Noxious Challenge

Sherlock Scenario
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.

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.

I checked on Google how to find LLMNR Poisoning in Wireshark with Responder and accessed the first article from Cynet
https://www.cynet.com/attack-techniques-hands-on/llmnr-nbt-ns-poisoning-and-credential-access-using-responder/

Then I saw the "Poisoning with Responder" section

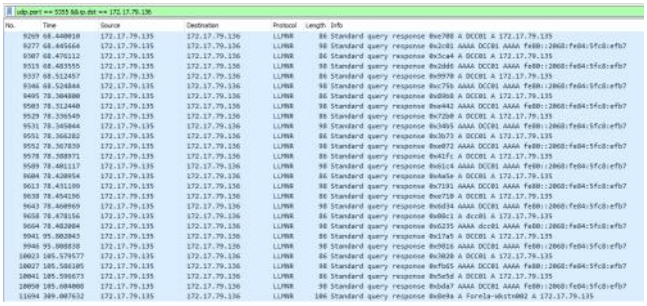
Poisoning with Responder

Responder is an open-source python-based LLMNR/NBT-NS/mDNS poisoner acting in two stages as described above:

1. First, it will listen to multicast NR queries (LLMNR – UDP/5355, NBT-NS – UDP/137) and, under the right conditions, spoof a response – directing the victim to the machine on which it is running.
2. Once a victim will try and connect to our machine, Responder will exploit the connection to steal credentials and other data.

In this demonstration we will use Responder to access credentials through SMB and WPAD authentication. We used a Kali Linux machine, which has this tool pre-installed and can be accessed under */usr/share/responder*.

The port should be 5355 in UDP so I filtered in Wireshark for udp.port == 5355 && ip.dst == 172.17.79.136

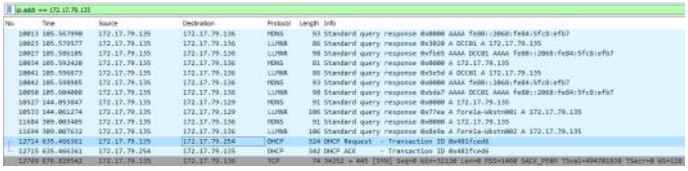


Then I found the only IP which was response is 172.17.79.135

Answer: 172.17.79.135

Task 2:
What is the hostname of the rogue machine?

I filtered for ip.addr == 172.17.79.135 and found a DHCP packet and reviewed the logs to find an hostname




```
    Seconds elapsed: 1
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 172.17.79.135
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: VMware_36:18:82 (00:0c:29:36:18:82)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Request)
  > Option: (61) Client identifier
  > Option: (55) Parameter Request List
  > Option: (57) Maximum DHCP Message Size
  v Option: (12) Host Name
      Length: 4
      Host Name: kali
  > Option: (255) End
```

Answer: kali

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?

I filtered for ip.src == 172.17.79.135 && ip.dst == 172.17.79.136 and then Followed the TCP Stream

Wireshark · Follow TCP Stream (tcp.stream eq 340) · capture.pcap

```
...1,.....Cookie: mstshash=john.deacon
.....L|R|...u.....T...t.#Y....C. ..j.
...9.8.....3.2....E.D.....Q.....P.=...<...5.../...A.............
```

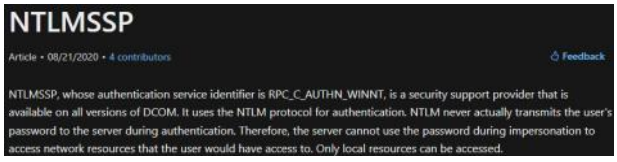
Answer: john.deacon

Task 4:
In NTLM traffic we can see that the victim credentials were relayed multiple times to the attacker's machine. When were the hashes captured the First time?

I tried to filter for only NTLM but Wireshark has shown other option for "ntlmssp"

No.

I checked on Google what is ntlmssp



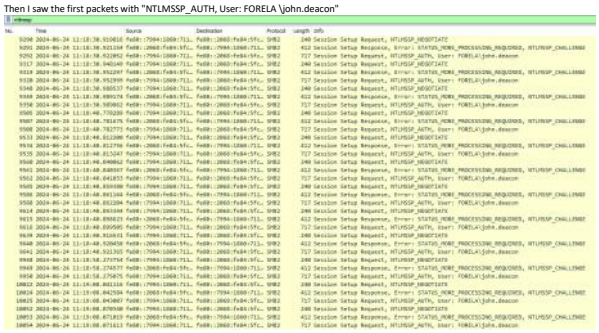
NTLMSSP

Article • 08/21/2020 • 4 contributors

Feedback

NTLMSSP, whose authentication service identifier is RPC_C_AUTHN_WINNT, is a security support provider that is available on all versions of DCOM. It uses the NTLM protocol for authentication. NTLM never actually transmits the user's password to the server during authentication. Therefore, the server cannot use the password during impersonation to access network resources that the user would have access to. Only local resources can be accessed.

