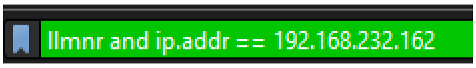
**CyberDefenders: PoisonedCredentials Lab**

The following writeup is for PoisonedCredentials Lab on CyberDefenders, it involves investigating a pcap using Wireshark.

**Scenario:** Your organisation'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.

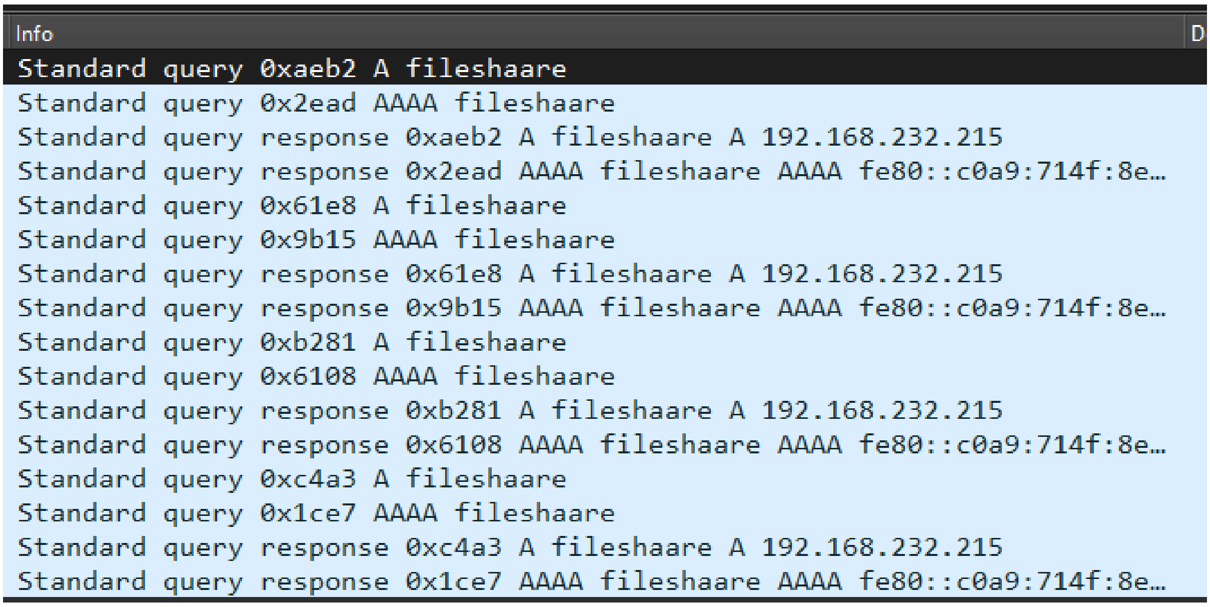
**In the context of the incident described in the scenario, the attacker initiated their actions by taking advantage of benign network traffic from legitimate machines. Can you identify the specific mistypes query made by the machine with the IP address 192.168.232.162?**

To cut down the traffic, we can search for LLMNR and the specified IP address like as follows:



```
llmnr and ip.addr == 192.168.232.162
```

If you look through the queries made, we can determine that "fileshaare" was mistyped:



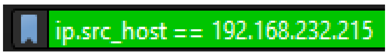
```
Standard query 0xaeb2 A fileshaare
Standard query 0x2ead AAAA fileshaare
Standard query response 0xaeb2 A fileshaare A 192.168.232.215
Standard query response 0x2ead AAAA fileshaare AAAA fe80::c0a9:714f:8e…
Standard query 0x61e8 A fileshaare
Standard query 0x9b15 AAAA fileshaare
Standard query response 0x61e8 A fileshaare A 192.168.232.215
Standard query response 0x9b15 AAAA fileshaare AAAA fe80::c0a9:714f:8e…
Standard query 0xb281 A fileshaare
Standard query 0x6108 AAAA fileshaare
Standard query response 0xb281 A fileshaare A 192.168.232.215
Standard query response 0x6108 AAAA fileshaare AAAA fe80::c0a9:714f:8e…
Standard query 0xc4a3 A fileshaare
Standard query 0x1ce7 AAAA fileshaare
Standard query response 0xc4a3 A fileshaare A 192.168.232.215
Standard query response 0x1ce7 AAAA fileshaare AAAA fe80::c0a9:714f:8e…
```

