

Group:
Essential Group

Report Number:
Report No. 8

Report id
8-lec-13-Detection and analysis Using
IDS&IPS Suricata-6_ess

Detection and analysis PCAP File

Prepared By:

Kazim Ali Obad

Supervisor:

Anmar Mohammed

Date of Task Assignment :

2/7/2026

Due Date:

2/17/2026

Table of Contents

Scenario	2
Summary	3
What Happened:.....	3
Scope and Impact	3
2. Victim Details.....	4
3. Indicators of Compromise (IOCs).....	4
Critical Internal Indicators:.....	5
Conclusion:.....	8

Scenario

You are a junior security analyst working in a Security Operations Center (SOC). Your organization operates a local network (LAN) with the following details:

LAN Segment Range: 172.17.0.0/24

Domain: bepositive.com

Active Directory Domain Controller: IP Address: 172.17.0.17

Hostname: WIN-CTL9XBQ9Y19

AD Environment Name: BEPOSITIVE

Gateway: 172.17.0.1

Broadcast Address: 172.17.0.255

During routine monitoring, security alerts were triggered after suspicious activity was observed in a captured network traffic file (PCAP). These alerts indicate potential malicious behavior inside the LAN.

Task

Write an **incident report** based on:

The malicious network activity observed in the PCAP

The alerts generated by the detection system

The incident report must include **exactly three sections**:

Executive Summary Describe **what happened, when it happened, and who was affected**

Use clear, simple, non-technical language suitable for management

Victim Details Hostname

IP address

MAC address

Windows user account name

Indicators of Compromise (IOCs) Malicious IP addresses

Domains and URLs related to the activity

SHA256 hashes **only if malware binaries can be extracted from the PCAP**

Summary

Date of Incident: September 4, 2024

Time of Incident: 13:32:31 - 14:31:52

Report Date: [Current date]

What Happened:

On September 4, 2024, between 13:32 and 14:31, I detected a critical security breach involving the compromise of user credentials and Active Directory enumeration. The affected workstation, **DESKTOP-RNV09AT** (IP: 172.17.0.99), was found to have been infected with malware, establishing persistent communications with multiple external command-and-control (C2) servers.

During the investigation, it was identified that the attacker exploited stolen credentials from **user afletcher** to perform **DRSUAPI** calls to the Domain Controller (**WIN-CTL9XBQ9Y19**, IP: 172.17.0.17). This is a significant attack technique often associated with **DCSync attacks**, enabling attackers to request replication of sensitive Active Directory data, including password hashes and Kerberos credentials. These actions pose a severe risk to the integrity of our entire domain, as the attacker could potentially forge **Golden Tickets** and gain unauthorized, persistent access to the domain.

Scope and Impact

- **Primary Victim:** Workstation **DESKTOP-RNV09AT** (IP: 172.17.0.99)
- **Compromised User:** **afletcher**
- **Domain Controller Impacted:** **WIN-CTL9XBQ9Y19** (IP: 172.17.0.17),

This attack has the potential to expose all domain credentials and allow attackers to impersonate any user, including Domain Admins, through the Golden Ticket technique. Immediate action is required to contain and investigate this compromise.

2. Victim Details

Attribute	Value	Source
Hostname	DESKTOP-RNV09AT	NBNS Registration / Kerberos Traffic
IP Address	172.17.0.99	PCAP Statistics
MAC Address	00:23:ae:50:ba:fd	Ethernet Statistics

3. Indicators of Compromise (IOCs)

Malicious External IP Addresses:

IP Address	Traffic	Risk Level	Action
46.254.34.201	782 packets / 720 kB	CRITICAL	Block at firewall
79.124.78.197	591 packets / 64 kB	CRITICAL	Block at firewall
23.45.119.144	376 packets / 189 kB	HIGH	Investigate
23.221.24.69	215 packets / 171 kB	HIGH	Investigate

Critical Internal Indicators:

IOC Type	Value	Description	Risk
Compromised Host	DESKTOP-RNV09AT	Infected workstation	CRITICAL
Compromised User	afletcher	Stolen credentials	CRITICAL
DCSync Attack	DRSUAPI Calls	AD hash extraction	CRITICAL
LDAP Enumeration	Multiple Binds	AD reconnaissance	HIGH

