Opdracht Security Advanced – Blue Teaming aspect: Vulnerability Analysis / Forensics

Inhoud

Level C requirements

Voorbereiding

Installeren VM met Kali

Download van Kali voor VMWare via
https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/
Run Virtual machine and type in terminal:
> sudo passwd (to change root password)
> su - (to activate root)
> apt update && apt upgrade

Installeren Nessus Essentials op Kali

Download Nessus Essentials van https://www.tenable.com/downloads/nessus?loginAttempted=true
(in dit geval de versie voor Debian 9, 10 / Kali Linux 1, 2017.3, 2018, 2019, 2020 AMD64)
>sudo apt install Nessus-8.14.0-debian6_amd64.deb
> /bin/systemctl start nessusd.service (om de Nessus Scanner te starten)
Dan via de webbrowser naar https://kali:8834/ om de activatiecode en dergelijke in te kunnen geven (verkregen via studentenregistratie op https://www.tenable.com/tenable-for-education/nessus-essentials?edu=true)

Installeren van nmap op Kali

Installatie was al gebeurd in de VM gedownload van Offensive Security.
Nmap is the most powerful network mapping tool.
Nmap komt met een GUI, Zenmap genaamd. Deze is niet standaard geinstalleerd in onze Kali.
Procedure:
Download zenmap van https://nmap.org/download.html
Installeer Alien om het redhat package om te zetten in een Debian package file
> sudo apt-get install alien

Converteer file zenmap-7.91-1.noarch.rpm
>sudo alien zenmap*.rpm
zenmap_7.91-2_all.deb generated
Installeer zenmap
>sudo dpkg -i zenmap*.deb
Zenmap gebruikt Python GTK als GUI => afhalen package
>wget http://archive.ubuntu.com/ubuntu/pool/universe/p/pygtk/python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
Installeren Python GTK
>sudo apt install ./python-gtk2_2.24.0-5.1ubuntu2_amd64.deb
Start zenmap GUI (met elevated rights)
>sudo zenmap

Installeren van OWASP ZAP op Kali

Installatie was al gebeurd in de VM gedownload van Offensive Security => versie 2.10.0

Downloaden en installeren van 2 VMs: SimpleWin en Server16

Importeren met Network connection Bridged, zodat iedere VM zijn eigen IP-Adres krijgt.

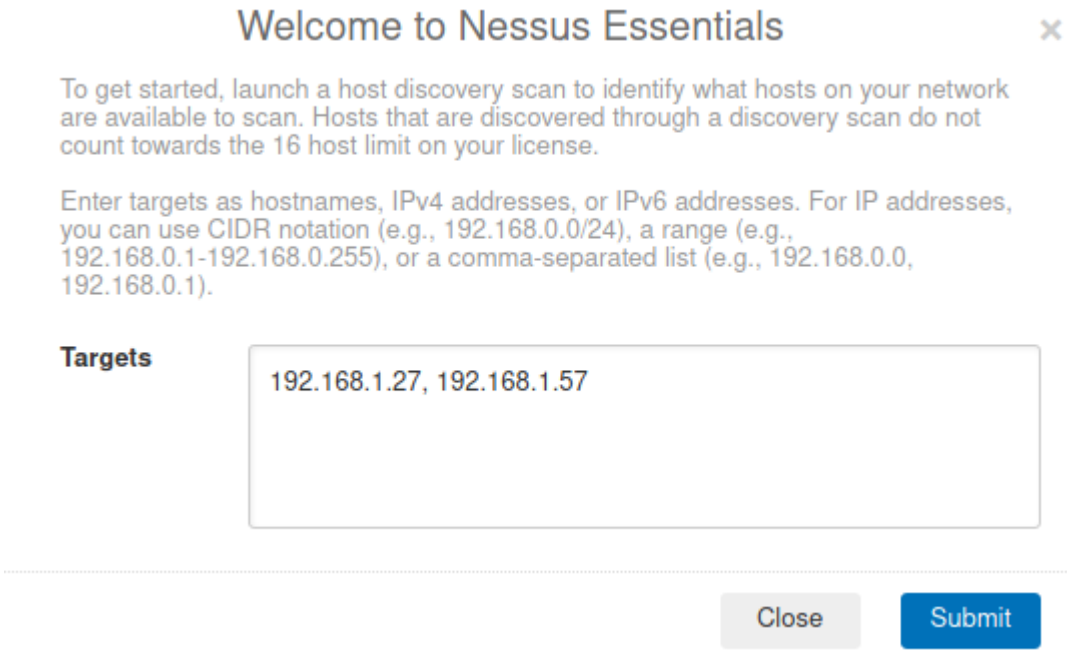
Scanning en Analyses

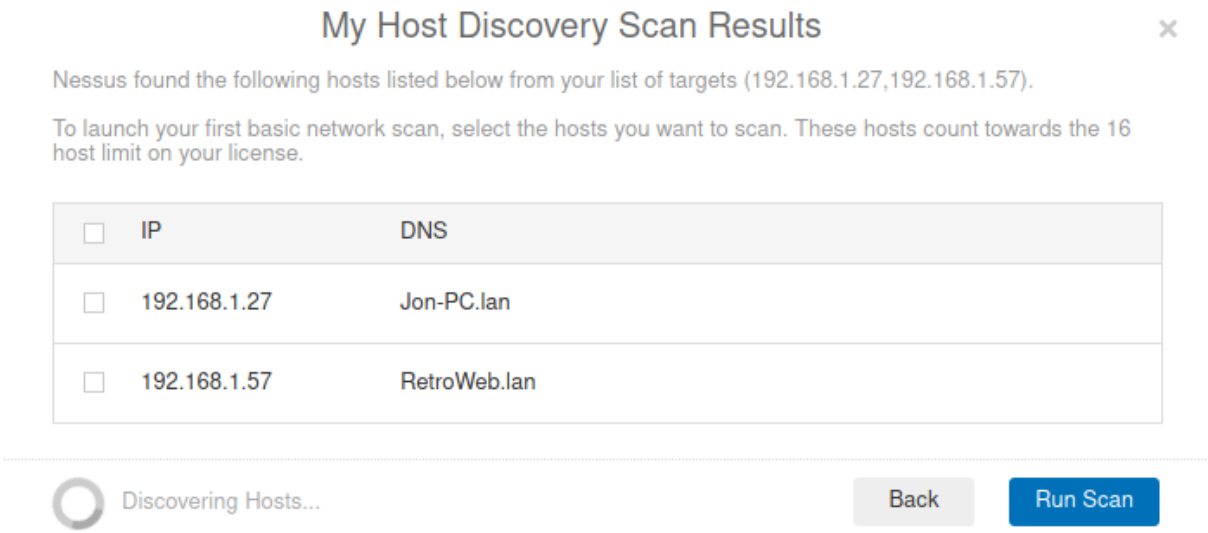
Scan en analyse targets met Nessus

Werkwijze gebaseerd op PluralSight courses:
https://app.pluralsight.com/library/courses/nessus-vulnerability-analysis/table-of-contents
https://app.pluralsight.com/library/courses/discover-network-weaknesses-nessus/table-of-contents

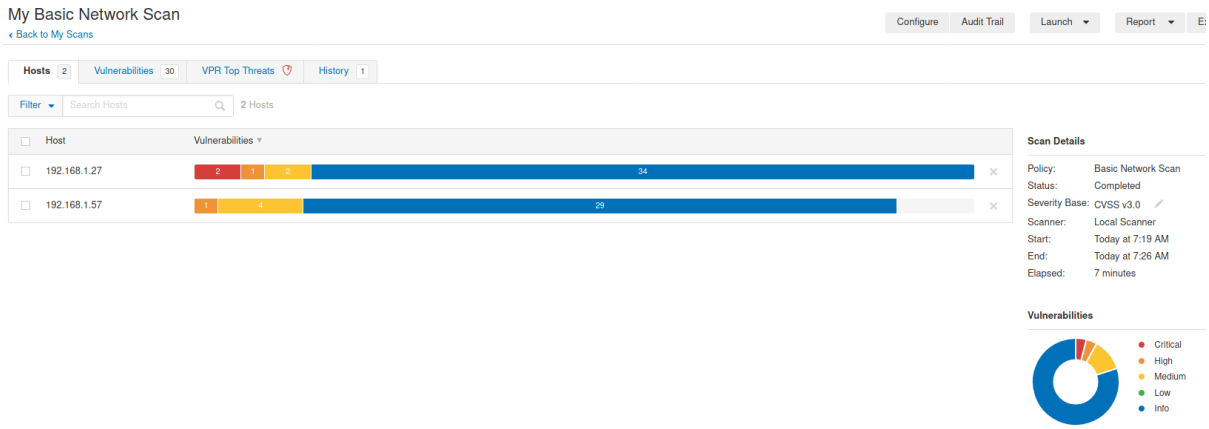
Scan

1. Start Nessus in een browser via https://kali:8834
2. Insert hostnames to scan (IP addresses gevonden via een snelle nmap scan)



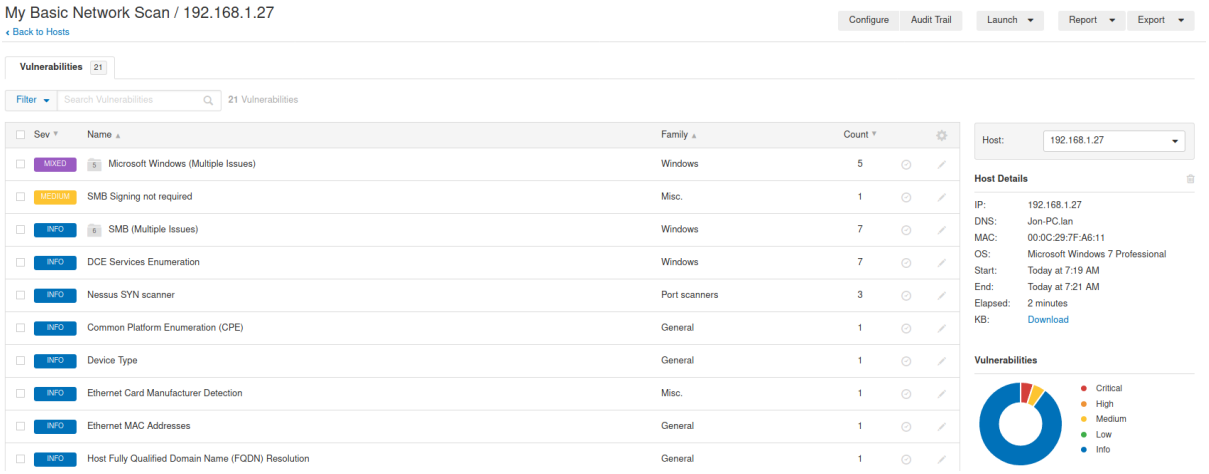


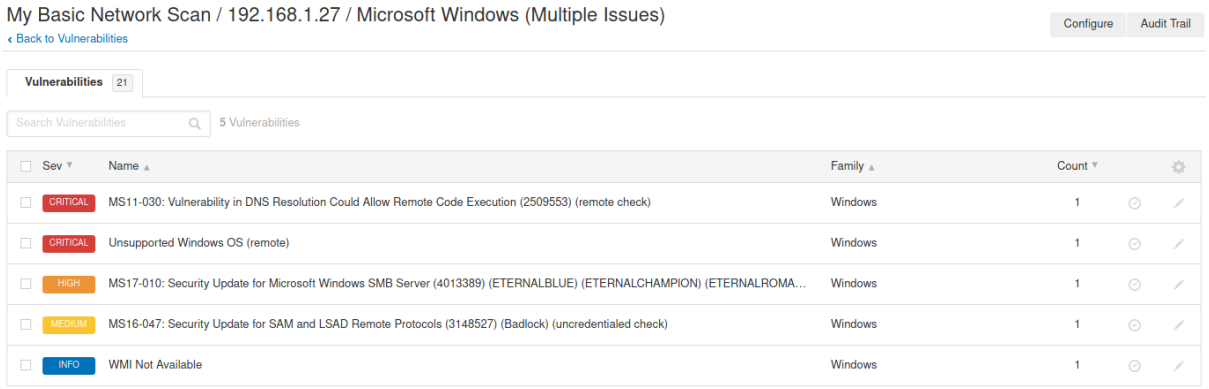
3. Run scans



Analyse Jon-PC

4. Analyse kwetsbaarheden Jon-PC

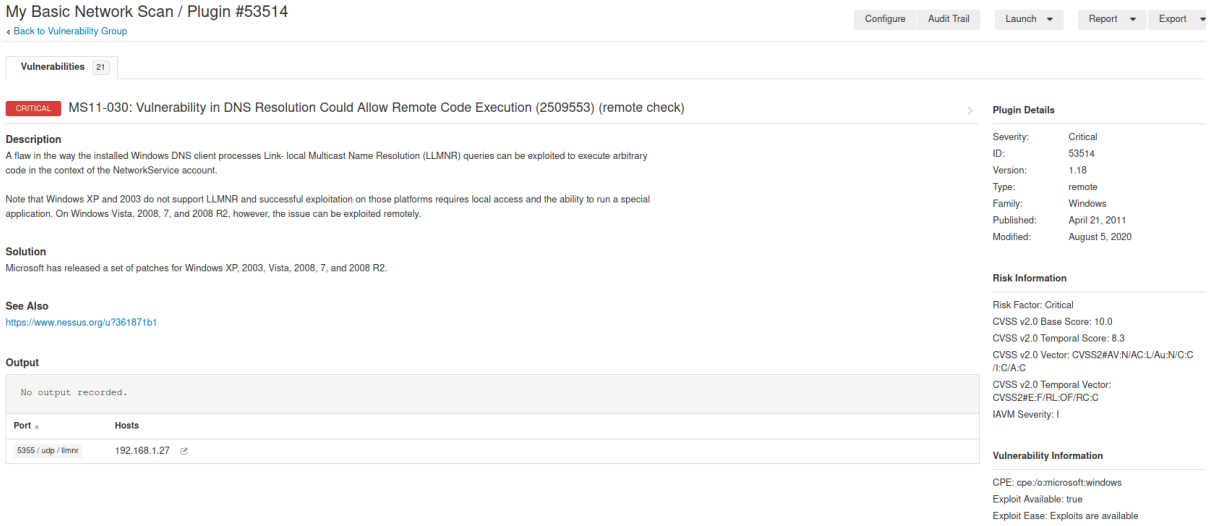




Threat 1 en oplossing

CRITICAL1 : CVSS (Common Vulnerability Scoring System) van 10.0. Dit is de hoogst mogelijke score! Windows DNS client processes Link-local Multicast Name Resolution queries laten het toe remotely code uit te voeren.

Oplossing: Windows heeft patches klaar.

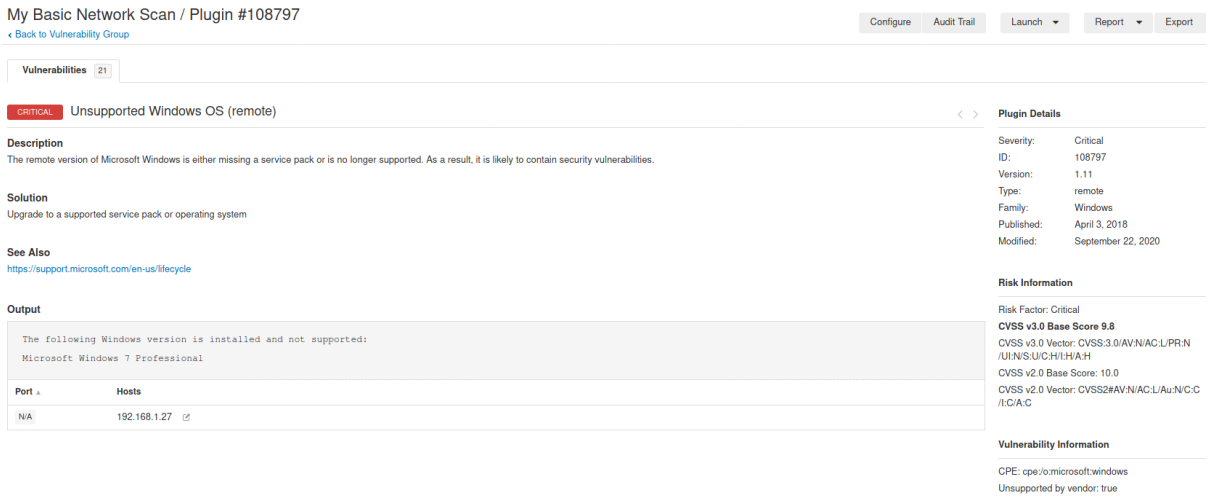


Threat 2 en oplossing

CRITICAL2 : CVSS van 9.8

Het OS “Windows 7 Professional” wordt niet meer ondersteund door Microsoft.

Oplossing: upgrade van het OS.

