ATTACKS

Active Directory Authentication

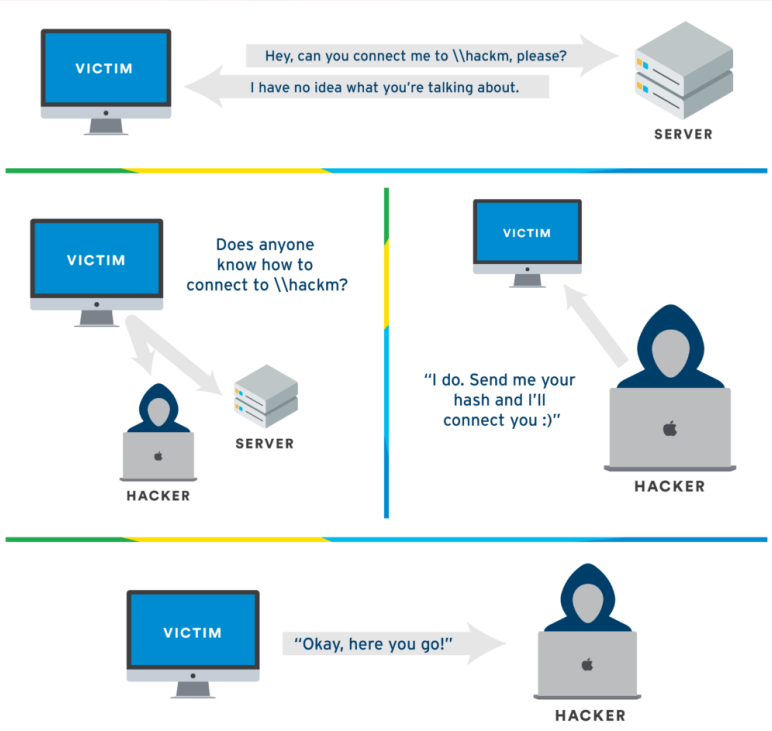
1

LLMNR/NBT-NS POISONING

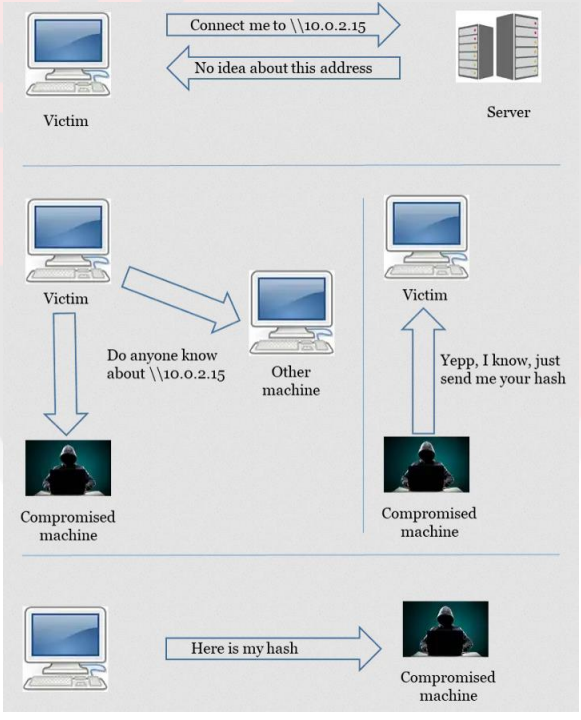
What is LLMNR?

- Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are components of Microsoft Windows systems that are alternate methods of host identification when DNS fails.
- LLMNR and NBT-NS can be spoofed by listening for LLMNR (UDP 5455) or NBT-NS (UDP 137) broadcasts going over the wire and respond to them.
- The attacker can then trick the target into sending the NTLMv2 or v1 hash which is used for network level authentication making access to network resources seamless for the end user.

