Quiet Recon: Gathering Everything You Need with LDAP and Native AD Services

fenrir

Slides at
github.com/layer8secure/
The-Storfield-Methodology

fenrir

echo $USER

- Longtime hacker
- Practice Manager, Offensive Security @ Layer 8 Security
- https://github.com/cwolff411
- https://twitter.com/cwolff411

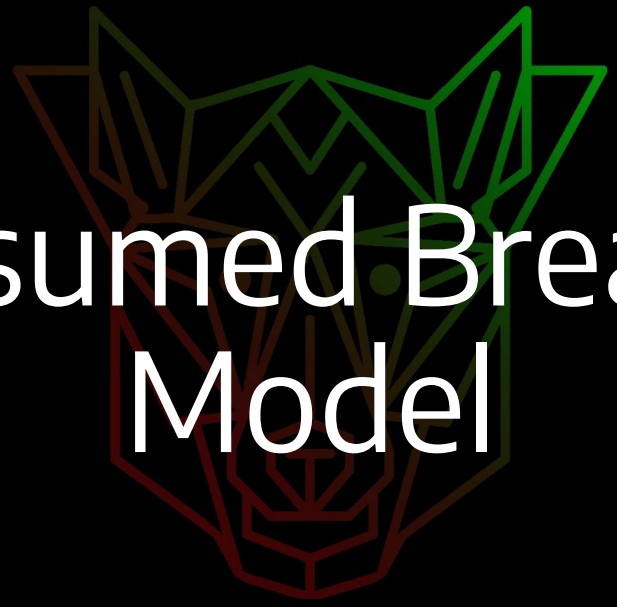
What today is about

- A real-world methodology that can be used on every engagement
- A back-to-basics approach
- Pre-exploitation

What today is not about

- Fancy new EDR evasion tactics
- Advanced techniques

fenrir



Assumed Breach Model

fenrir

Hop up on the soapbox…

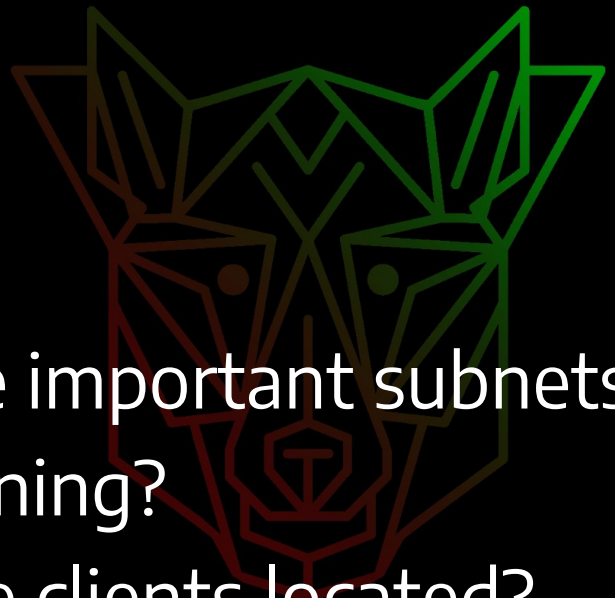
- We've become obsessed with tooling
- Most APT's aren't doing buffer overflows, ROP chains, etc
- We should understand the basics

Being quiet means keeping it simple

fenrir

Questions We Want Answered

- Where am I?
- Where is the DC?
- Where is the servers?
- What hosts are on the important subnets?
- What services are running?
- Where are most of the clients located?



fenrir

The Storfield Methodology

- A methodology to formulate attack paths in a quiet manner
- Use what we have at our disposal
- Live off the (network) land
- Keep it simple which keeps it quiet

The quietest room on Earth

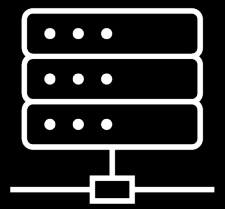
Orfield Laboratories uses its -9 decibel room to conduct audio research.

Steve Orfield stands in the anechoic chamber located inside his research facility, Orfield Labaorties, located in the West Bank/Seward neighborhood. The chamber was awarded a Guiness Book record for its negative decibel sound, and is often referred to as the world's quietest room. Orfield has long been noted for the testing and research done out of his facilities.

https://mndaily.com/203663/news/metro-state/quietest-room-earth/

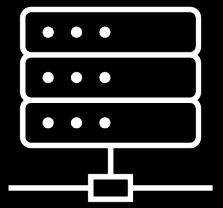
The Storfield Methodology

Where am I?



