

# INTRODUCTION

**Following a request from TechSecure Inc., our team at OSPenTek Solutions conducted a detailed analysis of the corporate network traffic using Wireshark. The objective was to identify potential anomalies or signs of malicious activity that could indicate intrusion attempts or security compromises.**

**This work is part of our ongoing collaboration with TechSecure Inc. to ensure the highest efficiency and security of their IT systems.**



# Identification of Indicators of Compromise (IOCs)

a)

**High volume of TCP SYN and DST flagged packets:**  
These often indicate port scanning attempts or Denial of Service (DoS) attacks, which aim to exploit vulnerabilities or overload systems

b)

**Intensive communication between few IP addresses:**  
A limited number of IP addresses were involved in significant traffic volume, potentially suggesting a compromised host or command-and-control server communications.

c)

**Red-flagged packets:**  
These indicate TCP communication interruptions or anomalies, suggesting potential transmission errors or abnormally terminated connections.

# Packet Analysis

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000000	192.168.200.150	192.168.200.255	BROWSER	286 Host Announcement METASPOLOITABLE, Workstation, Server, Print Queue Server, Xenix Server, NT Workstation, NT Server, Potential...
2	23.764214995	192.168.200.100	192.168.200.150	TCP	74 53060 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
3	23.76427789	192.168.200.100	192.168.200.150	TCP	74 33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
4	23.764777323	192.168.200.150	192.168.200.100	TCP	74 80 - 53060 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
5	23.764777427	192.168.200.150	192.168.200.100	TCP	68 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
6	23.764815289	192.168.200.150	192.168.200.100	TCP	66 53060 - 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSecr=0 WS=128
7	23.764899991	192.168.200.150	192.168.200.100	TCP	66 53060 - 80 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0 TSecr=0 WS=128
8	28.761629461	PcsCompu_fd:87:fe	PcsCompu_39:7d:fe	ARP	69 Who has 192.168.200.100 Tel 192.168.200.150
9	28.761644619	PcsCompu_fd:87:fe	PcsCompu_39:7d:fe	ARP	42 192.168.200.100 is at 08:00:27:39:7d:fe
10	28.76165257	PcsCompu_fd:87:fe	PcsCompu_39:7d:fe	ARP	42 Who has 192.168.200.150 Tel 192.168.200.100
11	28.775230099	PcsCompu_fd:87:fe	PcsCompu_39:7d:fe	ARP	66 192.168.200.150 is at 08:00:27:fd:87:fe
12	36.774434453	192.168.200.150	192.168.200.100	TCP	74 41384 - 23 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
13	36.774218111	192.168.200.100	192.168.200.150	TCP	54 56120 - 111 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
14	36.774257841	192.168.200.100	192.168.200.150	TCP	74 33876 - 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
15	36.774366308	192.168.200.100	192.168.200.150	TCP	54 58636 - 554 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
16	36.774495627	192.168.200.100	192.168.200.150	TCP	74 52358 - 135 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
17	36.774535534	192.168.200.100	192.168.200.150	TCP	74 46138 - 93 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
18	36.774614776	192.168.200.100	192.168.200.150	TCP	74 41182 - 21 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
19	36.774685595	192.168.200.100	192.168.200.150	TCP	74 23 - 41384 [SYN, ACK] Seq=1 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=64
20	36.774685652	192.168.200.100	192.168.200.150	TCP	74 111 - 56120 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 TSecr=0 WS=64
21	36.774685692	192.168.200.150	192.168.200.100	TCP	68 443 - 33876 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
22	36.774685737	192.168.200.150	192.168.200.100	TCP	68 554 - 58636 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
23	36.77468577	192.168.200.150	192.168.200.100	TCP	68 139 - 52358 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
24	36.774708464	192.168.200.100	192.168.200.150	TCP	66 41384 - 23 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSecr=0 WS=128
25	36.774711072	192.168.200.100	192.168.200.150	TCP	66 56120 - 111 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSecr=0 WS=128
26	36.775141184	192.168.200.150	192.168.200.100	TCP	66 993 - 46138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
27	36.77514127	192.168.200.150	192.168.200.100	TCP	74 21 - 41184 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=64
28	36.77514044	192.168.200.100	192.168.200.150	TCP	66 41182 - 21 [ACK] Seq=1 Ack=1 Win=64240 Len=0 TSecr=0 WS=128
29	36.77533789	192.168.200.100	192.168.200.150	TCP	74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
30	36.775366094	192.168.200.100	192.168.200.150	TCP	74 55656 - 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
31	36.775524204	192.168.200.100	192.168.200.150	TCP	74 53062 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
32	36.775589898	192.168.200.100	192.168.200.150	TCP	66 113 - 59174 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
33	36.77561945	192.168.200.100	192.168.200.150	TCP	66 41384 - 23 [RST, ACK] Seq=0 Ack=1 Win=64259 Len=0 TSecr=0 WS=128
34	36.77562497	192.168.200.100	192.168.200.150	TCP	66 56120 - 111 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
35	36.77533789	192.168.200.100	192.168.200.150	TCP	74 59174 - 113 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
36	36.77579004	192.168.200.100	192.168.200.150	TCP	74 80 - 53062 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
37	36.775893786	192.168.200.100	192.168.200.150	TCP	66 55656 - 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
38	36.775813232	192.168.200.100	192.168.200.150	TCP	66 53862 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
39	36.775816964	192.168.200.100	192.168.200.150	TCP	66 41182 - 21 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
40	36.775975876	192.168.200.100	192.168.200.150	TCP	66 55656 - 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
Frame 1: 286 bytes on wire (2288 bits), 286 bytes captured (2288 bits) on interface eth1, id 0					
0000	ff ff ff ff ff ff 08 00 27 fd 87 1e 08 00 45 80	.....E	.....a	.....a	.....a

