AD - Initial attack vectors

i) LLMNR poising

★ LLMNR

- used to id hosts when DNS fails
- previously known as Netbios - NS
- service uses user's username and NTLMv2 hash when appropriately responded to.

Use **Responder**

↳ run first thing in morning

i) or after lunch → when most traffic

ii) Listen for events → wrong address → DNS fail

iii) Get NTLM hash → crack it

Mitigation

→ Disable LLMNR and NBT-NS

→ If can't disable, require network access control. → Looks at MAC to verify

→ Require strong passwords
↳ 14 chars + complex

2) SMB Relay :

⇒ In LLMNR poisioning we get hashes.

- Instead of cracking them, we can simply pass to other machines to gain access.

Requirements :

- SMB signing must be disabled on the target.
- Relayed user credentials must be admin on the machine.

Steps

1) Run responder for listening for events
2) Receivs credentials and relays to specified targets. using ntlmrelayx
3) If received hash is of admin on target, our ~~to~~ attack is done.

How to identify if SMB signing enabled / disabled.

↳ use nmap / nessus

↓

```
$ nmap --script=smb2-security-mode.nse -p445 <ip>
```

↳ subnet or range

- If we get "msg signing enabled but not required"
  we can explbit using relay.

- put all such ip's in a targets.txt file.

  ↓

  run ntlmrelayx.py

  Finally, you get SAM hashes ☆ → save

  ↓

  just like /etc/shadow

- to get a shell run the ntlmrelayx command with -i

  ↓

  SMB shell ~~⇒ can use target~~

  or

  use -c "<reverse shell>"
  somthing

Mitigation :

1) Enable smb signing on all devices (can cause performance issues) [stops the attack]

2) Disable NTLM authn (but nothing to fall back to, if Kerberos stops working). [stops the attack]

3). Account Tiering (enforcing is difficult)

4) Local admin restriction :
(potential increase in the amount of service desk tickets).

3) gaining shell excess

u have samb user and passwd → use psexec

to get shell ←

If mfconsole fails (win Defender can pick it up) ↓

use psexec.py → impacket toolkit

use multiple options

Note : psexec is noisy, start with smbexec and wmiexec, get in, try to disable AV. and then try to run windows meterpretor -

4) IPv6 attack ← very good and reliable!!!

- If IPv6 on but not utilized, chances are that ~~no~~ there is no DNS for it.
- We can spoof DNS and get authn to Domain Controller.

Run m9tm6 on a domain, use ntlmrelayx to run credentials and do a host of things.

Mitigation :

1) IPv6 poisoning takes advantage of fact that windows queries for ipv6 even in ipv4 env.

safest → disable DHCPv6 traffic and incoming router advertisements via firewall.

★ But disabling ipv6 may have side effects.

Disable : → inbound DHCPv 6
→ outbound DHCPv6
→ Inbound Router advertisement

2) If WAPD not used → disable it via Group Policy.
Disable winHttp Auto Proxy Svc

3) Mitigate ~~LADP~~ LDAP relay by enabling both LDAP signing and LDAP channel binding.

4). Consider Administrative users to Protected users group or marking Account is sensitive and cannot be delegated.
↓
prevents any impersonation via delegation.

Stragety:

- Begin day with mitm6 or responder.
- Run Scans to generate traffic.

  ↓

  if scans taking too long, look at websites in scope (tool: http-version)
- Look for default creds on web Logins
  - Printers
  - Jenkins etc

★ Think outside the box.