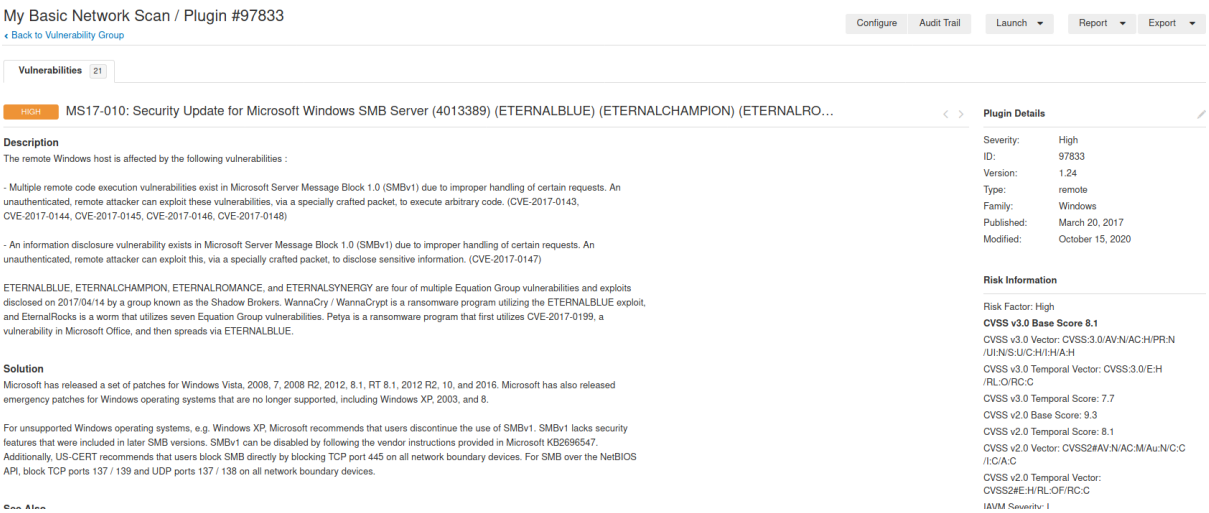


Threat 3 en oplossing

HIGH : CVSS van 8.1

Het Server Message Block of Common Internet File System netwerkprotocol (dat gebruikt wordt om bestandsuitwisseling tussen meerdere computers mogelijk maakt) bevat kwetsbaarheden waardoor remote code uitgevoerd kan worden. Een zeer bekende ransomware dat hier gebruik van maakt is WannaCry.

Oplossing: patches van Windows bestaan. Nieuwere Windows versies gebruiken SMBv2 of hoger.

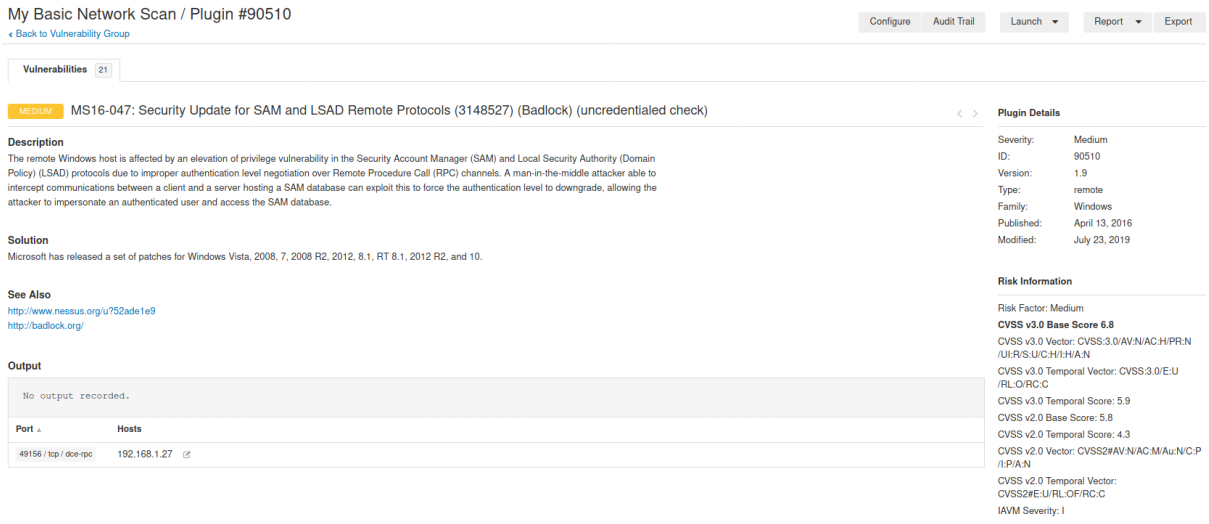


Threat 4 en oplossing

MEDIUM1: CVSS van 6.8

SAM (Security Account Manager) en LSAD (Local Security Authority Domain) protocols laten man-in-the-middle aanvallen toe wanneer via RPC (Remote Procedure Call) gecommuniceerd wordt door onvolledige controle van de credentials.

Oplossing: Microsoft heeft patches voorzien

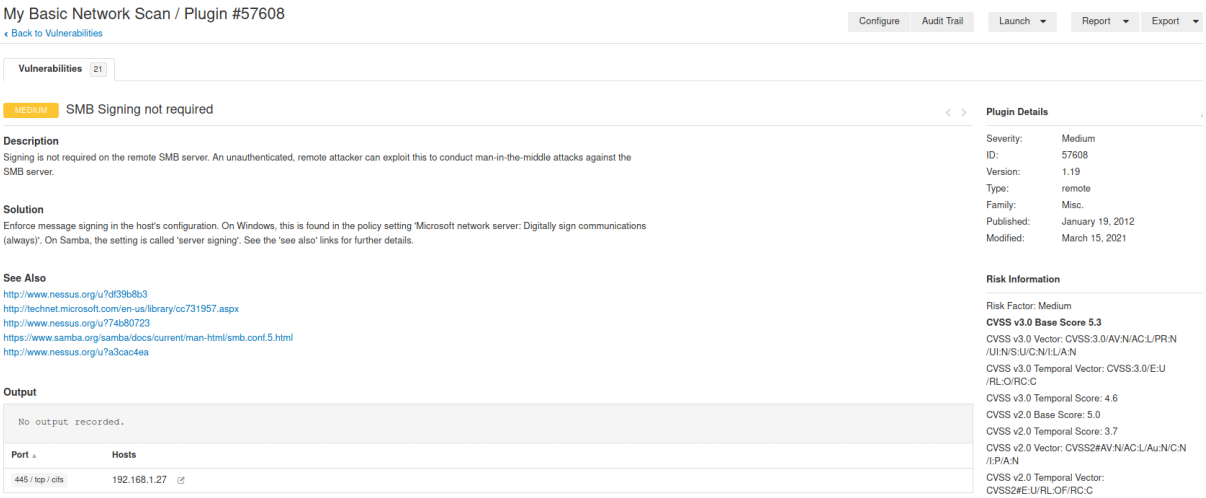


Threat 5 en oplossing

MEDIUM2: CVSS van 5.3

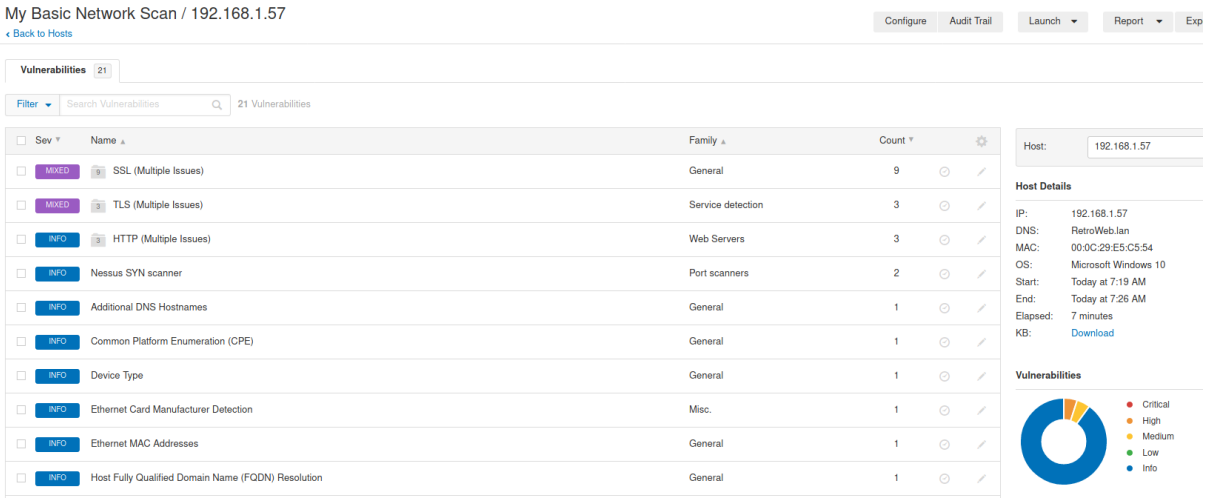
Gelinkt met “HIGH” hierboven. Het SMB-protocol laat ook nog eens man-in-the-middle aanvallen toe van niet-geautenticeerde, remote aanvallers op de SMB server

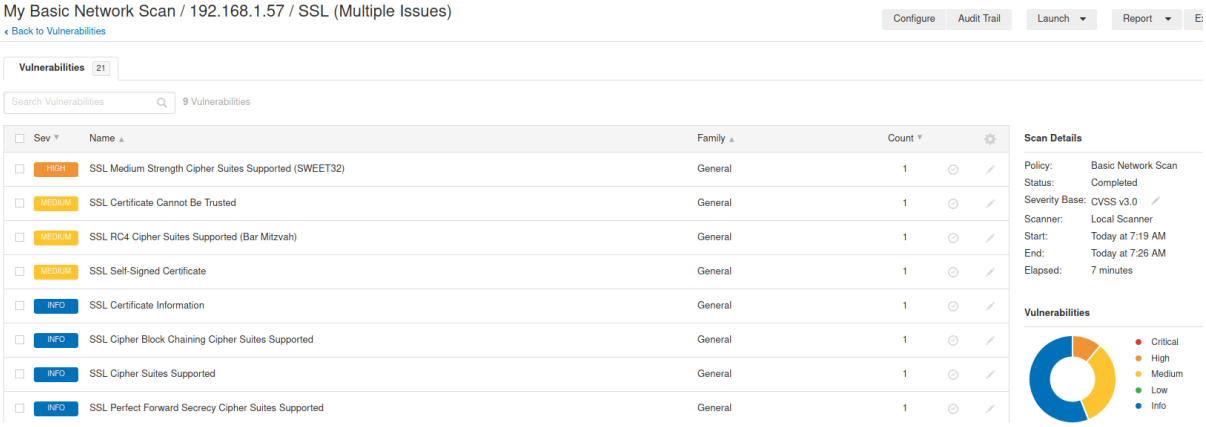
Oplossing: Verplicht digital “signing” via de settings op de host.



Analyse RetroWeb-PC

5. Analyse kwetsbaarheden RetroWeb-PC





Threats en oplossingen

SSL-kwetsbaarheden:

1. SSL ciphers van medium strength zijn toegelaten (keylengtes tussen 64 en 112 bits of 3DES) die gemakkelijk te omzeilen zijn wanneer een aanvaller op hetzelfde fysieke netwerk zit.
   Oplossing: Herconfigureer en verstreng de encryptie
2. Het SSL certificaat van de server is onbetrouwbaar
   Oplossing: Koop of genereer een correct SSL certificaat voor deze service
3. RC4 Cipher suites worden ondersteund. Deze Cipher wordt als zwak beschreven, zeker wanneer er herhaaldelijk plaintexts geencrypteerd worden en een aanvaller deze kan bemachtigen.
   Oplossing: Herconfigureer en verstreng de encryptie (bij voorkeur TLS1.2)
4. Self-Signed SSL Certificaat. Idem punt 2

TLS-kwetsbaarheid: Transport Layer Security Protocol 1.0 wordt nog geaccepteerd.
Oplossing : enable support voor TLS 1.2 en 1.3 en disable TLS 1.0

Scan targets en analyse met nmap

Werkwijze gebaseerd op 2 PluralSight courses:
https://app.pluralsight.com/library/courses/nmap-getting-started/table-of-contents en
https://app.pluralsight.com/library/courses/scanning-vulnerabilities-nse/table-of-contents

*

Scanning het netwerk met command "***sudo nmap -sn 192.168.1.0/24***" (discover network machines in mijn lokaal netwerk (range 192.168.1.0 tem 192.168.1.255)) -ook wel pingscan genoemd- toont de volgende twee netwerkmachines, belangrijk voor onze testen:

Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0067s latency).
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0012s latency).
MAC Address: 00:0C:29:E5:C5:54 (VMware)

*

sudo nmap -sS -p80 192.168.1.0/24 (scan alle devices op status van poort 80):

PORT STATE SERVICE
80/tcp *closed* http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

PORT STATE SERVICE
80/tcp *open* http
MAC Address: 00:0C:29:E5:C5:54 (VMware)

*

Om legaal te kunnen werken, kunnen we best ons te scannen netwerk en/of hosts oplijsten. Dit kunnen we doen door de ip-adressen in een file te zetten en de file op te roepen via "***sudo nmap -sL -iL ./Downloads/wbcscanlist***"

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 11:26 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00021s latency).
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00069s latency).
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Nmap done: 2 IP addresses (2 hosts up) scanned in 0.15 seconds
```

*

Verdedigen tegen PingScans kan door de firewall zo te configureren dat ICMP traffic geblokkeerd wordt of dat TCP packets op poorten 80 en 443 te blokkeren wanneer deze niet nodig zijn.

Poort scanning is belangrijk om outdated of kwetsbare of onnodige services te detecteren en kwetbare applications of hosts die niet gevonden worden met een ping te vinden.
>***sudo nmap -p1-1023 -iL ./Downloads/wbcscanlist*** (scan poorten 1 tem 1023 van de hosts in te file)
of
> ***sudo nmap -iL ./Downloads/wbcscanlist*** (scan de 1000 meest voorkomende poorten)

Om ALLE poorten te scannen dienen we
> ***sudo nmap -p1-1023,[1024-] -iL ./Downloads/wbcscanlist*** uit te voeren, waarbij [1024-] enkel poorten gescanned zullen worden die geregistreerd zijn in nmap services (dus nmap weet dat een poort toegewezen is aan een specifieke service)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p1-1023,[1024-] -iL ./Downloads/wbcscanlist
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:26 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0013s latency).
Not shown: 8366 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0014s latency).
Not shown: 8371 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
5985/tcp open  wsman
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 22.08 seconds
```

Enkele opmerkingen:
80/tcp draait nog over http en is dus clear text. Recommendatie is eerder om hier https te gebruiken (gebruikelijk over poort 443)
Het is gebruikelijk om alle niet gebruikte poorten te sluiten.
Een extra veiligheid is IDS en IPS op te zetten.

*

Service and Application version detection
> ***sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:41 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0022s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0014s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
3389/tcp open  ms-wbt-server Microsoft Terminal Services
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 64.37 seconds
```

*

OS Detection
> ***sudo nmap -sV -T4 -iL ./Downloads/wbcscanlist***

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O -T4 -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 16:52 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0027s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7::- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.0018s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:E5:C5:54 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2016
OS CPE: cpe:/o:microsoft:windows_server_2016
OS details: Microsoft Windows Server 2016
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 2 IP addresses (2 hosts up) scanned in 7.00 seconds
```

Voor de 2 laatste punten is de beste remedie steeds updaten naar de laatste versie en security patches, zowel voor services, applications als operating systems. Bovenstaande testen maken duidelijk dat het Windows 7 OS zo snel mogelijk ge-upgrade dient te worden.

*

Nmap NSE scripting om authentication controls te testen (scripting taal = Lua)
VB: test of http default accounts heeft geactiveerd (authentication script):

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap --script=http-default-accounts -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:31 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.0012s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00087s latency).
Not shown: 998 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
3389/tcp open  ms-wbt-server
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 5.32 seconds
```

In bovenstaande geval hebben beide geen default accounts .

Of een brute force script op de IIS service waarbij gebruik gemaakt werd van een tilde als mogelijke vulnerability:

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p80 --script=http-iis-short-name-brute -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:41 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00081s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00086s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.70 seconds
```

De IIS service op RetroWeb heeft hier geen last van en behoeft geen aanpassing.

