

hacktheblue,pcap(wireshark)

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.

* * *

About Noxious

In this sherlock, players will go through network traffic and uncover credential-stealing technique by abusing the LLMNR protocol feature in Windows. Players will learn how a victim made a typo navigating to a network share and how the attacker was using the Responder tool to steal hashes and pose as a legitimate device in the internal network. Players will also learn to crack NTLMV2 hashes by gathering information from SMB traffic.

文件：capture.pcap

使用工具：wireshark

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.

filter : llmnr and ip.dst_host==172.17.79.136

No.	Time	Source	Destination	Protocol	Length	Info
11694	309.007632	172.17.79.135	172.17.79.136	LLMNR	106	Standard query response 0x8e9a A Forela-Wkstn002 A 172.17.79.136
10050	105.604008	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0xbda7 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
10041	105.596673	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x5e5d A DCC01 A 172.17.79.135
10027	105.586105	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0xfb65 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
10023	105.579577	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x3020 A DCC01 A 172.17.79.135
9946	95.808838	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x9816 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9941	95.802043	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x17a5 A DCC01 A 172.17.79.135
9664	78.482084	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x6235 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9658	78.478156	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x08c1 A DCC01 A 172.17.79.135
9643	78.460969	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0xd6d3 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9638	78.454196	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0xe710 A DCC01 A 172.17.79.135
9613	78.431199	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x7191 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9604	78.420954	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x4a5e A DCC01 A 172.17.79.135
9589	78.401117	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x61c4 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9578	78.388971	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x41fc A DCC01 A 172.17.79.135
9552	78.367839	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0xe072 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9551	78.366282	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x3b73 A DCC01 A 172.17.79.135
9531	78.345044	172.17.79.135	172.17.79.136	LLMNR	98	Standard query response 0x34b5 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135
9529	78.336549	172.17.79.135	172.17.79.136	LLMNR	86	Standard query response 0x72b0 A DCC01 A 172.17.79.135
0502	78.312449	172.17.79.135	172.17.79.126	LLMNR	98	Standard query response 0xc442 AAAA DCC01 AAAA fe80::2068:1ff:fe00:135

172.17.79.135

Task 2

What is the hostname of the rogue machine?

filter : ip.src_host==172.17.79.135 and dhcp

No.	Time	Source	Destination	Protocol	Info
12714	635.466361	172.17.79.135	172.17.79.254	DHCP	DHCP Request - Transaction ID 0x481fced6
1666	11.510185	172.17.79.135	255.255.255.255	DHCP	DHCP Discover - Transaction ID 0xa7ea9ba0

Option: (55) Parameter Request List
Length: 17
Parameter Request List Item: (1) Subnet Mask
Parameter Request List Item: (2) Time Offset
Parameter Request List Item: (6) Domain Name Server
Parameter Request List Item: (12) Host Name
Parameter Request List Item: (15) Domain Name
Parameter Request List Item: (26) Interface MTU
Parameter Request List Item: (28) Broadcast Address
Parameter Request List Item: (121) Classless Static Route
Parameter Request List Item: (3) Router
Parameter Request List Item: (33) Static Route
Parameter Request List Item: (40) Network Information Service Domain
Parameter Request List Item: (41) Network Information Service Servers
Parameter Request List Item: (42) Network Time Protocol Servers
Parameter Request List Item: (119) Domain Search
Parameter Request List Item: (249) Private/Classless Static Route (Microsoft)
Parameter Request List Item: (252) Private/Proxy autodiscovery
Parameter Request List Item: (17) Root Path

Option: (57) Maximum DHCP Message Size
Length: 2
Maximum DHCP Message Size: 65535

Option: (12) Host Name
Length: 4
Host Name: kali

Option: (255) End
Option End: 255

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?

filter : smb2

Time	Source	Destination	Protocol	Info	Length
190 115.465292	172.17.79.4	172.17.79.136	SMB2	Tree Connect Response	138
189 115.465183	172.17.79.136	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01\IPC\$	152
188 115.464711	172.17.79.4	172.17.79.136	SMB2	Session Setup Response	314
186 115.464025	172.17.79.136	172.17.79.4	SMB2	Session Setup Request	3452
185 115.462684	172.17.79.4	172.17.79.136	SMB2	Negotiate Protocol Response	390
184 115.462466	172.17.79.136	172.17.79.4	SMB2	Negotiate Protocol Request	274
183 115.462137	172.17.79.4	172.17.79.136	SMB2	Negotiate Protocol Response	306
185 115.462137	172.17.79.4	172.17.79.136	SMB2	Session Setup Response, Error: STATUS_ACCESS_DENIED	150
154 105.609468	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Request, NTLMSSP_AUTH, User: FORELA\john.deacon	717
153 105.608874	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED	412
152 105.608195	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE	240
151 105.606947	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Negotiate Protocol Response	314
148 105.603448	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Negotiate Protocol Request	314
128 105.589286	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_ACCESS_DENIED	150

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?

