber Security Centrum, https://www.ncsc.nl/ 2. Security.NL, http://www.security.nl 3. Iusmentis, http://www.iusmentis.com/ 4. AIVD, https://www.aivd.nl/english/publications-press/press-releases/@2664/aivd-annual-report/ 5. Patch management by NCSC, http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/patch-management.html 6. UNICRI Cybercrime Home Page, http://www.unicri.it/emerging_crimes/cybercrime/ 7. The Ten Biggest Legends of the Hacker Universe, http://voices.yahoo.com/the-ten-biggest-legends-hacker-universe-369297.html 8. Anonymous, http://www.indybay.org/newsitems/2010/12/09/18666107.php, http://nl.wikipedia.org/wiki/Anonymous_(groep) 9. Lulzsec, http://en.wikipedia.org/wiki/LulzSec 10. OWASP Top 10, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project 11. Data Exfiltration, http://www.iamit.org/blog/2012/01/advanced-data-exfiltration/