


Responder as an Entrypoint

Low Hanging Fruit

Jon Buhagiar (Bohack)

Jon Buhagiar

- Director of Network Operations
  - Pittsburgh Technical College
- Instructor
  - Cisco and Microsoft (Since NT 4.0)
- Author/Editor
  - Wiley/Sybex
- YouTube Creator
  - @NetworkedMinds
- Electronics and Ham Radio (KB3KGS) Enthusiast

Responder

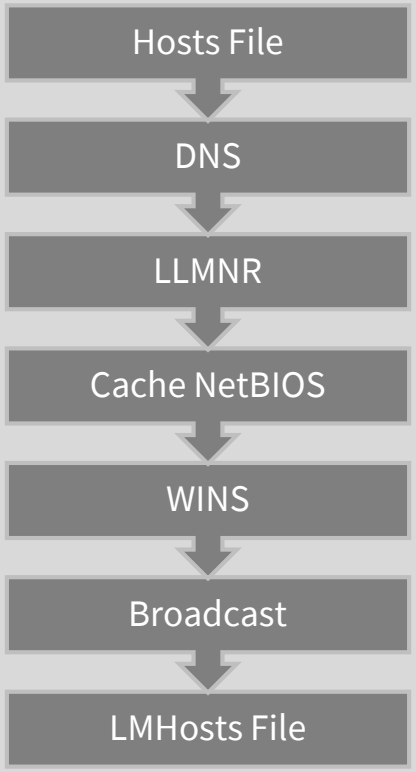
- A Python script:
  - Downloaded from GitHub (https://github.com/SpiderLabs/Responder)
  - Installed natively on Kali Linux
  - Tactics can even be found in PowerShell tools
- Red team (threat actor) tool
  - Penetration testers (good guys)
  - APT28 (Russians)
  - Lazarus Group (North Koreans)
- Exploits Microsoft's willingness to help resolve server names
- Helps a threat actor gain the milestone of initial access or privilege escalation (Mitre ATT&CK framework)

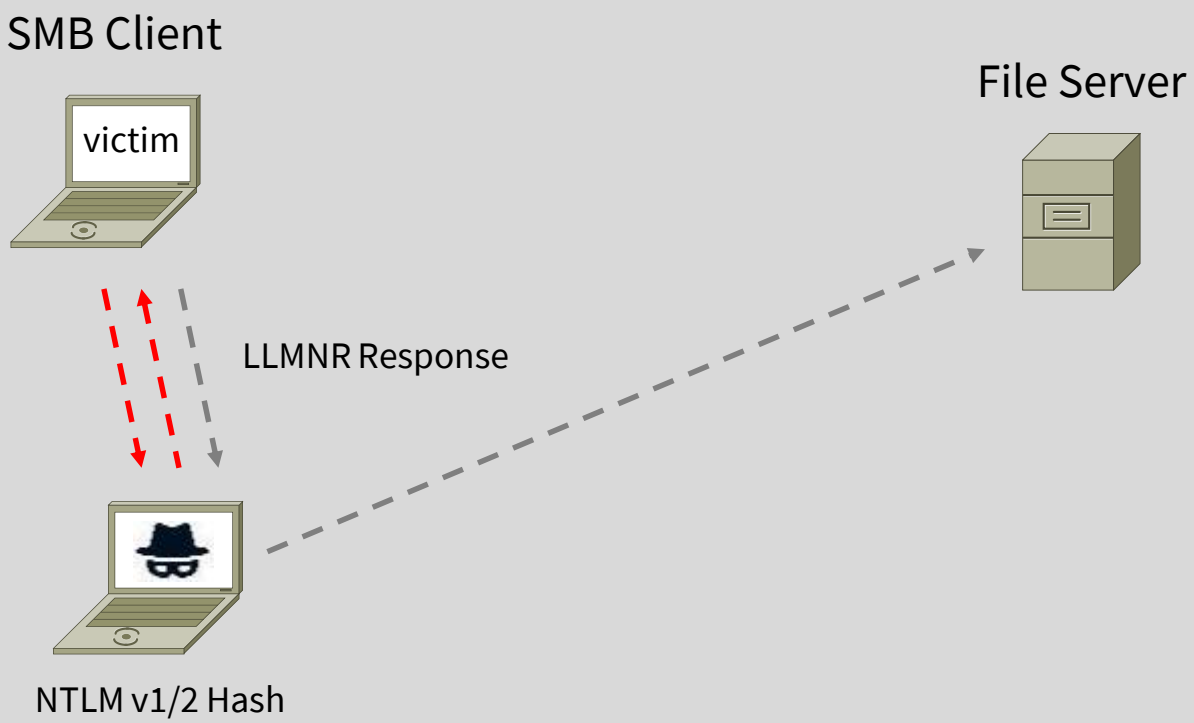
Ref: https://attack.mitre.org/software/S0174/