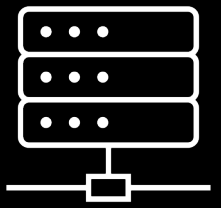
Recon the subnet

Where is the DC?

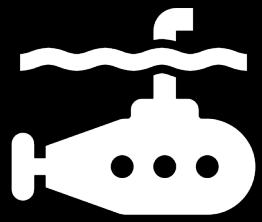


Recon the subnet & AD

Where are the member servers?



Recon the subnet



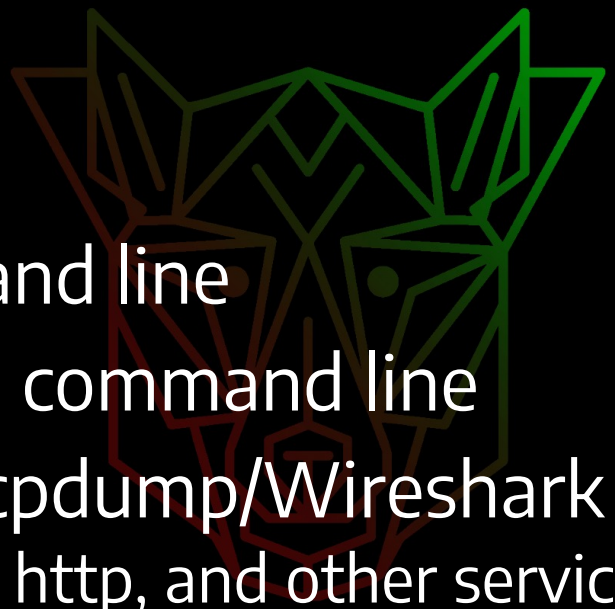
Formulate Attacks

Recon a Subnet

fenrir

Recon A Subnet

- arp –a / arpscan
- Discover services
- Ping sweep on command line
- TCP sweep with nc on command line
- Packet capture with tcpdump/Wireshark
  - Filter for smb, netbios, http, and other services



fenrir

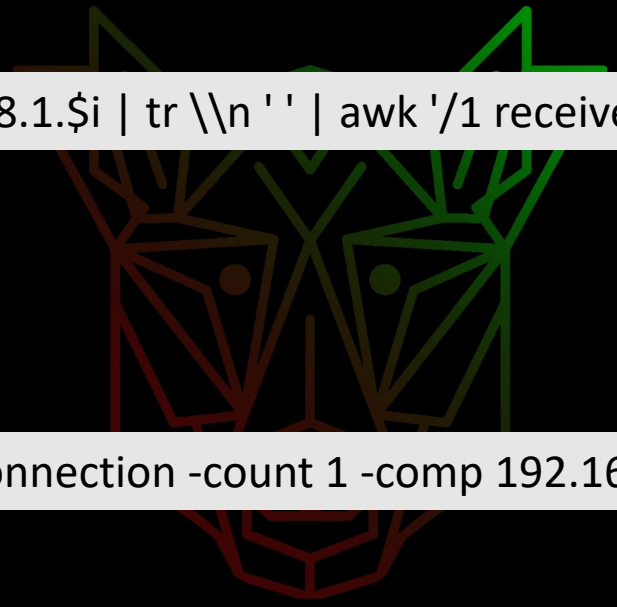
Host Discovery – Ping Sweep

bash

```
for i in `seq 1 255`; do ping -c 1 192.168.1.$i | tr \\n ' ' | awk '/1 received/ {print $2}'; done
```

PowerShell

```
1..254 | % {"192.168.1.$($_): $(Test-Connection -count 1 -comp 192.168.1.$($_) -quiet)"}
```