Idem voor Cross Side Reference Forgery.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p80 --script=http-csrf -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:50 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00039s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00072s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.58 seconds
```

Idem voor SQL-injection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -p80 --script=http-sql-injection -iL ./Downloads/wbcscanlist
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 17:52 EDT
Nmap scan report for Jon-PC.lan (192.168.1.27)
Host is up (0.00047s latency).

PORT   STATE  SERVICE
80/tcp closed http
MAC Address: 00:0C:29:7F:A6:11 (VMware)

Nmap scan report for RetroWeb.lan (192.168.1.57)
Host is up (0.00057s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:E5:C5:54 (VMware)

Nmap done: 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

*

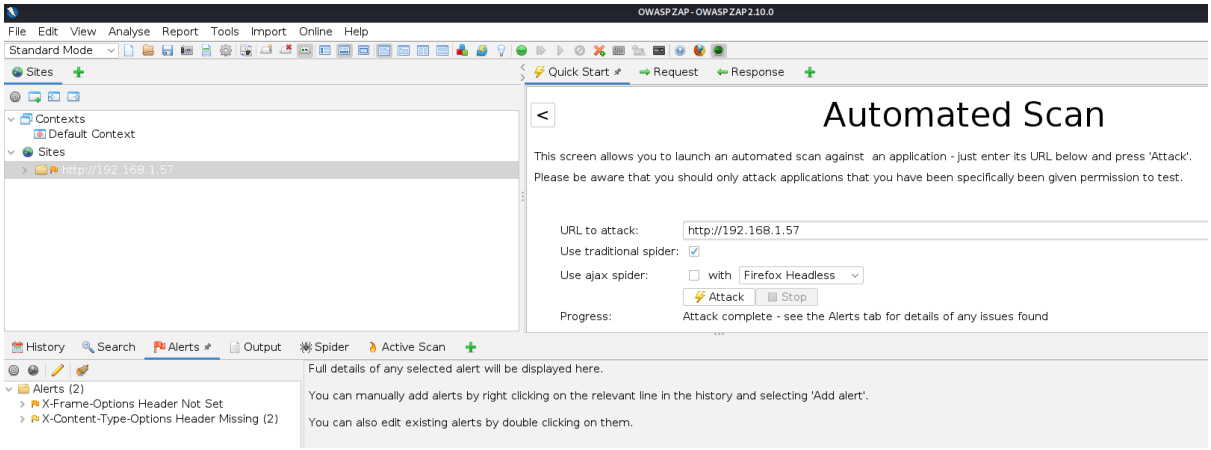
Fuzzer (ingave van ongeldige en onverwachte data) en DoS (Denial of Service) scripts niet getest, maar zijn mogelijk om als Blue team uit te voeren.

Scan en analyse targets met OWASP ZAP

Werkwijze gebaseerd op PluralSight course https://app.pluralsight.com/library/courses/owasp-zap-web-app-pentesting/table-of-contents

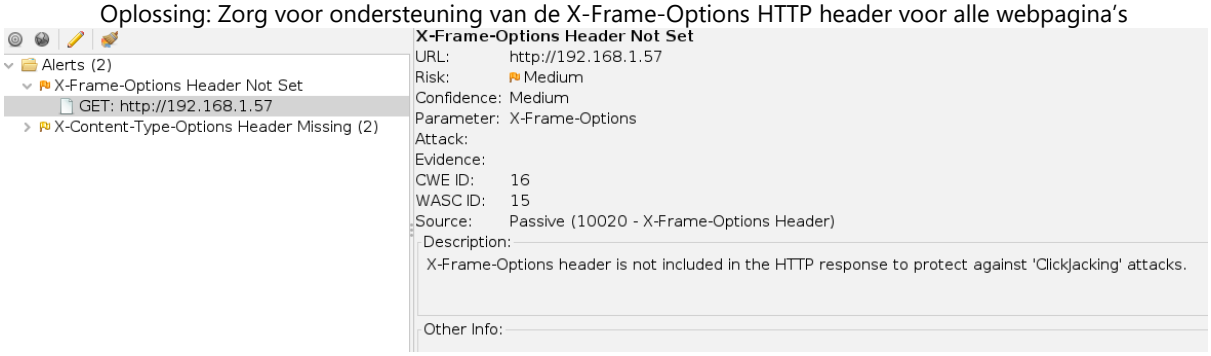
Aangezien OWASP ZAP een beveiligingsscanner voor webtoepassingen is en we via nmap hebben vastgesteld dat er 1 webserver is, nl RetroWeb, zullen we onze scan ook enkel op deze server uitvoeren.

>Start an autmated scan on URL http://192.168.1.57

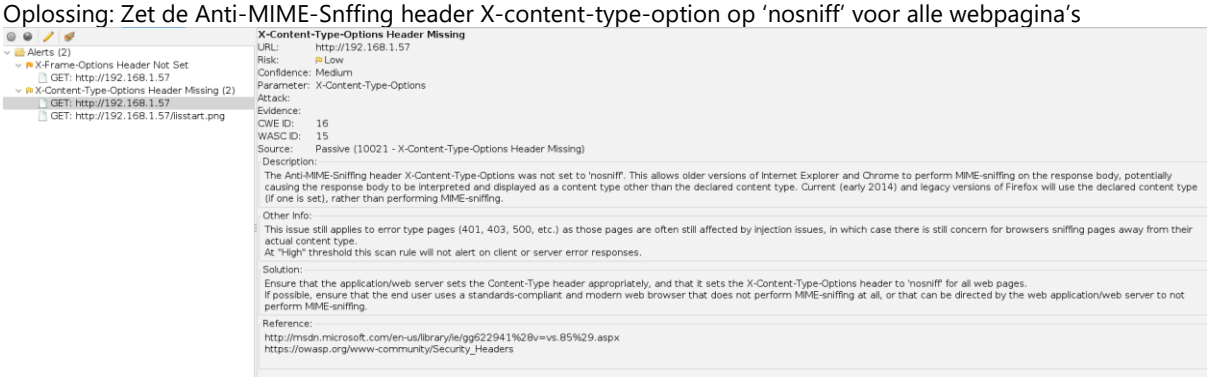


Dit resulteert in 3 alerts:

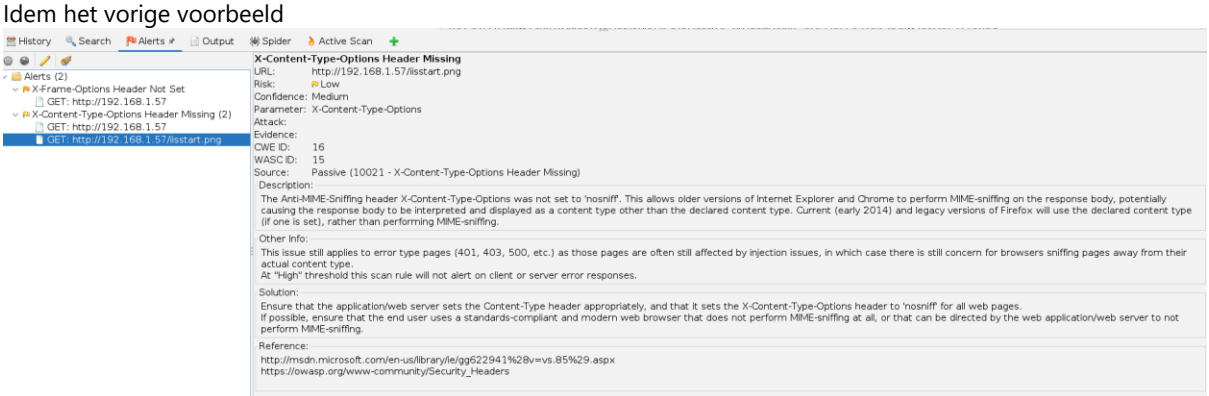
1. X-Frame-Options Header Not Set, waardoor de webserver vatbaar wordt tegen “ClickJacking” attacks
   Oplossing: Zorg voor ondersteuning van de X-Frame-Options HTTP header voor alle webpagina’s



2. X-Content-Type-Options Header Missing, waardoor er nog steeds sniffing mogelijk is.
   Oplossing: Zet de Anti-MIME-Snffing header X-content-type-option op ‘nosniff’ voor alle webpagina’s



3. Idem het vorige voorbeeld



Aangezien sniffing nog mogelijk is, kan er via tools als gobuster naar webpagina’s gezocht worden, die op hun beurt dan weer op kwetsbaarheden gescanned kunnen worden, maar dat brengt ons te ver van ons initiële doel.

Level B requirements

Werkwijze gebaseerd op PluralSight course https://app.pluralsight.com/library/courses/getting-started-memory-forensics-volatility/table-of-contents

Extra documentatie uit:
Volatility officiële website: https://www.volatilityfoundation.org/
Handige volatility commands en Plugins:
https://atalaysblog.wordpress.com/2019/07/13/useful-volatility-commands-plugins/
Volatility github and Kali Command reference:
https://github.com/volatilityfoundation/volatility/wiki/Command-Reference
https://tools.kali.org/forensics/volatility

De Kali VM van Offensive Security uit de level A testen zal ook gebruikt worden voor het Level B forensisch onderzoek.

Voorbereiding

Download Volatility source code van github

```
┌──(kali㉿kali)-[~/Downloads]
└─$ git clone https://github.com/volatilityfoundation/volatility.git
Cloning into 'volatility'...
remote: Enumerating objects: 27411, done.
remote: Total 27411 (delta 0), reused 0 (delta 0), pack-reused 27411
Receiving objects: 100% (27411/27411), 21.10 MiB | 4.20 MiB/s, done.
Resolving deltas: 100% (19758/19758), done.
```

Met ***> sudo python vol.py --info*** kunnen wij zien welke profiles, Address Spaces, Scanner Checks en Plugins default meegekomen zijn in de Volatility tool

Scanning van de dump van het werkgeheugen

Profile finding

* Algemene informatie memdump via plugin imageinfo:

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Downloads/Alissas-PC.raw)
                      PAE type : No PAE
                           DTB : 0x187000L
                          KDBG : 0xf800028100a0L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0xfffff80002811d00L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2019-12-11 14:38:00 UTC+0000
     Image local date and time : 2019-12-11 20:08:00 +0530
```

Hier kunnen we al nuttige info uithalen zoals welk profile we kunnen proberen met de volatility-tool om meer gerichte analyses te doen.

* Een uitbreiding hierop is **>sudo python vol.py -f ../Alissas-PC.raw kdbgscan** dat meer accurate informatie toont over het te gebruiken profiel. Deze plugin is extreem belangrijk om memory images te analyseren omdat ze informatie bevat over het systeem, de pointers naar de start van de lijst met actieve processen en de kernel modules

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw kdbgscan
Volatility Foundation Volatility Framework 2.6.1
**************************************************
Instantiating KDBG using: /home/kali/Downloads/Alissas-PC.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x28100a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x64
PsActiveProcessHead           : 0x2846b90
PsLoadedModuleList            : 0x2864e90
KernelBase                    : 0xfffff8000261f000

**************************************************
Instantiating KDBG using: /home/kali/Downloads/Alissas-PC.raw WinXPSP2x86 (5.1.0 32bit)
Offset (P)                    : 0x28100a0
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win2008R2SP1x64
PsActiveProcessHead           : 0x2846b90
PsLoadedModuleList            : 0x2864e90
KernelBase                    : 0xfffff8000261f000
```

Hier wordt duidelijk dat het OS WinXP met SP2 is.

Process Listing

* pslist lijst alle processen van een systeem op, op het moment van de geheugendump.

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 pslist
Volatility Foundation Volatility Framework 2.6.1
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xfffffa8000ca0040 System                    4      0     80      570 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800148f040 smss.exe                248      4      3       37 ------      0 2019-12-11 13:41:25 UTC+0000
0xfffffa800154f740 csrss.exe               320    312      9      457      0      0 2019-12-11 13:41:32 UTC+0000
0xfffffa8000ca81e0 csrss.exe               368    360      7      199      1      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c45060 psxss.exe               376    248     18      786      0      0 2019-12-11 13:41:33 UTC+0000
0xfffffa8001c5f060 winlogon.exe            416    360      4      118      1      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c5f630 wininit.exe             424    312      3       75      0      0 2019-12-11 13:41:34 UTC+0000
0xfffffa8001c98530 services.exe            484    424     13      219      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca0580 lsass.exe               492    424      9      764      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001ca4b30 lsm.exe                 500    424     11      185      0      0 2019-12-11 13:41:35 UTC+0000
0xfffffa8001cf4b30 svchost.exe             588    484     11      358      0      0 2019-12-11 13:41:39 UTC+0000
0xfffffa8001d327c0 VBoxService.ex          652    484     13      137      0      0 2019-12-11 13:41:40 UTC+0000
0xfffffa8001d49b30 svchost.exe             720    484      8      279      0      0 2019-12-11 13:41:41 UTC+0000
0xfffffa8001d8c420 svchost.exe             816    484     23      569      0      0 2019-12-11 13:41:42 UTC+0000
0xfffffa8001da5b30 svchost.exe             852    484     28      542      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001da96c0 svchost.exe             876    484     32      941      0      0 2019-12-11 13:41:43 UTC+0000
0xfffffa8001e1bb30 svchost.exe             472    484     19      476      0      0 2019-12-11 13:41:47 UTC+0000
0xfffffa8001e50b30 svchost.exe            1044    484     14      366      0      0 2019-12-11 13:41:48 UTC+0000
0xfffffa8001eba230 spoolsv.exe            1208    484     13      282      0      0 2019-12-11 13:41:51 UTC+0000
0xfffffa8001eda060 svchost.exe            1248    484     19      313      0      0 2019-12-11 13:41:52 UTC+0000
0xfffffa8001f58890 svchost.exe            1372    484     22      295      0      0 2019-12-11 13:41:54 UTC+0000
0xfffffa8001f91b30 TCPSVCS.EXE            1416    484      4       97      0      0 2019-12-11 13:41:55 UTC+0000
0xfffffa8000d3c400 sppsvc.exe             1508    484      4      141      0      0 2019-12-11 14:16:06 UTC+0000
0xfffffa8001c38580 svchost.exe             948    484     13      322      0      0 2019-12-11 14:16:07 UTC+0000
0xfffffa8002170630 wmpnetwk.exe           1856    484     16      451      0      0 2019-12-11 14:16:08 UTC+0000
0xfffffa8001d376f0 SearchIndexer.          480    484     14      701      0      0 2019-12-11 14:16:09 UTC+0000
0xfffffa8001eb47f0 taskhost.exe            296    484      8      151      1      0 2019-12-11 14:32:24 UTC+0000
0xfffffa8001dfa910 dwm.exe                1988    852      5       72      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa8002046960 explorer.exe            604   2016     33      927      1      0 2019-12-11 14:32:25 UTC+0000
0xfffffa80021c75d0 VBoxTray.exe           1844    604     11      140      1      0 2019-12-11 14:32:35 UTC+0000
0xfffffa80021da060 audiodg.exe            2064    816      6      131      0      0 2019-12-11 14:32:37 UTC+0000
0xfffffa80022199e0 svchost.exe            2368    484      9      365      0      0 2019-12-11 14:32:51 UTC+0000
0xfffffa8002222780 cmd.exe                1984    604      1       21      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa8002227140 conhost.exe            2692    368      2       50      1      0 2019-12-11 14:34:54 UTC+0000
0xfffffa80022bab30 mspaint.exe            2424    604      6      128      1      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8000eac770 svchost.exe            2660    484      6      100      0      0 2019-12-11 14:35:14 UTC+0000
0xfffffa8001e68060 csrss.exe              2760   2680      7      172      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000ecbb30 winlogon.exe           2808   2680      4      119      2      0 2019-12-11 14:37:05 UTC+0000
0xfffffa8000f3aab0 taskhost.exe           2908    484      9      158      2      0 2019-12-11 14:37:13 UTC+0000
0xfffffa8000f4db30 dwm.exe                3004    852      5       72      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f4c670 explorer.exe           2504   3000     34      825      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000f9a4e0 VBoxTray.exe           2304   2504     14      144      2      0 2019-12-11 14:37:14 UTC+0000
0xfffffa8000fff630 SearchProtocol         2524    480      7      226      2      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8000ecea60 SearchFilterHo         1720    480      5       90      0      0 2019-12-11 14:37:21 UTC+0000
0xfffffa8001010b30 WinRAR.exe             1512   2504      6      207      2      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001020b30 SearchProtocol         2868    480      8      279      0      0 2019-12-11 14:37:23 UTC+0000
0xfffffa8001048060 DumpIt.exe              796    604      2       45      1      1 2019-12-11 14:37:54 UTC+0000
0xfffffa800104a780 conhost.exe            2260    368      2       50      1      0 2019-12-11 14:37:54 UTC+0000
```

* pstree werkt hetzelfde als pslist, maar toont daarbovenop ook de parent/child relatie.