Responder Tactics

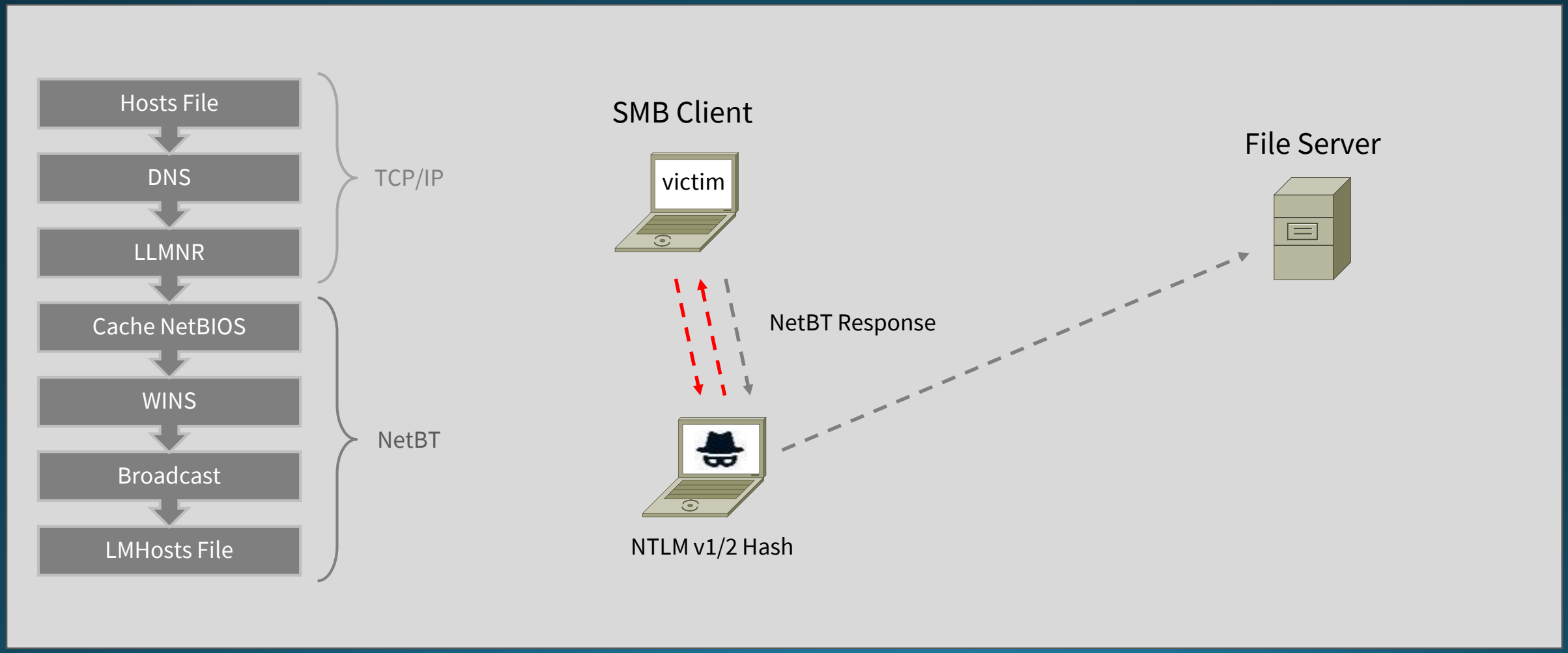
- Link Local Multicast Name Resolution (LLMNR)
- Multicast DNS (mDNS)
- NetBIOS Name Service (NBT-NS)
  - NTLM v1/v2 Listener
- Web Proxy Auto-Discovery (WPAD)
- IPv6 Protocol
  - Router Advertisements (RA)
  - Network Discover (ND)

