Category : Network Forensics

LEVEL : EASY

Scenario:

Your organization’s security team has detected a surge in suspicious network activity. There are concerns that LLMNR (Link-Local Multicast Name Resolution) and NBT-NS (NetBIOS Name Service) poisoning attacks may be occurring within your network. These attacks are known for exploiting these protocols to intercept network traffic and potentially compromise user credentials. Your task is to investigate the network logs and examine captured network traffic.

Tools:

- Wireshark

Challenge download link : https://cyberdefenders.org/blueteam-ctf-challenges/enroll/146

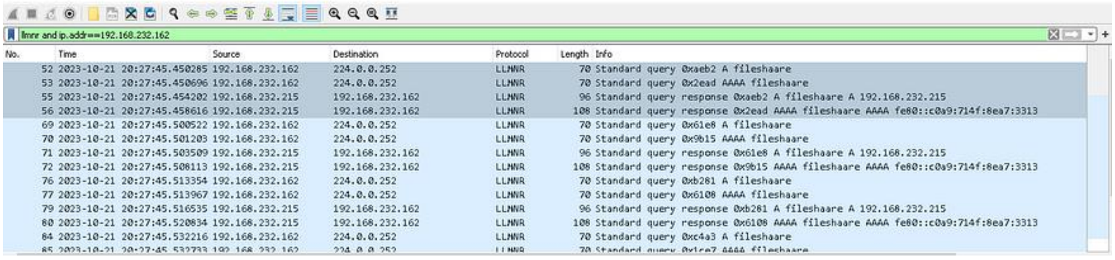
Q1-
In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistyped query made by the machine with the IP address 192.168.232.162?

- Frist of all I filtered LLMNR Protocol (Link-local Multicast Name Resolution) and the IP-add 192.168.232.162

Using This Filter :

llmnr and ip.addr==192.168.232.162

Press enter or click to view image in full size



```
llmnr and ip.addr==192.168.232.162
No.   Time                          Source            Destination       Protocol  Length Info
   52 2023-10-21 20:27:45.450285 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0xaeb2 A fileshaare
   53 2023-10-21 20:27:45.450696 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0x2ead AAAA fileshaare
   55 2023-10-21 20:27:45.454202 192.168.232.215   192.168.232.162   LLMNR       96 Standard query response 0xaeb2 A fileshaare A 192.168.232.215
   56 2023-10-21 20:27:45.458616 192.168.232.215   192.168.232.162   LLMNR      108 Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
   69 2023-10-21 20:27:45.500522 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0x61e8 A fileshaare
   70 2023-10-21 20:27:45.501203 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0x9b15 AAAA fileshaare
   71 2023-10-21 20:27:45.503509 192.168.232.215   192.168.232.162   LLMNR       96 Standard query response 0x61e8 A fileshaare A 192.168.232.215
   72 2023-10-21 20:27:45.508113 192.168.232.215   192.168.232.162   LLMNR      108 Standard query response 0x9b15 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
   76 2023-10-21 20:27:45.513354 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0xb281 A fileshaare
   77 2023-10-21 20:27:45.513967 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0x6108 AAAA fileshaare
   79 2023-10-21 20:27:45.516535 192.168.232.215   192.168.232.162   LLMNR       96 Standard query response 0xb281 A fileshaare A 192.168.232.215
   80 2023-10-21 20:27:45.520834 192.168.232.215   192.168.232.162   LLMNR      108 Standard query response 0x6108 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
   84 2023-10-21 20:27:45.532216 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0xc4a3 A fileshaare
   85 2023-10-21 20:27:45.532733 192.168.232.162   224.0.0.252       LLMNR       70 Standard query 0x1ce7 AAAA fileshaare
```

From packet 52 I Saw a LLMNR Query with name (fileshaare)

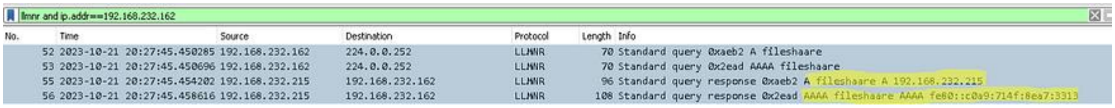
which is mistyped query (the correct query is fileshare)

- THE ANSWER : fileshaare

Q2-We are investigating a network security incident. For a thorough investigation, we need to determine the IP address of the rogue machine. What is the IP address of the machine acting as the rogue entity?