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xfffffa8000f4c670:explorer.exe                     2504   3000     34    825 2019-12-11 14:37:14 UTC+0000
. 0xfffffa8000f9a4e0:VBoxTray.exe                    2304   2504     14    144 2019-12-11 14:37:14 UTC+0000
. 0xfffffa8001010b30:WinRAR.exe                      1512   2504      6    207 2019-12-11 14:37:23 UTC+0000
 0xfffffa8001c5f630:wininit.exe                       424    312      3     75 2019-12-11 13:41:34 UTC+0000
. 0xfffffa8001c98530:services.exe                     484    424     13    219 2019-12-11 13:41:35 UTC+0000
.. 0xfffffa8002170630:wmpnetwk.exe                   1856    484     16    451 2019-12-11 14:16:08 UTC+0000
.. 0xfffffa8001f91b30:TCPSVCS.EXE                    1416    484      4     97 2019-12-11 13:41:55 UTC+0000
.. 0xfffffa8001da96c0:svchost.exe                     876    484     32    941 2019-12-11 13:41:43 UTC+0000
.. 0xfffffa8001d327c0:VBoxService.ex                  652    484     13    137 2019-12-11 13:41:40 UTC+0000
.. 0xfffffa8000eac770:svchost.exe                    2660    484      6    100 2019-12-11 14:35:14 UTC+0000
.. 0xfffffa80022199e0:svchost.exe                    2368    484      9    365 2019-12-11 14:32:51 UTC+0000
.. 0xfffffa8001e50b30:svchost.exe                    1044    484     14    366 2019-12-11 13:41:48 UTC+0000
.. 0xfffffa8001d8c420:svchost.exe                     816    484     23    569 2019-12-11 13:41:42 UTC+0000
... 0xfffffa80021da060:audiodg.exe                   2064    816      6    131 2019-12-11 14:32:37 UTC+0000
.. 0xfffffa8001c38580:svchost.exe                     948    484     13    322 2019-12-11 14:16:07 UTC+0000
.. 0xfffffa8001eba230:spoolsv.exe                    1208    484     13    282 2019-12-11 13:41:51 UTC+0000
.. 0xfffffa8001d376f0:SearchIndexer.                  480    484     14    701 2019-12-11 14:16:09 UTC+0000
... 0xfffffa8000fff630:SearchProtocol                2524    480      7    226 2019-12-11 14:37:21 UTC+0000
... 0xfffffa8001020b30:SearchProtocol                2868    480      8    279 2019-12-11 14:37:23 UTC+0000
... 0xfffffa8000ecea60:SearchFilterHo                1720    480      5     90 2019-12-11 14:37:21 UTC+0000
.. 0xfffffa8000f3aab0:taskhost.exe                   2908    484      9    158 2019-12-11 14:37:13 UTC+0000
.. 0xfffffa8001cf4b30:svchost.exe                     588    484     11    358 2019-12-11 13:41:39 UTC+0000
.. 0xfffffa8001d49b30:svchost.exe                     720    484      8    279 2019-12-11 13:41:41 UTC+0000
.. 0xfffffa8001da5b30:svchost.exe                     852    484     28    542 2019-12-11 13:41:43 UTC+0000
... 0xfffffa8000f4db30:dwm.exe                       3004    852      5     72 2019-12-11 14:37:14 UTC+0000
... 0xfffffa8001dfa910:dwm.exe                       1988    852      5     72 2019-12-11 14:32:25 UTC+0000
.. 0xfffffa8001e1bb30:svchost.exe                     472    484     19    476 2019-12-11 13:41:47 UTC+0000
.. 0xfffffa8000d3c400:sppsvc.exe                     1508    484      4    141 2019-12-11 14:16:06 UTC+0000
.. 0xfffffa8001f58890:svchost.exe                    1372    484     22    295 2019-12-11 13:41:54 UTC+0000
.. 0xfffffa8001eda060:svchost.exe                    1248    484     19    313 2019-12-11 13:41:52 UTC+0000
.. 0xfffffa8001eb47f0:taskhost.exe                    296    484      8    151 2019-12-11 14:32:24 UTC+0000
. 0xfffffa8001ca0580:lsass.exe                        492    424      9    764 2019-12-11 13:41:35 UTC+0000
. 0xfffffa8001ca4b30:lsm.exe                          500    424     11    185 2019-12-11 13:41:35 UTC+0000
 0xfffffa800154f740:csrss.exe                         320    312      9    457 2019-12-11 13:41:32 UTC+0000
 0xfffffa8000ca0040:System                              4      0     80    570 2019-12-11 13:41:25 UTC+0000
. 0xfffffa800148f040:smss.exe                         248      4      3     37 2019-12-11 13:41:25 UTC+0000
.. 0xfffffa8001c45060:psxss.exe                       376    248     18    786 2019-12-11 13:41:33 UTC+0000
 0xfffffa8001c5f060:winlogon.exe                      416    360      4    118 2019-12-11 13:41:34 UTC+0000
 0xfffffa8000ca81e0:csrss.exe                         368    360      7    199 2019-12-11 13:41:33 UTC+0000
. 0xfffffa8002227140:conhost.exe                     2692    368      2     50 2019-12-11 14:34:54 UTC+0000
. 0xfffffa800104a780:conhost.exe                     2260    368      2     50 2019-12-11 14:37:54 UTC+0000
 0xfffffa8002046960:explorer.exe                      604   2016     33    927 2019-12-11 14:32:25 UTC+0000
. 0xfffffa80021c75d0:VBoxTray.exe                    1844    604     11    140 2019-12-11 14:32:35 UTC+0000
. 0xfffffa8002222780:cmd.exe                         1984    604      1     21 2019-12-11 14:34:54 UTC+0000
. 0xfffffa80022bab30:mspaint.exe                     2424    604      6    128 2019-12-11 14:35:14 UTC+0000
. 0xfffffa8001048060:DumpIt.exe                       796    604      2     45 2019-12-11 14:37:54 UTC+0000
 0xfffffa8001e68060:csrss.exe                        2760   2680      7    172 2019-12-11 14:37:05 UTC+0000
 0xfffffa8000ecbb30:winlogon.exe                     2808   2680      4    119 2019-12-11 14:37:05 UTC+0000
```

* Bovenstaande commando’s werken door het doorlopen van de dubbelgelinkte lijst waarnaar verwezen wordt in de psactive process head (en deze bevat een lijst met eprocess objecten voor processen). Sommige malware kan deze eprocess objecten weliswaar ‘unlinken’ waardoor pslist en pstree deze processen dus niet kunnen opsporen. Hiervoor bestaat gelukkig psscan, dat verborgen en niet-gelinkte processes kan vinden door een techniek die pool tag scanning wordt genoemd.

```
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 psscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)          Name                PID   PPID PDB                Time created                   Time exited
------------------ ---------------- ------ ------ ------------------ ------------------------------ ------------------------------
0x000000003e8199e0 svchost.exe        2368    484 0x000000002f8cf000 2019-12-11 14:32:51 UTC+0000
0x000000003e822780 cmd.exe            1984    604 0x000000002457b000 2019-12-11 14:34:54 UTC+0000
0x000000003e827140 conhost.exe        2692    368 0x0000000023e17000 2019-12-11 14:34:54 UTC+0000
0x000000003e8bab30 mspaint.exe        2424    604 0x000000003a581000 2019-12-11 14:35:14 UTC+0000
0x000000003ea46960 explorer.exe        604   2016 0x0000000035a79000 2019-12-11 14:32:25 UTC+0000
0x000000003eb70630 wmpnetwk.exe       1856    484 0x000000000e83e000 2019-12-11 14:16:08 UTC+0000
0x000000003ebc75d0 VBoxTray.exe       1844    604 0x0000000034c66000 2019-12-11 14:32:35 UTC+0000
0x000000003ebda060 audiodg.exe        2064    816 0x000000003218c000 2019-12-11 14:32:37 UTC+0000
0x000000003ec1bb30 svchost.exe         472    484 0x000000001aa76000 2019-12-11 13:41:47 UTC+0000
0x000000003ec50b30 svchost.exe        1044    484 0x000000001a6be000 2019-12-11 13:41:48 UTC+0000
0x000000003ec68060 csrss.exe          2760   2680 0x000000001b94e000 2019-12-11 14:37:05 UTC+0000
0x000000003ecb47f0 taskhost.exe        296    484 0x0000000036347000 2019-12-11 14:32:24 UTC+0000
0x000000003ecba230 spoolsv.exe        1208    484 0x00000000177ce000 2019-12-11 13:41:51 UTC+0000
0x000000003ecda060 svchost.exe        1248    484 0x000000001729c000 2019-12-11 13:41:52 UTC+0000
0x000000003ed58890 svchost.exe        1372    484 0x0000000013f1b000 2019-12-11 13:41:54 UTC+0000
0x000000003ed91b30 TCPSVCS.EXE        1416    484 0x000000000098c0000 2019-12-11 13:41:55 UTC+0000
0x000000003ee38580 svchost.exe         948    484 0x000000000eab3000 2019-12-11 14:16:07 UTC+0000
0x000000003ee45060 psxss.exe           376    248 0x000000001f70a000 2019-12-11 13:41:33 UTC+0000
0x000000003ee5f060 winlogon.exe        416    360 0x000000001f20c000 2019-12-11 13:41:34 UTC+0000
0x000000003ee5f630 wininit.exe         424    312 0x000000001f079000 2019-12-11 13:41:34 UTC+0000
0x000000003ee98530 services.exe        484    424 0x000000001e531000 2019-12-11 13:41:35 UTC+0000
0x000000003eea0580 lsass.exe           492    424 0x000000001e3d2000 2019-12-11 13:41:35 UTC+0000
0x000000003eea4b30 lsm.exe             500    424 0x000000001e55a000 2019-12-11 13:41:35 UTC+0000
0x000000003eef4b30 svchost.exe         588    484 0x000000001d4f4000 2019-12-11 13:41:39 UTC+0000
0x000000003ef327c0 VBoxService.ex      652    484 0x000000001d0dc000 2019-12-11 13:41:40 UTC+0000
0x000000003ef376f0 SearchIndexer.      480    484 0x000000000dc08000 2019-12-11 14:16:09 UTC+0000
0x000000003ef49b30 svchost.exe         720    484 0x000000001cdac000 2019-12-11 13:41:41 UTC+0000
0x000000003ef8c420 svchost.exe         816    484 0x000000001c795000 2019-12-11 13:41:42 UTC+0000
0x000000003efa5b30 svchost.exe         852    484 0x000000001bfde000 2019-12-11 13:41:43 UTC+0000
0x000000003efa96c0 svchost.exe         876    484 0x000000001c0e4000 2019-12-11 13:41:43 UTC+0000
0x000000003effa910 dwm.exe            1988    852 0x0000000360d7000 2019-12-11 14:32:25 UTC+0000
0x000000003f68f040 smss.exe            248      4 0x00000000261ec000 2019-12-11 13:41:25 UTC+0000
0x000000003f74f740 csrss.exe           320    312 0x000000001fcb3000 2019-12-11 13:41:32 UTC+0000
0x000000003fa10b30 WinRAR.exe         1512   2504 0x0000000019835000 2019-12-11 14:37:23 UTC+0000
0x000000003fa20b30 SearchProtocol     2868    480 0x0000000017b1b000 2019-12-11 14:37:23 UTC+0000
0x000000003fa48060 DumpIt.exe          796    604 0x00000000143d6000 2019-12-11 14:37:54 UTC+0000
0x000000003fa4a780 conhost.exe        2260    368 0x0000000012d9b000 2019-12-11 14:37:54 UTC+0000
0x000000003fa95b30 WinRAR.exe         1512   2504 0x0000000019835000 2019-12-11 14:37:23 UTC+0000
0x000000003faa5b30 SearchProtocol     2868    480 0x0000000017b1b000 2019-12-11 14:37:23 UTC+0000
0x000000003facd060 DumpIt.exe          796    604 0x00000000143d6000 2019-12-11 14:37:54 UTC+0000
0x000000003facf780 conhost.exe        2260    368 0x0000000012d9b000 2019-12-11 14:37:54 UTC+0000
0x000000003fb1ab30 WinRAR.exe         1512   2504 0x0000000019835000 2019-12-11 14:37:23 UTC+0000
0x000000003fb2ab30 SearchProtocol     2868    480 0x0000000017b1b000 2019-12-11 14:37:23 UTC+0000
0x000000003fb52060 DumpIt.exe          796    604 0x00000000143d6000 2019-12-11 14:37:54 UTC+0000
0x000000003fb54780 conhost.exe        2260    368 0x0000000012d9b000 2019-12-11 14:37:54 UTC+0000
0x000000003fcac770 svchost.exe        2660    484 0x0000000001d2e000 2019-12-11 14:35:14 UTC+0000
0x000000003fccbb30 winlogon.exe       2808   2680 0x00000000261d3000 2019-12-11 14:37:05 UTC+0000
0x000000003fccea60 SearchFilterHo     1720    480 0x0000000019b05000 2019-12-11 14:37:21 UTC+0000
0x000000003fd3aab0 taskhost.exe       2908    484 0x000000000b291000 2019-12-11 14:37:13 UTC+0000
0x000000003fd4c670 explorer.exe       2504   3000 0x0000000008771000 2019-12-11 14:37:14 UTC+0000
0x000000003fd4db30 dwm.exe            3004    852 0x0000000016de7000 2019-12-11 14:37:14 UTC+0000
0x000000003fd9a4e0 VBoxTray.exe       2304   2504 0x0000000007a54000 2019-12-11 14:37:14 UTC+0000
0x000000003fdff630 SearchProtocol     2524    480 0x0000000037d69000 2019-12-11 14:37:21 UTC+0000
0x000000003febb400 sppsvc.exe         1508    484 0x000000000f4ee000 2019-12-11 14:16:06 UTC+0000
0x000000003ff5f040 System                4      0 0x0000000000187000 2019-12-11 13:41:25 UTC+0000
0x000000003ff671e0 csrss.exe           368    360 0x000000003bd46000 2019-12-11 13:41:33 UTC+0000
```

Andere nuttige commands te gebruiken als toevoeging op de process listing commands:
dlllist toont de ingeladen DLLs van een process. Aangezien dit een enorme lange lijst is, wordt deze meestal enkel gebruikt om de details van een bepaalde pid te vinden. Dit kan door parameter -p <PID> toe te voegen.

handles toont de open handles van een process en bevat dus zeer nuttige informatie over welke files, registry keys, threads en andere objecten bezig waren met een process.

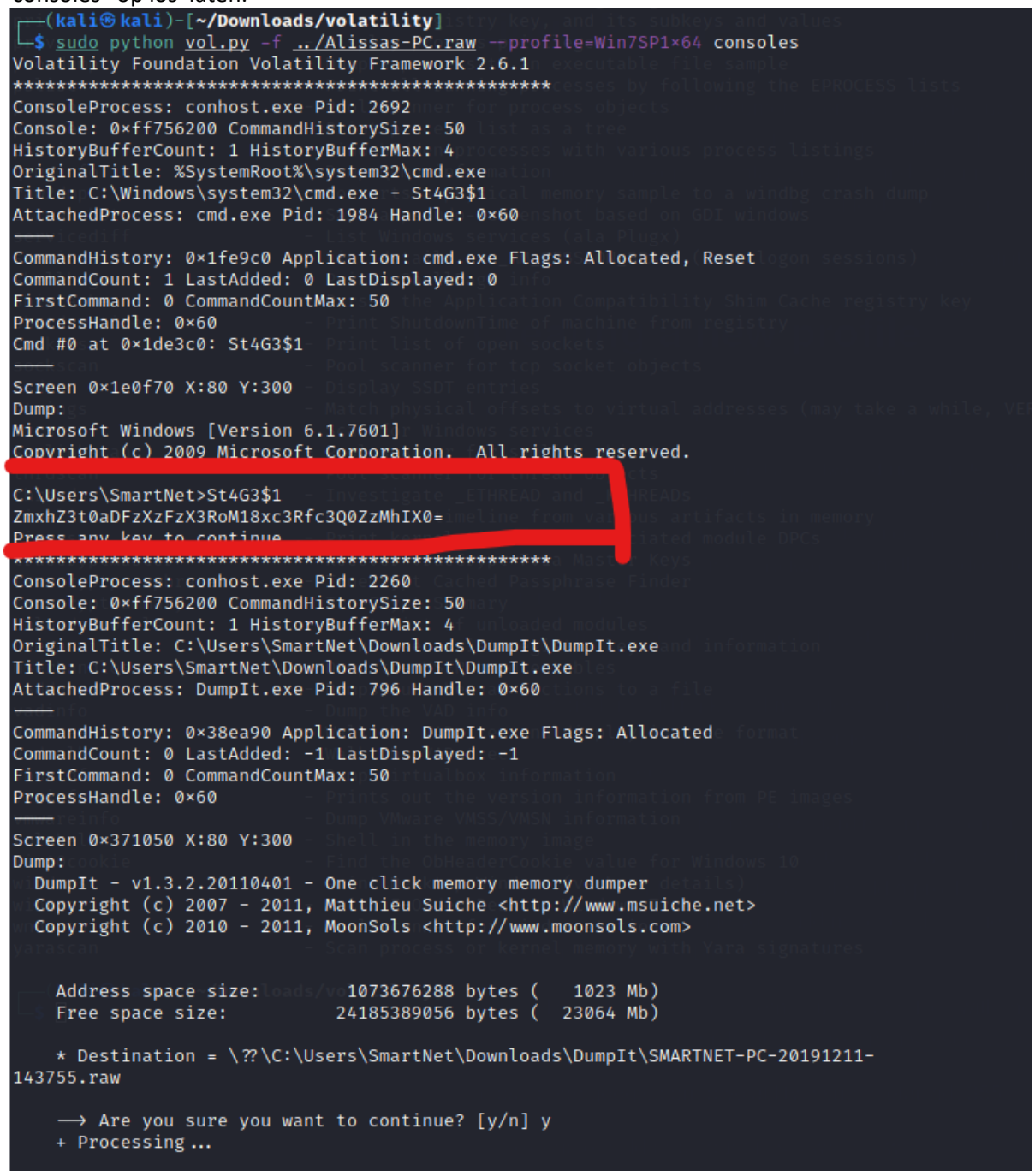
Analyse van de dump van het werkgeheugen

Met bovenstaande wetenschap gaan we aan de slag met het oplossen van de vragen:

Opdracht 1: Recover het windows wachtwoord

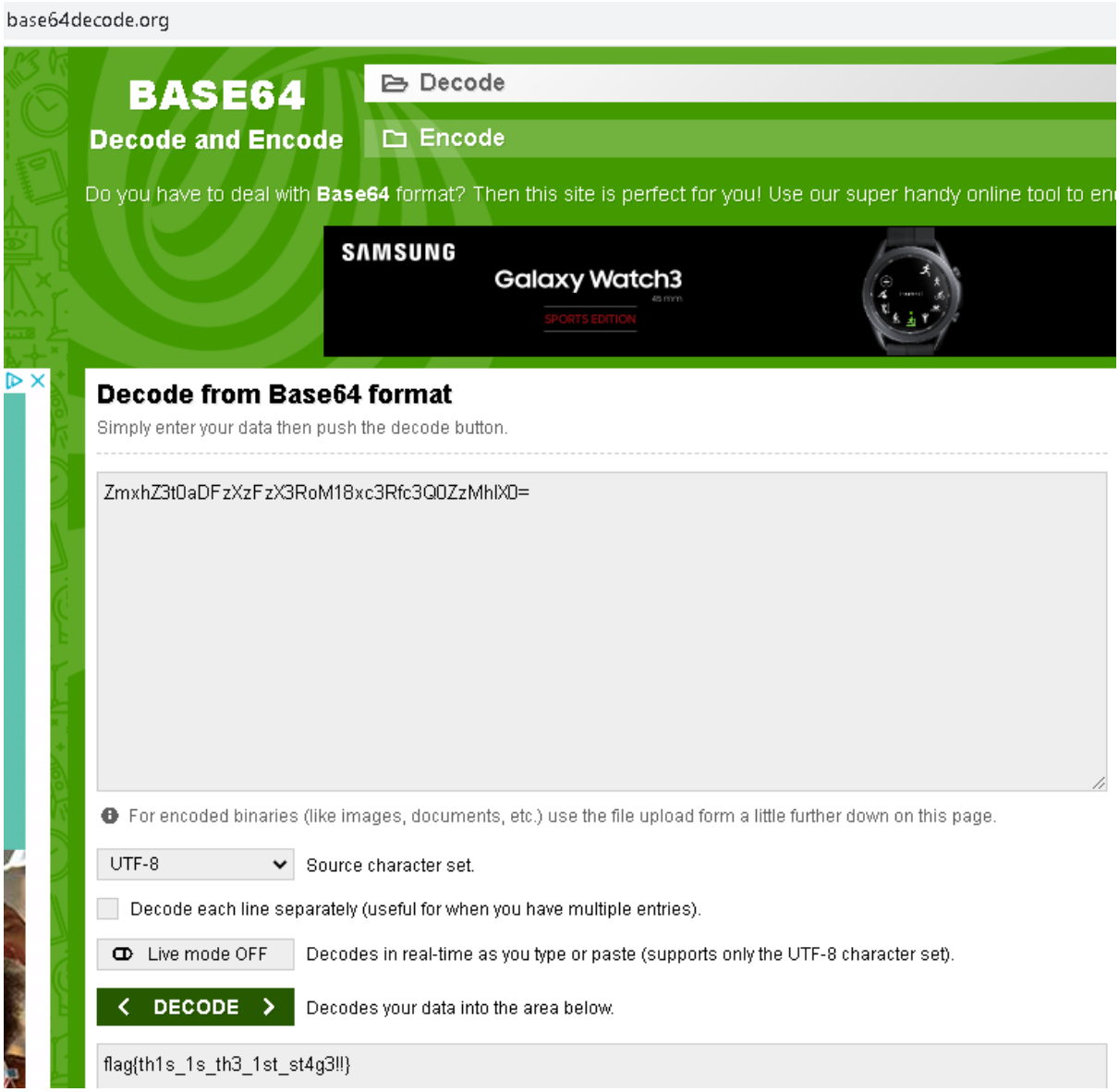
1. Imageinfo leert ons profiel “Win7SP1x64”te gebruiken.

2. een belangrijk proces voor paswoordrecovery kan cmd.exe zijn aangezien hier de hele geschiedenis kan uitgelezen worden, inclusief command outputs. We kunnen hier commando “consoles” op los laten:



We zien dat conhost.exe een soort van commandline had, maar belangrijker:
C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzMhIX0=

- ⇨ dit is Base64 code. Decoden via website https://www.base64decode.org/ geeft



Voila! Het windows paswoord is gevonden! (flag{th1s_1s_th3_1st_st4g3!!})

Opdracht 2 : Vind 'important.rar' en toon de inhoud

1. Uit pslist zien we hier proces WinRAR.exe op de machine.
2. de cmdline module leert ons dat dit proces inderdaad Important.rar 'vast' heeft

