

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.

tcp.flags.syn == 1 and tcp.flags.ack == 0									
No.	Time	Source	S Port	Destination	D Port	Protocol	Length	Info	
3664	2023-06-06 11:36:54.557482032	172.16.14.3	47374	172.16.14.52	4125	TCP	60	47374 → 4125 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3666	2023-06-06 11:36:54.558053566	172.16.14.3	47374	172.16.14.52	902	TCP	60	47374 → 902 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3668	2023-06-06 11:36:54.558903155	172.16.14.3	47374	172.16.14.52	901	TCP	60	47374 → 901 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3670	2023-06-06 11:36:54.559557786	172.16.14.3	47374	172.16.14.52	898	TCP	60	47374 → 898 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3672	2023-06-06 11:36:54.560022217	172.16.14.3	47374	172.16.14.52	9200	TCP	60	47374 → 9200 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3675	2023-06-06 11:36:54.560635481	172.16.14.3	47374	172.16.14.52	6669	TCP	60	47374 → 6669 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3677	2023-06-06 11:36:54.561093964	172.16.14.3	47374	172.16.14.52	1085	TCP	60	47374 → 1085 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3679	2023-06-06 11:36:54.561792953	172.16.14.3	47374	172.16.14.52	18988	TCP	60	47374 → 18988 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3681	2023-06-06 11:36:54.562147955	172.16.14.3	47374	172.16.14.52	8500	TCP	60	47374 → 8500 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3683	2023-06-06 11:36:54.566586853	172.16.14.3	47374	172.16.14.52	8086	TCP	60	47374 → 8086 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3685	2023-06-06 11:36:54.567038092	172.16.14.3	47374	172.16.14.52	9594	TCP	60	47374 → 9594 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3687	2023-06-06 11:36:54.567582306	172.16.14.3	47374	172.16.14.52	1066	TCP	60	47374 → 1066 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3689	2023-06-06 11:36:54.568045445	172.16.14.3	47374	172.16.14.52	5950	TCP	60	47374 → 5950 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3691	2023-06-06 11:36:54.568720970	172.16.14.3	47374	172.16.14.52	515	TCP	60	47374 → 515 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3693	2023-06-06 11:36:54.569247318	172.16.14.3	47374	172.16.14.52	1875	TCP	60	47374 → 1875 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3695	2023-06-06 11:36:54.569908236	172.16.14.3	47374	172.16.14.52	3404	TCP	60	47374 → 3404 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3697	2023-06-06 11:36:54.570493649	172.16.14.3	47374	172.16.14.52	32770	TCP	60	47374 → 32770 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3699	2023-06-06 11:36:54.571174274	172.16.14.3	47374	172.16.14.52	40193	TCP	60	47374 → 40193 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3701	2023-06-06 11:36:54.571906150	172.16.14.3	47374	172.16.14.52	3914	TCP	60	47374 → 3914 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3703	2023-06-06 11:36:54.572650764	172.16.14.3	47374	172.16.14.52	1984	TCP	60	47374 → 1984 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3705	2023-06-06 11:36:54.573230899	172.16.14.3	47374	172.16.14.52	1050	TCP	60	47374 → 1050 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3707	2023-06-06 11:36:54.573872090	172.16.14.3	47374	172.16.14.52	3826	TCP	60	47374 → 3826 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3709	2023-06-06 11:36:54.575214716	172.16.14.3	47374	172.16.14.52	8009	TCP	60	47374 → 8009 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3711	2023-06-06 11:36:54.575654104	172.16.14.3	47374	172.16.14.52	6156	TCP	60	47374 → 6156 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3713	2023-06-06 11:36:54.576353275	172.16.14.3	47374	172.16.14.52	1105	TCP	60	47374 → 1105 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3715	2023-06-06 11:36:54.576952558	172.16.14.3	47374	172.16.14.52	3390	TCP	60	47374 → 3390 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3717	2023-06-06 11:36:54.577430776	172.16.14.3	47374	172.16.14.52	18040	TCP	60	47374 → 18040 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3719	2023-06-06 11:36:54.577977166	172.16.14.3	47374	172.16.14.52	6547	TCP	60	47374 → 6547 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3721	2023-06-06 11:36:54.578810392	172.16.14.3	47374	172.16.14.52	6792	TCP	60	47374 → 6792 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3723	2023-06-06 11:36:54.579427869	172.16.14.3	47374	172.16.14.52	1122	TCP	60	47374 → 1122 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	
3725	2023-06-06 11:36:54.579938289	172.16.14.3	47374	172.16.14.52	82	TCP	60	47374 → 82 [SYN] Seq=0 Win=1024 Len=0 MSS=1460	

