

## Table of Contents

<b>Task 1:</b> .....	2
<b>Task 2:</b> .....	3
<b>Task 3:</b> .....	4
<b>Task 4:</b> .....	5
<b>Task 5:</b> .....	5
<b>Task 6:</b> .....	6
<b>Task 7:</b> .....	7
<b>Task 8:</b> .....	7
<b>Task 9:</b> .....	8

### Intro:

The IDS device alerted us to a possible rogue device in the internal Active Directory network. The Intrusion Detection System also indicated signs of LLMNR traffic, which is unusual. It is suspected that an LLMNR poisoning attack occurred. The LLMNR traffic was directed towards Forela-WKstn002, which has the IP address 172.17.79.136. A limited packet capture from the surrounding time is provided to you, our Network Forensics expert. Since this occurred in the Active Directory VLAN, it is suggested that we perform network threat hunting with the Active Directory attack vector in mind, specifically focusing on LLMNR poisoning.

Tools that I used in this Sherlock:

1. Wireshark
2. Network Miner
3. Hashcat

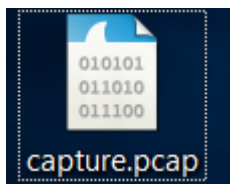
# HTB- Sherlocks: Noxious – Level: Very Easy

## Amit Persky

### Task 1:

Its suspected by the security team that there was a rogue device in Forela's internal network running responder tool to perform an LLMNR Poisoning attack. Please find the malicious IP Address of the machine.

Ok so basically when we are talking about LLMNR we need to remember that this service running on UDP port 5355 and we know that 172.17.79.136 is a legitimate IP of the network. We got a pcap file that we are going to work with:



I decided to run Wireshark and to filter exactly to this LLMNR traffic:

No.	Time	Source	Destination	Protocol	Length	Info
9262	68.433468	fe80::7994:1860:711...	ff02::1:3	LLMNR	85	Standard query 0xe708 A DCC01
9263	68.433621	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0xe708 A DCC01
9264	68.433867	fe80::7994:1860:711...	ff02::1:3	LLMNR	85	Standard query 0x2c01 AAAA DCC01
9265	68.433932	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0x2c01 AAAA DCC01
9268	68.438072	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	LLMNR	106	Standard query response 0xe708 A DCC01 A 172.17.79.135
9269	68.440010	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0xe708 A DCC01 A 172.17.79.135
9274	68.441285	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	LLMNR	118	Standard query response 0x2c01 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
9277	68.445664	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x2c01 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
9301	68.470335	fe80::7994:1860:711...	ff02::1:3	LLMNR	85	Standard query 0x3ca4 A DCC01
9302	68.470336	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0x3ca4 A DCC01
9303	68.470774	fe80::7994:1860:711...	ff02::1:3	LLMNR	85	Standard query 0x2dd6 AAAA DCC01
9304	68.471005	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0x2dd6 AAAA DCC01
9305	68.473837	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	LLMNR	106	Standard query response 0x3ca4 A DCC01 A 172.17.79.135
9307	68.476112	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x3ca4 A DCC01 A 172.17.79.135
9309	68.479127	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	LLMNR	118	Standard query response 0x2dd6 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
9315	68.483555	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x2dd6 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7

If we look more closely we can see that the IP 172.17.79.136 made queries for the name DCC01 its a typo since it should be DC01 (most of the time)

Then we can see that the IP 172.17.79.135 is response back. Because of seeing this, we can say that the LLMNR Poisoning attack happened through these addresses, and we know that only one of this addresses is a legitimate IP, and one is not legitimate IP, and we already from the intro who is the legitimate IP.