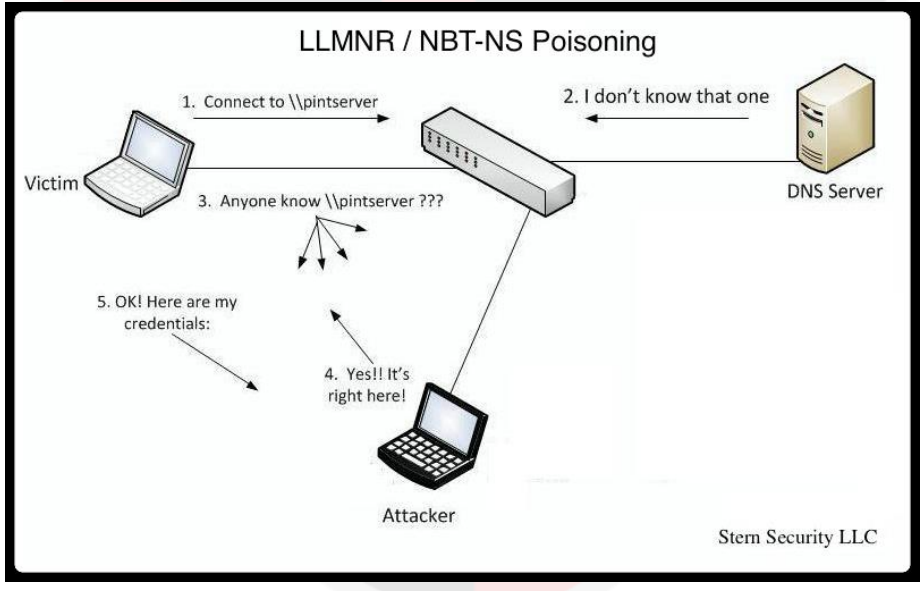
What is LLMNR Poisoning?



What is LLMNR Poisoning?



What is LLMNR Poisoning?



Popular Tools Used

- **Linux**
  - Responder – Developed by SpiderLabs
  - Man-in-the-Middle Framework (MiTMf) – Developed by Byt3bl33d3r
  - LLMNR_Response Module in the Metasploit Framework
  - Nbnspoof –Developed by Robert McGrew
- **Windows**
  - Inveigh–Developed by Kevin Robertson

Mitigation

- Disable LLMNR/NBT-NS service (from Group Policy Editor)
- Leverage Network Access Control
- Use strong passwords

CACHED CREDENTIAL RETRIEVAL

What are Cached Credentials?

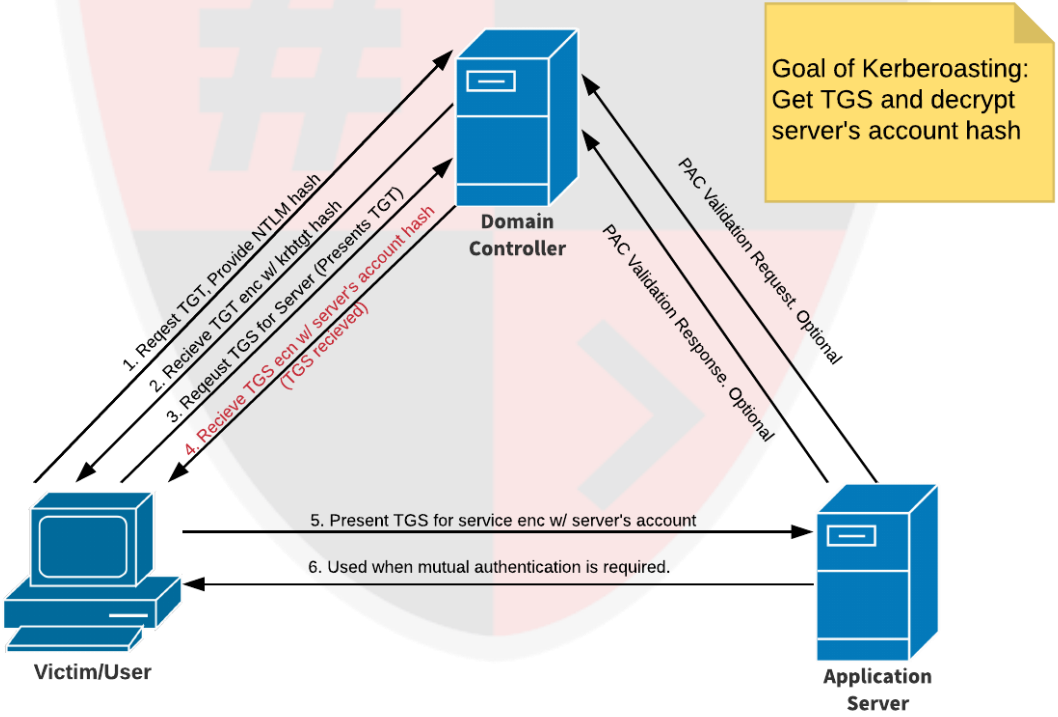
- In Windows, password hashes are stored in LSASS memory space to enable single sign on via Kerberos.
- The process runs as SYSTEM, so we need SYSTEM privs to obtain the hashes.
- Tools like Mimikatz can be used to extract those hashes
- It can even be used to extract cached TGT/TGS for logged in users, and can even import custom TGT/TGS into LSASS.