Frame 2526: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens3, id 0		0000	50 01 00 05 00 00 00 56 9f
Ethernet II, Src: VMware_9f:66:38 (00:50:56:9f:66:38), Dst: 50:01:00:05:00:00 (50:01:00:05:00:00)		0010	00 2c 4b 65 00 00 31 06 ca 09
Destination: 50:01:00:05:00:00 (50:01:00:05:00:00)		0020	0e 34 b7 20 01 6e 0e ff 77 95
Source: VMware_9f:66:38 (00:50:56:9f:66:38)		0030	04 00 e0 ab 00 00 02 04 05 b4
Type: IPv4 (0x0800)			
Padding: 0000			
Internet Protocol Version 4, Src: 172.16.14.3, Dst: 172.16.14.52			
0100 = Version: 4			
.... 0101 = Header Length: 20 bytes (5)			
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)			
Total Length: 44			
Identification: 0x4b6b (19307)			
0000 = Flags: 0x0			
...0 0000 0000 0000 = Fragment Offset: 0			
Time to Live: 49			

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.

No.	Time	Source	S Port	Destination	D Port	Protocol	Length	Info
527	2023-06-06 11:36:46.443404049	172.16.14.52	3389	172.16.14.3	46880	TCP	58	3389 → 46880 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
534	2023-06-06 11:36:46.446242109	172.16.14.52	80	172.16.14.3	46880	TCP	58	80 → 46880 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2115	2023-06-06 11:36:47.080501181	172.16.14.52	9200	172.16.14.3	46880	TCP	58	9200 → 46880 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3077	2023-06-06 11:36:54.286587901	172.16.14.52	80	172.16.14.3	47374	TCP	58	80 → 47374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3084	2023-06-06 11:36:54.288993706	172.16.14.52	3389	172.16.14.3	47374	TCP	58	3389 → 47374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
3073	2023-06-06 11:36:54.560052780	172.16.14.52	9200	172.16.14.3	47374	TCP	58	9200 → 47374 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
5051	2023-06-06 11:36:55.293833686	172.16.14.52	80	172.16.14.3	61033	TCP	66	80 → 61033 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5053	2023-06-06 11:36:55.293932270	172.16.14.52	3389	172.16.14.3	61034	TCP	66	3389 → 61034 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5055	2023-06-06 11:36:55.294174507	172.16.14.52	9200	172.16.14.3	61035	TCP	66	9200 → 61035 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5064	2023-06-06 11:37:01.305554023	172.16.14.52	80	172.16.14.3	61033	TCP	54	80 → 61033 [ACK] Seq=1 Ack=19 Win=64256 Len=0
5065	2023-06-06 11:37:01.305738127	172.16.14.52	3389	172.16.14.3	61034	TCP	54	3389 → 61034 [ACK] Seq=1 Ack=43 Win=64256 Len=0
5067	2023-06-06 11:37:01.305864689	172.16.14.52	9200	172.16.14.3	61035	TCP	54	9200 → 61035 [ACK] Seq=1 Ack=5 Win=64256 Len=0
5068	2023-06-06 11:37:01.308193065	172.16.14.52	80	172.16.14.3	61033	TCP	2974	80 → 61033 [PSH, ACK] Seq=1 Ack=19 Win=64256 Len=2920 [TCP segment of a
5069	2023-06-06 11:37:01.308316395	172.16.14.52	80	172.16.14.3	61033	TCP	2974	80 → 61033 [PSH, ACK] Seq=2921 Ack=19 Win=64256 Len=2920 [TCP segment of