fenrir

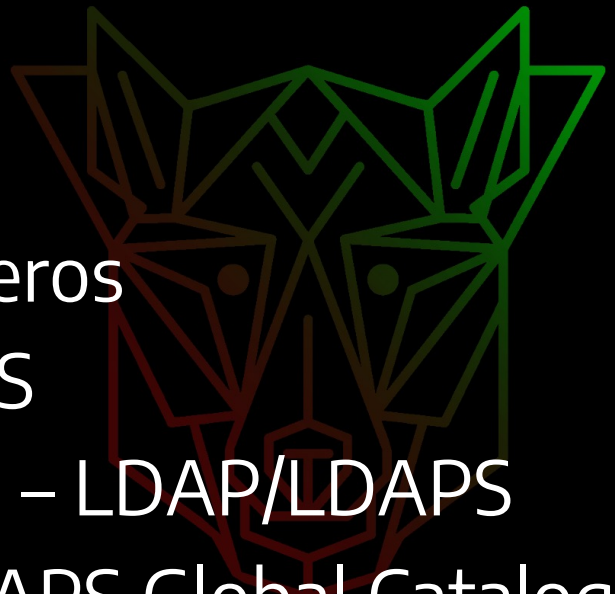
Host Discovery - ARP

- Address Resolution Protocol
- Maps IP addresses to MAC addresses
- Keeps an ARP table of local Ips and MACs

arp –a –i INTERFACE

```
~ » arp -a -i en0

? (169.254.169.254) at (incomplete) on en0 [ethernet]
? (172.19.0.1) at 0:a0:bc:c0:83:1e on en0 ifscope [ethernet]
? (172.19.0.44) at 98:46:a:9b:8:14 on en0 ifscope [ethernet]
? (172.19.0.47) at 6e:da:87:d1:b7:3a on en0 ifscope [ethernet]
? (172.19.0.49) at b2:ae:52:1:13:44 on en0 ifscope [ethernet]
? (172.19.0.50) at 6a:a0:31:ba:27:f1 on en0 ifscope [ethernet]
? (172.19.0.58) at 6:7:ee:c7:55:8e on en0 ifscope [ethernet]
? (172.19.0.107) at 86:1:5e:40:61:96 on en0 ifscope [ethernet]
? (172.19.0.110) at 3c:a6:f6:a:b7:98 on en0 ifscope [ethernet]
? (172.19.0.113) at f6:3c:7a:7d:e9:7 on en0 ifscope [ethernet]
? (172.19.0.142) at f0:2f:4b:ee:27:4f on en0 ifscope [ethernet]
? (172.19.0.162) at 2a:e5:42:43:c7:94 on en0 ifscope [ethernet]
? (172.19.0.166) at 7a:3b:c4:f1:85:28 on en0 ifscope [ethernet]
? (172.19.0.182) at e:53:f0:78:2:1e on en0 ifscope [ethernet]
? (172.19.0.188) at 2e:79:52:b:79:b4 on en0 ifscope [ethernet]
? (172.19.0.203) at e:69:77:4b:96:4b on en0 ifscope [ethernet]
? (172.19.0.222) at d6:e7:ad:38:a3:84 on en0 ifscope [ethernet]
? (172.19.0.223) at e2:cf:f1:82:4d:e5 on en0 ifscope [ethernet]
? (172.19.0.239) at 92:12:31:8d:39:bf on en0 ifscope [ethernet]
? (172.19.0.254) at 42:3c:d9:f6:d6:49 on en0 ifscope [ethernet]
? (172.19.1.10) at fa:96:e2:78:85:d3 on en0 ifscope [ethernet]
? (172.19.1.19) at d6:9d:aa:e6:26:c4 on en0 ifscope [ethernet]
? (172.19.1.25) at 36:37:d:be:d9:64 on en0 ifscope [ethernet]
? (172.19.1.30) at 62:f2:bd:79:62:3f on en0 ifscope [ethernet]
? (172.19.1.37) at 5e:58:ac:56:a1:85 on en0 ifscope [ethernet]
? (172.19.1.51) at f2:a2:95:e1:9c:c7 on en0 ifscope [ethernet]
? (172.19.1.53) at 32:d9:9:82:5b:70 on en0 ifscope [ethernet]
? (172.19.1.64) at c6:e:2e:5b:40:7c on en0 ifscope [ethernet]
? (172.19.1.68) at 62:e7:b6:c:de:bb on en0 ifscope [ethernet]
? (172.19.1.82) at 86:1e:1d:44:c2:b8 on en0 ifscope [ethernet]
? (172.19.1.142) at 84:fd:d1:6b:8:8c on en0 ifscope [ethernet]
? (172.19.1.146) at 2:c0:3d:8a:8f:4e on en0 ifscope [ethernet]
? (172.19.1.152) at 72:66:16:18:13:4b on en0 ifscope [ethernet]
? (172.19.1.156) at 2e:60:fc:89:c5:29 on en0 ifscope [ethernet]
? (172.19.1.183) at 42:b9:50:c3:f4:ac on en0 ifscope [ethernet]
? (172.19.1.186) at e6:94:81:86:22:e5 on en0 ifscope [ethernet]
? (172.19.1.188) at 2:a2:4a:59:53:7 on en0 ifscope [ethernet]
? (172.19.1.206) at 82:be:e3:4f:4:89 on en0 ifscope [ethernet]
? (172.19.1.225) at da:af:d5:98:11:9e on en0 ifscope [ethernet]
? (172.19.1.236) at 7a:b3:db:ed:30:c8 on en0 ifscope [ethernet]
? (172.19.1.255) at ff:ff:ff:ff:ff:ff on en0 ifscope [ethernet]
? (224.0.0.251) at 1:0:5e:0:0:fb on en0 ifscope permanent [ethernet]
```