Answer:

**172.17.79.135**

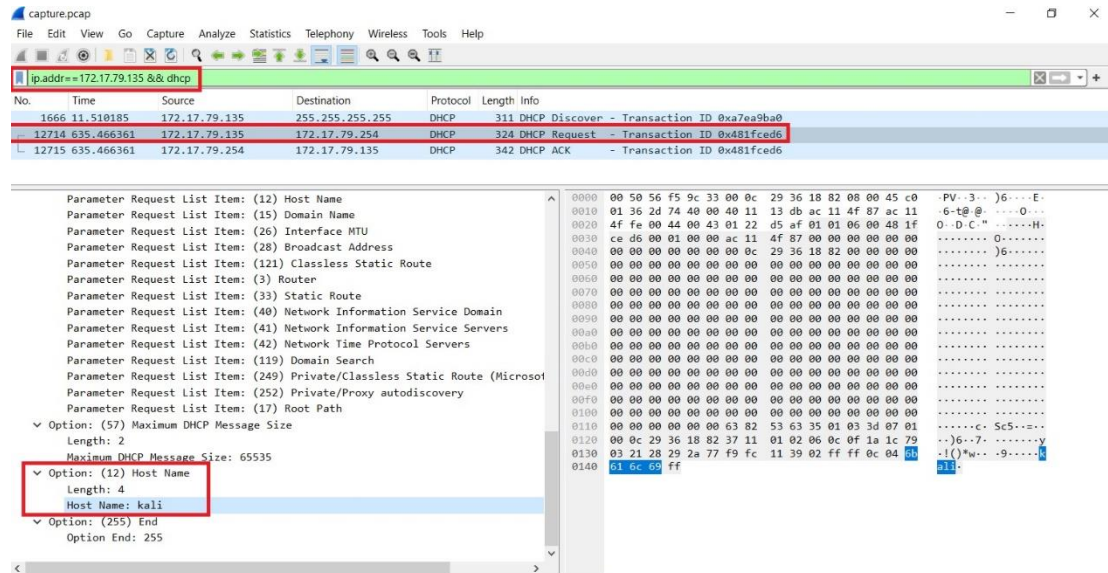
# HTB- Sherlock: Noxious – Level: Very Easy

## Amit Persky

### Task 2:

What is the hostname of the rogue machine?

ok so for this question we need to filter 2 things on Wireshark. The first one is the IP of the rogue machine (the answer from the last question) and the DHCP protocol we can do that like that:



As we can see that I filtered 2 things, then I inspected the DHCP request, then I opened the Host Name tab and then you will see the Host Name.

Answer:

**Kali**

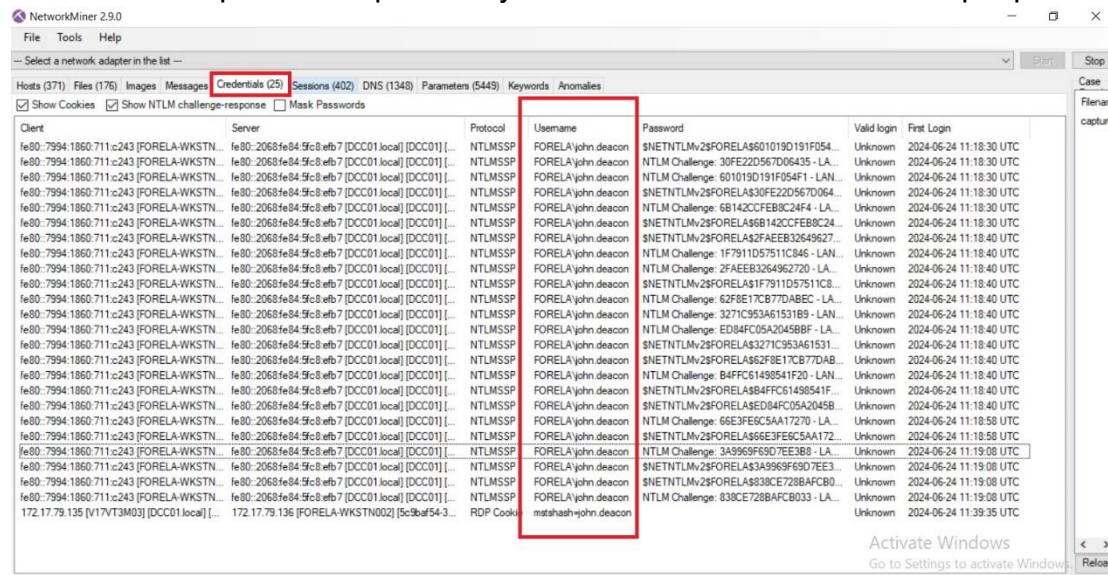
# HTB- Sherlocks: Noxious – Level: Very Easy

## Amit Persky

### Task 3:

Now we need to confirm whether the attacker captured the user's hash and it is crackable!! What is the username whose hash was captured?