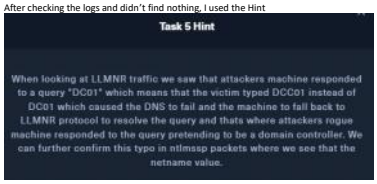
Then I saw the first packets with "NTLMSSP_AUTH, User: FORELA \john.deacon"



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?

After checking the logs and didn't find nothing, I used the Hint



Task 5 Hint

When looking at LLMNR traffic we saw that attackers machine responded to a query "DC01" which means that the victim typed DCC01 instead of DC01 which caused the DNS to fail and the machine to fall back to LLMNR protocol to resolve the query and thats where attackers rogue machine responded to the query pretending to be a domain controller. We can further confirm this typo in ntlmssp packets where we see that the netname value.

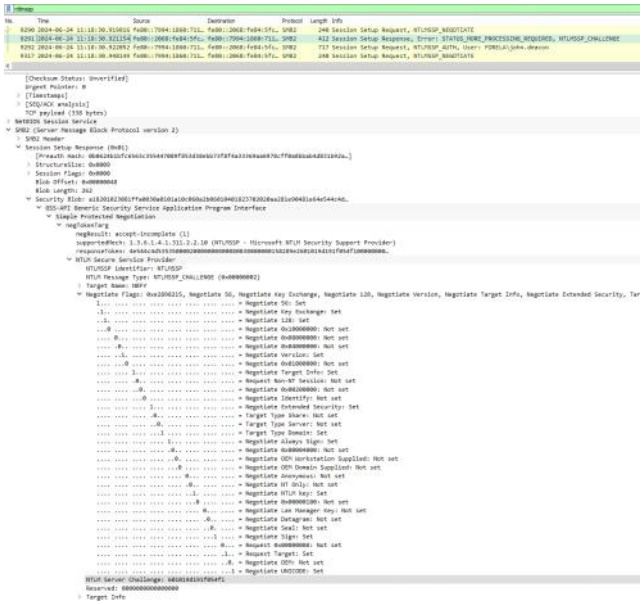
I already saw this queries with the typo of "DCC 01" when I looked for the LLMNR traffic.

```
9267 2024-06-24 11:18:30.899576 172.17.79.135  172.17.79.136  MDNS   93 Standard query response 0x0000 AAAA fe80::2068:fe84:5fc8:efb7
9269 2024-06-24 11:18:30.902155 172.17.79.135  172.17.79.136  LLMNR  86 Standard query response 0xe708 A DCC01 A 172.17.79.135
9277 2024-06-24 11:18:30.907809 172.17.79.135  172.17.79.136  LLMNR  98 Standard query response 0x2c01 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
9300 2024-06-24 11:18:30.931598 172.17.79.135  172.17.79.136  MDNS   81 Standard query response 0x0000 A 172.17.79.135
9307 2024-06-24 11:18:30.938257 172.17.79.135  172.17.79.136  LLMNR  86 Standard query response 0x3ca4 A DCC01 A 172.17.79.135
9308 2024-06-24 11:18:30.939183 172.17.79.135  172.17.79.136  MDNS   93 Standard query response 0x0000 AAAA fe80::2068:fe84:5fc8:efb7
9315 2024-06-24 11:18:30.945708 172.17.79.135  172.17.79.136  LLMNR  98 Standard query response 0x2dd6 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
9330 2024-06-24 11:18:30.970939 172.17.79.135  172.17.79.136  MDNS   81 Standard query response 0x0000 A 172.17.79.135
9337 2024-06-24 11:18:30.974602 172.17.79.135  172.17.79.136  LLMNR  86 Standard query response 0x9970 A DCC01 A 172.17.79.135
9338 2024-06-24 11:18:30.976630 172.17.79.135  172.17.79.136  MDNS   93 Standard query response 0x0000 AAAA fe80::2068:fe84:5fc8:efb7
9346 2024-06-24 11:18:30.986989 172.17.79.135  172.17.79.136  LLMNR  98 Standard query response 0xc75b AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7
```

Answer: DCC01

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?

I filtered again for ntlmssp and examined the first packets when the timestamp is 2024-06-24 11:18:30 from task 4.
After expanding all the logs I found the "NTLM Server Challenge"



Answer: 601019d191f054f1

Task 7:
Now doing something similar find the NTProofStr value.