Know Your Ports



- 53 UDP & TCP – DNS
- 139, 445 – SMB
- 88 UDP & TCP – Kerberos
- 80, 443 – HTTP/HTTPS
- 389, 636 - UDP & TCP – LDAP/LDAPS
- 3268,3269 – LDAP/LDAPS Global Catalog Services
- 3389 – RDP
- 5985, 5986 – WinRM (Windows Remote Management)

Service Discovery

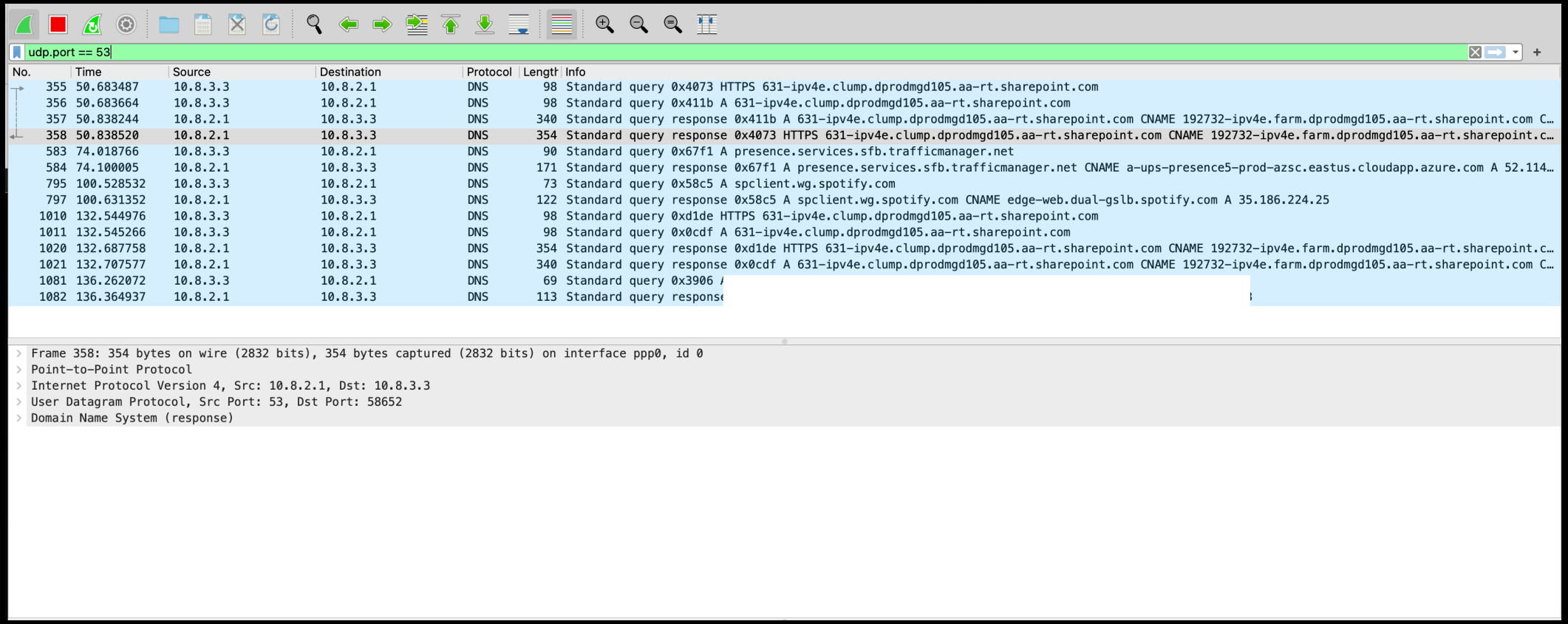
For SMB

```
nbtscan –v –s : x.x.x.x/24 | cut -d “:“ –f 1 > smb-hosts.txt
```