Ok so for this question I opened my Network Miner and loaded our pcap.



We can see the I moved to the tab Credentials. We can see one the Username Colum the username that we are looking for.

Answer:

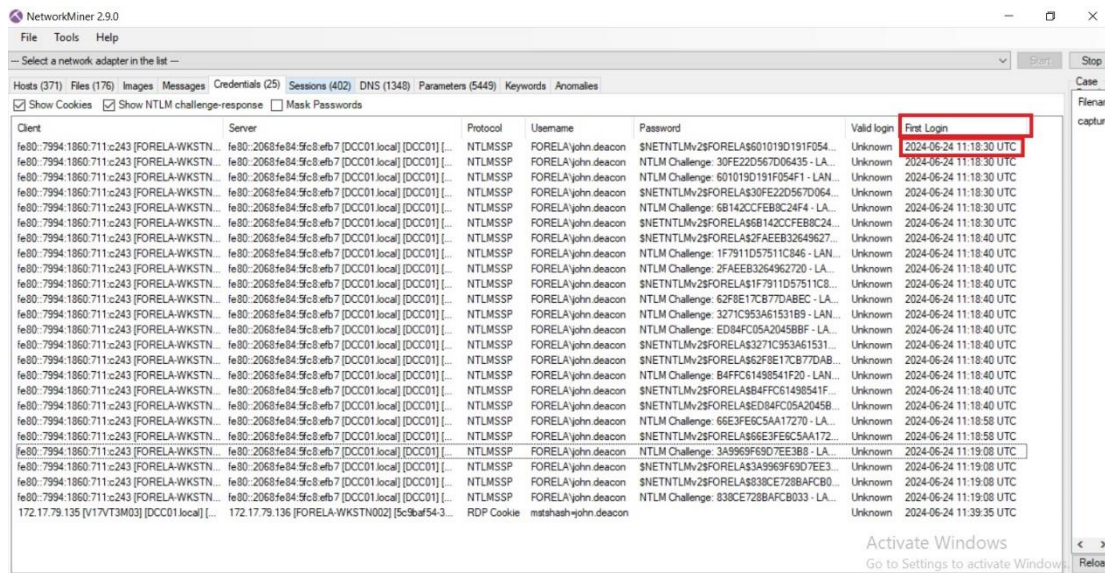
**john.deacon**

# HTB- Sherlocks: Noxious – Level: Very Easy

## Amit Persky

### Task 4:

Like the last question, we are at the same tab of Credentials. We are inside the tab and we need to navigate to First Login column, and pressing on this in aim to sort. As we can see the first answer is the answer we are looking for.



Client	Server	Protocol	Username	Password	Valid login	First Login
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$6010190191F054...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 30FE22D567D06435 - LA...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 6010190191F054F1 - LAN...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$30FE22D567D064...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 6B142CCFEB8C24F4 - LA...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$6B142CCFEB8C24...	Unknown	2024-06-24 11:18:30 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$2FAEEB32649627...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 1F7911D57511C846 - LA...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 2FAEEB3264962720 - LA...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$1F7911D57511C8...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 62F8E17CB77DABEC - LA...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 3271C953461531B9 - LAN...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: ED84FC05A20458BF - LA...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$3271C953461531...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$62F8E17CB77DAB...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: B4FFC614985A1F20 - LAN...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$B4FFC614985A1F...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$ED84FC05A20458...	Unknown	2024-06-24 11:18:40 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 66E3FE6C5AA17270 - LA...	Unknown	2024-06-24 11:18:58 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$66E3FE6C5AA172...	Unknown	2024-06-24 11:18:58 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 3A9969F69D7EE3B8 - LA...	Unknown	2024-06-24 11:19:08 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$3A9969F69D7EE3...	Unknown	2024-06-24 11:19:08 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	\$NETNTLMv2\$FORELA\$838CE728B8AFCB...	Unknown	2024-06-24 11:19:08 UTC
fe80-7994-1860-711c243 [FORELA-WKSTN...	fe80-2068-fe84-5fc8-efb7 [DCC01.local] [DCC01] [...]	NTLMSSP	FORELA\john.deacon	NTLM Challenge: 838CE728B8AFCB033 - LA...	Unknown	2024-06-24 11:39:35 UTC
172.17.79.135 [17V7T3M03] [DCC01.local] [...]	172.17.79.136 [FORELA-WKSTN002] [5c9eaf54-3...	RDP Cookie	matashash-john.deacon			

