




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

fenrir

The Fenrir logo is a stylized, geometric representation of a wolf's head, composed of overlapping green and brown lines. It is positioned in the background, centered behind the text.

Slides at
[github.com/layer8secure/
The-Storfield-Methodology](https://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>



fenrir

What today is about

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



fenrir

What today is not about

- Fancy new EDR evasion tactics
- Advanced techniques



fenrir

The Fenrir logo is a stylized, geometric representation of a wolf's head. It is composed of various colored lines (green, brown, and red) that form the outline and internal structure of the head, including the ears, snout, and jaw. The logo is centered in the background of the slide.

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



fenrir

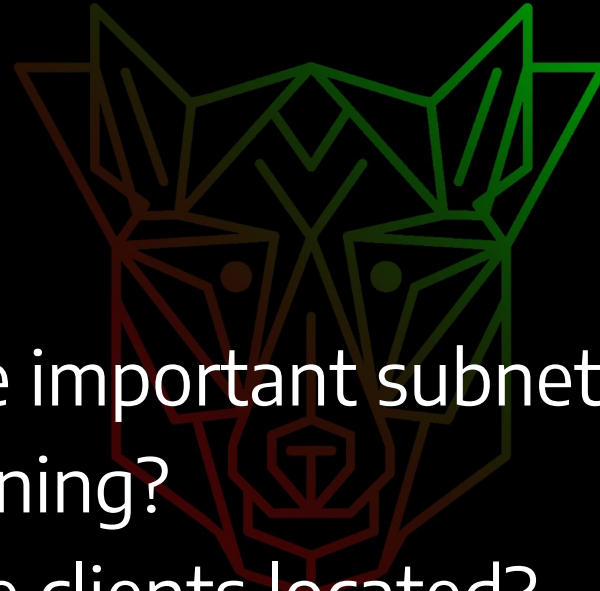
The logo for Fenrir is a stylized, geometric representation of a wolf's head. It is composed of numerous overlapping triangles and polygons, creating a complex, crystalline structure. The color palette is primarily green and brown, with some darker tones in the shadows. The overall shape is roughly circular, with the points of the triangles extending outwards to form the ears and snout.

