Case Study: Identify the attack

Incident Disclosure Report# 01001

Daniel(Zhiyi) Deng

Date filed: July 6th, 2024

Date of incident: June 6th, 2023

Incident description: Identified possible reconnaissance and vulnerability scanning activities targeting our network.

Executive summary:

During a recent Wireshark network scan, our security team identified possible reconnaissance and vulnerability scanning activities targeting our network. The attacker potentially used Nmap tools to scan for our open ports, conducted ARP scans to locate our network devices, and potentially employed ARP spoofing to initiate a man-in-the-middle attack. Additionally, the attacker established a successful TLS connection, potentially aiming to downgrade our encryption strength to sniff sensitive data.

To address these threats, it is recommended that we block the attacker's host at the firewall and implement a stronger network monitoring policy, especially enhancing the monitoring policy for certain Open Port (3389) on our network. Implementing HTTPS connection instead of HTTP. Furthermore, deploying an Intrusion Detection System (IDS) will enhance our ability to detect and respond to such activities, bolstering our network's security and resilience.

Description of the actual incident:

On June 6th, 2023, our security team identified two instances of potential vulnerability scanning activities targeting our network. The first incident occurred from 11:36 to 11:37, and the second incident took place from 15:36 to 15:37.

Attacker IP(s): 172.16.14.3

Attacker MAC(s): VMware_9f:66:38 (00:50:56:9f:66:38)

Time of attack (first packet of attack): 17:36:41 - June 6, 2023 (File 2.4.3) / 11:36:44 June 6, 2023 (File 2.4.4)

Packet number of first packet in attack: 2 (File 2.4.3) / 10 (File 2.4.4)

Protocol(s) used in the attack: File 2.4.3: ARP, TCP, TLSv1.2 File 2.4.4: ARP, TCP, TLSv1.2, TLSv1.3

Suspected Nmap/scan configuration: nmap -sS -sT -sF -sV

List any NVD records that may apply to the attack; describe how they are related

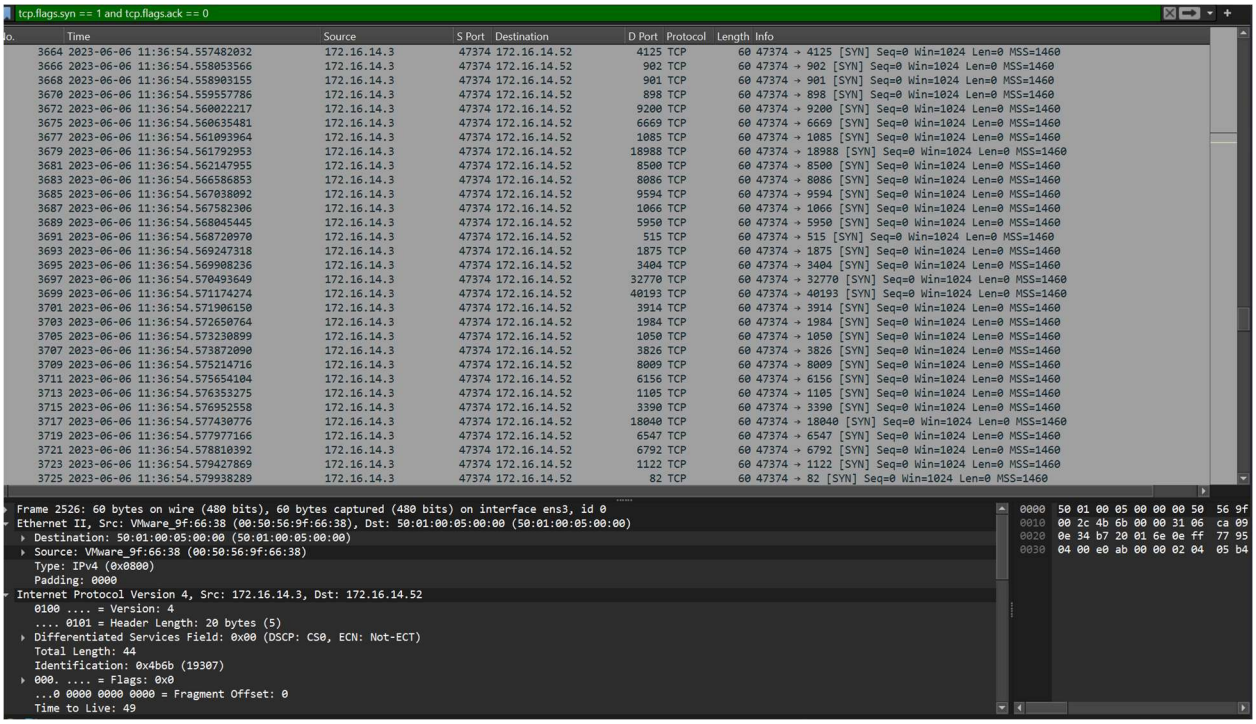
CVE-1999-0667: The ARP protocol allows any host to spoof ARP replies and poisons the ARP cache to conduct Man in the middle attack or a denial of service.