For any port

```
for i in `seq 1 254`; do nc -zvw1 x.x.x.$i SERVICE_PORT 2>&1 | grep
"Connected" | cut -d " " -f4 | cut -d ":" -f1 >> x-hosts.txt;done
```

Packet Capture

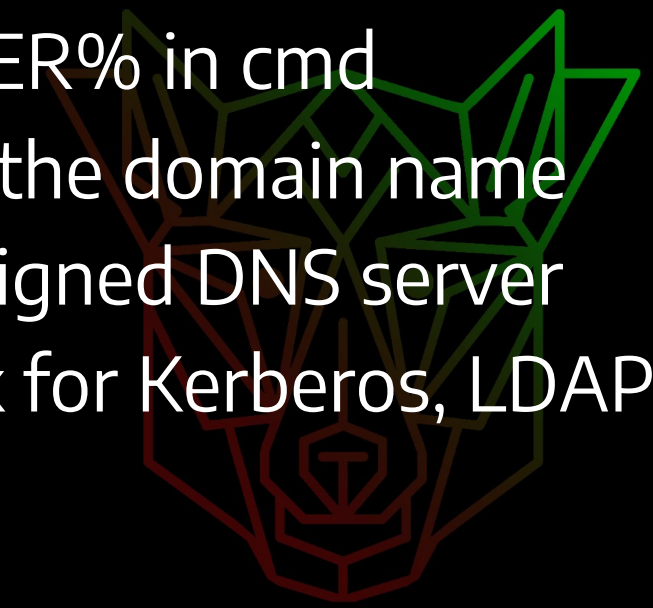


Recon Active Directory

fenrir

Locating the Domain Controller

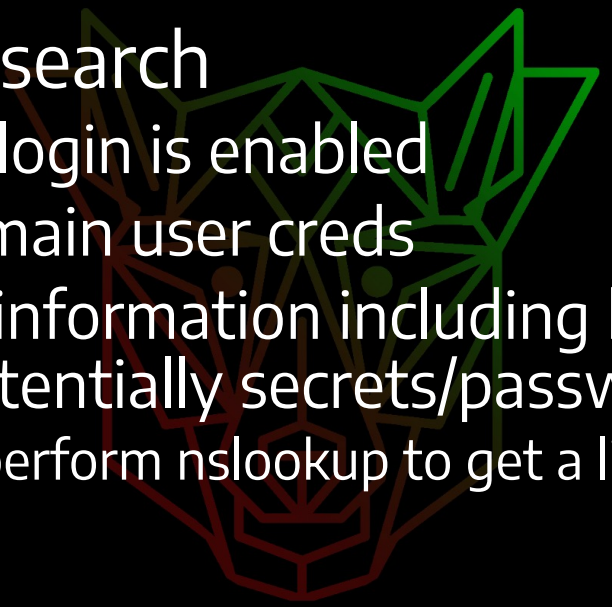
- echo %LOGONSERVER% in cmd
- perform nslookup of the domain name
- DHCP – check for assigned DNS server
- Packet capture – look for Kerberos, LDAP traffic



fenrir

Recon Active Directory

- Dump LDAP with ldapsearch
  - Hopefully anonymous login is enabled
  - If not, this requires domain user creds
  - LDAP Provides lots of information including hostnames, computer names, groups, and potentially secrets/passwords
    - Parse hostnames and perform nslookup to get a list of machines and IPs on the network



fenrir

Recon Active Directory

ldapsearch –x –h 10.0.0.1 –b “DC=contoso,DC=com”