```
**************************************************
WinRAR.exe pid:   1512
Command line : "C:\Program Files\WinRAR\WinRAR.exe" "C:\Users\Alissa Simpson\Documents\Important.rar"
**************************************************
```

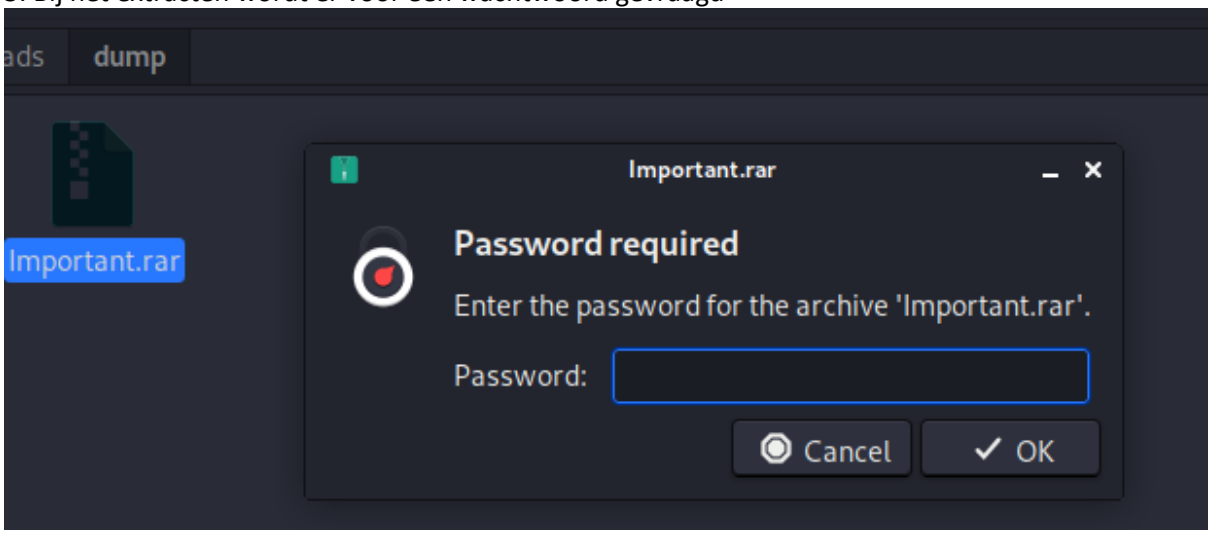
3. Een memdump kan meer licht op de file werpen

>sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 memdump -p 1512 -D ../dump/

4. De offset kunnen wij uit onze psscan eerder in deze opdracht lezen om de file met “dumpfiles” te extracten.

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 dumpfiles -D ../dump/ -Q 0x000000003fb48bc0 -n
Volatility Foundation Volatility Framework 2.6.1
DataSectionObject 0x3fb48bc0   None   \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar

┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ cd ../dump

┌──(kali㉿kali)-[~/Downloads/dump]
└─$ ls
1512.dmp  file.None.0xfffffa8001034450.dat

┌──(kali㉿kali)-[~/Downloads/dump]
└─$ ls
1512.dmp  file.None.0xfffffa8001034450.dat

┌──(kali㉿kali)-[~/Downloads/dump]
└─$ mv file.None.0xfffffa8001034450.dat Important.rar
```

5. Bij het extracten wordt er voor een wachtwoord gevraagd



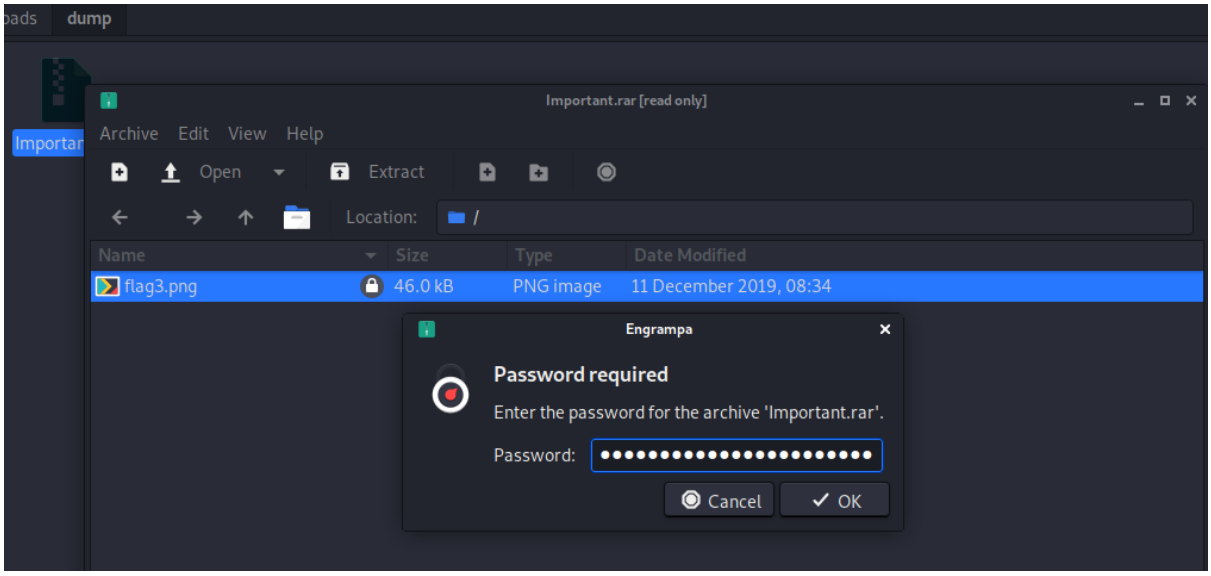
6. Met volatility strings op de dumpfile en een grep op string “pass” leert ons “Password is NTLM hash(in uppercase) of Alissa's account passwd.”

7. LM/NTLM hashes kunnen rechtstreeks uit het geheugen gehaald worden via een hashdump

```
┌──(kali㉿kali)-[~/Downloads/volatility]
└─$ sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 hashdump
Volatility Foundation Volatility Framework 2.6.1
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7e0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5:::
Alissa Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba6:::
```

f4ff64c8baac57d22f22edc681055ba6 in allemaal hoofdletters moet volgens voorgaande tip dus het paswoord zijn.

8. Succes! =>

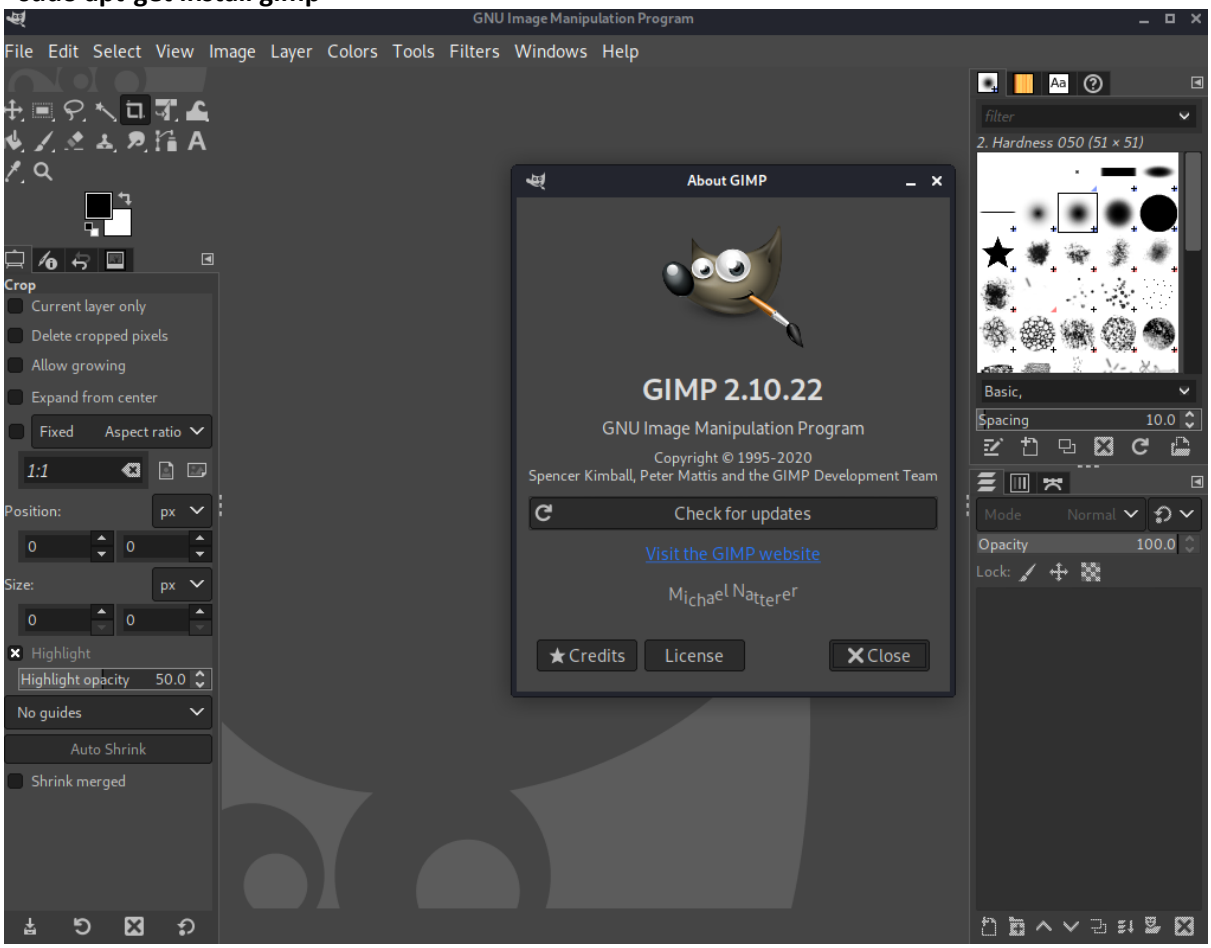

dump
Important.rar [read only]
Archive Edit View Help
Open
Extract
Location: /
Name
Size
Type
Date Modified
flag3.png
46.0 kB
PNG image
11 December 2019, 08:34
Engrampa
Password required
Enter the password for the archive 'Important.rar'.
Password:
Cancel
OK


flag3.png - Image Viewer
flag{w3ll_
3rd_stag
e_was_e
asy}
MEM LABS

Opdracht 3: Terughalen tekening MSPaint

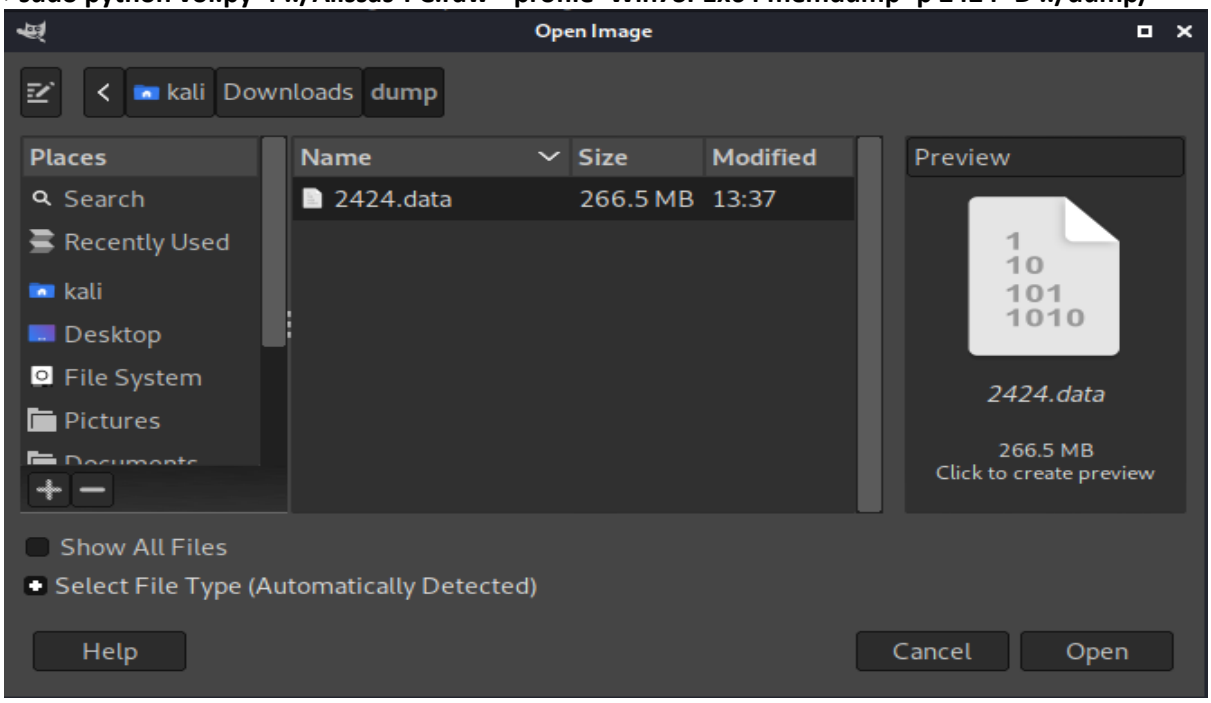
Gimp is een handig beeldverwerkingsprogramma geschreven in Python dat cross-platform werkt en ideaal is om MSPaint van Microsoft te vervangen in Linux. Méér nog! Gimp kan raw image data lezen!

