Move in Silence: Staying Quite in Mature Networks

fenrir

echo $USER

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

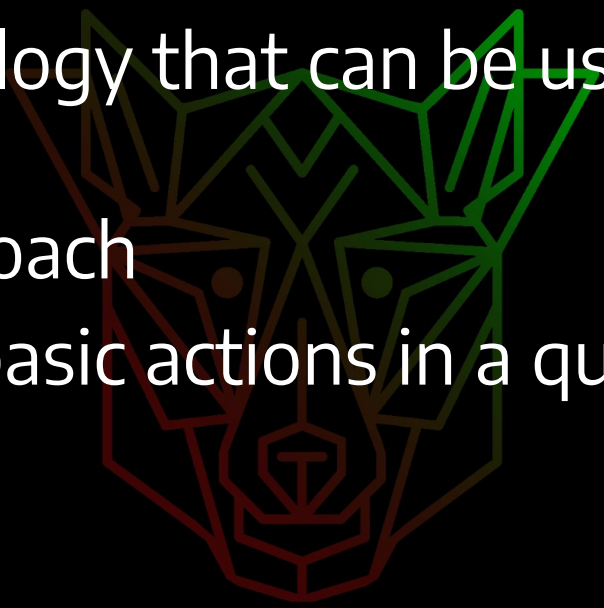
What today is not about

- Fancy new EDR evasion tactics
- Advanced techniques
- Actual exploitation

fenrir

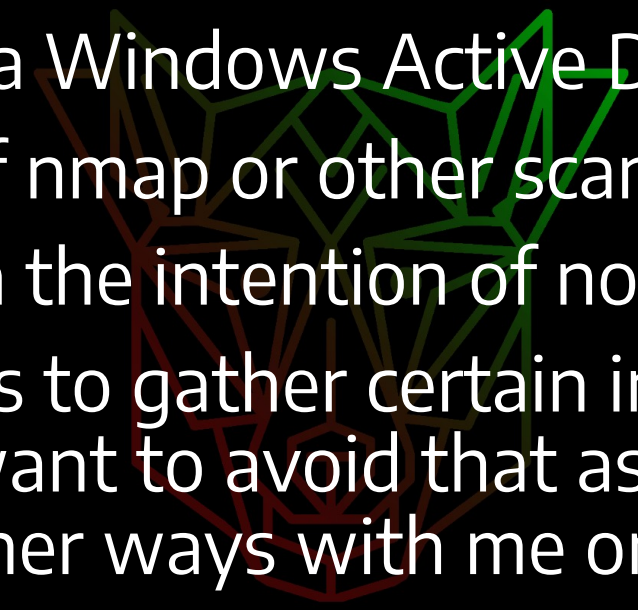
What today is about

- A real-world methodology that can be used on every engagement
- A back-to-basics approach
- Common ways to do basic actions in a quiet manner
- Boring – but works



Things to know

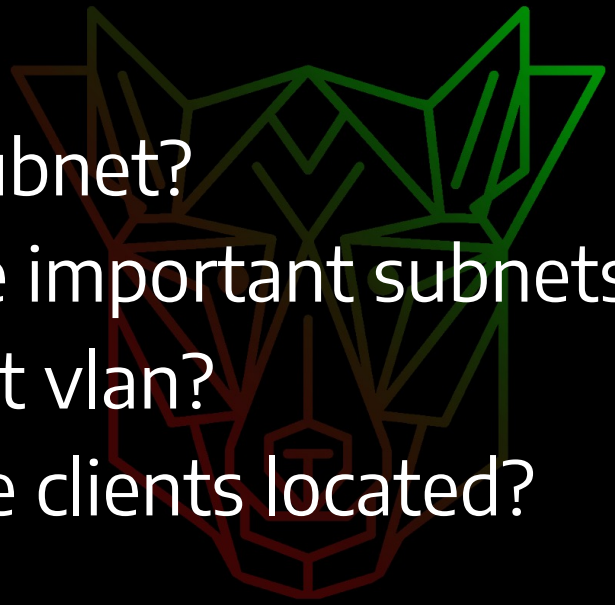
- Today we'll focus on a Windows Active Directory Network
- We'll avoid the use of nmap or other scanners
- We're doing this with the intention of not being detected
- There are lots of ways to gather certain information using Powershell, but we want to avoid that as EDR will most likely pick this up. Share other ways with me on Twitter



fenrir

Questions We Want Answered

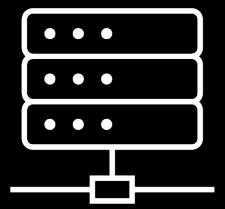
- Where is the DC?
- Where is the server subnet?
- What hosts are on the important subnets?
- Is there a management vlan?
- Where are most of the clients located?
- Is ADCS in use?



fenrir

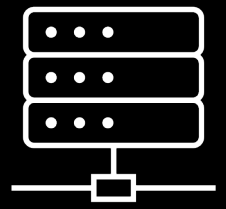
Workflow

Where am I?



