IOC and Network Analysis

Lorenzo Croci

INTRODUCTION

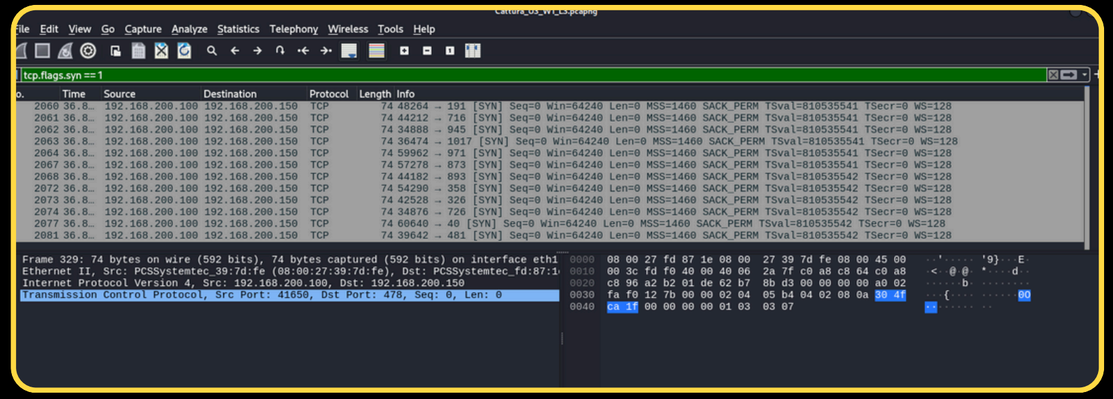
During the analysis of the provided network capture file, packets were examined to identify potential Indicators of Compromise (IOC). The goal was to detect evidence of suspicious activity, hypothesize possible attack vectors, and propose mitigation measures to reduce the impact of attacks.

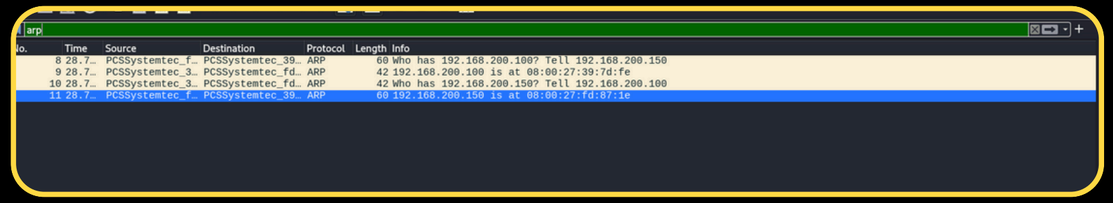
ATTACK VECTORS

Methods or pathways used by attackers to exploit vulnerabilities and gain unauthorized access to systems or data.

INDICATORS OF COMPROMISE (IOC)

Observable signs, such as unusual network activity, that indicate a system may have been compromised by an attack.





Indicators of Compromise (IOC)

Port Scanning

Numerous TCP SYN requests were sent from IP 192.168.200.100 to 192.168.200.150, targeting ports such as:

- 80 (HTTP), 443 (HTTPS), 23 (Telnet), 21 (FTP), 22 (SSH), and other common ports.
- This systematic scanning indicates potential reconnaissance activity, typical of a port scan attack.

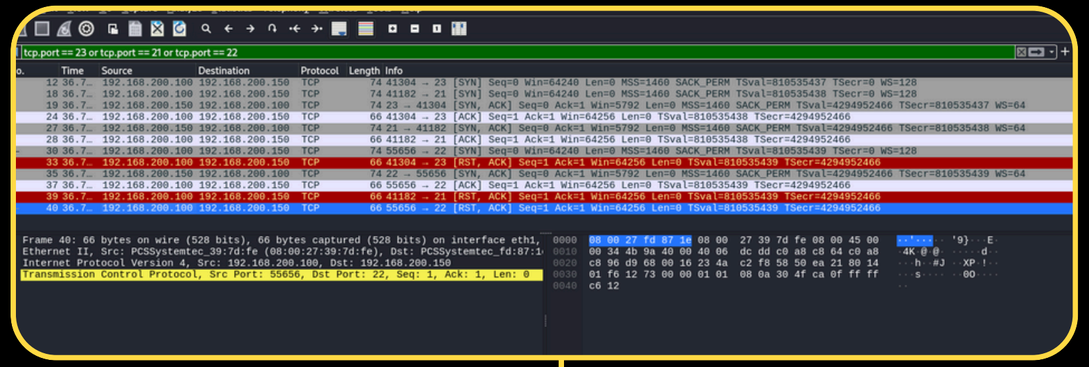
Reset and unexpected responses

In several cases, the server (192.168.200.150) responded with RST or RST, ACK packets, signaling either inactive services or rejected connection attempts.

Suspicious ARP traffic

A sequence of rapid ARP packets ("Who has…?") was observed, which may suggest potential ARP table manipulation (e.g., ARP spoofing attacks).

HYPOTHESES ON ATTACK VECTORS



PORT SCANNING

IP address 192.168.200.100 is likely performing a port scan to identify active and potentially vulnerable services on 192.168.200.150. This activity is typically a reconnaissance phase for preparing exploits.

REMOTE ACCESS ATTEMPTS

Requests to Telnet (23), SSH (22), and FTP (21) ports suggest potential brute-force attempts to gain access to these services.

MAN IN THE MIDDLE (MITM)

The high volume of ARP traffic could indicate an attempt to redirect network traffic via ARP spoofing, aiming to intercept or manipulate data.

RECOMMENDED ACTIONS

BLOCK THE ATTACKER

Configure the firewall to block all traffic originating from IP address 192.168.200.100. Please verify beforehand that this isn't an authorized user with your network administrator.

PORT FILTERING

Close **unused** ports and restrict access to authorized IP addresses only. Please verify beforehand that these aren't critical services and or users with your network administrator.

ENABLE STRONG AUTHENTICATION

Ensure services like SSH, FTP, and Telnet are protected with strong credentials and, where possible, enable two-factor authentication.

PROTECTION AGAINST ARP SPOOFING

Use security features like static IP-MAC bindings to prevent ARP manipulation.

CONCLUSION

The analysis of the capture file highlights port scanning activities and other possible reconnaissance maneuvers. It is critical to adopt appropriate countermeasures to mitigate the risk of compromise. Implementing firewall policies, reducing exposed services, and actively monitoring the network are key steps to improve system security.

Please find hereunder the complete technical report for your use:

Project S9L5 - Network Traffic Analysis and Indicators of Compromise.pdf