5070	2023-06-06 11:37:01.308438496	172.16.14.52	80	172.16.14.3	61033	TCP	2974	80 → 61033 [PSH, ACK] Seq=5841 Ack=19 Win=64256 Len=2920 [TCP segment of
5071	2023-06-06 11:37:01.308613687	172.16.14.52	80	172.16.14.3	61033	HTTP	2486	HTTP/1.1 200 OK (text/html)
5072	2023-06-06 11:37:01.308776275	172.16.14.52	80	172.16.14.3	61033	TCP	54	80 → 61033 [FIN, ACK] Seq=11193 Ack=19 Win=64256 Len=0
5073	2023-06-06 11:37:01.311287401	172.16.14.52	3389	172.16.14.3	61034	RDP	73	Negotiate Response
5080	2023-06-06 11:37:05.303546379	172.16.14.52	9200	172.16.14.3	61035	TCP	54	9200 → 61035 [FIN, ACK] Seq=1 Ack=5 Win=64256 Len=0
5084	2023-06-06 11:37:05.305518429	172.16.14.52	9200	172.16.14.3	61043	TCP	66	9200 → 61043 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5087	2023-06-06 11:37:05.309115968	172.16.14.52	9200	172.16.14.3	61043	TCP	54	9200 → 61043 [ACK] Seq=1 Ack=19 Win=64256 Len=0
5088	2023-06-06 11:37:05.309532708	172.16.14.52	9200	172.16.14.3	61043	TCP	54	9200 → 61043 [FIN, ACK] Seq=1 Ack=19 Win=64256 Len=0
5092	2023-06-06 11:37:05.311081029	172.16.14.52	9200	172.16.14.3	61044	TCP	66	9200 → 61044 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5093	2023-06-06 11:37:05.311239586	172.16.14.52	9200	172.16.14.3	61043	TCP	54	9200 → 61043 [ACK] Seq=2 Ack=20 Win=64256 Len=0
5096	2023-06-06 11:37:05.313649983	172.16.14.52	9200	172.16.14.3	61044	TCP	54	9200 → 61044 [ACK] Seq=1 Ack=23 Win=64256 Len=0
5098	2023-06-06 11:37:05.324534539	172.16.14.52	9200	172.16.14.3	61035	TCP	54	9200 → 61035 [ACK] Seq=2 Ack=6 Win=64256 Len=0
5099	2023-06-06 11:37:05.326398047	172.16.14.52	9200	172.16.14.3	61044	TCP	54	9200 → 61044 [FIN, ACK] Seq=1 Ack=23 Win=64256 Len=0
5102	2023-06-06 11:37:05.327466904	172.16.14.52	9200	172.16.14.3	61044	TCP	54	9200 → 61044 [ACK] Seq=2 Ack=24 Win=64256 Len=0
5104	2023-06-06 11:37:05.328097799	172.16.14.52	9200	172.16.14.3	61045	TCP	66	9200 → 61045 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM W
5107	2023-06-06 11:37:05.340871660	172.16.14.52	9200	172.16.14.3	61045	TCP	54	9200 → 61045 [ACK] Seq=1 Ack=23 Win=64256 Len=0
5108	2023-06-06 11:37:05.341605404	172.16.14.52	9200	172.16.14.3	61045	TCP	54	9200 → 61045 [FIN, ACK] Seq=1 Ack=23 Win=64256 Len=0

Frame 527: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface ens3, id 0

Ethernet II, Src: VMware_9f:66:38 (00:50:56:9f:66:38), Dst: VMware_56:9f:66:38 (00:50:56:9f:66:38)

Internet Protocol Version 4, Src: 172.16.14.52, Dst: 172.16.14.3

Transmission Control Protocol, Src Port: 3389, Dst Port: 46880, Seq: 0, Ack: 1, Len: 0

Source Port: 3389

Destination Port: 46880

[Stream index: 1]

[Conversation completeness: Incomplete (35)]

[TCP Segment Len: 0]

Sequence Number: 0 (relative sequence number)

Sequence Number (raw): 253229279

[Next Sequence Number: 1 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 251623318

0110 = Header Length: 24 bytes (6)

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.