No.	Time	Source	Destination	Protocol	Length	Info
20	13:32:31.396549	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<20>
21	13:32:31.396549	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<00>
22	13:32:31.396549	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<00>
60	13:32:32.150023	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<00>
61	13:32:32.150023	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<00>
62	13:32:32.150023	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<20>
64	13:32:32.912861	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<20>
65	13:32:32.912861	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<00>
66	13:32:32.912861	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<00>
81	13:32:33.663907	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<00>
82	13:32:33.663907	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<00>
83	13:32:33.663907	172.17.0.99	172.17.0.255	NBNS	110	Registration NB DESKTOP-RNV09AT<20>
85	13:32:34.449002	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<1e>
91	13:32:35.224995	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<1e>
92	13:32:35.975604	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<1e>
96	13:32:36.745729	172.17.0.99	172.17.0.255	NBNS	110	Registration NB BEPOSITIVE<1e>
...	13:33:08.167295	172.17.0.99	172.17.0.255	NBNS	92	Name query NB WIN-CTL9XBQY19<20>

**FIGURE (1) Hostname Discovery – NBNS Registration showing victim hostname
DESKTOP-RNV09AT.**

kerberos and ip.addr == 172.17.0.99S					
No.	Time	Source	Destination	Protocol	Length Info
483	13:34:35.576097	172.17.0.17	172.17.0.99	KRB5	331 TGS-REP
492	13:34:35.577463	172.17.0.17	172.17.0.99	SMB2	314 Session Setu
1070	13:34:40.063118	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
1097	13:34:40.074307	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
1110	13:34:40.079136	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
1437	13:35:06.288839	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
1465	13:35:06.301060	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
1478	13:35:06.307290	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
2267	13:35:36.275112	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
2294	13:35:36.299715	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
2307	13:35:36.309847	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3009	13:37:50.872547	172.17.0.17	172.17.0.99	KRB5	361 TGS-REP
3017	13:37:50.874745	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3030	13:37:50.886990	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3103	13:39:36.759128	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3114	13:39:36.768679	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3299	13:44:38.248800	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3486	13:47:58.213715	172.17.0.17	172.17.0.99	SMB2	314 Session Setu
3562	13:49:35.783159	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
3589	13:49:35.795404	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
3602	13:49:35.800184	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
4201	14:02:58.212460	172.17.0.17	172.17.0.99	SMB2	314 Session Setu
4566	14:13:02.135864	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
4597	14:13:02.254343	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
4610	14:13:02.266232	172.17.0.17	172.17.0.99	LDAP	264 bindResponse
4770	14:17:58.195427	172.17.0.17	172.17.0.99	SMB2	314 Session Setu
5055	14:31:52.483837	172.17.0.17	172.17.0.99	DCERPC	338 Bind_ack: ca
31	13:32:31.433000	172.17.0.99	172.17.0.17	LDAP	668 bindRequest
120	13:32:58.214912	172.17.0.99	172.17.0.17	SMB2	814 Session Setu
293	13:34:35.303608	172.17.0.99	172.17.0.17	KRB5	283 AS-REQ
301	13:34:35.309704	172.17.0.99	172.17.0.17	KRB5	363 AS-REQ

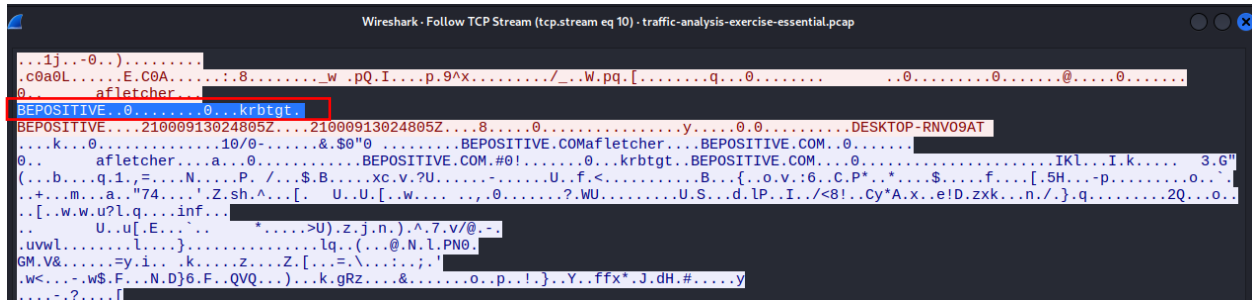


FIGURE (2) Compromised User Account – Kerberos AS-REQ showing user afletcher authenticating to the Domain Controller.