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

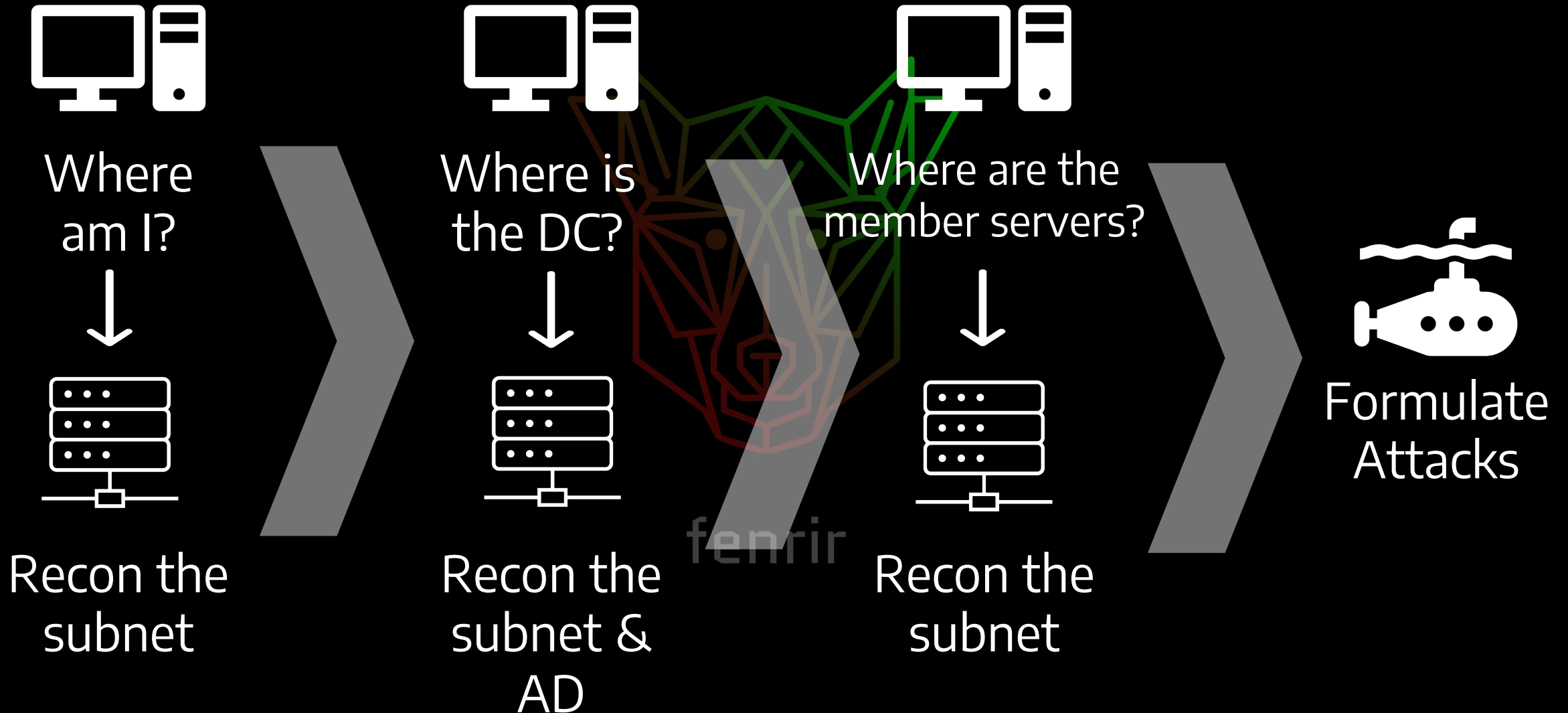
The quietest room on Earth

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



Steve Orfield stands in the anechoic chamber located inside his research facility, Orfield Laboratories, located in the West Bank/Seward neighborhood. The chamber was awarded a Guinness 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.

The Storfield Methodology



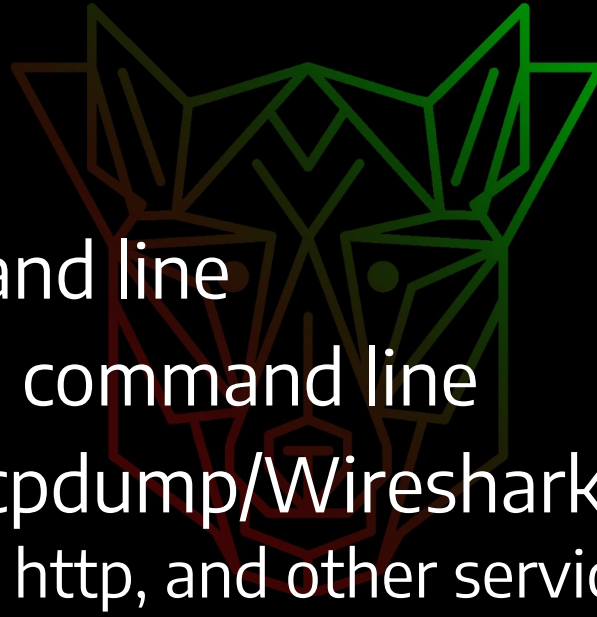
The logo is a stylized, geometric representation of a wolf's head, composed of various polygons. It features a color gradient from dark red at the bottom to bright green at the top. The text "Recon a Subnet" is centered over the logo in a white, sans-serif font.