Since we know it was a poisoning attack , if we go to packet 55 or 56

Press enter or click to view image in full size



```
llmnr and ip.addr==192.168.232.162
No.   Time                        Source           Destination      Protocol  Length Info
   52 2023-10-21 20:27:45.450285 192.168.232.162  224.0.0.252      LLMNR         70 Standard query 0xaeb2 A fileshaare
   53 2023-10-21 20:27:45.450696 192.168.232.162  224.0.0.252      LLMNR         70 Standard query 0x2ead AAAA fileshaare
   55 2023-10-21 20:27:45.454202 192.168.232.215  192.168.232.162  LLMNR         96 Standard query response 0xaeb2 A fileshaare A 192.168.232.215
   56 2023-10-21 20:27:45.458616 192.168.232.215  192.168.232.162  LLMNR        108 Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
```

we will see the IP-add 192.168.232.215 reply to the mistyped query from the

first question !!!! , so I was sure the attacker IP is 192.168.232.215

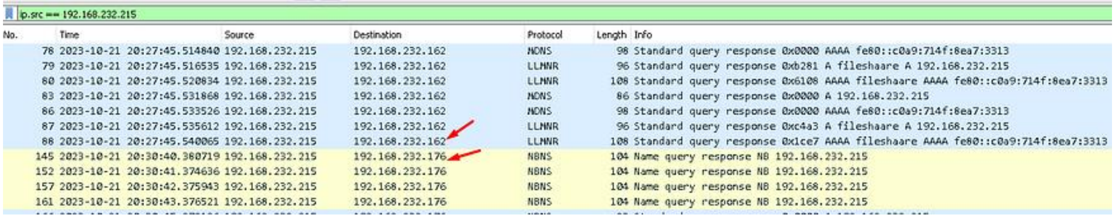
- THE ANSWER : 192.168.232.215

Q3-During our investigation, it's crucial to identify all affected machines. What is the IP address of the second machine that received poisoned responses from the rogue machine?

He is asking about victim IP-add so I Filtered The PCAP With the

Attacker IP- add :

Press enter or click to view image in full size



```
ip.src == 192.168.232.215
No.   Time                        Source           Destination      Protocol  Length Info
   78 2023-10-21 20:27:45.514840 192.168.232.215  192.168.232.162  MDNS          98 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
   79 2023-10-21 20:27:45.516535 192.168.232.215  192.168.232.162  LLMNR         96 Standard query response 0xb281 A fileshaare A 192.168.232.215
   80 2023-10-21 20:27:45.520834 192.168.232.215  192.168.232.162  LLMNR        108 Standard query response 0x6108 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
   83 2023-10-21 20:27:45.531868 192.168.232.215  192.168.232.162  MDNS          86 Standard query response 0x0000 A 192.168.232.215
   86 2023-10-21 20:27:45.533526 192.168.232.215  192.168.232.162  MDNS          98 Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
   87 2023-10-21 20:27:45.535612 192.168.232.215  192.168.232.162  LLMNR         96 Standard query response 0xc4a3 A fileshaare A 192.168.232.215
   88 2023-10-21 20:27:45.540065 192.168.232.215  192.168.232.162  LLMNR        108 Standard query response 0x1ce7 AAAA fileshaare AAAA fe80::c0a9:714f:8ea7:3313
  145 2023-10-21 20:30:40.360719 192.168.232.215  192.168.232.176  NBNS         104 Name query response NB 192.168.232.215
  152 2023-10-21 20:30:41.374636 192.168.232.215  192.168.232.176  NBNS         104 Name query response NB 192.168.232.215
  157 2023-10-21 20:30:42.375943 192.168.232.215  192.168.232.176  NBNS         104 Name query response NB 192.168.232.215
  161 2023-10-21 20:30:43.376521 192.168.232.215  192.168.232.176  NBNS         104 Name query response NB 192.168.232.215
```

The Attacker is communicating with 2 IP-adds :

1– 192.168.232.162

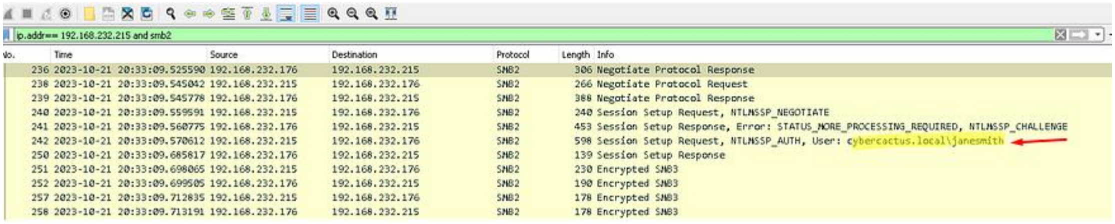
2- 192.168.232.176

- THE ANSWER : 192.168.232.176

Q4-We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?

To solve this question I filtered the PCAP with attacker IP and SMP2 Protocol , Using this filter :

Press enter or click to view image in full size



```
ip.addr== 192.168.232.215 and smb2
```