No.	Time	Source	Destination	Protocol	Length	Info
1334:35.477336	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1334:35.477680	172.17.0.17	172.17.0.99	DCERPC	162	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1334:35.484610	172.17.0.99	172.17.0.17	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1334:35.486212	172.17.0.17	172.17.0.99	DCERPC	338	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1334:35.486414	172.17.0.99	172.17.0.17	DCERPC	274	Alter_context: call id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)	
1334:35.486900	172.17.0.99	172.17.0.17	DCERPC	159	Alter_context_resp: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance	
1334:35.491224	172.17.0.99	172.17.0.17	DCERPC	330	Bind: call id: 2, Fragment: Single, 3 context items: SAMR V1.0 (32bit NDR), SAMR V1.0 (64bit NDR), SAMR V1.0 (6cb71c2c-98b1, 3 results: Provider rejection, Acceptance, Negotiation)	
1334:35.491677	172.17.0.17	172.17.0.99	DCERPC	254	Bind_ack: call id: 2, Fragment: Single, max_xmit: 4280 max_recv: 4280, 3 results: Provider rejection, Acceptance, Negotiation	
1334:40.859544	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1334:40.861665	172.17.0.99	172.17.0.17	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1334:40.863118	172.17.0.17	172.17.0.99	DCERPC	338	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1334:40.863308	172.17.0.99	172.17.0.17	DCERPC	274	Alter_context: call id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)	
1334:40.863840	172.17.0.17	172.17.0.99	DCERPC	159	Alter_context_resp: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance	
1335:06.285043	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1335:06.285043	172.17.0.17	172.17.0.99	DCERPC	162	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1335:06.287429	172.17.0.17	172.17.0.99	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1335:06.288839	172.17.0.17	172.17.0.99	DCERPC	338	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1335:06.289228	172.17.0.99	172.17.0.17	DCERPC	274	Alter_context: call id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)	
1335:06.289700	172.17.0.17	172.17.0.99	DCERPC	159	Alter_context_resp: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance	
1335:36.266603	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1335:36.266980	172.17.0.17	172.17.0.99	DCERPC	162	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1335:36.273610	172.17.0.99	172.17.0.17	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1335:36.275112	172.17.0.99	172.17.0.17	DCERPC	338	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1335:36.275997	172.17.0.99	172.17.0.17	DCERPC	274	Alter_context: call id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)	
1335:36.276636	172.17.0.17	172.17.0.99	DCERPC	159	Alter_context_resp: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance	
1349:35.779135	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1349:35.779178	172.17.0.17	172.17.0.99	DCERPC	162	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1349:35.781710	172.17.0.99	172.17.0.17	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1349:35.783159	172.17.0.17	172.17.0.99	DCERPC	338	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1349:35.783541	172.17.0.99	172.17.0.17	DCERPC	274	Alter_context: call id: 2, Fragment: Single, 1 context items: DRSUAPI V4.0 (64bit NDR)	
1349:35.784074	172.17.0.17	172.17.0.99	DCERPC	159	Alter_context_resp: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 1 results: Acceptance	
1413:02.131643	172.17.0.99	172.17.0.17	DCERPC	214	Bind: call id: 2, Fragment: Single, 3 context items: EPMv4 V3.0 (32bit NDR), EPMv4 V3.0 (64bit NDR), EPMv4 V3.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	
1413:02.131886	172.17.0.17	172.17.0.99	DCERPC	162	Bind_ack: call id: 2, Fragment: Single, max_xmit: 5840 max_recv: 5840, 3 results: Provider rejection, Acceptance, Negotiation	
1413:02.134595	172.17.0.99	172.17.0.17	DCERPC	751	Bind: call id: 2, Fragment: Single, 3 context items: DRSUAPI V4.0 (32bit NDR), DRSUAPI V4.0 (64bit NDR), DRSUAPI V4.0 (6cb71c2c-5840, 3 results: Provider rejection, Acceptance, Negotiation)	

FIGURE (3) DRSUAPI DCSync Attack Evidence – DRSUAPI Bind requests showing DCSync attack in progress.

