Zurich 29.11.2024

Per l’esercizio pratico di oggi, trovate in allegato una cattura di rete effettuata con Wireshark. Analizzate la cattura attentamente e rispondere ai seguenti quesiti:
● Identificare ed analizzare eventuali IOC, ovvero evidenze di attacchi in corso
● In base agli IOC trovati, fate delle ipotesi sui potenziali vettori di attacco utilizzati
● Consigliate un’azione per ridurre gli impatti dell’attacco attuale ed eventualmente un simile attacco futuro

For today's practical exercise, please find attached a network capture made with Wireshark. Analyze the capture carefully and answer the following questions:
● Identify and analyze any IOCs, i.e. evidence of ongoing attacks
● Based on the IOCs found, make assumptions about the potential attack vectors used
● Recommend an action to reduce the impacts of the current attack and possibly a similar future attack

Network Traffic Analysis and Vulnerability Assessment Report - Threat Intelligence&IOC **(Indicator of Compromission)**

Introduction

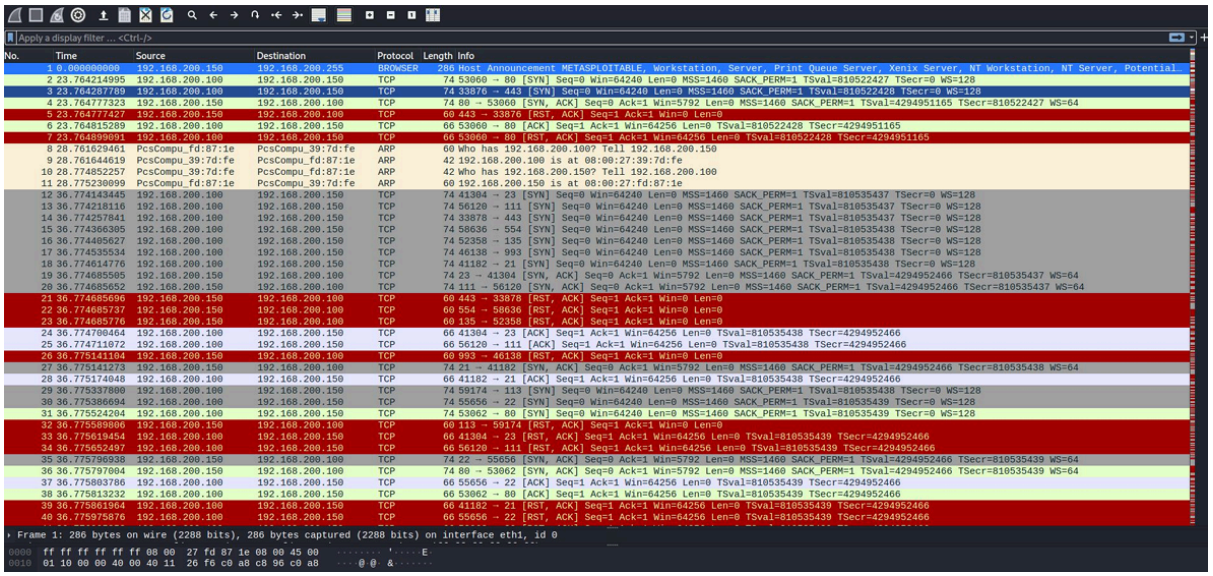
This report presents the findings of a network traffic analysis conducted using Wireshark on a simulated network environment within a cybersecurity laboratory.

The primary objective of this analysis was to identify potential vulnerabilities and security threats by examining network traffic patterns.

Methodology

Network traffic was captured using a network interface within the simulated environment. Wireshark was employed to analyze the captured packets. The analysis focused on identifying suspicious activities, such as port scanning, and correlating them with known vulnerabilities.

Here we have a view of the screenshot we got for the exercise.



As we can see source 192.168.200.150 is sending a Broadcast request (of course on 192.168.200.255) using the “Browser Protocol”.

In Wireshark, the protocol referred to as "Browser" refers to the "Microsoft Browser Protocol" (also called SMB Browser Service or NetBIOS Browser Protocol). This protocol is primarily used in Microsoft networks to facilitate discovery and communication between devices.

The Browser Protocol is used to create and maintain a list (called a "browse list") of devices and services available on the local network and it is part of the NetBIOS (Network Basic Input/Output System) suite used in older Microsoft environments and Windows-based systems.