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

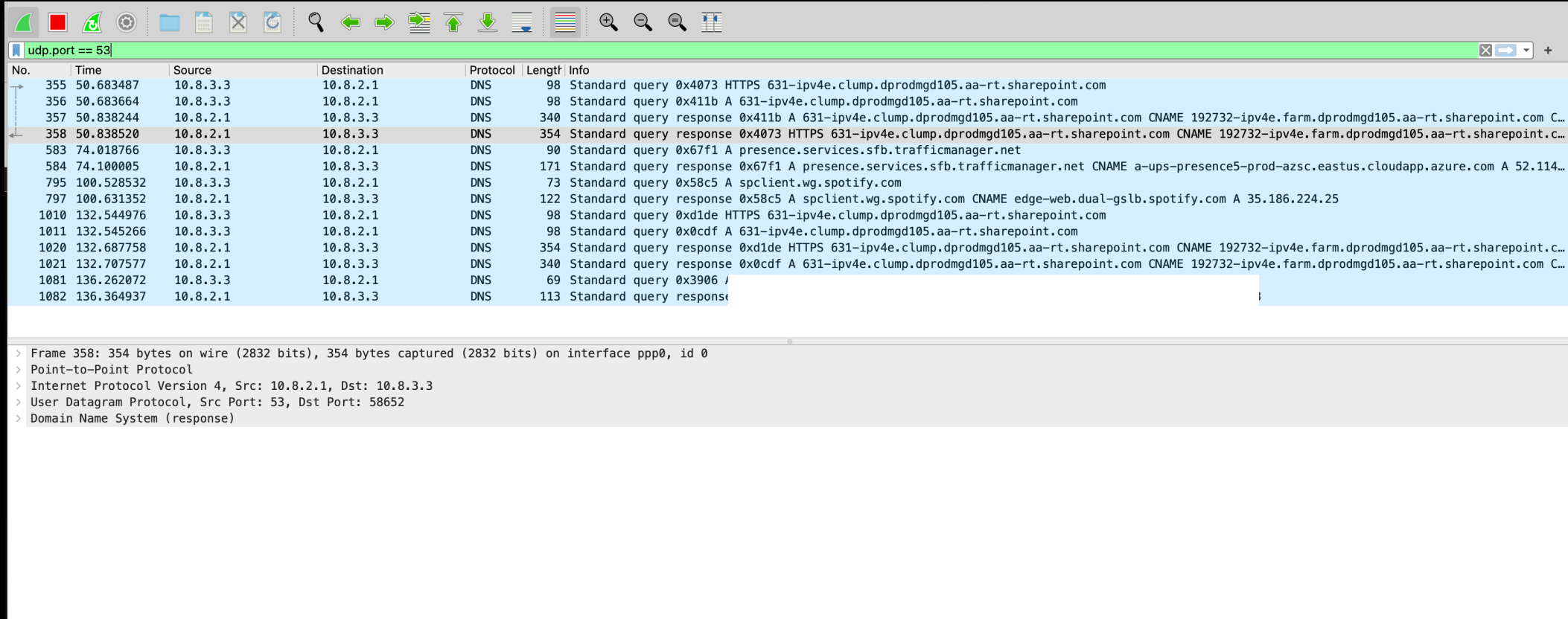
```
nbtscan -v -s : x.x.x.x/24 | cut -d ":" -f 1 > smb-hosts.txt
```

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
```

fenrir

Packet Capture



The image shows a Wireshark packet capture window. The top toolbar contains various icons for file operations, packet navigation, and analysis. Below the toolbar is a green filter bar with the text "udp.port == 53". The main packet list table displays the following data:

No.	Time	Source	Destination	Protocol	Length	Info
355	50.683487	10.8.3.3	10.8.2.1	DNS	98	Standard query 0x4073 HTTPS 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com
356	50.683664	10.8.3.3	10.8.2.1	DNS	98	Standard query 0x411b A 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com
357	50.838244	10.8.2.1	10.8.3.3	DNS	340	Standard query response 0x411b A 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com CNAME 192732-ipv4e.farm.dprodmgd105.aa-rt.sharepoint.com C...
358	50.838520	10.8.2.1	10.8.3.3	DNS	354	Standard query response 0x4073 HTTPS 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com CNAME 192732-ipv4e.farm.dprodmgd105.aa-rt.sharepoint.com C...
583	74.018766	10.8.3.3	10.8.2.1	DNS	90	Standard query 0x67f1 A presence.services.sfb.trafficmanager.net
584	74.100005	10.8.2.1	10.8.3.3	DNS	171	Standard query response 0x67f1 A presence.services.sfb.trafficmanager.net CNAME a-ups-presence5-prod-azsc.eastus.cloudapp.azure.com A 52.114...
795	100.528532	10.8.3.3	10.8.2.1	DNS	73	Standard query 0x58c5 A spclient.wg.spotify.com
797	100.631352	10.8.2.1	10.8.3.3	DNS	122	Standard query response 0x58c5 A spclient.wg.spotify.com CNAME edge-web.dual-gslb.spotify.com A 35.186.224.25
1010	132.544976	10.8.3.3	10.8.2.1	DNS	98	Standard query 0xd1de HTTPS 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com
1011	132.545266	10.8.3.3	10.8.2.1	DNS	98	Standard query 0x0cdf A 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com
1020	132.687758	10.8.2.1	10.8.3.3	DNS	354	Standard query response 0xd1de HTTPS 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com CNAME 192732-ipv4e.farm.dprodmgd105.aa-rt.sharepoint.com C...
1021	132.707577	10.8.2.1	10.8.3.3	DNS	340	Standard query response 0x0cdf A 631-ipv4e.clump.dprodmgd105.aa-rt.sharepoint.com CNAME 192732-ipv4e.farm.dprodmgd105.aa-rt.sharepoint.com C...
1081	136.262072	10.8.3.3	10.8.2.1	DNS	69	Standard query 0x3906 /
1082	136.364937	10.8.2.1	10.8.3.3	DNS	113	Standard query response

Below the packet list, the detailed view for packet 358 is expanded, showing the following structure:

- > Frame 358: 354 bytes on wire (2832 bits), 354 bytes captured (2832 bits) on interface ppp0, id 0
- > Point-to-Point Protocol
- > Internet Protocol Version 4, Src: 10.8.2.1, Dst: 10.8.3.3
- > User Datagram Protocol, Src Port: 53, Dst Port: 58652
- > Domain Name System (response)

The logo is a stylized, geometric representation of a wolf's head, specifically Fenrir. It is composed of various line segments in shades of green and brown, creating a complex, angular shape that resembles a wireframe or a low-poly model. The head is facing forward, with pointed ears and a snout.

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

The Fenrir logo is a stylized, geometric representation of a wolf's head, composed of various colored lines (green, red, and brown) forming a complex, web-like structure.

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"