同上，只是選最早時間

Time	Source	Destination	Protocol	Info
3 2024-06-24 11:18:30.910756	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Negotiate Protocol Response
9 2024-06-24 11:18:30.911316	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Negotiate Protocol Request
9 2024-06-24 11:18:30.912373	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Negotiate Protocol Response
9 2024-06-24 11:18:30.919816	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE
L 2024-06-24 11:18:30.921154	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED
2 2024-06-24 11:18:30.922052	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_AUTH, User: FORELA\john.
3 2024-06-24 11:18:30.925867	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_ACCESS_DENIED

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?

filter : llmnr and ip.addr==172.17.79.135

llmnr and ip.addr==172.17.79.135					
Packet list		Narrow & Wide	Case sensitive	Display filter	Enter a display filter ...
1.902155	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xe708 A DCC01 A 172.17.79.135	
1.907809	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x2c01 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.938257	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x3ca4 A DCC01 A 172.17.79.135	
1.945700	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x2dd6 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.974602	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x9970 A DCC01 A 172.17.79.135	
1.986989	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xc75b AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.766945	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x89b8 A DCC01 A 172.17.79.135	
1.774585	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xe442 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.798694	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x72b0 A DCC01 A 172.17.79.135	
1.807189	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x34b5 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.828427	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x3b73 A DCC01 A 172.17.79.135	
1.829984	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xe072 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.851116	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x41fc A DCC01 A 172.17.79.135	
1.863262	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x61c4 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.883099	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x4a5e A DCC01 A 172.17.79.135	
1.893344	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x7191 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.916341	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xe710 A DCC01 A 172.17.79.135	
1.923114	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xd34 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.940301	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x08c1 A dcc01 A 172.17.79.135	
1.944229	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x6235 AAAA dcc01 AAAA fe80::2068:fe84:5fc8:efb7	
1.264188	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x17a5 A DCC01 A 172.17.79.135	
1.270983	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x9816 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.041722	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x3020 A DCC01 A 172.17.79.135	
1.048250	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xfb65 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	
1.058818	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0x5e5d A DCC01 A 172.17.79.135	
1.66152	172.17.79.135	172.17.79.136	LLMNR	Standard query response 0xbfd7 AAAA DCC01 AAAA fe80::2068:fe84:5fc8:efb7	

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?

filter : ntlmssp

ntlmssp					
Packet list		Narrow & Wide	Case sensitive	Display filter	Enter a display filter ...
.9816	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE	240
1154	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412
12052	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_AUTH, User: FORELA\john.deacon	717
18149	fe80::7994:1860:711...	fe80::2068:fe84:5fc...	SMB2	Session Setup Request, NTLMSSP_NEGOTIATE	240
12297	fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412
Signature: 00000000000000000000000000000000 [Response to: 9290] [Time from request: 0.001338000 seconds]					
▾ Session Setup Response (0x01) [Preattent Hash: 0b0624b1bf6c563c355447089f853d38ebb73f8f4a33369aa6978cff0a8bbab4c] ▾ StructureSize: 0x0009 0000 0000 0000 100. = Fixed Part Length: 4 1 = Dynamic Part: True					
▾ Session Flags: 0x0000 Blob Offset: 0x00000048 Blob Length: 262					
▾ Security Blob [truncated]: a18201023081fffa0030a0101a10c060a2b06010401823702020a ▾ GSS-API Generic Security Service Application Program Interface ▾ Simple Protected Negotiation ▾ negTokenTarg negResult: accept-incomplete (1) supportedMech: 1.3.6.1.4.1.311.2.2.10 (NTLMSSP - Microsoft NTLM Security Service) responseToken [truncated]: 4e544c4d5353500002000000080008003800000158: ▾ NTLM Secure Service Provider NTLMSSP identifier: NTLMSSP NTLM Message Type: NTLMSSP_CHALLENGE (0x00000002)					
▾ Target Name: NBFY ▾ Negotiate Flags: 0xe2898215, Negotiate 56, Negotiate Key Exchange, Negotiate 50 NTLM Server Challenge: 601019d191f054f1 Reserved: 0000000000000000 ▾ Target Info Version: 6.2 (Build 9600) - NTLM Current Revision: 15					
0000 00 0c 29 85 78 cb 00 0c 29 36 18 82 86 dd 0010 c6 23 01 66 06 40 fe 80 00 00 00 00 00 00 0020 fe 84 5f c8 ef b7 fe 80 00 00 00 00 00 00 0030 18 60 07 11 c2 43 01 bd ca d4 2b de 33 4c 0040 d3 8a 50 18 01 01 07 03 00 00 00 00 01 4e 0050 4d 42 40 00 01 00 16 00 00 c0 01 00 21 00 0060 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 0070 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0080 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0090 00 00 48 00 06 01 a1 82 01 02 30 81 ff a0 00a0 01 01 a1 0c 06 0a 2b 06 01 04 01 82 37 02 00b0 a2 81 e9 04 81 e6 4e 54 4c 4d 53 53 50 00 00c0 00 00 08 00 08 00 38 00 00 00 15 82 89 e2 00d0 19 d1 91 f0 54 f1 00 00 00 00 00 00 00 00 00 00e0 a6 00 40 00 00 00 06 03 80 25 00 00 00 0f 00f0 42 00 46 00 59 00 02 00 08 00 4e 00 42 00 0100 59 00 01 00 1e 00 57 00 49 00 4e 00 2d 00 0110 36 00 41 00 53 00 35 00 4c 00 31 00 47 00 0120 57 00 54 00 04 00 34 00 57 00 49 00 4e 00 0130 36 00 41 00 53 00 35 00 4c 00 31 00 47 00 0140 52 00 57 00 54 00 2e 00 4e 00 42 00 46 00 0150 2e 00 4c 00 4f 00 43 00 41 00 4c 00 03 00 0160 4e 00 42 00 46 00 59 00 2e 00 4c 00 4f 00 0170 41 00 4c 00 05 00 14 00 4e 00 42 00 46 00 0180 2e 00 4c 00 4f 00 43 00 41 00 4c 00 07 00 0190 80 e4 d5 94 06 c6 da 01 00 00 00 00					