Since it’s an old suite we can understand that we are in a test based environment as I think that nowadays this kind of Protocol is not used anymore unless it’s a test.

When Wireshark reports "Browser" as the protocol, it is analyzing packets related to the Browser Protocol, and in this case it’s a “Host Announcement” : METASPOITABLE is announcing as a workstation, Server….!

In a Host Announcement A device communicates its presence in the local network to the Master Browser.

Understanding the Broadcast Announcement and Subsequent TCP Connection

Broadcast Announcement:

- The initial broadcast message from 192.168.200.150 is a standard broadcast (sent to 192.168.200.255) to announce its presence on the network and its services. This is a common behavior for devices to advertise their capabilities and discover other devices on the network.

TCP Connection Attempt:

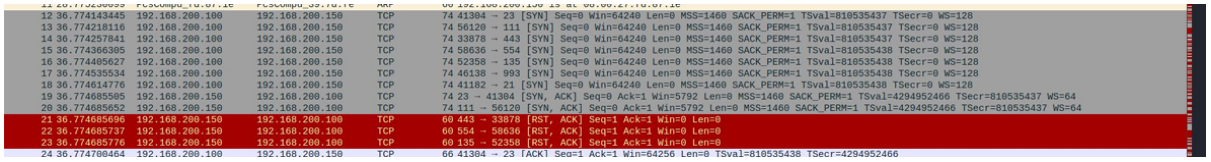
As soon as 192.168.200.150 enters the network it receives TCP connections on ports 80 and 443 (HTTP and HTTPS) from 192.168.200.100 (the attacker - or scanner) that are refused as 192.168.200.150 doesn't recognise 192.168.200.100; in fact there's a ARP request immediately afterwards.

Why the ARP Request After the TCP Connection Attempt?

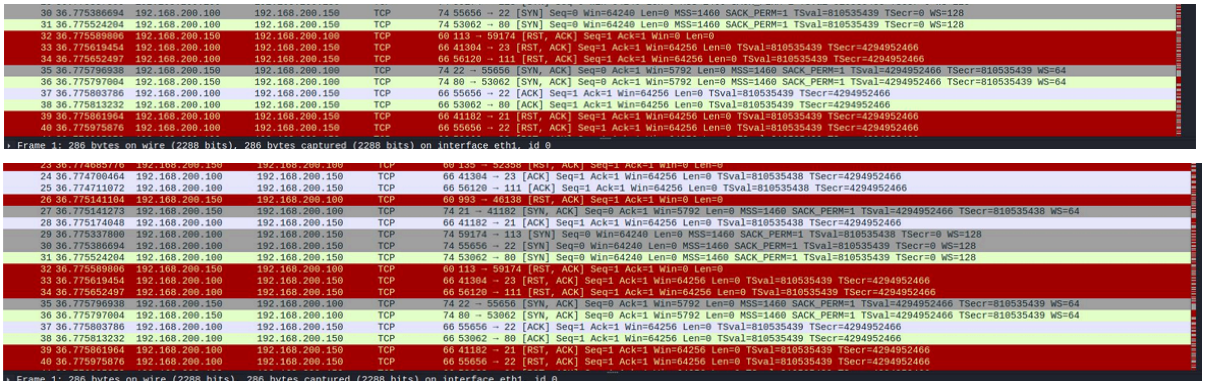
If the system doesn't have a cached ARP entry for the destination IP (192.168.200.100), it will need to perform an ARP request to obtain the corresponding MAC address. This is necessary to send the TCP packets to the correct destination hardware address.

Once both machines (or IP addresses) are into the ARP routing table can start to communicate being identified thanks to the MAC addresses.