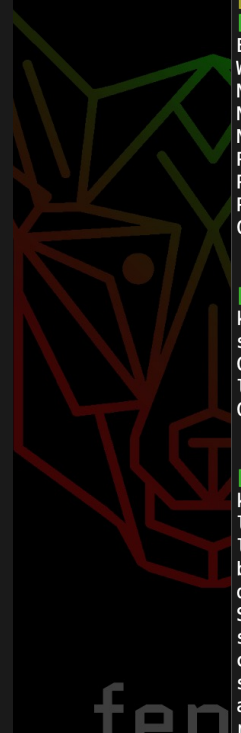
```
# extended LDIF
#
# LDAPv3
# base <DC=contoso,DC=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# contoso.com
dn: DC=contoso,DC=com
objectClass: top
objectClass: domain
objectClass: domainDNS
description: Contoso Inc.
distinguishedName: DC=contoso,DC=com
instanceType: 5
whenCreated: 20030209023721.0Z
whenChanged: 20220322161919.0Z
subRefs: DC=DomainDnsZones,DC=contoso,DC=com
subRefs: DC=ForestDnsZones,DC=contoso,DC=com
subRefs: CN=Configuration,DC=contoso,DC=com
```

```
# Microsoft Exchange Security Groups, contoso.com
dn: OU=Microsoft Exchange Security Groups,DC=contoso,DC=com
objectClass: top
objectClass: organizationalUnit
ou: Microsoft Exchange Security Groups
distinguishedName: OU=Microsoft Exchange Security Groups,DC=contoso,DC=com
instanceType: 4
whenCreated: 20080411130044.0Z
whenChanged: 20220110094612.0Z
uSNCreated: 21279
uSNChanged: 21279
name: Microsoft Exchange Security Groups
objectGUID:: mdlJF2a8W0eiO2Ei4cB1eg==
systemFlags: 1073741824
objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=wengerfee
 ds,DC=com
dSCorePropagationData: 20220111205857.0Z
dSCorePropagationData: 20220111203909.0Z
dSCorePropagationData: 20220111194948.0Z
dSCorePropagationData: 16010101181633.0Z
```

Recon Active Directory

https://github.com/layer8secure/SlientHound

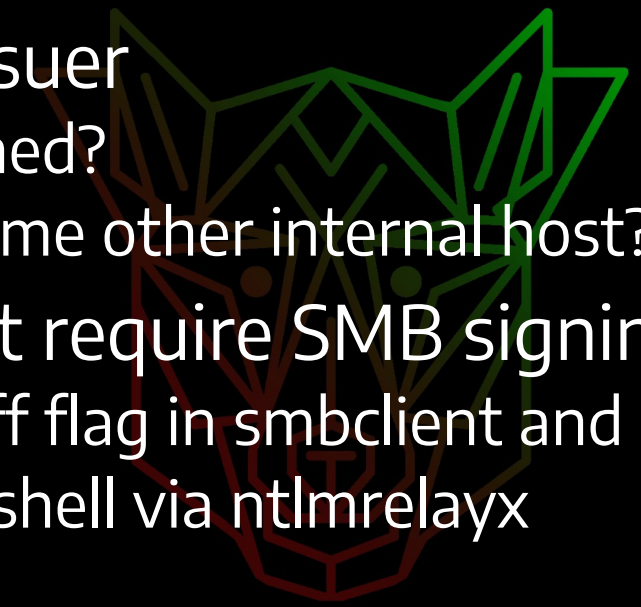
```
[+] Descriptions
labuser@HOME.local - User for lab
SQLService@HOME.local - password is MY_password2022!
svc-account@HOME.local - secret_p@$$w0rd


[+] Group Memberships Found
CN=Developers,CN=Users,DC=HOME,DC=local
jsmith@HOME.local
rjames@HOME.local
agreene@HOME.local
shenderson@HOME.local
cyoung@HOME.local


CN=Managers,CN=Users,DC=HOME,DC=local
smorrison@HOME.local
ewright@HOME.local
mmclean@HOME.local
blangdon@HOME.local
sburgess@HOME.local


CN=Operations,CN=Users,DC=HOME,DC=local
kjackson@HOME.local
jlambert@HOME.local
smacleod@HOME.local
vtaylor@HOME.local
vsmith@HOME.local
shenderson@HOME.local


CN=Schema Admins,OU=Groups,DC=HOME,DC=local
CN=Administrator,CN=Users,DC=HOME,DC=local


CN=Enterprise Admins,OU=Groups,DC=HOME,DC=local
sburgess@HOME.local
dan.mint@HOME.local
CN=Administrator,CN=Users,DC=HOME,DC=local


CN=Cert Publishers,OU=Groups,DC=HOME,DC=local
CN=CORN-DC,OU=Domain Controllers,DC=HOME,DC=local
```



```
---------------------------------------------------------------------------

[*] Located LDAP cache '.home-local.cache'. Delete cache to run updated query ...
[+] Hosts
EVILPC - ?
WIN10LAB - 192.168.1.10
NYC10-A - ?
NYC10-B - ?
NYC10-C - ?
PA10-X - ?
PA10-Y - ?
PA10-Z - ?
CORN-DC - 192.168.1.20


[+] Domain Admins
kjackson@HOME.local
sburgess@HOME.local
CN=Service Accounts,OU=Groups,DC=HOME,DC=local
labadmin@HOME.local
CN=Administrator,CN=Users,DC=HOME,DC=local


[+] Domain Users
krbtgt
labuser@HOME.local
labadmin@HOME.local
bob.dole@HOME.local
dan.mint@HOME.local
SQLService@HOME.local
svc-account@HOME.local
cyoung@HOME.local
shenderson@HOME.local
agreene@HOME.local
rjames@HOME.local
jsmith@HOME.local
sburgess@HOME.local
blangdon@HOME.local
mmclean@HOME.local
ewright@HOME.local
Administrator
smorrison@HOME.local
Guest
```