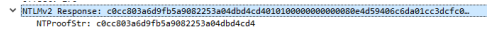
From same filter like task 6, this time I used the string search for "NTProofStr" and change to "Packet details"

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.

I used the hint for this question

Just like the hint says, I found the NTLMv 2 Response in the same place like task 7



Then I gave ChatGPT all the details to combine it together

"john.deacon::FORELA:601019d191f054f1:c0cc803a6d9fb5a9082253a04dbd4cd4:01010000000000
0080e4d59406c6da01cc3dcfc0de9b5f260000000002000800 4e00420046005900010 01e0057004900
4e002d0036003600410053003500 4c0031004700520057005400400340057004900 4e002d003600
360041005300350 04c0031004700520057005400400340057004900 4e002d003600360041005300
35004c0031004700520057005400 2e004e00420046005900 2e004c004f00430041004c0003001400
4e00420046005900 2e004c004f00430041004c0005001400 4e00420046005900 2e004c004f00430041004
c0007000800 0e4d59406c6da01060004000200000008003000300000000000000000000000000
0000000000000200000eb2ecbc5200a40b89ad5831abf821f4f20a2c7f352283a35600377e1f294f1c90a
0010000000000000000000000000000000000090014006300690066007300 2f00440043004300300
0310000000000000000"

Then I used Hashcat with the command in the hint

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?

I filtered for SMB and looked for file share path

10189	2024-06-24 11:19:17.927328	172.17.79.136	172.17.79.4	SMB2	152	Tree Connect Request Tree: \\DC01\IPC$
10190	2024-06-24 11:19:17.927437	172.17.79.4	172.17.79.136	SMB2	138	Tree Connect Response
10191	2024-06-24 11:19:17.927686	172.17.79.136	172.17.79.4	SMB2	178	Ioctl Request FSCTL_QUERY_NETWORK_INTERFACE_INFO
10192	2024-06-24 11:19:17.927904	172.17.79.136	172.17.79.4	SMB2	190	Create Request File: srvsvc
10194	2024-06-24 11:19:17.928146	172.17.79.4	172.17.79.136	SMB2	474	Ioctl Response FSCTL_QUERY_NETWORK_INTERFACE_INFO
10195	2024-06-24 11:19:17.928272	172.17.79.4	172.17.79.136	SMB2	210	Create Response File: srvsvc
10197	2024-06-24 11:19:17.928392	172.17.79.136	172.17.79.4	SMB2	162	GetInfo Request FILE_INFO/SMB2_FILE_STANDARD_INFO File: srvsvc
10198	2024-06-24 11:19:17.928527	172.17.79.4	172.17.79.136	SMB2	154	GetInfo Response
10199	2024-06-24 11:19:17.928828	172.17.79.136	172.17.79.4	DCERPC	330	Bind: call_id: 2, Fragment: Single, 3 context items: SRVSVC V3.0 (32bit NDR), SRVSVC V3.0 (64bit NDR), SRVSVC V3.0 (6cb71c2c-9812-4540-0300-000000000000)
10200	2024-06-24 11:19:17.928962	172.17.79.4	172.17.79.136	SMB2	138	Write Response
10201	2024-06-24 11:19:17.929351	172.17.79.136	172.17.79.4	SMB2	171	Read Request Len:1024 Off:0 File: srvsvc
10202	2024-06-24 11:19:17.929458	172.17.79.4	172.17.79.136	DCERPC	254	Bind_ack: call_id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiate ACK
10203	2024-06-24 11:19:17.929668	172.17.79.136	172.17.79.4	SRVSVC	298	NetShareEnumAll request[Long frame (4 bytes)]
10204	2024-06-24 11:19:17.929772	172.17.79.4	172.17.79.136	SMB2	138	Write Response
10205	2024-06-24 11:19:17.930131	172.17.79.136	172.17.79.4	SMB2	171	Read Request Len:1024 Off:0 File: srvsvc
10206	2024-06-24 11:19:17.930204	172.17.79.4	172.17.79.136	SRVSVC	950	NetShareEnumAll response[Malformed Packet]
10207	2024-06-24 11:19:17.930548	172.17.79.136	172.17.79.4	SMB2	146	Close Request File: srvsvc
10208	2024-06-24 11:19:17.930630	172.17.79.4	172.17.79.136	SMB2	182	Close Response
10214	2024-06-24 11:19:18.419272	172.17.79.136	172.17.79.4	SMB2	174	Tree Connect Request Tree: \\DC01\DC-Confidential

Answer: \\DC01\DC-Confidential