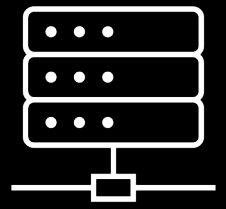
Recon the subnet

Where is the DC?

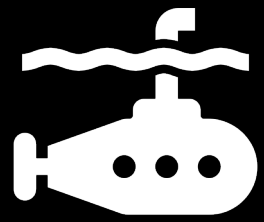


Recon the subnet & AD

Where are the member servers?



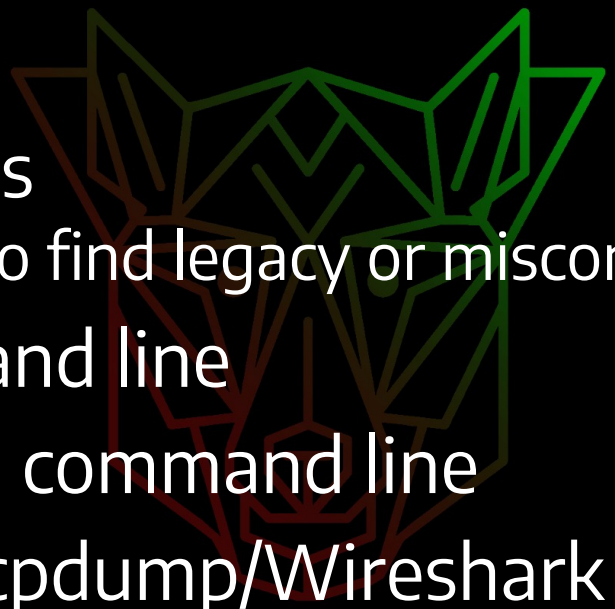
Recon the subnet



Formulate Attacks

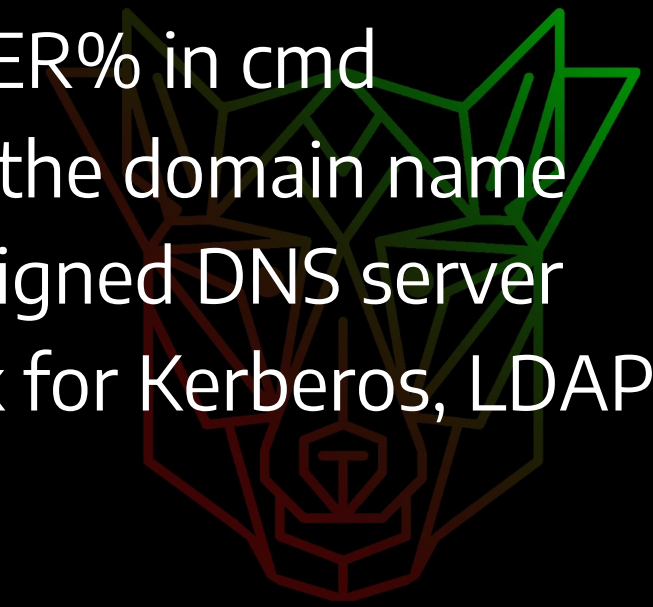
Recon A Subnet

- arp –a / arpscan
- Ping broadcast address
  - Could be a good way to find legacy or misconfigured hosts
- 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