CVE-2020-16863: A denial of service vulnerability exists in Windows Remote Desktop Service when an attacker connects to the target system using RDP (Port 3389) and sends specially crafted requests. An attacker who successfully exploited this vulnerability could cause the Remote Desktop Service on the target system to stop responding.

MITRE ID: T1557: Adversary-in-the-Middle, the attacker tries to downgrade our communication protocol (SSL/TLS) to a weaker version, then sniff our data in transit.

Screen captures from Wireshark showing the attack with explanations (Appendix A)

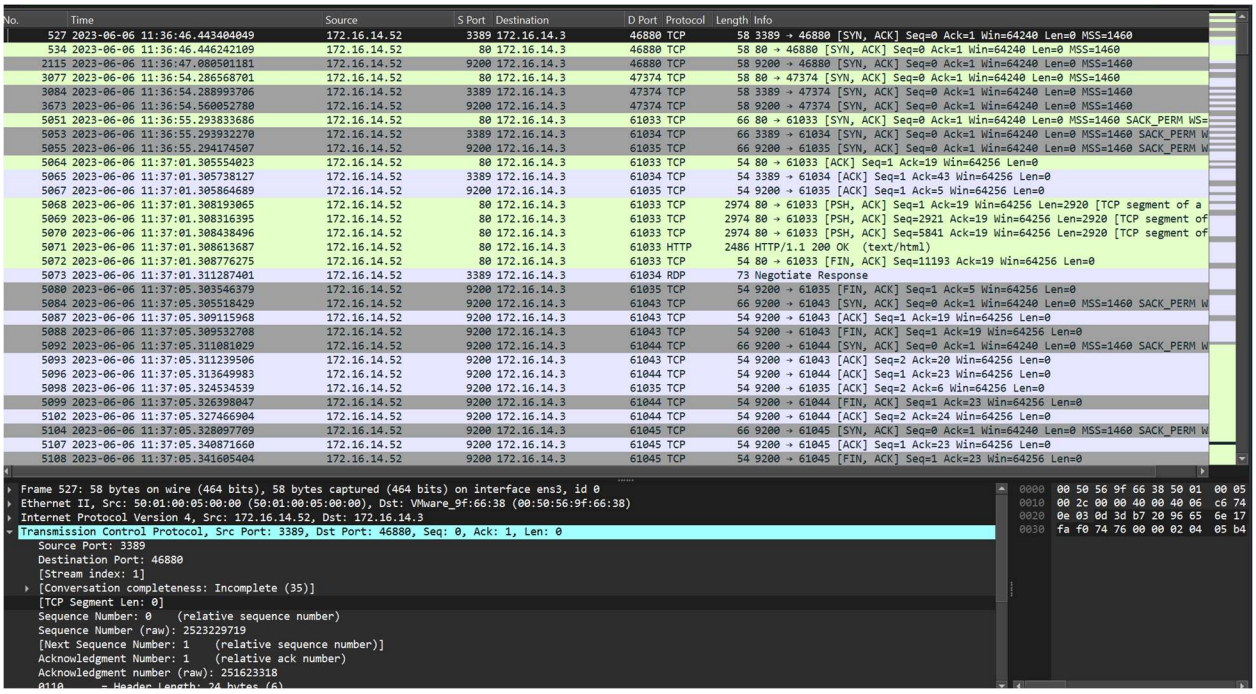
Port scan from source ports 473474, 46880 targeting multiple ports on our network, trying to identify our open ports.