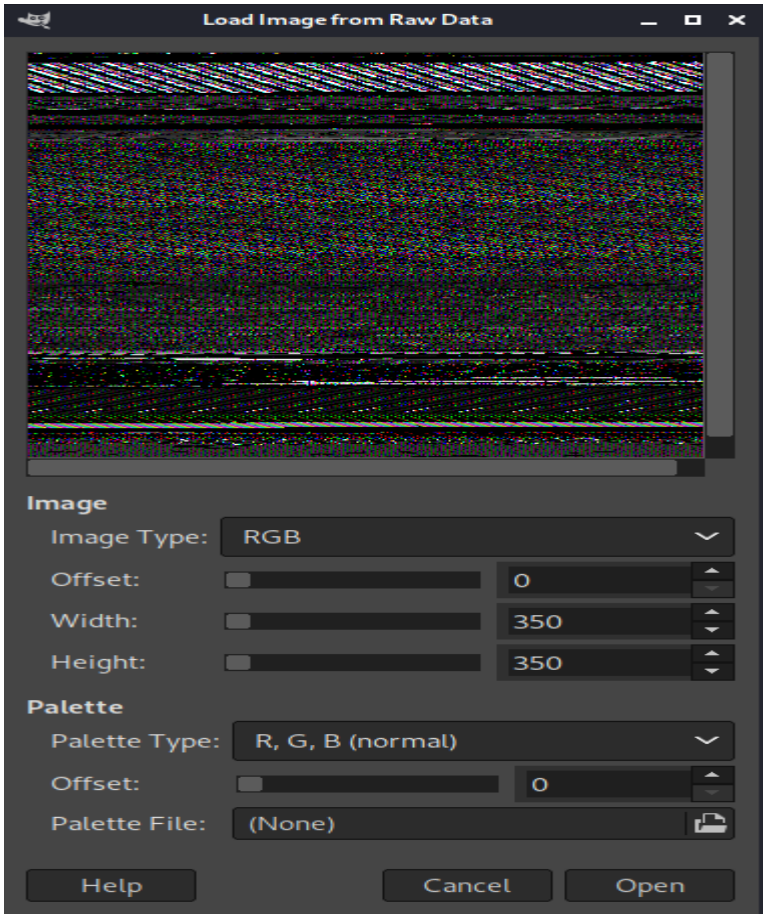
>sudo apt-get install gimp



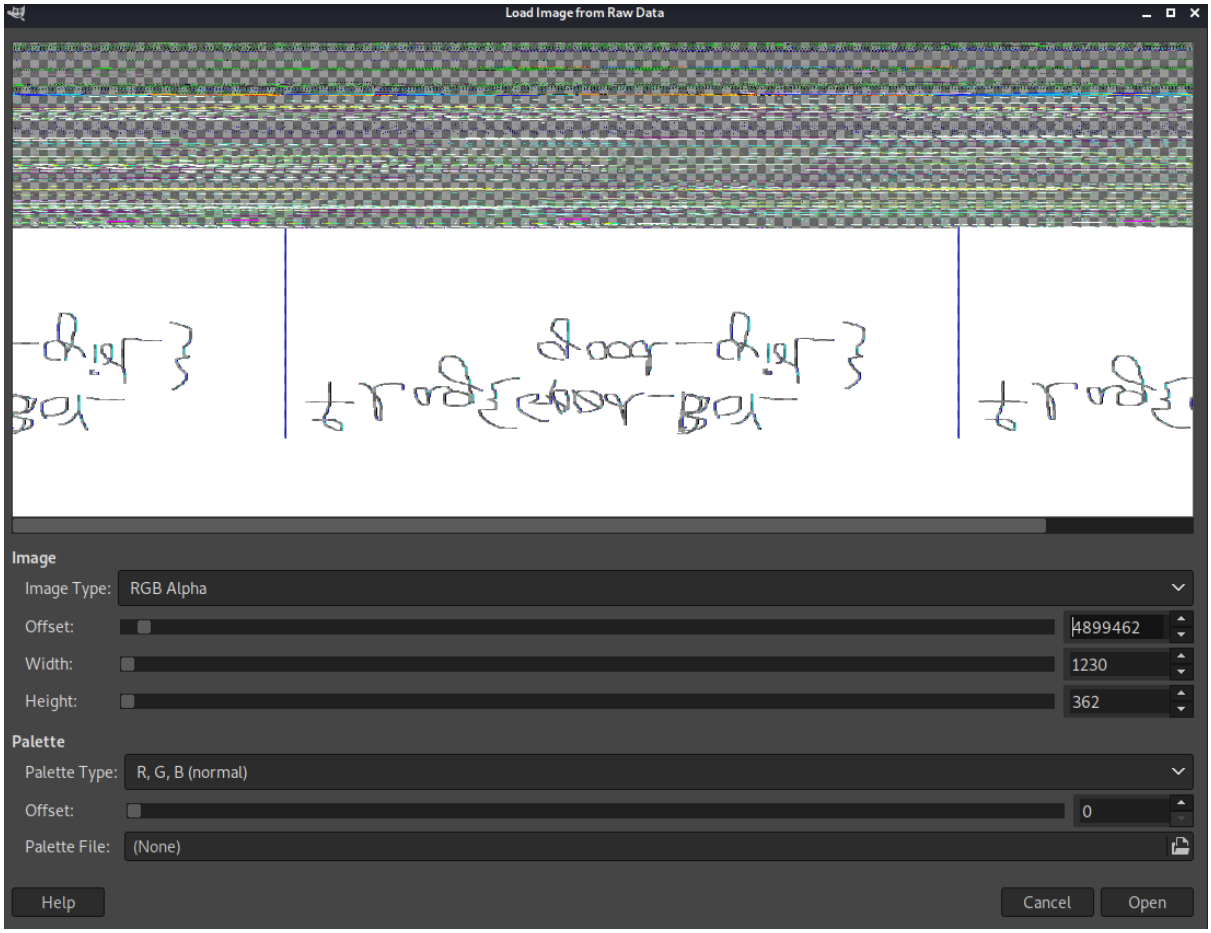
Na installatie nemen we een memdump van het mspaint.exe proces en renamen we het naar .data zodat Gimp deze herkent en kan openen.

>sudo python vol.py -f ../Alissas-PC.raw --profile=Win7SP1x64 memdump -p 2424 -D ../dump/

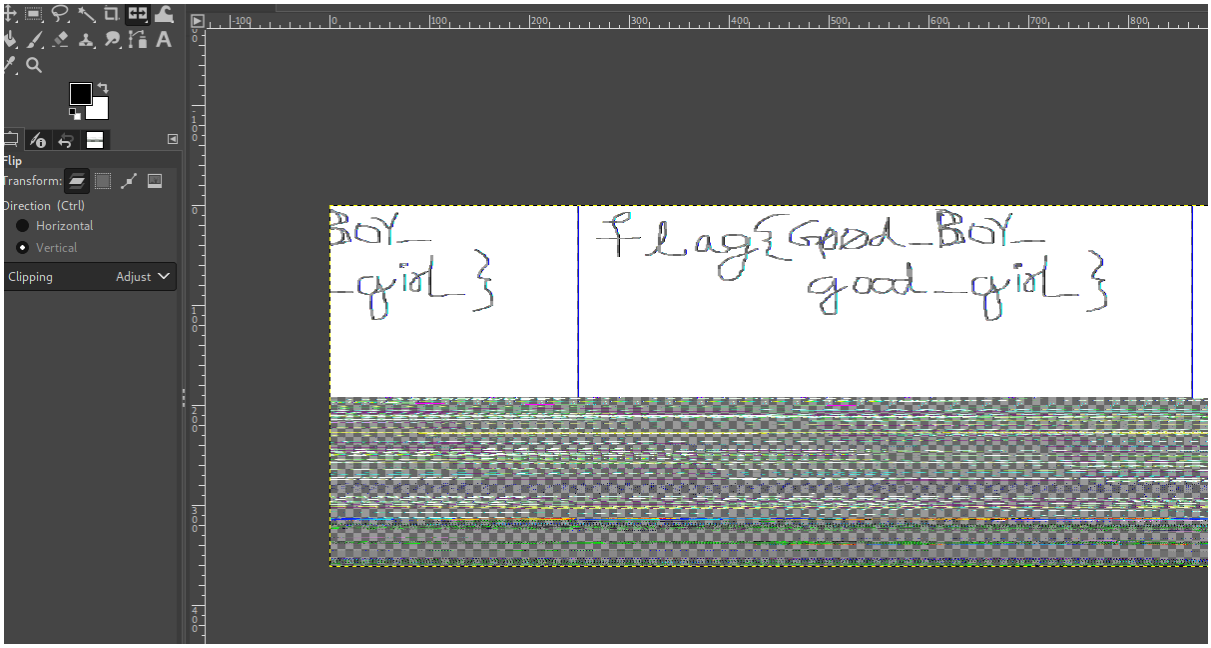




Na wat spelen met de offset krijgen we onderstaande resultaat!



En als we de picture omdraaien, krijgen we de oplossing!
=> flag{G00d_BOY_good_girL_}



Samenvatting:
Opdracht1 : Windows Wachtwoord = flag{th1s_1s_th3_1st_st4g3!!}
Opdracht2: Important.rar = flag{w311_3rd_stage_was_easy}
Opdracht3: MSPaint = flag{G00d_BOY_good_girL_}

Level A(+) requirements

Voorbereiding

Installeren Autopsy op Kali

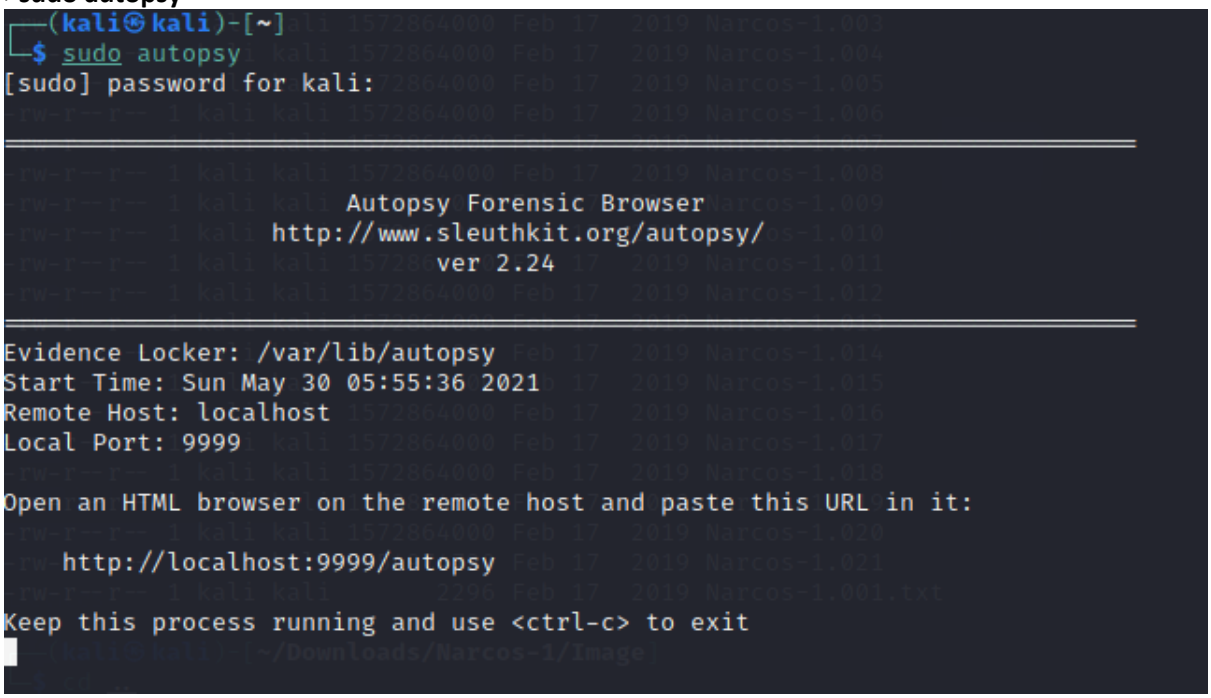
Installatie was al gebeurd in de VM gedownload van Offensive Security => versie 2.24

Downloaden forensic image and memory dump of Steve Kowhai (Narcos-1) van
https://digitalcorpora.org/corpora/scenarios/2019-narcos

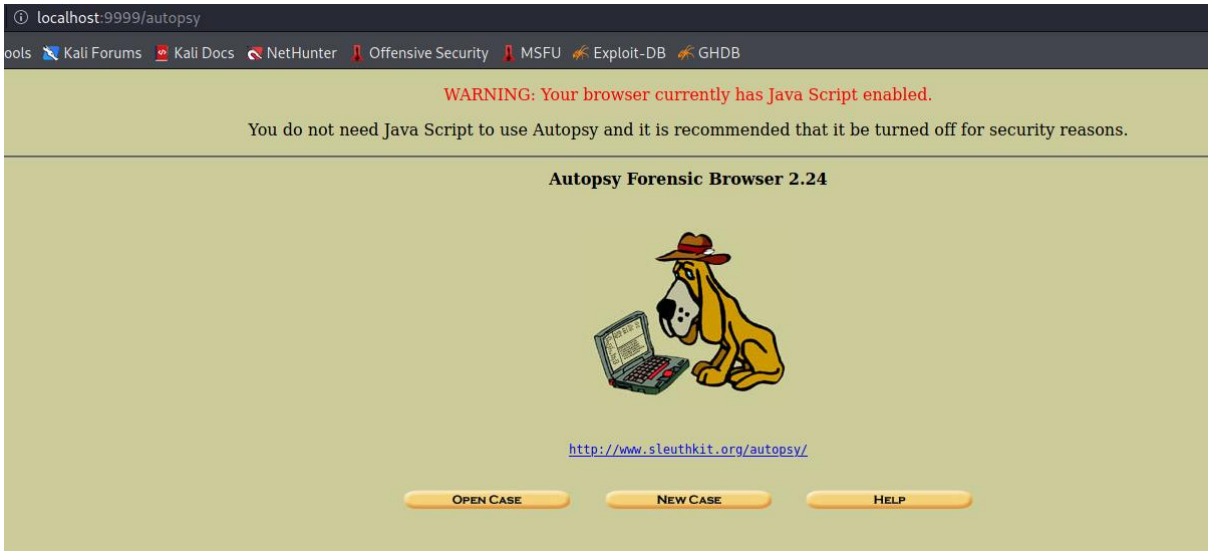
Start nieuwe Autopsy Case

* Start autopsy in Kali Linux:

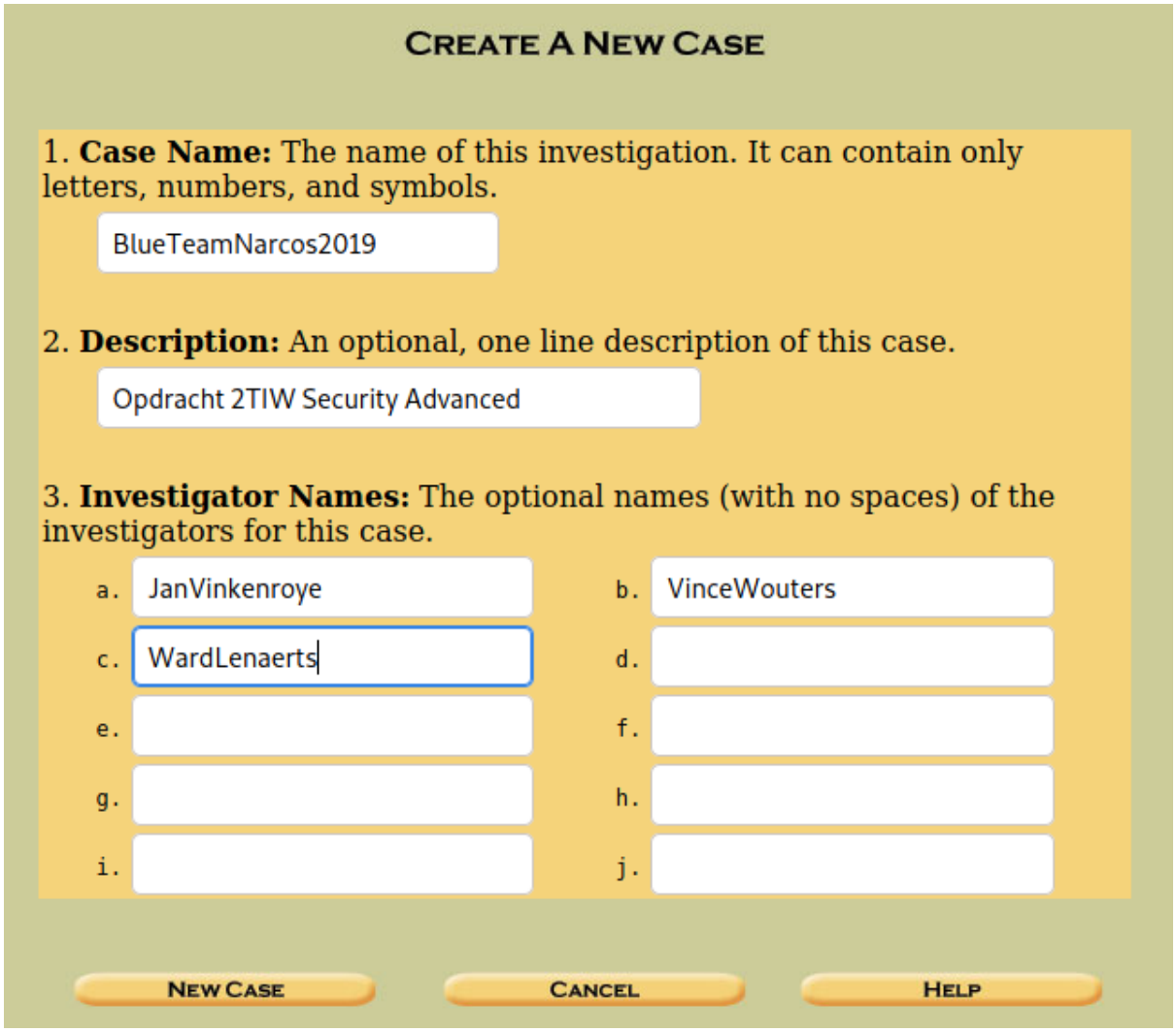
>sudo autopsy



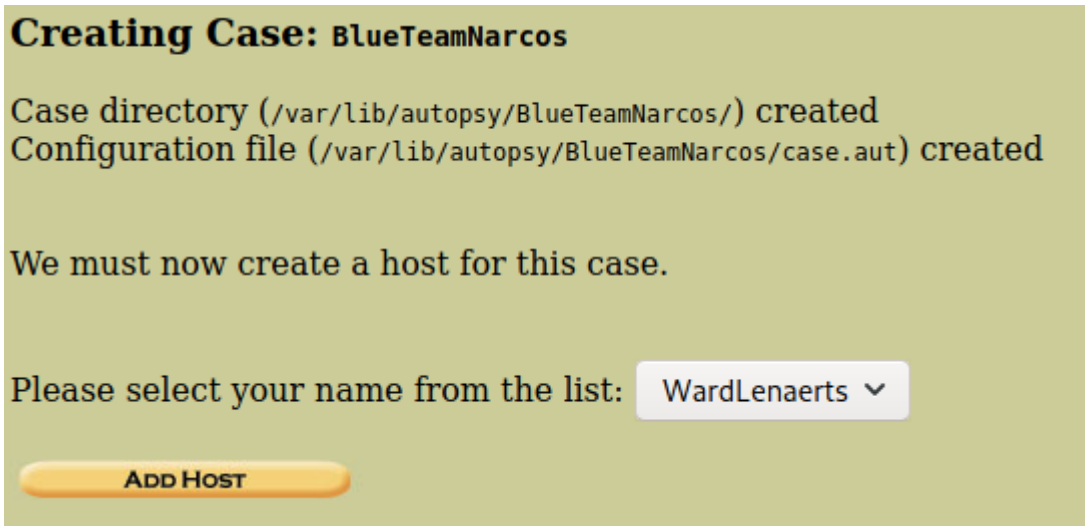
* Ga naar http://localhost:9999/autopsy in de browser.
* Kies “New Case”