```
1  # extended LDIF
2  #
3  # LDAPv3
4  # base <DC=contoso,DC=com> with scope subtree
5  # filter: (objectclass=*)
6  # requesting: ALL
7  #
8
9  # contoso.com
10 dn: DC=contoso,DC=com
11 objectClass: top
12 objectClass: domain
13 objectClass: domainDNS
14 description: Contoso Inc.
15 distinguishedName: DC=contoso,DC=com
16 instanceType: 5
17 whenCreated: 20030209023721.0Z
18 whenChanged: 20220322161919.0Z
19 subRefs: DC=DomainDnsZones,DC=contoso,DC=com
20 subRefs: DC=ForestDnsZones,DC=contoso,DC=com
21 subRefs: CN=Configuration,DC=contoso,DC=com
```

```
249
250 # Microsoft Exchange Security Groups, contoso.com
251 dn: OU=Microsoft Exchange Security Groups,DC=contoso,DC=com
252 objectClass: top
253 objectClass: organizationalUnit
254 ou: Microsoft Exchange Security Groups
255 distinguishedName: OU=Microsoft Exchange Security Groups,DC=contoso,DC=com
256 instanceType: 4
257 whenCreated: 20080411130044.0Z
258 whenChanged: 20220110094612.0Z
259 uSNCreated: 21279
260 uSNChanged: 21279
261 name: Microsoft Exchange Security Groups
262 objectGUID:: mdLJF2a8W0ei02Ei4cB1eg==
263 systemFlags: 1073741824
264 objectCategory: CN=Organizational-Unit,CN=Schema,CN=Configuration,DC=wengerfee
265 ds,DC=com
266 dSCorePropagationData: 20220111205857.0Z
267 dSCorePropagationData: 20220111203909.0Z
268 dSCorePropagationData: 20220111194948.0Z
269 dSCorePropagationData: 16010101181633.0Z
270
```

Recon Active Directory

<https://github.com/layer8secure/SilentHound>

[+] 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?

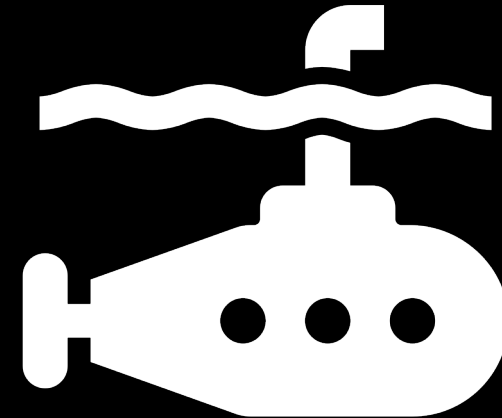
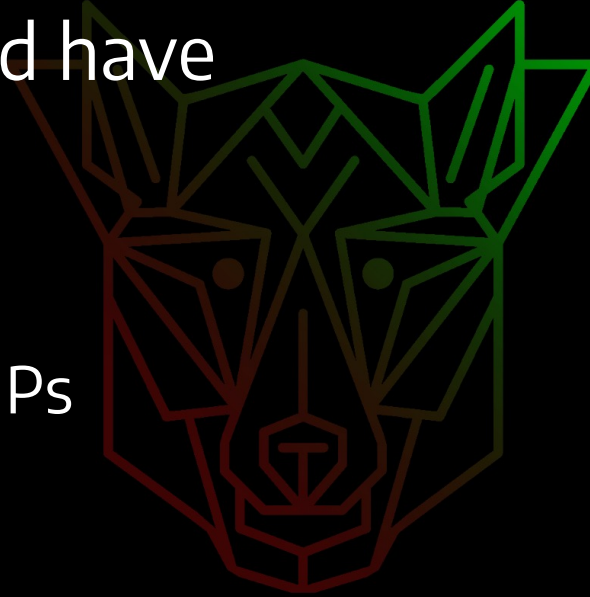
fenrir

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

fenrir