Link Local Multicast Name Resolution (LLMNR) and Multicast DNS (mDNS)

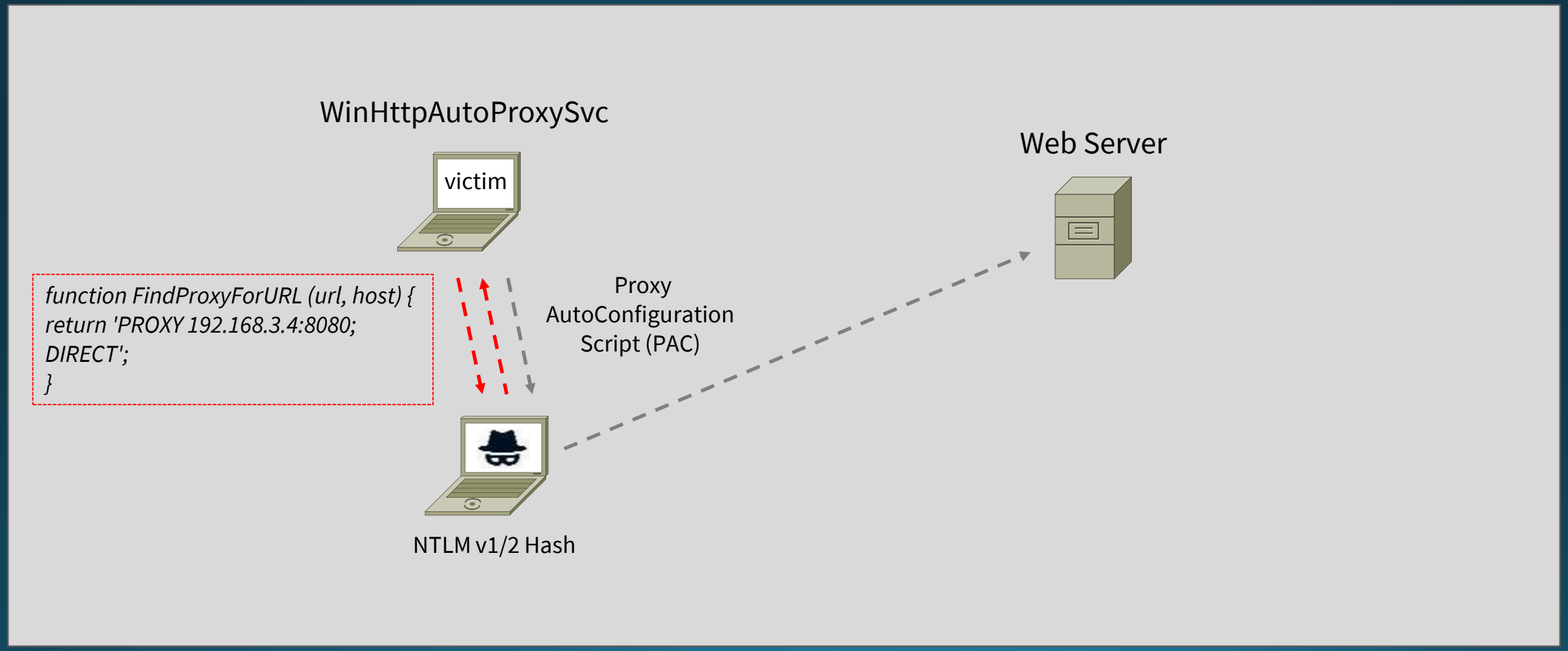




NetBIOS over TCP/IP (NetBT)