Recon Active Directory

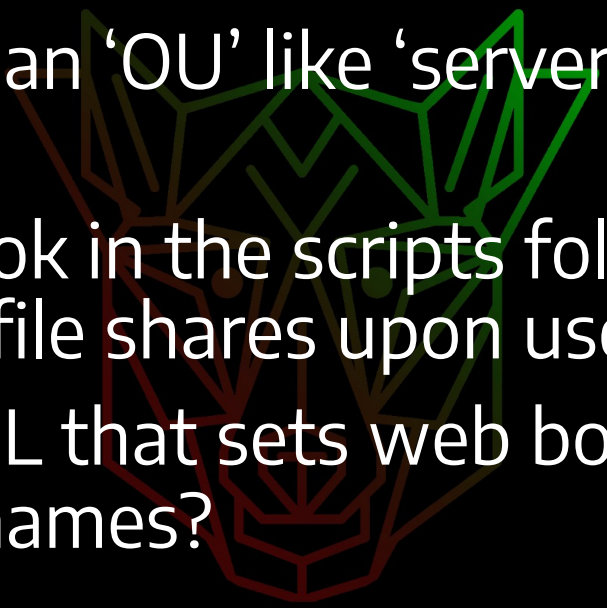
- Check SSL certs for issuer
  - Are the certs self-signed?
  - Are they signed by some other internal host?
- Find hosts that do not require SMB signing
  - --client-protection=off flag in smbclient and observe response
  - Easiest way to pop a shell via ntlmrelayx



fenrir

Locating Member Servers

- LDAP dump – look for an ‘OU’ like ‘servers’, member servers’, etc.
- Mount SYSVOL and look in the scripts folder to discover current and archived mapped file shares upon user logon
- Look at GPO in SYSVOL that sets web bookmarks. What are those addresses/hostnames?

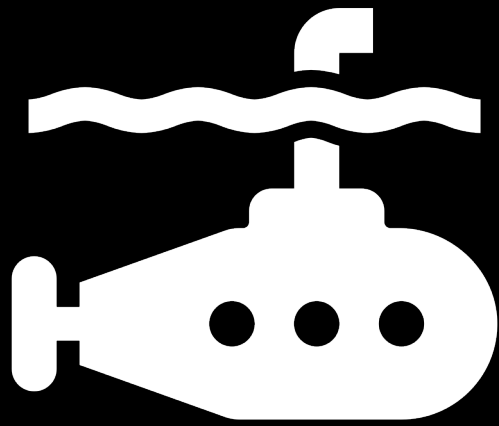


fenrir

Formulate Attacks

- By this point we should have
  - a list of active targets
  - A list of SMB Hosts
  - A list of RDP Hosts
  - Computer Names and IPs
  - AD Groups
  - AD Users
  - Location of DC
  - Location of member servers

fenrir



Fin

- Find me in the RTV and DEFCON discords. My username is @aGsudofenrir
- Slides and files are available on GitHub
  - github.com/layer8secure/The-Storfield-Methodology
- Come yell at me on Twitter and tell me how you would improve this process
  - @cwolff411