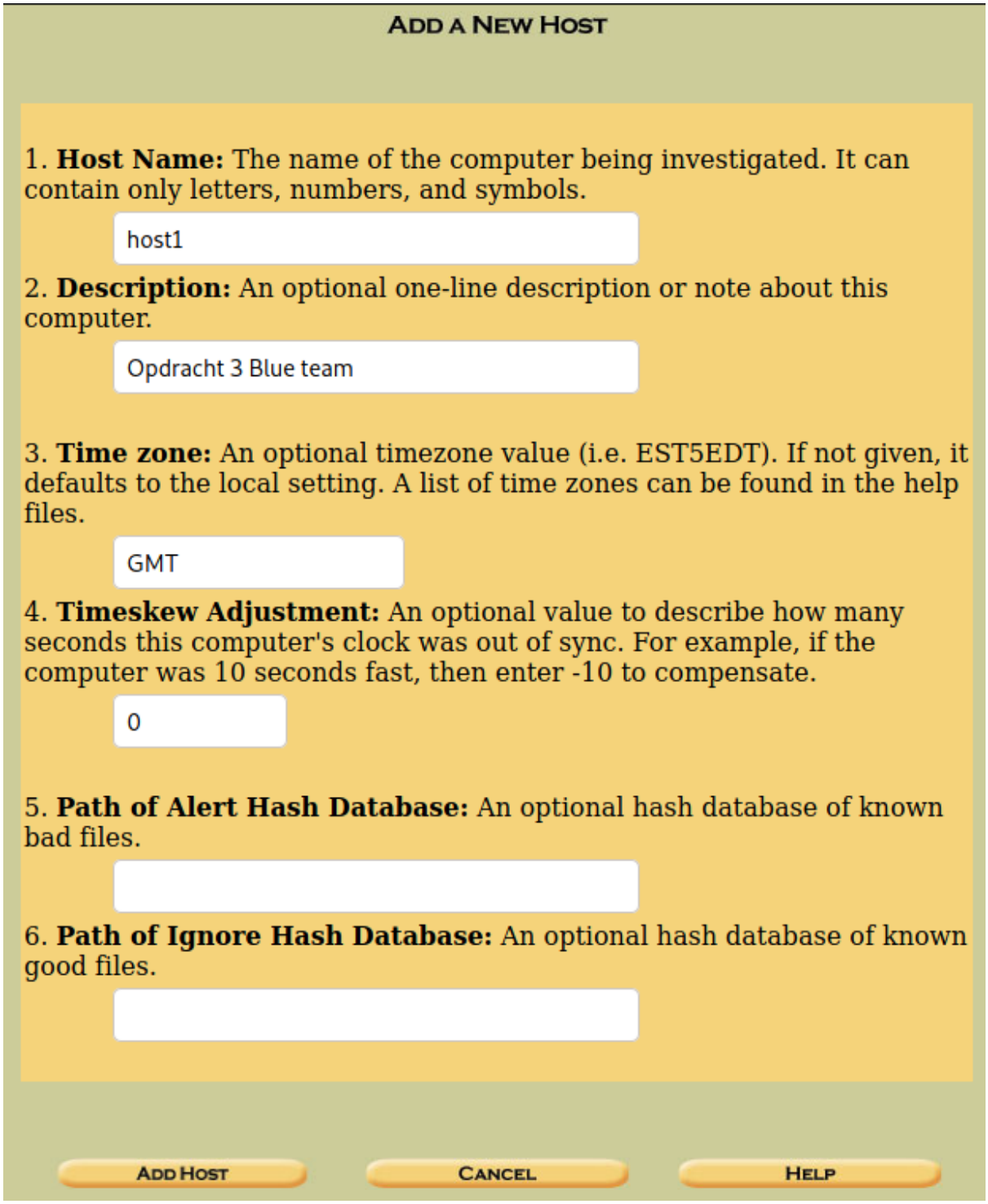
* Kies weer ”New Case” na het invullen van enkele gegevens



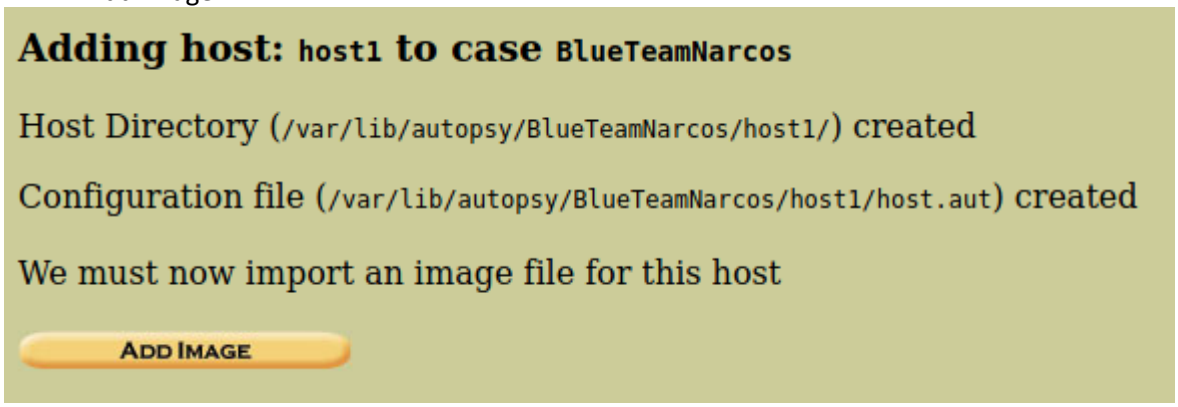
* Klik “Add Host”



* Klik weer “Add Host” na het invullen van enkele velden



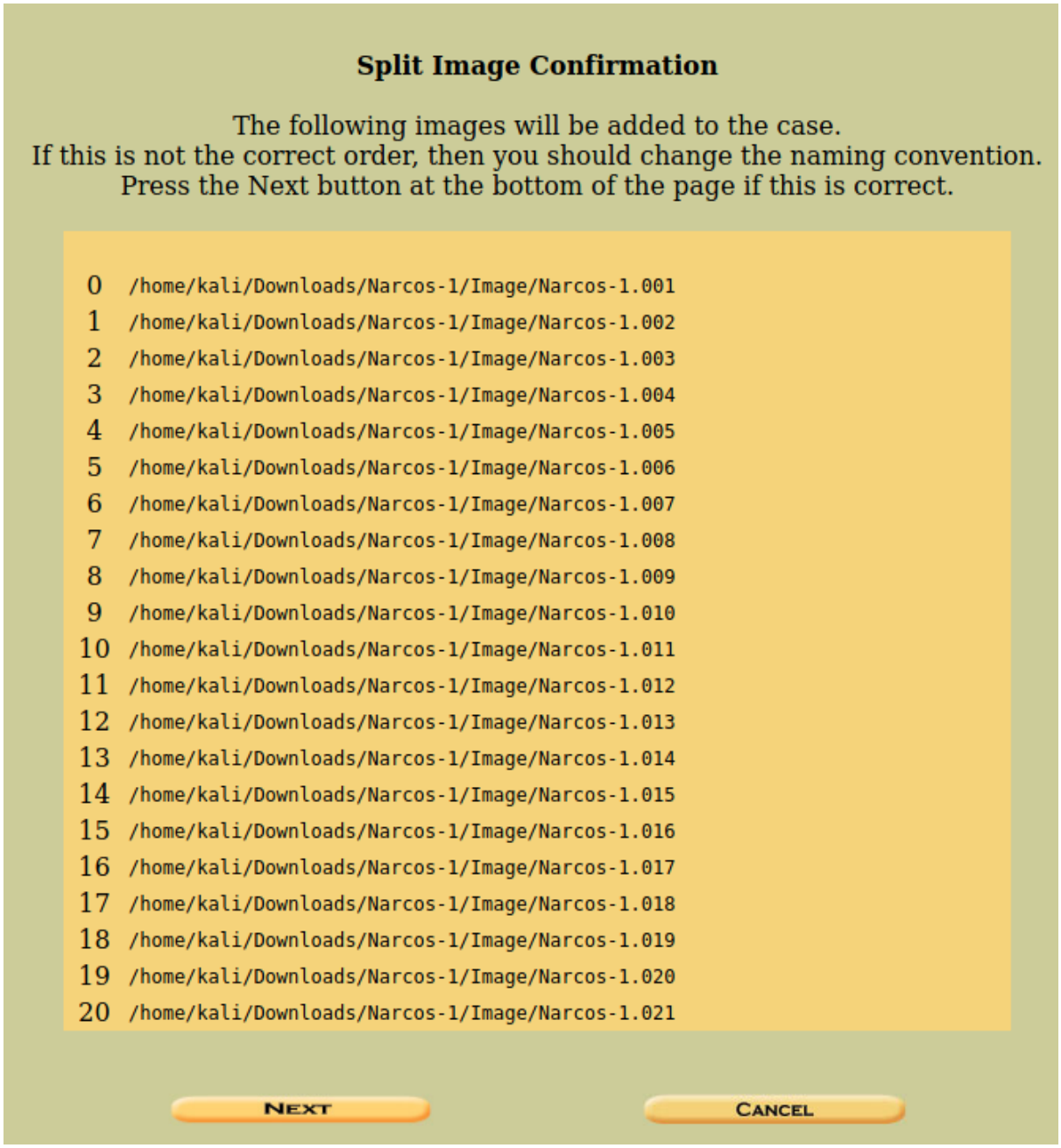
* Klik “Add Image”



* Klik “Add Image File”

* Klik “Next” na het invullen van de nodige velden

* Klik weer “Next”



* Vul de meegeleverde hash in om de integriteit te controleren . Klik “Add”

Image File Details

Local Name: "/home/kali/Downloads/Narcos-1/Image/Narcos-1.001" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.002" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.003" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.004" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.005" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.006" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.007" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.008" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.009" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.010" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.011" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.012" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.013" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.014" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.015" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.016" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.017" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.018" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.019" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.020" "/home/kali/Downloads/Narcos-1/Image/Narcos-1.021"

Data Integrity: An MD5 hash can be used to verify the integrity of the image. (With split images, this hash is for the full image file)

- ○ Ignore the hash value for this image.
- ○ Calculate the hash value for this image.
- ◉ Add the following MD5 hash value for this image:

  c63a3d19e9c9495b573f45be544e50f9

  ☑ Verify hash after importing?

File System Details

Analysis of the image file shows the following partitions:

Partition 1 (Type: Basic data partition)
Add to case? ☑
Sector Range: 2048 to 1023999
Mount Point: C: File System Type: ntfs

Partition 2 (Type: EFI system partition)
Add to case? ☑
Sector Range: 1024000 to 1226751
Mount Point: D: File System Type: fat32

Partition 3 (Type: Microsoft reserved partition)
Add to case? ☑
Sector Range: 1226752 to 1259519
Mount Point: /3/ File System Type: raw

Partition 4 (Type: Basic data partition)
Add to case? ☑
Sector Range: 1259520 to 62912511
Mount Point: E: File System Type: ntfs

ADD CANCEL HELP

For your reference, the `mmls` output was the following:

```
GUID Partition Table (EFI)
Offset Sector: 0
Units are in 512-byte sectors

      Slot      Start        End          Length       Description
004:  000       0000002048   0001023999   0001021952   Basic data partition
005:  001       0001024000   0001226751   0000202752   EFI system partition
006:  002       0001226752   0001259519   0000032768   Microsoft reserved partition
007:  003       0001259520   0062912511   0061652992   Basic data partition
```

* Calculating MD5 (this could take a while)

* Klik “OK”

Calculating MD5 (this could take a while)
Current MD5: `C63A3D19E9C9495B573F45BE544E50F9`
Integrity Check Passed
Testing partitions
Linking image(s) into evidence locker
Image file added with ID `img1`

Disk image (type gpt) added with ID `vol1`

Volume image (2048 to 1023999 - ntfs - C:) added with ID `vol2`

Volume image (1024000 to 1226751 - fat32 - D:) added with ID `vol3`

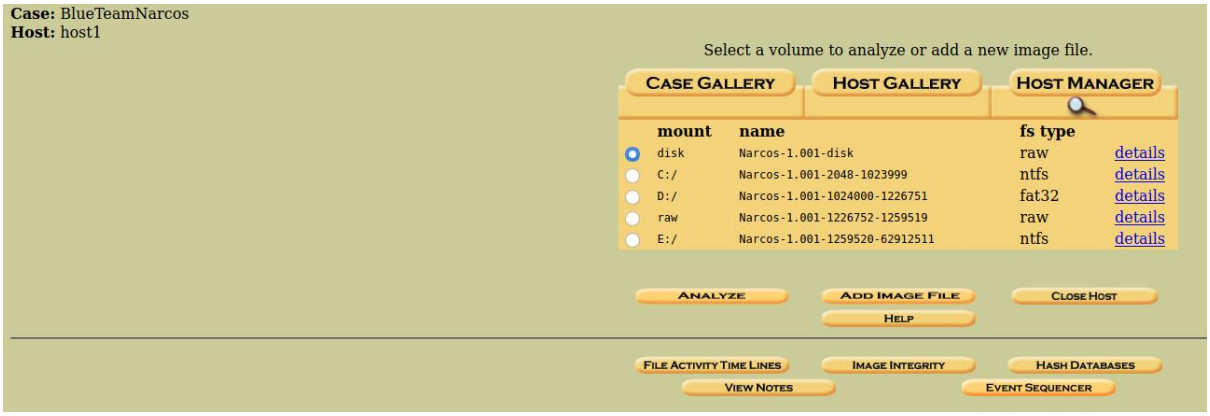
Volume image (1226752 to 1259519 - raw - /3/) added with ID `vol4`

Volume image (1259520 to 62912511 - ntfs - E:) added with ID `vol5`

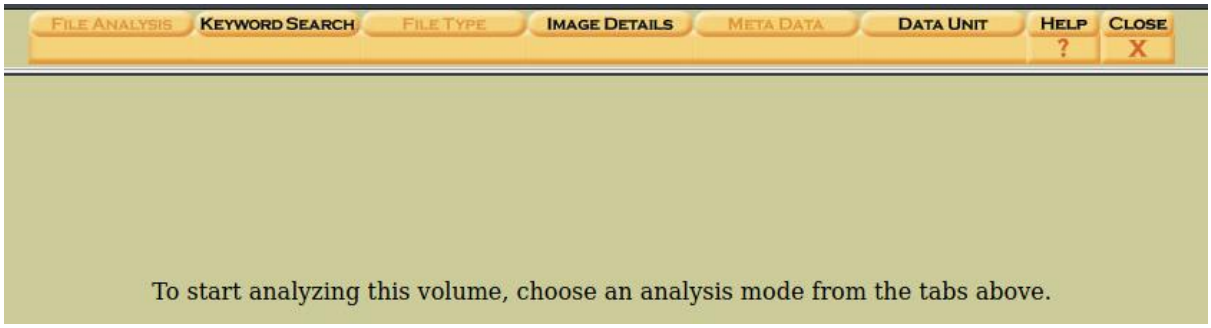
OK ADD IMAGE

Analyse

* Selecteer een disk een klik “Analyze”



* Om te zien of er iets nuttig te vinden is, gaan we alle opties van alle disks af



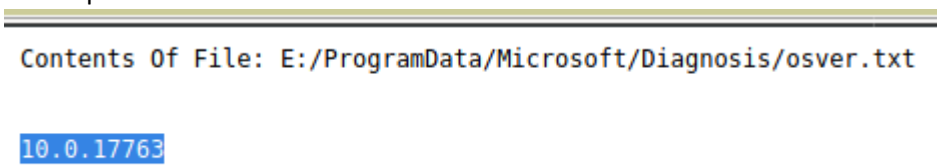
* We onderzoeken enkel “nuttige” informatie gebaseerd op de info die we ontvangen hebben:

1. “Their chat contains information on where they are going and what he wants John Fredricksen to deliver. Furthermore, Steve shares some documents via (email, cloud, etc) that will assist with his job.”

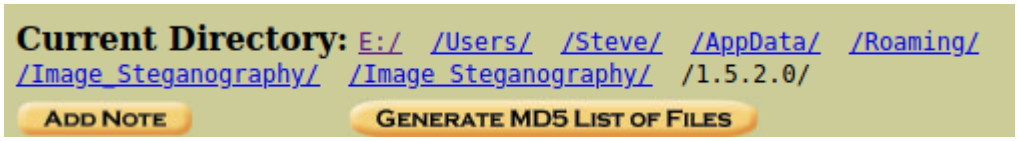
2.” Steve has provided John with information about New Zealand and points on how best to smuggle the product into Wellington without raising any alarms at customs. Steve knows a thing or two about digital forensics and decided to use steganography to hide the document within a picture.”