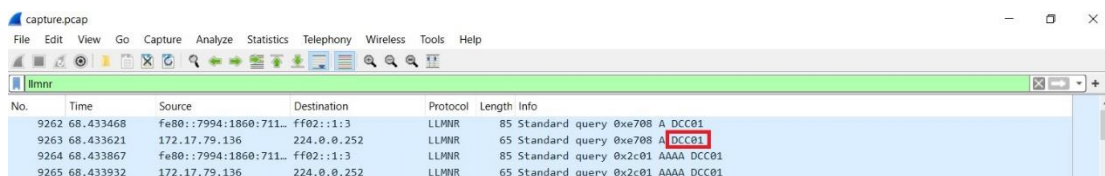
Answer:

2024-06-24 11:18:30

### Task 5:

What was the typo made by the victim when navigating to the file share that caused his credentials to be leaked?

In the Wireshark capture, I looked at the LLMNR queries again being sent out by the victim's machine. These queries contained the hostname that the victim tried to resolve, which included the typo, as we saw the before and this is the answer.



No.	Time	Source	Destination	Protocol	Length	Info
9262	68.433468	fe80::7994:1860:711c243	ff02::1:3	LLMNR	85	Standard query 0xe708 A DCC01
9263	68.433621	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0xe708 A DCC01
9264	68.433867	fe80::7994:1860:711c243	ff02::1:3	LLMNR	85	Standard query 0x2c01 AAAA DCC01
9265	68.433932	172.17.79.136	224.0.0.252	LLMNR	65	Standard query 0x2c01 AAAA DCC01

Answer:

DCC01



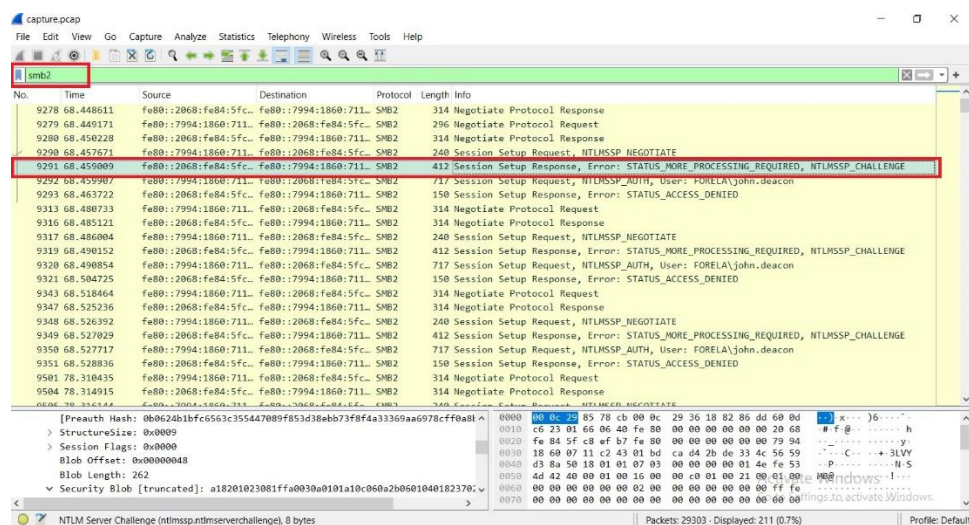
# HTB- Sherlock: Noxious – Level: Very Easy