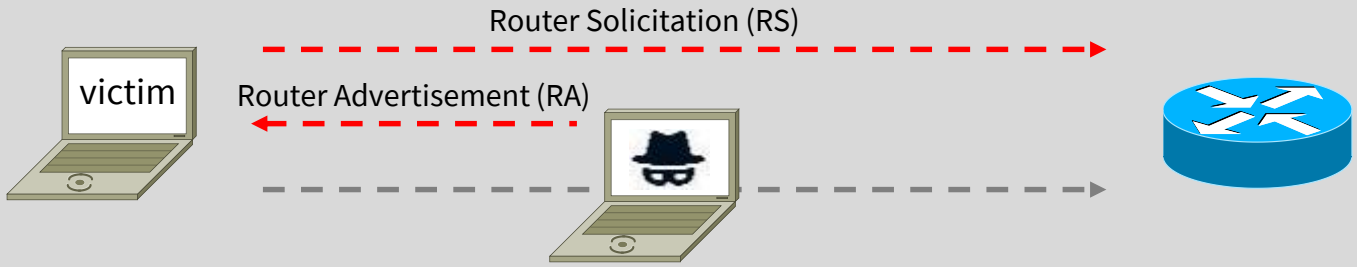


Web Proxy Auto Discovery (WPAD)