No.	Time	Source	Destination	Protocol	Length Info
79	36.777623149	192.168.200.150	192.168.200.100	TCP	68 78 - 49708 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645037	192.168.200.100	192.168.200.150	TCP	74 41378 - 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
81	36.777690898	192.168.200.100	192.168.200.150	TCP	74 51506 - 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
82	36.7775863	192.168.200.150	192.168.200.100	TCP	66 588 - 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.7775869	192.168.200.150	192.168.200.100	TCP	66 962 - 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.77761245	192.168.200.150	192.168.200.100	TCP	66 764 - 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.77781293	192.168.200.150	192.168.200.100	TCP	66 435 - 51966 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
86	36.777893298	192.168.200.100	192.168.200.150	TCP	66 33042 - 445 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSecr=0 WS=128
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66 46990 - 139 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 TSecr=0 WS=128
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66 66632 - 29 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
89	36.778031265	192.168.200.100	192.168.200.150	TCP	66 37282 - 53 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSecr=0 WS=128
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74 51459 - 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
91	36.778200161	192.168.200.100	192.168.200.150	TCP	74 48448 - 806 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
92	36.77830783	192.168.200.100	192.168.200.150	TCP	74 54566 - 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	66 148 - 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	66 886 - 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	66 221 - 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	T	

# Attack Vector Hypotheses

a)

## Port Scanning and DoS

### Attacks:

Attackers may have used scanning techniques to identify vulnerable services or launched DoS attacks to disrupt business operations.

b)

TCP Session Hijacking:  
Alterations in sequence and ACK numbers suggest attempts to intercept or manipulate TCP sessions - a common tactic in session hijacking attacks.



# Recommendations

- a) **IDS/IPS Implementation:**  
Deploy intrusion detection and prevention systems to monitor and intercept suspicious activity in real-time.
  
- b) **Access Control & Traffic Limitation:**  
Implement strict network access controls and traffic shaping measures to mitigate DoS attack impacts
  
- c) **Regular Updates & Patching:**  
Maintain all devices and software with current updates to reduce exposed vulnerabilities
  
- d) **Ongoing Security Awareness Training:**  
Conduct continuous staff education on potential risks and security best practices to prevent incidents

# Conclusion

Our analysis has revealed concerning indicators that require immediate attention to prevent potential damage. By implementing the proposed recommendations, TechSecure Inc. can significantly enhance the security and resilience of its network infrastructure.

OSPenTek Solutions remains committed to supporting TechSecure Inc. in implementing these measures and in the ongoing monitoring of their systems' security.