## Amit Persky

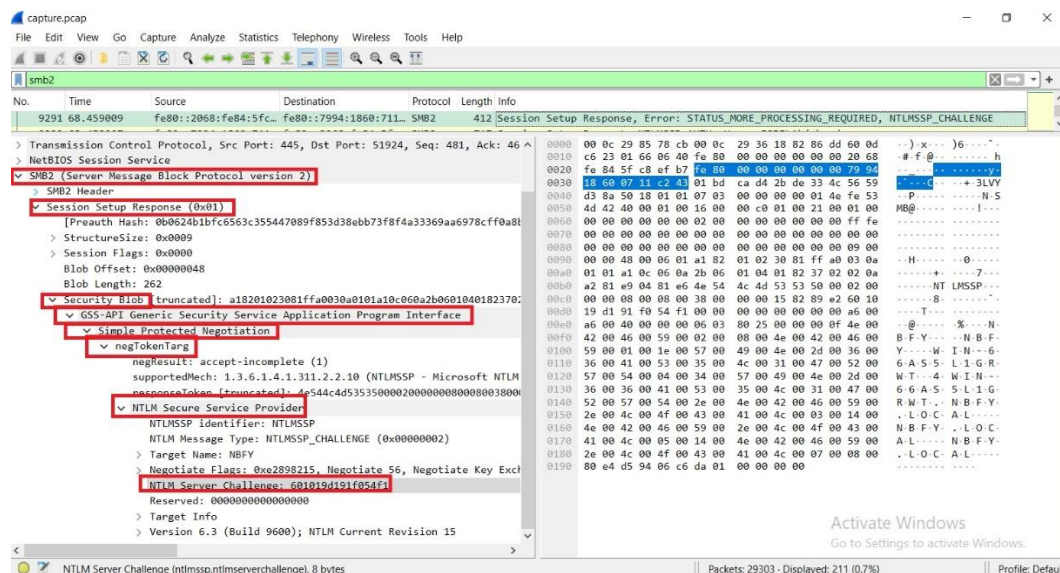
### Task 6:

To get the actual credentials of the victim user we need to stitch together multiple values from the ntlm negotiation packets. What is the NTLM server challenge value?

Ok to answer this question I opened Wireshark again and I searched smb (smb2 on the wireshark) packets. As you can see I inspected the first NTLMSSP\_CHALLENGE packet that I saw.



If we are going deep inside, we can see the NTLM server challenge value:



As we can observe, we found the NTLM server challenge value.

Answer:

**601019d191f054f1**

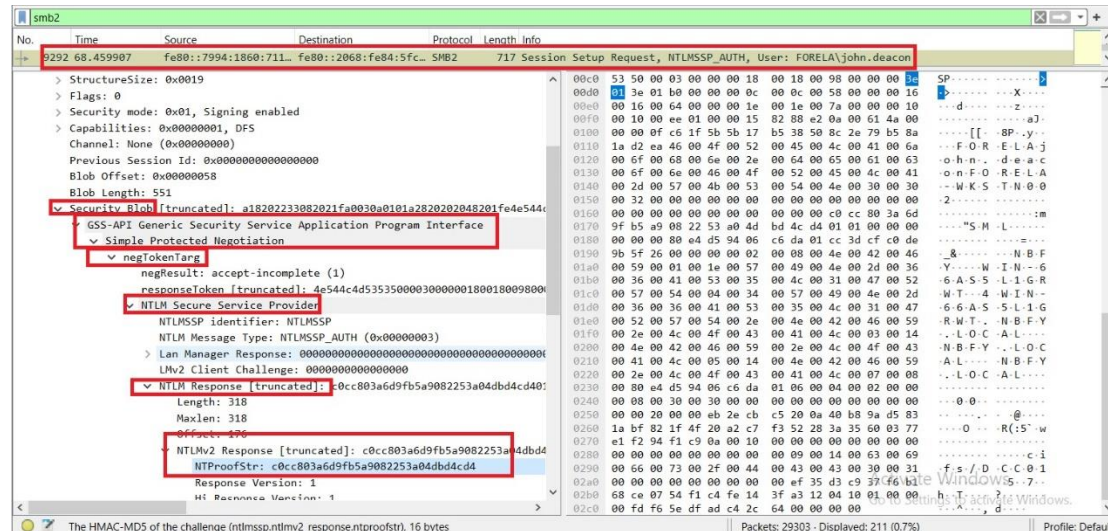
# HTB- Sherlocks: Noxious – Level: Very Easy

## Amit Persky

### Task 7:

Now doing something similar find the NTProofStr value.