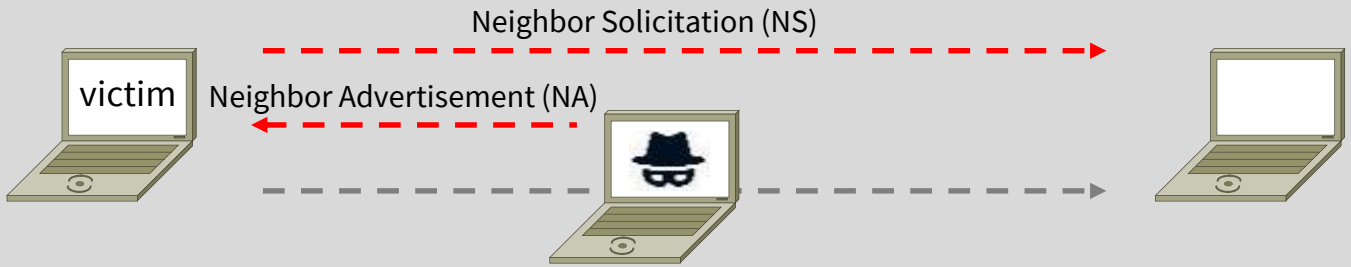


IPv6 Protocol

Router Advertisement

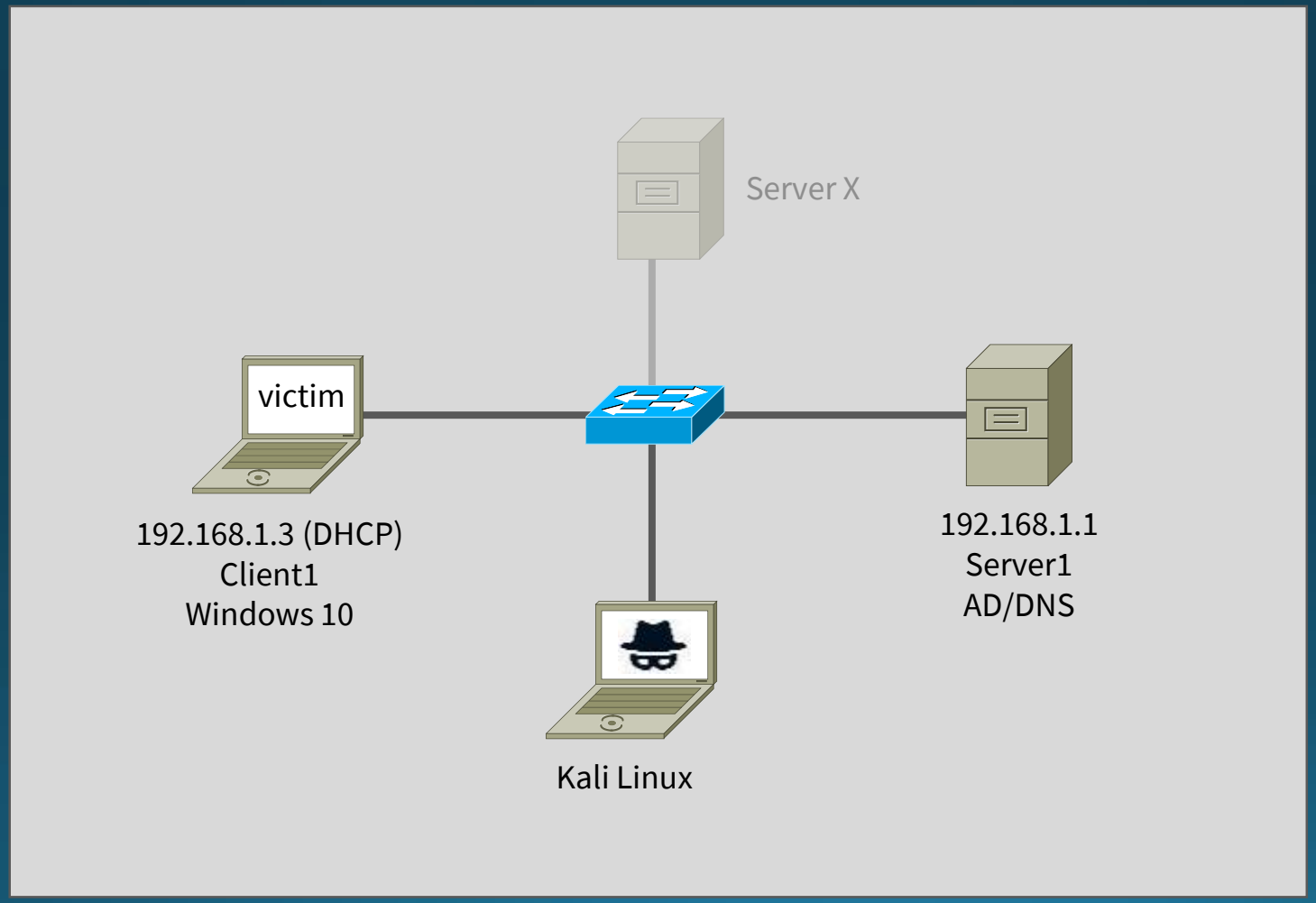


Neighbor Discovery



Demo Time – What could go wrong?

Demo Network



DEMO

So, how do we fix it…

Internal vs. External Controls

- Internal
  - Any setting or resource you control
    - Active Directory
    - DHCP
    - GPO
    - Registry
- External
  - Any setting you can’t control
    - Bring your own device (BYOD)
    - Personal devices

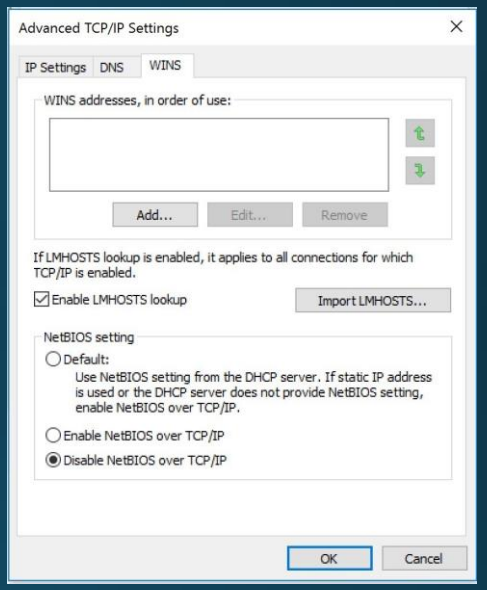
Fixing LLMNR

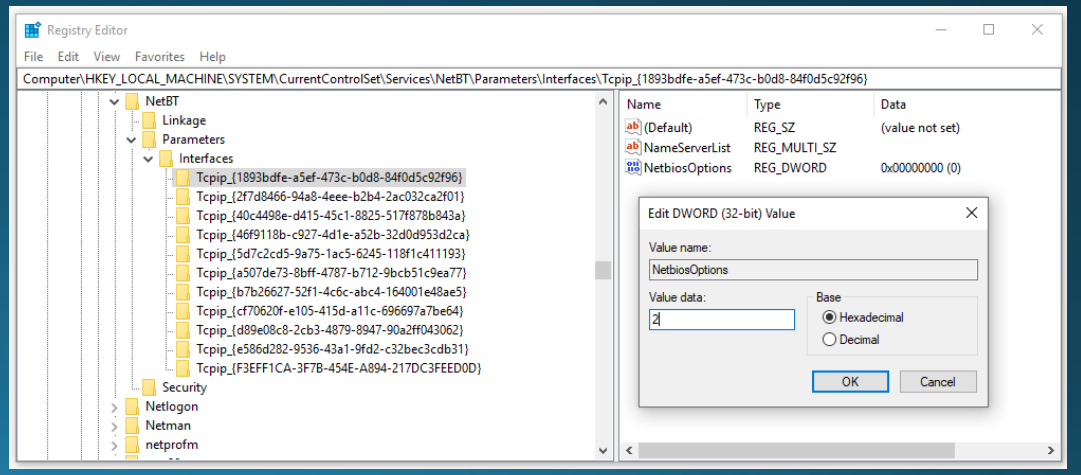
- Internal
  - Computer Configuration > Administrative Templates > Network > DNS Client > Turn Off Multicast Name Resolution (Enable)
  - Regedit HKLM\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient
    - Create key EnableMulticast = 0