Ethernet · 6	IPv4 · 42	IPv6	TCP · 195	UDP · 77			
Address	Packets	Bytes ^	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes Count	
172.17.0.99	4,793	2 MB	2,358	401 kB	2,435	2 MB	
46.254.34.201	782	720 kB	504	701 kB	278	18 kB	
172.17.0.17	1,310	322 kB	611	150 kB	699	172 kB	
23.45.119.144	376	189 kB	199	165 kB	177	24 kB	
23.221.24.69	215	171 kB	147	161 kB	68	10 kB	
204.79.197.203	261	103 kB	144	80 kB	117	24 kB	
23.221.24.58	192	102 kB	91	91 kB	101	12 kB	
79.124.78.197	591	64 kB	261	25 kB	330	40 kB	
52.113.194.132	141	57 kB	73	42 kB	68	14 kB	
23.195.212.189	78	38 kB	37	33 kB	41	5 kB	
20.96.153.111	61	21 kB	28	15 kB	33	6 kB	
20.189.173.18	52	21 kB	22	15 kB	30	5 kB	
40.126.28.12	55	17 kB	20	12 kB	35	5 kB	
20.42.73.28	36	16 kB	16	6 kB	20	10 kB	
40.119.249.228	48	14 kB	22	10 kB	26	4 kB	
20.60.228.1	30	14 kB	13	12 kB	17	2 kB	
23.220.251.153	41	14 kB	21	10 kB	20	4 kB	
20.10.31.115	59	12 kB	28	7 kB	31	5 kB	
23.40.145.142	28	12 kB	12	10 kB	16	2 kB	
20.189.173.1	33	11 kB	15	6 kB	18	5 kB	
52.109.0.91	37	11 kB	16	9 kB	21	2 kB	
13.70.79.200	32	10 kB	15	6 kB	17	5 kB	
52.109.0.142	29	9 kB	13	8 kB	16	2 kB	
23.45.119.147	25	9 kB	13	8 kB	12	1 kB	
23.45.119.143	25	9 kB	14	8 kB	11	1 kB	
13.107.246.57	36	9 kB	17	7 kB	19	2 kB	
23.194.68.140	21	9 kB	11	7 kB	10	1 kB	
20.189.173.26	28	9 kB	13	5 kB	15	3 kB	
20.241.44.114	21	9 kB	9	7 kB	12	1 kB	
13.89.179.9	26	8 kB	12	5 kB	14	3 kB	
40.126.28.22	25	8 kB	11	6 kB	14	2 kB	
172.17.0.255	35	6 kB	0	0 bytes	35	6 kB	
199.232.210.172	14	2 kB	7	817 bytes	7	981 bytes	
255.255.255.255	4	1 kB	0	0 bytes	4	1 kB	
199.232.214.172	11	1 kB	5	503 bytes	6	642 bytes	
184.29.137.96	10	1 kB	4	503 bytes	6	587 bytes	

FIGURE (4) Malicious External IP Traffic – Endpoints statistics showing suspicious external IPs: 46.254.34.201 and 79.124.78.197.

Conclusion:

The incident described in this report reveals a significant and sophisticated attack against the BEPOSITIVE.COM domain, which involved the exploitation of a compromised user account to conduct a DCSync attack. The malware infection on DESKTOP-RNV09AT (IP: 172.17.0.99), coupled with the attacker's use of stolen afletcher credentials, allowed for Active Directory enumeration and a direct attack on our Domain Controller (WIN-CTL9XBQ9Y19).

This attack involved multiple critical techniques:

1. **DCSync Attack (via DRSUAPI calls):**

The attacker exploited the DRSUAPI protocol to perform unauthorized directory replication. This is a well-known technique used in DCSync attacks, where an attacker impersonates a Domain Controller and requests the replication of sensitive Active Directory data, including password hashes and Kerberos credentials. By doing so, the attacker could potentially extract password hashes for all domain users, including Domain Admins, and obtain the krbtgt hash, which would allow the attacker to create Golden Tickets. These forged tickets would grant the attacker persistent access to the domain, bypassing authentication mechanisms.

2. **Kerberos Authentication Abuse (Kerberoasting):**

In addition to the DCSync attack, the TGS-REQ flood seen in the PCAP indicates possible Kerberoasting, where the attacker targeted service accounts to extract their Kerberos ticket-granting service (TGS) tickets.

3. LDAP Enumeration:

The attacker used LDAP requests to enumerate Active Directory objects and gather more information about the domain. Repeated LDAP bind requests further demonstrate the extent of the attacker’s efforts to map the domain, extract user details, and search for high-value targets for lateral movement.

4. Unusual External Communications:

The victim workstation communicated with external Command and Control (C2) infrastructure. Specifically, it established a connection to the IP address 46.254.34.201, showing an unusually high volume of traffic (720 kB over 782 packets) and potential C2 activity. Moreover, there was also an attempt at data exfiltration through unencrypted HTTP (port 80) with 79.124.78.197. The use of unencrypted HTTP is particularly alarming as it allows sensitive data to be transmitted in plaintext, making it susceptible to interception.