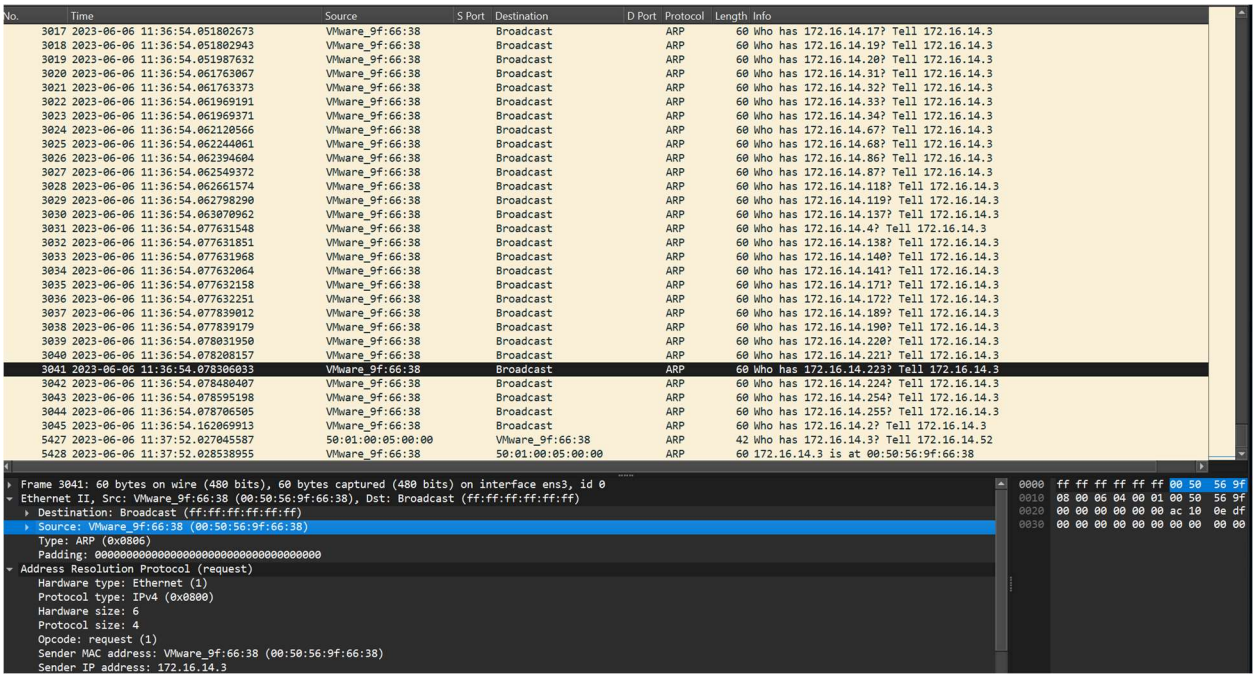
Filtering out our ports that have established connections with attackers (tcp.flags.syn == 0 && tcp.flags.ack == 1 && tcp.flags.reset == 0), these ports are: 3389, 80, 9200 (File 2.4.3), and port 38974, 38978 (File 2.4.4).

Port 3389 (RDP) poses significant security concerns. It is frequently targeted by DDoS attacks and brute force attacks, where attackers try to guess credentials to gain unauthorized access. Historical vulnerabilities in RDP implementations have been exploited, compromising systems. Leaving port 3389 open to the internet without adequate security measures exposes systems to potential threats and unauthorized access attempts, highlighting the critical need for robust security protocols and monitoring to safeguard against these risks.

Port 80 (HTTP) poses multiple security risks. It's a prime target for attacks like SQL injection and cross-site scripting, exploiting web app vulnerabilities. Misconfigured servers can inadvertently expose sensitive data, and attackers use compromised sites for phishing and malware. HTTP headers or error messages can also reveal server details, aiding further exploitation. It is recommended to use HTTPS (443) instead.



A surge of ARP (Address Resolution Protocol) traffic in Wireshark can be indicative of discovering devices on our network. In addition, the attacker may send fake ARP messages to associate their MAC address with the IP address of our device to intercept the traffic, initiating a Man-in-the-Middle attack.



Multiple Change Cipher Spec Messages found through TLSv1.2 protocol might indicate the attacker trying to force a re-negotiation to downgrade the encryption strength in order to sniff our data in transit.