- External
  - DNS tricks like wildcard subdomains? (*.contoso.com -> 127.0.0.1)
  - Block UDP port 5355 with a VLAN ACL (VACL)?
  - Ask users nicely to edit their GPO?

Fixing NetBIOS over TCP/IP

- Internal
  - Disable with GPO and startup scripts
  - Disable in the GUI
  - Regedit each TCPIP_GUID in HKLM\SYSTEM\CurrentControlSet\Services\NetBT\Parameters\Interfaces
- External
  - DHCP Option 001 (vendor class)
    - Microsoft Disable Netbios Option – 0x2



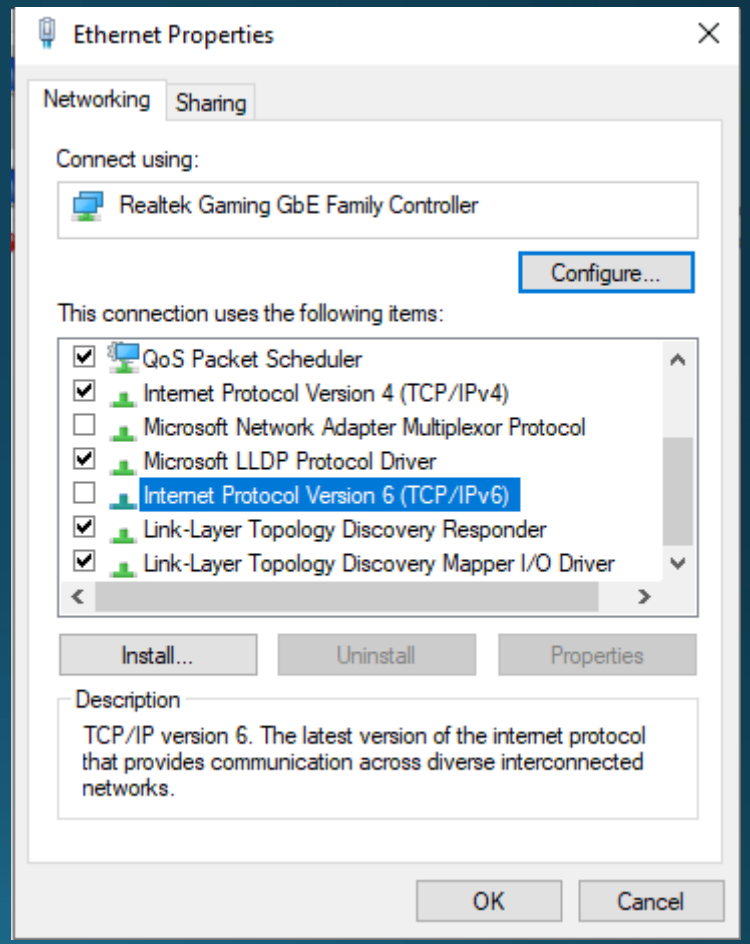


Fixing WPAD

- Internal
  - Configure GPO
    - User Configuration > Administrative Templates > Windows Components > Internet Explorer > Disable Caching of Auto-Proxy Scripts > (Enable)
  - HOSTS file entry
    - 255.255.255.255 wpad
  - Registry entry
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WinHttpAutoProxySvc\Start
      - Set to 4 to disable
    - HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp\DisableWpad
      - Set to 1 to disable
- External
  - Configure *wpad.domain-name* to 127.0.0.1 via DNS
  - Configure DHCP option number 252