De enige nuttige partitie lijkt de E-partitie. Hier vinden we sporen van Discord en verschillende mogelijk nuttige files en pictures terug.

* In E:/ProgramData/Microsoft/Diagnosis/osver.txt lezen we alvast dat er een windows 10 october 2018 update draait



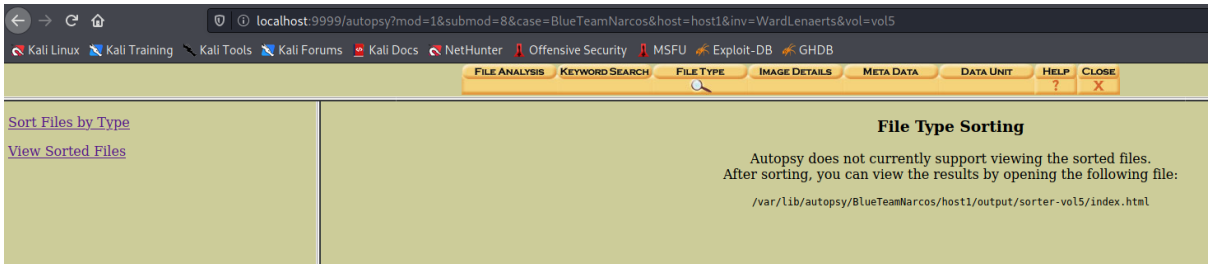
En een programma “Image Stenography”!



Deze versie kan gedownload worden van
https://www.softpedia.com/get/Multimedia/Graphic/Graphic-Editors/Image-Steganography.shtml

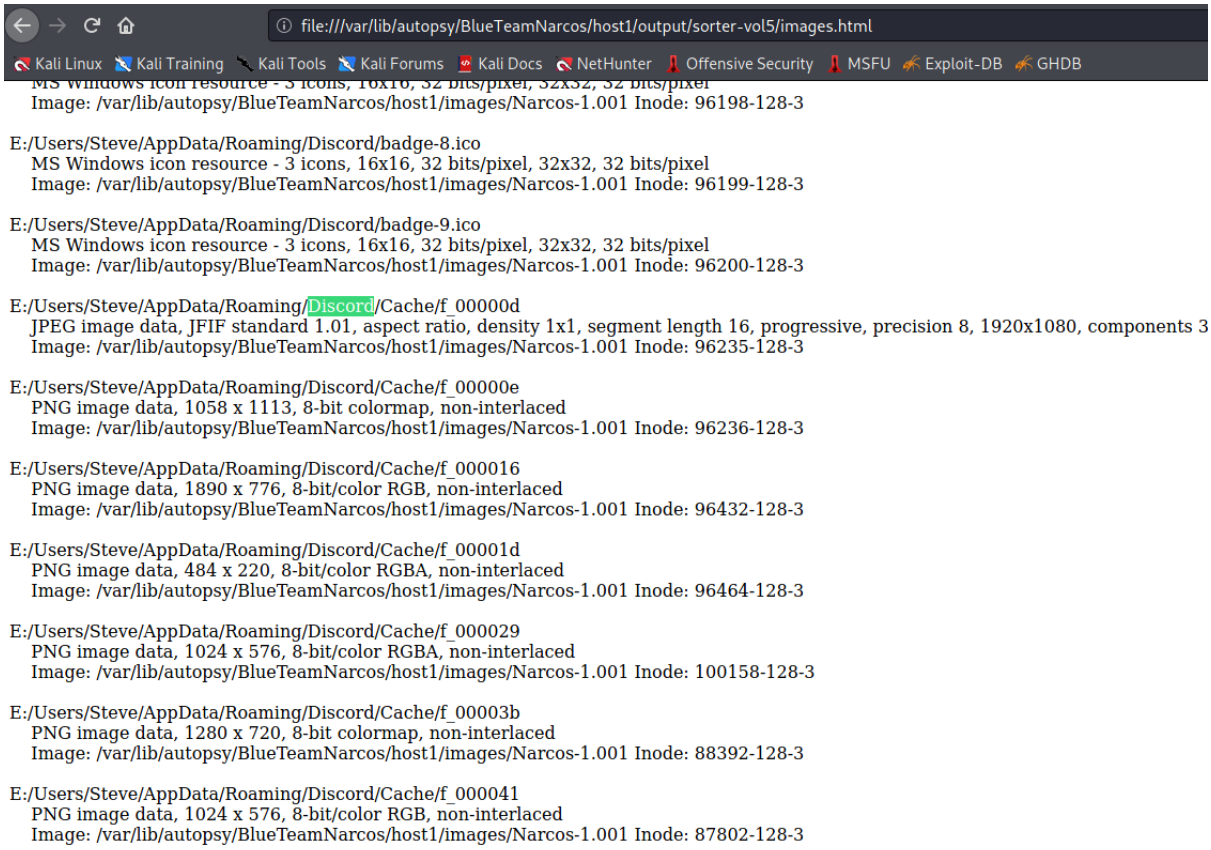
Onderzoeken van Discord

(source: https://abrignoni.blogspot.com/2018/03/finding-discord-app-chats-in-windows.html)
We trekken een volledige lijst van files aanwezig op deze drive.



Volledige lijst wordt door autopsy opgeslagen in
file:///var/lib/autopsy/BlueTeamNarcos/host1/output/sorter-vol5/data.html

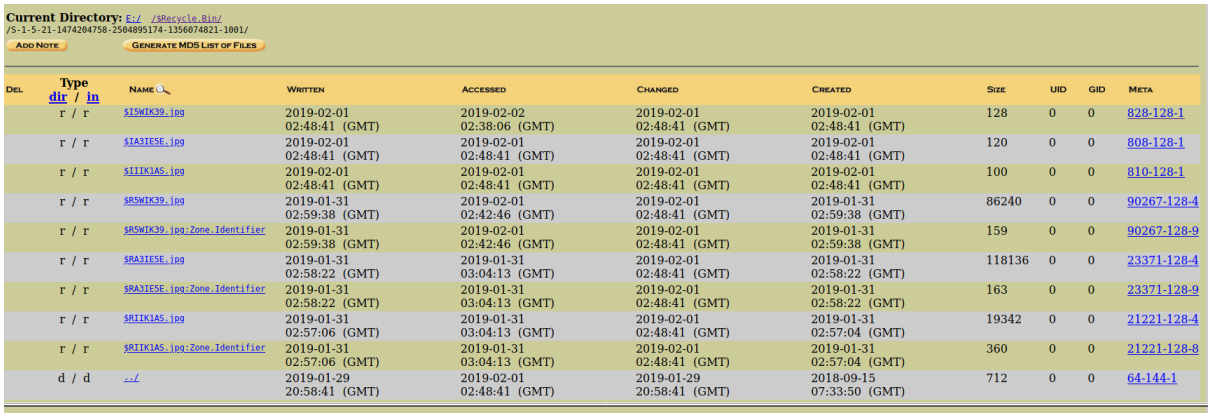
Enkele mogelijk belangrijke files hier:



En

E:/Users/Steve/AppData/Local/Google/Chrome/User Data/Default/Cache/f_000361
JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=19, height=3648, bps=242, PhotometricIntepretation=RGB, description=AUCKLAND, NEW ZEALAND - DECEMBER 13: Kendra Cocksedge holds the Kelvin R Tremain Memorial Player of the Year Award during the 2, manufacturer=Canon, model=Canon EOS-1D X Mark II, orientation=upper-left, width=5472], baseline, precision 8, 502x268, components 3
Image: /var/lib/autopsy/BlueTeamNarcos/host1/images/Narcos-1.001 Inode: 88304

Onderzoek van deleted files in the Recycle bin levert ons de volgende files op:



Del	Type dir / in	Name	Written	Accessed	Changed	Created	Size	UID	GID	Meta
	r / r	$I5WIK39.jpg	2019-02-01 02:48:41 (GMT)	2019-02-02 02:38:06 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	128	0	0	828-128-1
	r / r	$IA3IE5E.jpg	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	120	0	0	808-128-1
	r / r	$IIIK1AS.jpg	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-02-01 02:48:41 (GMT)	100	0	0	810-128-1
	r / r	$R5WIK39.jpg	2019-01-31 02:59:38 (GMT)	2019-02-01 02:42:46 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:59:38 (GMT)	86240	0	0	90267-128-4
	r / r	$R5WIK39.jpg:Zone.Identifier	2019-01-31 02:59:38 (GMT)	2019-02-01 02:42:46 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:59:38 (GMT)	159	0	0	90267-128-9
	r / r	$RA3IE5E.jpg	2019-01-31 02:58:22 (GMT)	2019-01-31 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:58:22 (GMT)	118136	0	0	23371-128-4
	r / r	$RA3IE5E.jpg:Zone.Identifier	2019-01-31 02:58:22 (GMT)	2019-01-31 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:58:22 (GMT)	163	0	0	23371-128-9
	r / r	$RIIK1AS.jpg	2019-01-31 02:57:06 (GMT)	2019-01-31 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:57:04 (GMT)	19342	0	0	21221-128-4
	r / r	$RIIK1AS.jpg:Zone.Identifier	2019-01-31 02:57:06 (GMT)	2019-01-31 03:04:13 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-31 02:57:04 (GMT)	360	0	0	21221-128-8
	d / d	../	2019-01-29 20:58:41 (GMT)	2019-02-01 02:48:41 (GMT)	2019-01-29 20:58:41 (GMT)	2018-09-15 07:33:50 (GMT)	712	0	0	64-144-1

We merken dat de eerste file eindigt op jpg, maar in feite geen picture, maar een datafile is! Dit is verdacht!

Pointed to by file:
E:/$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/$I5WIK39.jpg

File Type:
data

We vinden hier via Hex een path naar een picture

```
Hex Contents Of File: E:/vol5-meta-828-128-1


00000000:  0200 0000 0000 0000 E050 0100 0000 0000    .........P......
00000010:  4000 1CA4 D8B9 D401 3200 0000 4300 3A00    @.......2...C.:.
00000020:  5C00 5500 7300 6500 7200 7300 5C00 5300    \.U.s.e.r.s.\.S.
00000030:  7400 6500 7600 6500 5C00 5000 6900 6300    t.e.v.e.\.P.i.c.
00000040:  7400 7500 7200 6500 7300 5C00 6500 6900    t.u.r.e.s.\.e.i.
00000050:  6700 6800 7400 5F00 6300 6F00 6C00 5F00    g.h.t._.c.o.l._.
00000060:  7000 6100 7400 6300 6800 6500 7300 5F00    p.a.t.c.h.e.s._.
00000070:  6300 7200 7000 2E00 6A00 7000 6700 0000    c.r.p...j.p.g...
```

Voluit staat hier ....P...@2.c/Users/Steve/Pictures/eight_cols_patches_crp.jpg.

Iets soortgelijk vinden we voor de tweede file

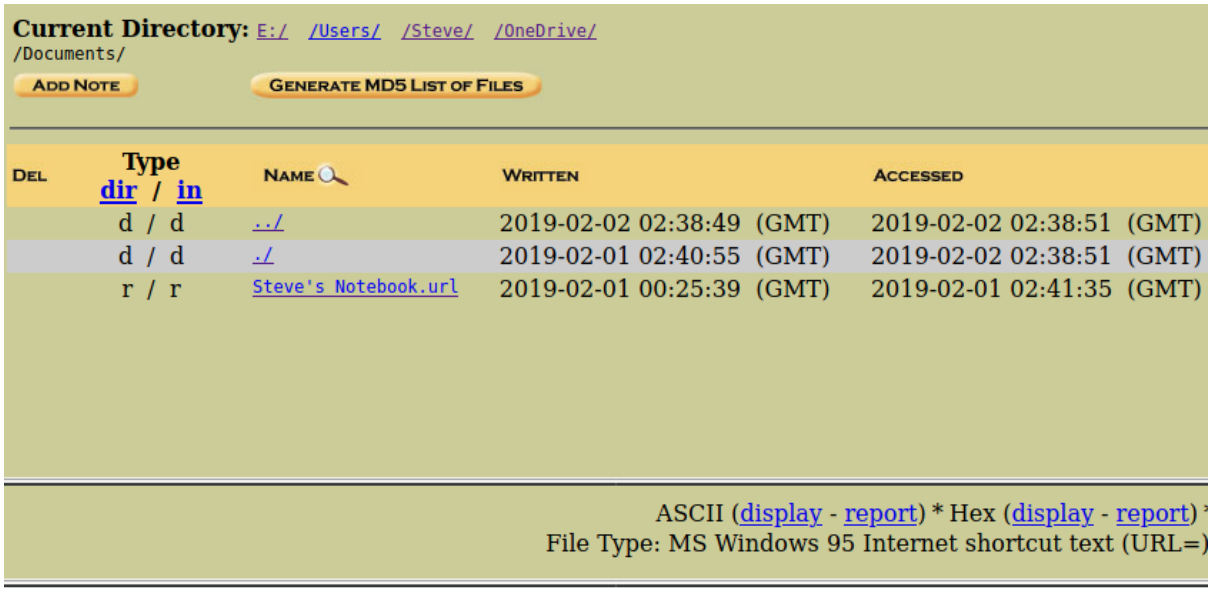
```
Hex Contents Of File: E:/$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/$IA3IE5E.jpg


00000000:  0200 0000 0000 0000 78CD 0100 0000 0000    ........x.......
00000010:  802B 1AA4 D8B9 D401 2E00 0000 4300 3A00    .+..........C.:.
00000020:  5C00 5500 7300 6500 7200 7300 5C00 5300    \.U.s.e.r.s.\.S.
00000030:  7400 6500 7600 6500 5C00 5000 6900 6300    t.e.v.e.\.P.i.c.
00000040:  7400 7500 7200 6500 7300 5C00 7000 7200    t.u.r.e.s.\.p.r.
00000050:  6900 6300 6500 2D00 6D00 6500 7400 6800    i.c.e.-.m.e.t.h.
00000060:  2D00 6200 7500 7300 7400 2D00 3400 2E00    -.b.u.s.t.-.4...
00000070:  6A00 7000 6700 0000                        j.p.g...
```

En voor de derde file

```
Hex Contents Of File: E:/$Recycle.Bin/S-1-5-21-1474204758-2504895174-1356074821-1001/$IIIK1AS.jpg


00000000:  0200 0000 0000 0000 8E4B 0000 0000 0000    .........K......
00000010:  20B2 1BA4 D8B9 D401 2400 0000 4300 3A00     .......$...C.:.
00000020:  5C00 5500 7300 6500 7200 7300 5C00 5300    \.U.s.e.r.s.\.S.
00000030:  7400 6500 7600 6500 5C00 5000 6900 6300    t.e.v.e.\.P.i.c.
00000040:  7400 7500 7200 6500 7300 5C00 3600 3200    t.u.r.e.s.\.6.2.
00000050:  3000 7800 3300 3400 3900 2E00 6A00 7000    0.x.3.4.9...j.p.
00000060:  6700 0000                                  g...
```

Onderzoek naar “cloud”-toepassingen

We vinden dan snel Onedrive



Current Directory: E:/ /Users/ /Steve/ /OneDrive/
/Documents/

ADD NOTE | GENERATE MD5 LIST OF FILES

DEL	Type dir / in	NAME	WRITTEN	ACCESSED
	d / d	../	2019-02-02 02:38:49 (GMT)	2019-02-02 02:38:51 (GMT)
	d / d	./	2019-02-01 02:40:55 (GMT)	2019-02-02 02:38:51 (GMT)
	r / r	Steve's Notebook.url	2019-02-01 00:25:39 (GMT)	2019-02-01 02:41:35 (GMT)

ASCII (display - report) * Hex (display - report) *
File Type: MS Windows 95 Internet shortcut text (URL=)

Contents Of File: E:/Users/Steve/OneDrive/Documents/Steve's Notebook.url

```
[InternetShortcut]
URL=https://onedrive.live.com/redir.aspx?cid=2418c0082017486a&resid=2418C0082017486A!105&type=3
```

Zelfreflectie na het doorlopen van de opdrachten:

NOTE van (lichte) frustratie: Ik heb Wine geinstalleerd op mijn Kali Linux om de 2 windows programma's te kunnen runnen in mijn VM, maar ik krijg ze niet aan de praat ... :-(
ChromeCacheView v1.77 om de discord files uit te lezen
image steganography 1.5.2.0 om de images die gecodeerd werden door Suspect Steve te kunnen "decoden"

Als "leek" in het security-gebeuren had ik verwacht dat alles zich voornamelijk in de linux-wereld zou afspelen, maar voor de laatste opdracht valt het vinden van alternatieve tools mij hard tegen.
Ik lees over Hindsight, Stegohide, Stegosuite,... en heb deze ook geprobeerd, maar ik blijf botsen tegen problemen waardoor ik niet helemaal tot aan de oplossing van 3 geraakt ben.
Ik heb het gevoel dat ik er heel kort bij zit, maar dat mijn persoonlijke hardware mij de das om doet. Mijn CPU heeft vaak tegen 100% gedraaid en ik heb mijn harde schijf van 500GB grondig moeten opkuisen om zelfs al maar te kunnen beginnen aan de opdracht.
Ik vond het wel heel leuke opdrachten en heb er ook enorm veel van opgestoken. Het niveau is voor mij persoonlijk erg hoog, maar dat maakt de uitdaging zoveel leuker.

MVG,

Ward Lenaerts