No.	Time	Source	S Port	Destination	D Port	Protocol	Length	Info
3017	2023-06-06 11:36:54.051802673	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.17? Tell 172.16.14.3
3018	2023-06-06 11:36:54.051802943	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.19? Tell 172.16.14.3
3019	2023-06-06 11:36:54.051987632	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.20? Tell 172.16.14.3
3020	2023-06-06 11:36:54.061763067	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.31? Tell 172.16.14.3
3021	2023-06-06 11:36:54.061763373	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.32? Tell 172.16.14.3
3022	2023-06-06 11:36:54.061969191	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.33? Tell 172.16.14.3
3023	2023-06-06 11:36:54.061969371	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.34? Tell 172.16.14.3
3024	2023-06-06 11:36:54.062120566	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.67? Tell 172.16.14.3
3025	2023-06-06 11:36:54.062244061	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.68? Tell 172.16.14.3
3026	2023-06-06 11:36:54.062394604	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.86? Tell 172.16.14.3
3027	2023-06-06 11:36:54.062549372	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.87? Tell 172.16.14.3
3028	2023-06-06 11:36:54.062661574	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.118? Tell 172.16.14.3
3029	2023-06-06 11:36:54.062798290	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.119? Tell 172.16.14.3
3030	2023-06-06 11:36:54.063070952	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.137? Tell 172.16.14.3
3031	2023-06-06 11:36:54.077631548	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.4? Tell 172.16.14.3
3032	2023-06-06 11:36:54.077631851	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.138? Tell 172.16.14.3
3033	2023-06-06 11:36:54.077631968	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.140? Tell 172.16.14.3
3034	2023-06-06 11:36:54.077632064	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.141? Tell 172.16.14.3
3035	2023-06-06 11:36:54.077632158	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.171? Tell 172.16.14.3
3036	2023-06-06 11:36:54.077632251	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.172? Tell 172.16.14.3
3037	2023-06-06 11:36:54.077839012	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.189? Tell 172.16.14.3
3038	2023-06-06 11:36:54.077839179	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.190? Tell 172.16.14.3
3039	2023-06-06 11:36:54.078031950	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.220? Tell 172.16.14.3
3040	2023-06-06 11:36:54.078208157	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.221? Tell 172.16.14.3
3041	2023-06-06 11:36:54.078306033	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.223? Tell 172.16.14.3
3042	2023-06-06 11:36:54.078480407	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.224? Tell 172.16.14.3
3043	2023-06-06 11:36:54.078595198	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.254? Tell 172.16.14.3
3044	2023-06-06 11:36:54.078706505	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.255? Tell 172.16.14.3
3045	2023-06-06 11:36:54.162069913	Vmware_9f:66:38		Broadcast		ARP	60	Who has 172.16.14.2? Tell 172.16.14.3
5427	2023-06-06 11:37:52.027845587	50:01:00:05:00:00		Vmware_9f:66:38		ARP	42	Who has 172.16.14.3? Tell 172.16.14.52
5428	2023-06-06 11:37:52.028538955	Vmware_9f:66:38		50:01:00:05:00:00		ARP	60	172.16.14.3 is at 00:50:56:9f:66:38

Frame 3041: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface ens3, id 0

Ethernet II, Src: Vmware_9f:66:38 (00:50:56:9f:66:38), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Source: Vmware_9f:66:38 (00:50:56:9f:66:38)

Type: ARP (0x0806)

Padding: 00000000000000000000000000000000

Address Resolution Protocol (request)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: request (1)

Sender MAC address: Vmware_9f:66:38 (00:50:56:9f:66:38)

Sender IP address: 172.16.14.3

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.