Fixing IPv6

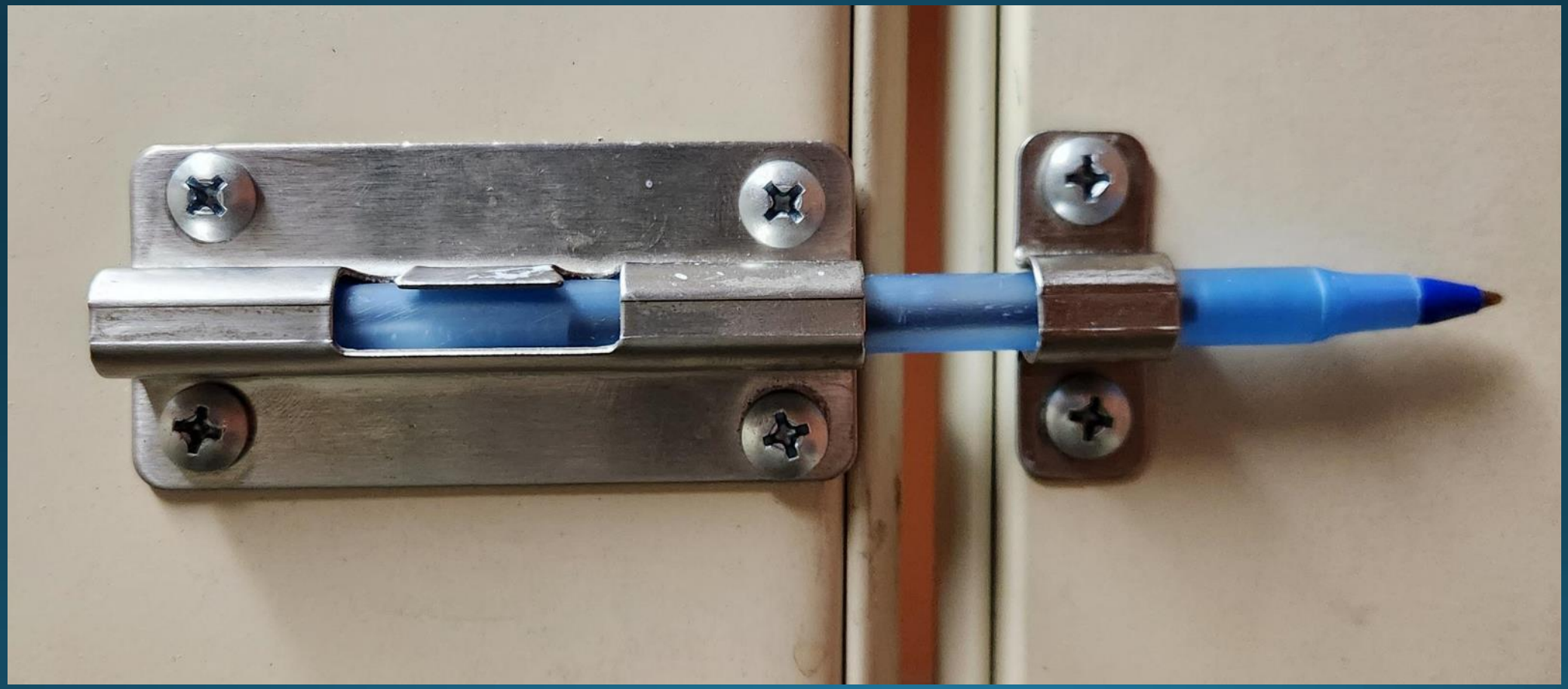
- Internal & External
  - Turn it OFF!
  - Configure IPv6 RA Guard
    - Similar to DHCP Guard – blocking rouge RA messages
  - Configure IPv6 Secure Neighbor Discovery (SeND)
    - Uses public key encryption to protect name resolution
  - Turn it OFF!
    - WAN good
    - LAN bad



Fixing mDNS

- Internal
  - Registry entry
    - HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters
      - Create key EnableMDNS = 0
  - Windows Defender with Advanced Security
    - Create an Outbound and Inbound rule to block UDP/5353
- External
  - Block UDP/5353 with VLAN ACL (VACL)
  - Ask users nicely to edit their registry?

Let’s take a look and fix it!



DEMO

Questions?