**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?**

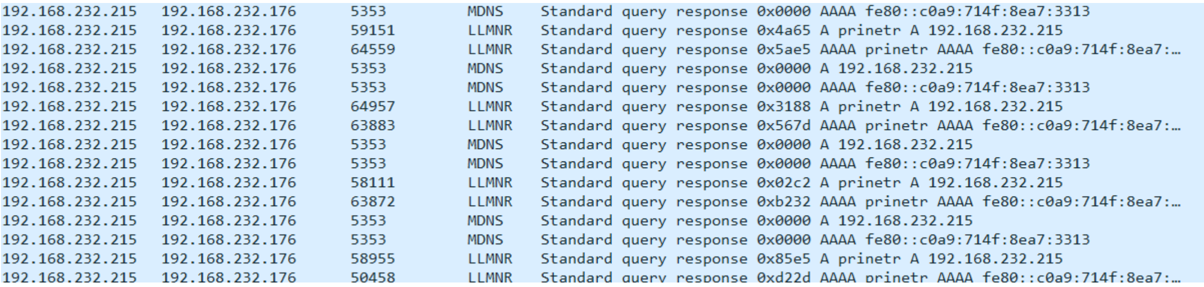
If we look at the packets after the fileshaare query, we can see that the response is from 192.168.232.215. This is the rogue machine that initiated the poisoning attack.

**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?**

If we filter for source traffic coming from 192.168.232.215 (the rogue machine) you can see another victim that received poisoned responses:



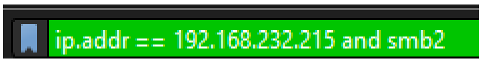
```
ip.src_host == 192.168.232.215
```



```
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
192.168.232.215   192.168.232.176      59151        LLMNR    Standard query response 0x4a65 A prinetr A 192.168.232.215
192.168.232.215   192.168.232.176      64559        LLMNR    Standard query response 0x5ae5 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:…
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 A 192.168.232.215
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
192.168.232.215   192.168.232.176      64957        LLMNR    Standard query response 0x3188 A prinetr A 192.168.232.215
192.168.232.215   192.168.232.176      63883        LLMNR    Standard query response 0x567d AAAA prinetr AAAA fe80::c0a9:714f:8ea7:…
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 A 192.168.232.215
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
192.168.232.215   192.168.232.176      58111        LLMNR    Standard query response 0x02c2 A prinetr A 192.168.232.215
192.168.232.215   192.168.232.176      63872        LLMNR    Standard query response 0xb232 AAAA prinetr AAAA fe80::c0a9:714f:8ea7:…
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 A 192.168.232.215
192.168.232.215   192.168.232.176      5353         MDNS     Standard query response 0x0000 AAAA fe80::c0a9:714f:8ea7:3313
192.168.232.215   192.168.232.176      58955        LLMNR    Standard query response 0x85e5 A prinetr A 192.168.232.215
192.168.232.215   192.168.232.176      50458        LLMNR    Standard query response 0xd22d AAAA prinetr AAAA fe80::c0a9:714f:8ea7:…
```

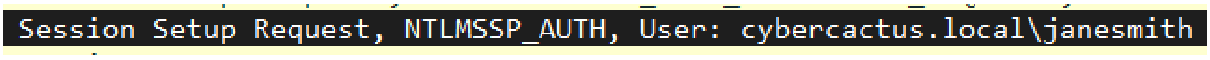
**We suspect that user accounts may have been compromised. To assess this, we must determine the username associated with the compromised account. What is the username of the account that the attacker compromised?**

We can start by filtering for the rogue machine and looking at SMB traffic:



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

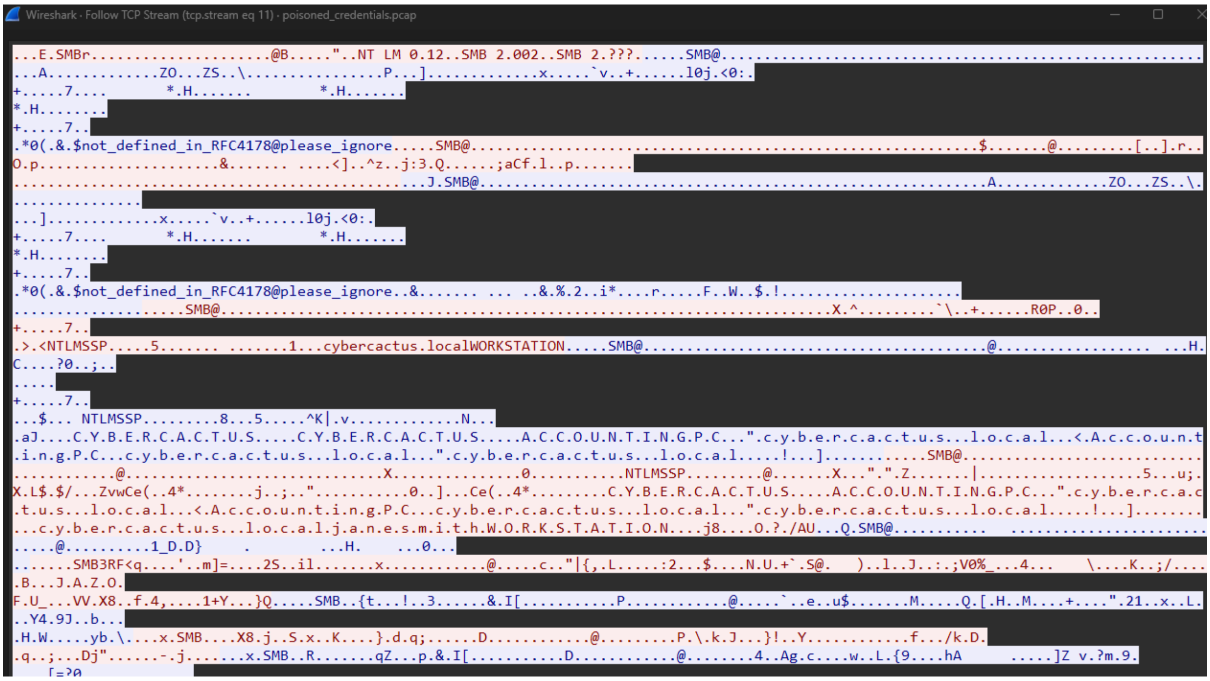
After looking through the results, we can see that the rogue machine is logging in as the user janesmith:



```
Session Setup Request, NTLMSSP_AUTH, User: cybercactus.local\janesmith
```

**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?**

If we follow the TCP stream of the session setup request we found previous (packet number 242, we can find the hostname of the machine that the attacker accessed via SMB:



Wireshark · Follow TCP Stream (tcp.stream eq 11) · poisoned_credentials.pcap

```
...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..
...$...  NTLMSSP.........8...5.....^K|.v.............N...
.aJ....C.Y.B.E.R.C.A.C.T.U.S.....C.Y.B.E.R.C.A.C.T.U.S.....A.C.C.O.U.N.T.I.N.G.P.C...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...<.A.c.c.o.u.n.t
.i.n.g.P.C...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.....!...]...........SMB@..........................
............@.............................X...............0...........NTLMSSP.........@.......X..."."..Z.......|...................5...u;.
X.L$.$/...ZvwCe(..4*........j..;.."...........0..]...Ce(..4*.........C.Y.B.E.R.C.A.C.T.U.S.....A.C.C.O.U.N.T.I.N.G.P.C...".c.y.b.e.r.c.a.c
.t.u.s...l.o.c.a.l...<.A.c.c.o.u.n.t.i.n.g.P.C...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l...".c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.....!...]........
...c.y.b.e.r.c.a.c.t.u.s...l.o.c.a.l.j.a.n.e.s.m.i.t.h.W.O.R.K.S.T.A.T.I.O.N....j8....O.?./AU...Q.SMB@...........    ......................
.....@..........1_D.D}      .          ...H.     ...0...
.......SMB3RF<q....'..m]=....2S..il.......x............@.....c.."|{,.L.....:2...$....N.U.+`.S@.    )..l..J..:.;V0%_...4...     \....K..;/....
.B...J.A.Z.O.
F.U_...VV.X8..f.4,....1+Y...}Q.....SMB..{t...!..3......&.I[...........P............@.....`..e..u$.......M.....Q.[.H..M....+....".21..x..L.
..Y4.9J..b...
.H.W.....yb.\....x.SMB....X8.j..S.x..K....}.d.q;......D............@.........P.\.k.J...}!..Y............f.../k.D.
.q..;...Dj"......-.j.......x.SMB..R.......qZ...p.&.I[...........D............@........4..Ag.c....w..L.{9....hA       .....]Z v.?m.9.
    [=?0
```

It is simply ACCOUNTINGPC.

This was a relatively challenging room for myself as it's the first time I have investigated network traffic related to LLMNR and NBT-NS poisoning. If you have any feedback or need help on any of these questions, I highly recommend using the hints and reading the featured writeups.