3 KERBEROASTING

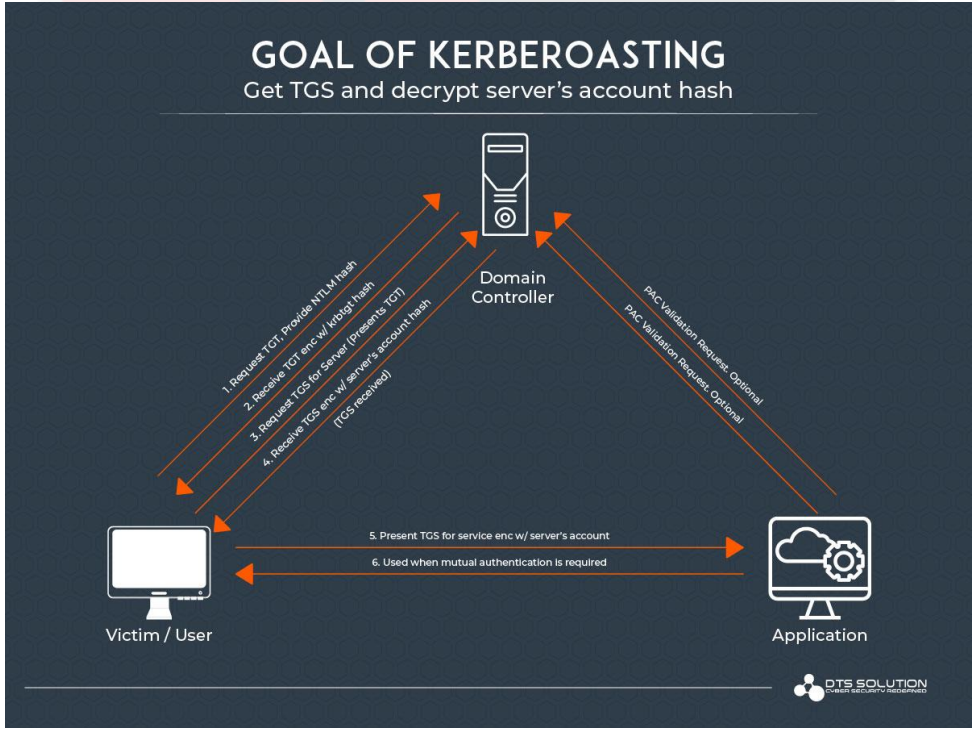
What is Kerberoasting?

- Service principal names (SPNs) are used to uniquely identify each instance of a Windows service.
- By logging into an Active Directory domain as any authenticated user, we are able to request service tickets (TGS) for service accounts by specifying their SPN value.
- Active Directory will return an encrypted ticket, which is encrypted using the NTLM hash of the account that is associated with that SPN.
- Used to harvest TGS tickets for services that run on behalf of user accounts in the AD, not computer accounts.

What is Kerberoasting?



What is Kerberoasting?



Popular Tools Used

- **Empire**
- **Impacket** (**GetUserSPNs**)
- **PowerSploit**
- Active Directory Module for PowerShell

Requirements

- Valid Credentials for a domain user account
- Target domain account should have a servicePrincipalName (SPN) set

Mitigation

- Enable AES Kerberos encryption rather than RC4
- Ensure strong password length (ideally 25+ characters) and complexity for service accounts
- Limit service accounts to minimal required privileges