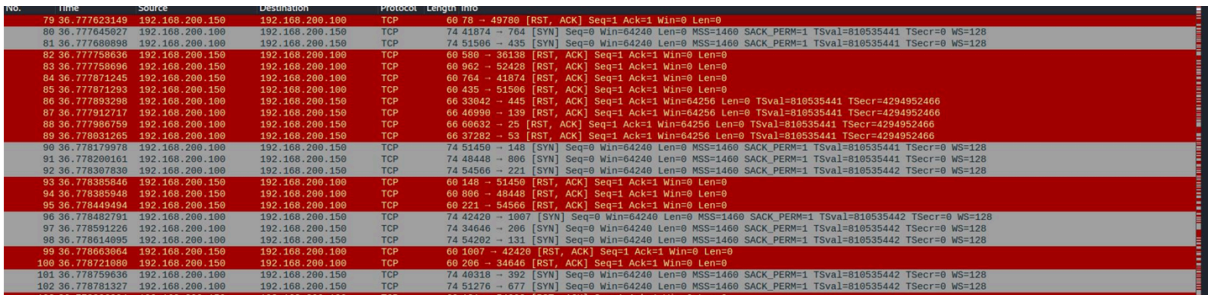
We can easily see a lot of TCP requests from 192.168.200.100 vs 192.168.200.150 using unknown port number directed to well known port numbers on 192.168.200.150



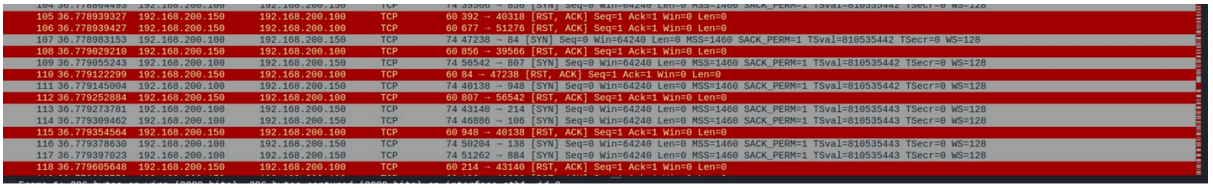
and actually the target host is setting up a connection where is possible and allowed



like ports 23, 111, 21, 22, 80 and suddenly the host that is attempting to make a TCP connection is closing the connection with a RST,ACK (Reset Ack) : it means that it's just checking for which ports are open on 192.168.200.150 .



No.	Time	Source	Destination	Protocol	Length	Info
79	36.777623149	192.168.200.150	192.168.200.100	TCP	60	78 → 49780 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
80	36.777645027	192.168.200.100	192.168.200.150	TCP	74	41074 → 764 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
81	36.777680898	192.168.200.100	192.168.200.150	TCP	74	51506 → 435 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 TSecr=0 WS=128
82	36.777758636	192.168.200.150	192.168.200.100	TCP	60	580 → 36138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
83	36.777758696	192.168.200.150	192.168.200.100	TCP	60	962 → 52428 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
84	36.777871245	192.168.200.150	192.168.200.100	TCP	60	764 → 41874 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
85	36.777871293	192.168.200.150	192.168.200.100	TCP	60	435 → 51506 [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=64256 Len=0 TSval=810535441 TSecr=4294952466
87	36.777912717	192.168.200.100	192.168.200.150	TCP	66	46990 → 139 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
88	36.777986759	192.168.200.100	192.168.200.150	TCP	66	60632 → 25 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=810535441 TSecr=4294952466
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 TSval=810535441 TSecr=4294952466
90	36.778179978	192.168.200.100	192.168.200.150	TCP	74	51450 → 148 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535441 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 TSval=810535441 TSecr=0 WS=128
92	36.778307830	192.168.200.100	192.168.200.150	TCP	74	54566 → 221 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
93	36.778385846	192.168.200.150	192.168.200.100	TCP	60	148 → 51450 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
94	36.778385948	192.168.200.150	192.168.200.100	TCP	60	806 → 48448 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
95	36.778449494	192.168.200.150	192.168.200.100	TCP	60	221 → 54566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
96	36.778482791	192.168.200.100	192.168.200.150	TCP	74	42420 → 1007 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
97	36.778591226	192.168.200.100	192.168.200.150	TCP	74	34646 → 206 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
98	36.778614095	192.168.200.100	192.168.200.150	TCP	74	54202 → 131 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
99	36.778663064	192.168.200.150	192.168.200.100	TCP	60	1007 → 42420 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
100	36.778721080	192.168.200.150	192.168.200.100	TCP	60	206 → 34646 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
101	36.778759636	192.168.200.100	192.168.200.150	TCP	74	40318 → 392 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
102	36.778781327	192.168.200.100	192.168.200.150	TCP	74	51276 → 677 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128