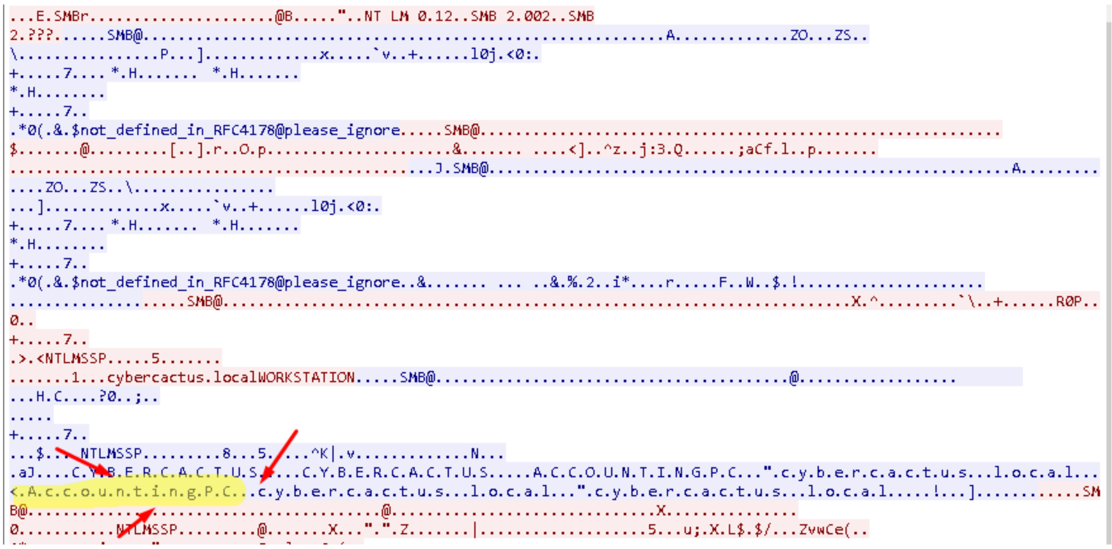
```
No.  Time                          Source           Destination      Protocol  Length Info
 236 2023-10-21 20:33:09.525590 192.168.232.176 192.168.232.215 SMB2      306 Negotiate Protocol Response
 238 2023-10-21 20:33:09.545042 192.168.232.215 192.168.232.176 SMB2      266 Negotiate Protocol Request
 239 2023-10-21 20:33:09.545778 192.168.232.176 192.168.232.215 SMB2      388 Negotiate Protocol Response
 240 2023-10-21 20:33:09.559591 192.168.232.215 192.168.232.176 SMB2      240 Session Setup Request, NTLMSSP_NEGOTIATE
 241 2023-10-21 20:33:09.560775 192.168.232.176 192.168.232.215 SMB2      453 Session Setup Response, Error: STATUS_MORE_PROCESSING_REQUIRED, NTLMSSP_CHALLENGE
 242 2023-10-21 20:33:09.570612 192.168.232.215 192.168.232.176 SMB2      598 Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith
 250 2023-10-21 20:33:09.685817 192.168.232.176 192.168.232.215 SMB2      139 Session Setup Response
 251 2023-10-21 20:33:09.698065 192.168.232.215 192.168.232.176 SMB2      230 Encrypted SMB3
 252 2023-10-21 20:33:09.699505 192.168.232.176 192.168.232.215 SMB2      190 Encrypted SMB3
 257 2023-10-21 20:33:09.712835 192.168.232.215 192.168.232.176 SMB2      178 Encrypted SMB3
 258 2023-10-21 20:33:09.713191 192.168.232.176 192.168.232.215 SMB2      178 Encrypted SMB3
```

- THE ANSWER : janesmith

Q5-As part of our investigation, we aim to understand the extent of the attacker’s activities. What is the hostname of the machine that the attacker accessed via SMB?

Going to packet 242 and follow TCP stream :

Press enter or click to view image in full size



```
...E.SMBr.....................@B....."..NT LM 0.12..SMB 2.002..SMB
2.???......SMB@..........................................................A.............ZO...ZS..
\................P...]............x.....`v..+......l0j.<0:.
+.....7.... *.H....... *.H.......
*.H........
+.....7..
.*0(.&.$not_defined_in_RFC4178@please_ignore.....SMB@.........................................................
$.......@.........[..].r..O.p.....................&....... ....<]..^z..j:3.Q......;aCf.l..p.......
.............................................J.SMB@.........................................................A.........
....ZO...ZS..\................
...]............x.....`v..+......l0j.<0:.
+.....7.... *.H....... *.H.......
*.H........
+.....7..
.*0(.&.$not_defined_in_RFC4178@please_ignore..&....... ... ..&.%.2..i*....r.....F..W..$.!.....................
...............SMB@......................................................................X.^..........`\..+......R0P..
0..
+.....7..
.>.<NTLMSSP.....5.......
.......1...cybercactus.localWORKSTATION.....SMB@.......................................@.................
...H.C....?0..;..
.....
+.....7..
...$....NTLMSSP.........8...5.......^K|.v.............N...
.aJ....C.Y.B.E.R.C.A.C.T.U.S....C.Y.B.E.R.C.A.C.T.U.S.....A.C.C.O.U.N.T.I.N.G.P.C...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...
<.A.c.c.o.u.n.t.i.n.g.P.C...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.....!...]............SM
B@.......................................@.............................X...............
0..........NTLMSSP.........@.......X...".".Z.......|...................5...u;.X.L$.$/...ZvwCe(..
```

tcp. stream eq 11

From the screenshot above the hostname of the victim machine is

AccountingPC.

- THE ANSWER : AccountingPC.

BY : Asad Dafalla