Ok for this question I scrolled 1 packet down to 9292 inspected deep inside at the same way, and I found the value:



Answer:

**c0cc803a6d9fb5a9082253a04dbd4cd4**

### Task 8:

To test the password complexity, try recovering the password from the information found from packet capture. This is a crucial step as this way we can find whether the attacker was able to crack this and how quickly.

Ok so for answering this question I checked the HTB hint to understand how to crack the password:

Task 8 Hint

Create a new file and plug in the values as follows.  
User::Domain:ServerChallenge:NTProofStr:NTLMv2Response(without first 16 bytes). The NTLMv2 Response value can be found from where we found NTProofStr. Remove the first 16 bytes(32 characters) from the value. Then crack the hash using hashcat. Hashcat syntax will be as follows. Hashcat -a0 -m5600 hashfile.txt rockyouwordlist.txt

## HTB- Sherlocks: Noxious – Level: Very Easy

Amit Persky

I checked the packets exactly how the hint tried to help and got this:

```
john.deacon::FORELA:601019d191f054f1:c0cc803a6d9fb5a9082253a04dbd4
cd4:0101000000000000080e4d59406c6da01cc3dcfc0de9b5f26000000000200
08004e0042004600590001001e00570049004e002d00360036004100530035
004c003100470052005700540004003400570049004e002d00360036004100
530035004c00310047005200570054002e004e004200460059002e004c004f
00430041004c00030014004e004200460059002e004c004f00430041004c000
50014004e004200460059002e004c004f00430041004c000700080080e4d59
406c6da0106000400020000000800300030000000000000000000000000200
000eb2ecbc5200a40b89ad5831abf821f4f20a2c7f352283a35600377e1f294f1
c90a00100000000000000000000000000000000000000000009001400630069006600
73002f0044004300430030003100000000000000000000
```

now all I have to do is to hashcat that:

```
(kali㉿kali)-[~/Desktop]
$ hashcat -a0 -m5600 crackme rockyou.txt
hashcat (v6.2.6) starting
```

[illegible]

Answer:

## NotMyPassword0k?

### Task 9:

Just to get more context surrounding the incident, what is the actual file share that the victim was trying to navigate to?

Ok so for answering this question I looked in the hint:

**Task 9 Hint**

Filter for SMB traffic. In Wireshark, it is "smb2". Then keep scrolling until you see a tree connect/disconnect of a NON-DEFAULT File share name. This will make sense if you keep in mind the typo the victim made in Question 5.



## HTB- Sherlock: Noxious – Level: Very Easy

### Amit Persky

I understood that we are looking for smb (smb2 on Wireshark) packet with connect/disconnect with some details that we already know. I started scrolling down after the filtering and at first look I saw that in some time:

10189	115.465183	172.17.79.136	172.17.79.4	SMB2	152	Tree Connect Request Tree: \\DC01\IPC\$
-------	------------	---------------	-------------	------	-----	---

But, we know that the share name IPC\$ is a **default** share in Windows environments so its not the answer. But know we can imagine how the real answer need to look like with unique path. I scrolled down and say this:

10214	115.957127	172.17.79.136	172.17.79.4	SMB2	174	Tree Connect Request Tree: \\DC01\DC-Confidential
-------	------------	---------------	-------------	------	-----	---

Unlike the previous IPC\$ share, which is a default administrative share, DC-Confidential appears to be a custom, non-default file share. It might be a share created specifically for sensitive or confidential data on the domain controller.

So this is the answer that we looked for:

Answer:

**\\DC01\DC-Confidential**