105	36.778939327	192.168.200.150	192.168.200.100	TCP	60	392 → 40318 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
106	36.778939427	192.168.200.150	192.168.200.100	TCP	60	677 → 51276 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
107	36.778893153	192.168.200.100	192.168.200.150	TCP	74	47238 → 84 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
108	36.779029210	192.168.200.150	192.168.200.100	TCP	60	856 → 39566 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
109	36.779055243	192.168.200.100	192.168.200.150	TCP	74	56542 → 807 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
110	36.779122299	192.168.200.150	192.168.200.100	TCP	60	84 → 47238 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
111	36.779145004	192.168.200.100	192.168.200.150	TCP	74	40138 → 948 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535442 TSecr=0 WS=128
112	36.779252884	192.168.200.150	192.168.200.100	TCP	60	807 → 56542 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
113	36.779273781	192.168.200.100	192.168.200.150	TCP	74	43140 → 214 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
114	36.779309462	192.168.200.100	192.168.200.150	TCP	74	46886 → 106 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
115	36.779354564	192.168.200.150	192.168.200.100	TCP	60	948 → 40138 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
116	36.779378630	192.168.200.100	192.168.200.150	TCP	74	50204 → 138 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
117	36.779397023	192.168.200.100	192.168.200.150	TCP	74	51262 → 884 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=810535443 TSecr=0 WS=128
118	36.779605648	192.168.200.150	192.168.200.100	TCP	60	214 → 43140 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Port Scanning Activity

A notable finding was the presence of multiple port scanning attempts originating from 192.168.200.100. The scanner targeted various ports on 192.168.200.150, including well-known ports associated with common services like HTTP, SSH, and FTP. The scanning technique primarily involved sending SYN packets and analyzing the responses.

- **SYN Scans:** The attacker sent SYN packets to open a connection but did not complete the three-way handshake. The absence of an ACK response indicated a closed port, while an RST,ACK response suggested an open port.
- **Vulnerability Implications:** Successful port scans can reveal open services that may have known vulnerabilities. For instance, an open SSH port on an older version of the SSH server could be exploited using a known vulnerability.

Packet Analysis

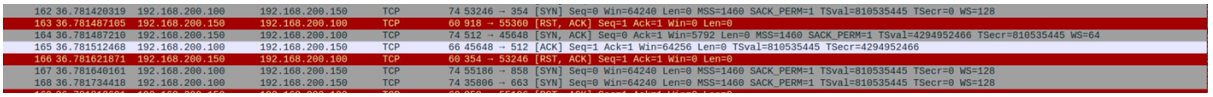
For a better research we should be able to scan the Payload of the attacker IP address to check if it’s malicious or not; actually, according to the small size of the packets, I think it’s only a port scan held to know ports vulnerabilities of the target machine, software and version installed.

The only port that is held open and connected is the 512.

Port 512 is typically associated with the following services:

- **Remote execution (rexec)**: This service allows remote execution of commands on a target system. It's generally considered insecure and is often disabled on modern systems.
- **COMSAT (mail notification daemon):** This service is used to notify users of new mail. However, it's not commonly used nowadays.

It's important to note that the specific services running on port 512 can vary depending on the system configuration and the installed software.



Vulnerability Assessment

The target machine appears to be very vulnerable to possible attacks.

This could also just be a scan port for a penetration test, or it could be a scan port by an insider hacker (remember that he left port 512 open and connected).

Recommendations

To mitigate the identified vulnerabilities and enhance the overall security posture, the following recommendations are made:

- **Patch Management:** Ensure all systems are up-to-date with the latest security patches.
- **Firewall Configuration:** Implement strict firewall rules to restrict incoming and outgoing traffic to essential services.
- **Intrusion Detection Systems (IDS):** Deploy an IDS to monitor network traffic for suspicious activity.
- **Vulnerability Scanning:** Conduct regular vulnerability assessments to identify and address new vulnerabilities.
- **Security Awareness Training:** Educate users about common cyber threats and best practices for security.

Conclusion

The network traffic analysis revealed several potential vulnerabilities in the simulated environment. By addressing these vulnerabilities, the organization can significantly reduce its risk exposure to cyberattacks. It is crucial to conduct regular security assessments and implement appropriate security measures to maintain a strong security posture.

Thank you,
Antonio Bevilacqua