Locating the Domain Controller

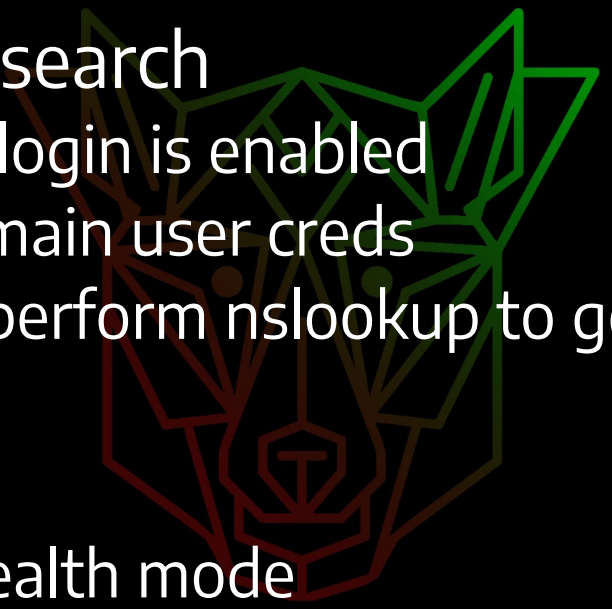
- echo %LOGONSERVER% in cmd
- perform nslookup of the domain name
- DHCP – check for assigned DNS server
- Packet capture – look for Kerberos, LDAP traffic



fenrir

Recon Active Directory

- Dump LDAP with ldapsearch
  - Hopefully anonymous login is enabled
  - If not, this requires domain user creds
  - Parse hostnames and perform nslookup to get a list of machines and IPs on the network
- Bloodhound
  - Limit collection, use stealth mode
  - Requires domain user creds
  - Might not be totally OpSec safe



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/dirkjanm/ldapdomaindump

LDAPDomainDump

Active Directory information dumper via LDAP

Introduction

In an Active Directory domain, a lot of interesting information can be retrieved via LDAP by any authenticated user (or machine). This makes LDAP an interesting protocol for gathering information in the recon phase of a pentest of an internal network. A problem is that data from LDAP often is not available in an easy to read format.

ldapdomaindump is a tool which aims to solve this problem, by collecting and parsing information available via LDAP and outputting it in a human readable HTML format, as well as machine readable json and csv/tsv/greppable files.

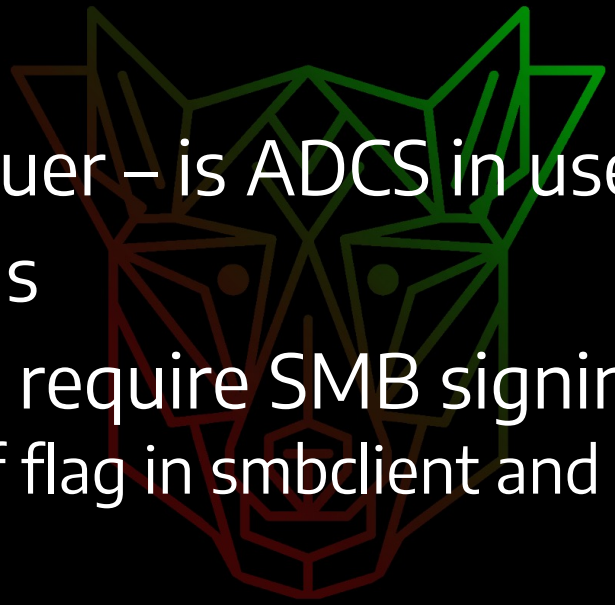
The tool was designed with the following goals in mind:

- Easy overview of all users/groups/computers/policies in the domain
- Authentication both via username and password, as with NTLM hashes (requires ldap3 >=1.3.1)
- Possibility to run the tool with an existing authenticated connection to an LDAP service, allowing for integration with relaying tools such as impackets ntlmrelayx

The tool outputs several files containing an overview of objects in the domain:

Recon Active Directory

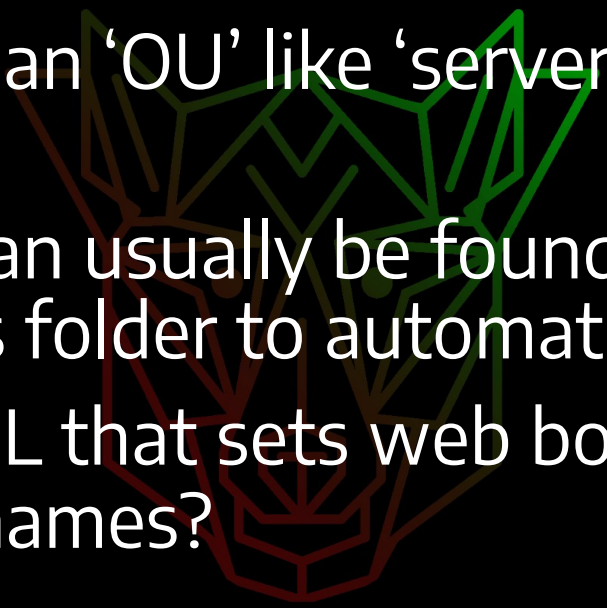
- net view /all
- Check SSL certs for issuer – is ADCS in use?
- Kerberoast to get SPNs
- Find hosts that do not require SMB signing
  - --client-protection=off flag in smbclient and observe response