601019d191f054f1

Task 7

Now doing something similar find the NTProofStr value.

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.

重點條件：User::Domain:ServerChallenge:NTProofStr:NTLMv2Response

NTLMv2Response => 從值中刪除前32 個字元

john.deacon::FORELA:601019d191f054f1:c0cc803a6d9fb5a9082253a04dbd4cd4:010100
00000000080e4d59406c6da01cc3dcfc0de9b5f2600000000020008004e0042004600590001
001e00570049004e002d00360036004100530035004c00310047005200570054000400340057

* * *

```
解碼：hashcat -a 0 -m 5600 hash.txt /usr/share/wordlists/rockyou.txt --potfile-disable --force
```

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?

filter : SMB2

Packet list				Narrow & Wide	Case sensitive	Display filter	Enter a display filter ...	Find	Cancel
Source	Destination	Protocol	Info	Length					
0367 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
1164 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
8623 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
0458 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
4577 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
2584 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
1019 fe80::2068:fe84:5fc...	fe80::7994:1860:711...	SMB2	Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSS...	412					
1706 172.17.79.129	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01.forela.local\IPC\$	178					
7321 172.17.79.136	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01.forela.local\IPC\$	178					
7246 172.17.79.129	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01.forela.local\IPC\$	178					
7926 172.17.79.136	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01.forela.local\IPC\$	178					
9272 172.17.79.136	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01\DC-Confidential	174					
7328 172.17.79.136	172.17.79.4	SMB2	Tree Connect Request Tree: \\DC01\IPC\$	152					
7437 172.17.79.4	172.17.79.136	SMB2	Tree Connect Response	138					
9655 172.17.79.4	172.17.79.136	SMB2	Tree Connect Response	138					
Channel Sequence: 0			
Reserved: 0000				0000	00 0c 29 56 44 f9 00 0c 29 85 78 cb 08 00 45				
Command: Tree Connect (3)				0010	00 a0 7f c5 40 00 80 06 83 e3 ac 11 4f 88				
Credits requested: 1				0020	4f 04 ca e9 01 bd c7 d7 71 2b 3f 59 f5 db 50				
Flags: 0x00000018, Signing, Priority				0030	20 14 c0 4c 00 00 00 00 00 74 fe 53 4d 42 40				
Chain Offset: 0x00000000				0040	01 00 00 00 00 00 03 00 01 00 18 00 00 00 00				
Message Id: 12				0050	00 00 0c 00 00 00 00 00 00 00 ff fe 00 00 00				
Process Id: 0x0000feff				0060	00 00 25 00 00 04 00 44 00 00 c0 e2 3c fe 30				
Tree Id: 0x00000000				0070	ee 5c 3e 10 3a 3d dd a6 53 8c 09 00 00 00 48				
Session Id: 0x0000440004000025				0080	2c 00 5c 00 5c 00 44 00 43 00 30 00 31 00 5c				
[Authenticated in Frame: 10188]				0090	44 00 43 00 2d 00 43 00 6f 00 6e 00 66 00 65				
Signature: c0e23cf304dee5c3e103a3ddda6538c				00a0	64 00 65 00 6e 00 74 00 69 00 61 00 6c 00				
[Response in: 10216]									
Tree Connect Request (0x03)									
StructureSize: 0x0009									
Flags: 0x0000									
Tree: \\DC01\DC-Confidential									

\DC01\DC-Confidential