No.	Time	Source	S Port	Destination	D Port	Protocol	Length	Info
10	2023-06-06 15:36:42.855363	172.16.14.53	61543	52.226.139.121	443	TLSv1.2	250	Client Hello (SNI=client.wns.windows.com)
13	2023-06-06 15:36:42.875645	52.226.139.121	443	172.16.14.53	61543	TLSv1.2	1272	Server Hello, Certificate, Server Key Exchange, Server Hello Done
15	2023-06-06 15:36:42.881740	172.16.14.53	61543	52.226.139.121	443	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
16	2023-06-06 15:36:42.906521	52.226.139.121	443	172.16.14.53	61543	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
17	2023-06-06 15:36:42.913421	172.16.14.53	61543	52.226.139.121	443	TLSv1.2	465	Application Data
18	2023-06-06 15:36:42.944087	52.226.139.121	443	172.16.14.53	61543	TLSv1.2	132	Application Data
26	2023-06-06 15:36:43.031871	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	250	Client Hello (SNI=client.wns.windows.com)
29	2023-06-06 15:36:43.051933	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	1272	Server Hello, Certificate, Server Key Exchange, Server Hello Done
31	2023-06-06 15:36:43.060041	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
32	2023-06-06 15:36:43.084244	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
33	2023-06-06 15:36:43.090748	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	382	Application Data
34	2023-06-06 15:36:43.091107	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	1120	Application Data
35	2023-06-06 15:36:43.091550	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	200	Application Data
38	2023-06-06 15:36:43.251247	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	335	Application Data
39	2023-06-06 15:36:43.257248	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	159	Application Data
41	2023-06-06 15:36:43.258651	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	236	Application Data
42	2023-06-06 15:36:43.272501	172.16.14.53	61544	52.226.139.121	443	TLSv1.2	244	Application Data
43	2023-06-06 15:36:43.291826	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	159	Application Data
304	2023-06-06 15:36:45.392647	52.226.139.121	443	172.16.14.53	61544	TLSv1.2	167	Application Data
2577	2023-06-06 15:36:49.175497	172.16.14.53	61545	52.226.139.121	443	TLSv1.2	250	Client Hello (SNI=client.wns.windows.com)
2580	2023-06-06 15:36:49.210833	52.226.139.121	443	172.16.14.53	61545	TLSv1.2	1272	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2582	2023-06-06 15:36:49.219487	172.16.14.53	61545	52.226.139.121	443	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2583	2023-06-06 15:36:49.240275	52.226.139.121	443	172.16.14.53	61545	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2584	2023-06-06 15:36:49.245671	172.16.14.53	61545	52.226.139.121	443	TLSv1.2	464	Application Data
2585	2023-06-06 15:36:49.267848	52.226.139.121	443	172.16.14.53	61545	TLSv1.2	132	Application Data
2593	2023-06-06 15:36:49.388604	172.16.14.53	61546	52.226.139.121	443	TLSv1.2	250	Client Hello (SNI=client.wns.windows.com)
2596	2023-06-06 15:36:49.409423	52.226.139.121	443	172.16.14.53	61546	TLSv1.2	1272	Server Hello, Certificate, Server Key Exchange, Server Hello Done
2598	2023-06-06 15:36:49.434887	172.16.14.53	61546	52.226.139.121	443	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
2599	2023-06-06 15:36:49.435506	52.226.139.121	443	172.16.14.53	61546	TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
2600	2023-06-06 15:36:49.440746	172.16.14.53	61546	52.226.139.121	443	TLSv1.2	382	Application Data
2601	2023-06-06 15:36:49.441264	172.16.14.53	61546	52.226.139.121	443	TLSv1.2	1132	Application Data
2602	2023-06-06 15:36:49.441697	172.16.14.53	61546	52.226.139.121	443	TLSv1.2	200	Application Data

Frame 16: 105 bytes on wire (840 bits), 105 bytes captured (840 bits) on interface \Device\NPF{2523F545-554E-44BA-9326-684149241DC5}, id 0

Ethernet II, Src: Cisco_70:a6:c0 (f4:cf:e2:70:a6:c0), Dst: 50:01:00:04:00:00 (50:01:00:04:00:00)

Destination: 50:01:00:04:00:00 (50:01:00:04:00:00)

Source: Cisco_70:a6:c0 (f4:cf:e2:70:a6:c0)

Type: IPv4 (0x0800)

Internet Protocol Version 4, Src: 52.226.139.121, Dst: 172.16.14.53

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x2a (DSCP: AF11, ECN: ECT(0))

Total Length: 91

Identification: 0x73f3 (29683)

010 = Flags: 0x2, Don't fragment

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 112

Protocol: TCP (6)

0000 50 01 00 04 00 00 f4 cf
0010 00 5b 73 f3 40 00 70 06
0020 0e 35 01 bb f0 67 5e 2a
0030 1e 9e 3c 3c 00 00 14 03
0040 28 00 00 00 00 00 00 00
0050 e2 da be df 1d 09 2c f3
0060 ec db 58 cf 53 0b e9 66