fenrir

Locating Member Servers

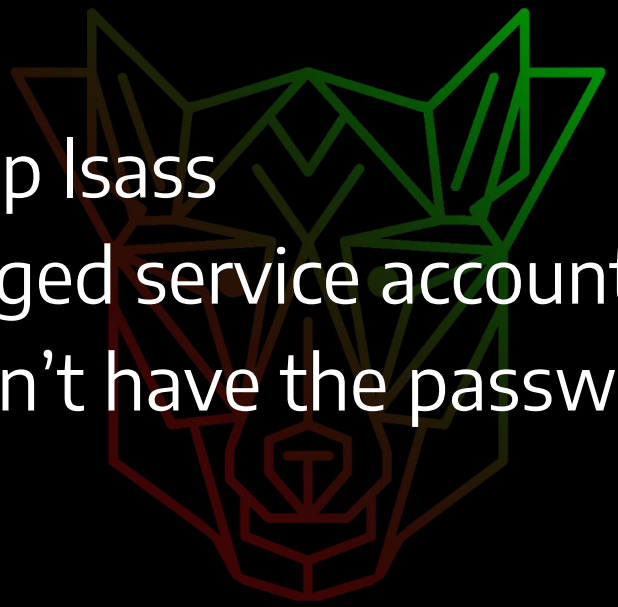
- LDAP dump – look for an ‘OU’ like ‘servers’, member servers’, etc.
- Mapped file shares - can usually be found in SYSVOL when Admins use the scripts folder to automatically map drives
- Look at GPO in SYSVOL that sets web bookmarks. What are those addresses/hostnames?



fenrir

Lateral Movement & Privilege Escalation

- Avoid mimikatz
- Use procdump to dump lsass
- Check for group managed service accounts
- Popped a shell, but don’t have the password? Use RPC ping to get the NTLMv2 hash.



fenrir

Communicating with C2's

- Use mTLS on 443
- Route traffic through an SSL tunnel with stunnel on 443
  - Firewall and SOC will be able to see the host, but not the data
- DNS over HTTPS
- IPv6

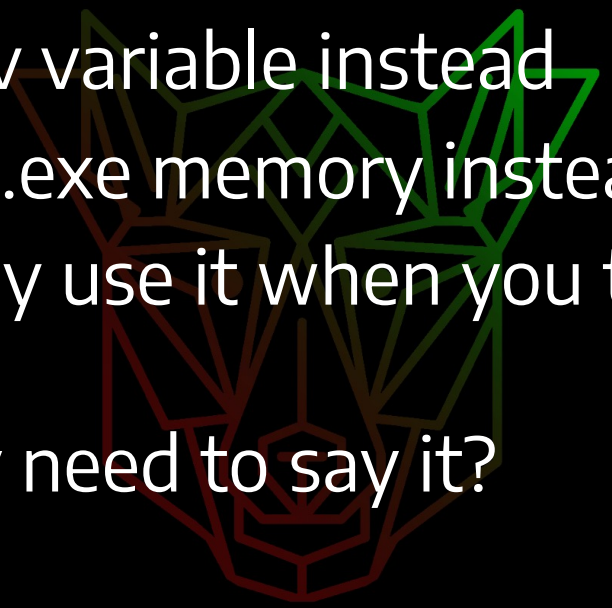
fenrir

Example Attack

- Landed on the network and did an arp scan. Investigated the hosts in the arp table.
- Determined to be on some kind of client vlan
- Checked the primary DNS server. Discovered to be 10.0.0.1
- Did a ping sweep with bash on 10.0.0.1/24. Discovered other hosts.
- Dumped LDAP
- SMB relay. Popped a shell
- Used procdump and found DA creds in LSASS

Things to avoid

- whoami – echo the env variable instead
- mimikatz – dump lsass.exe memory instead
- Powershell – try to only use it when you think EDR has been disabled
- Metasploit – do I really need to say it?



fenrir

Fin

- Find me in the WWHF Way West discord. My username is @aGsudofenrir
- Slides and files will be available on GitHub
  - github.com/cwolff411
- Check out my Twitter thread and share your favorite ways to be quiet in mature networks
  - twitter.com/cwolff411