Cybersecurity

Activity File

Module 9 Day 2

Activity File: Networking Review Part 2

Part 1: ARP Attacks

Open the network_attack_review.pcap.

1. Filter by ARP packets.
2. Review the packets captured, and explain in simple terms what is taking place in each of the three packets. A device is asking who owns 192.168.47.254, the device responds with their MAC address, then a malicious device responds with the same IP as well with their MAC address.
3. What type of attack is this? ARP poisoning
4. What is the MAC address of the good device? 00:50:56:f9:f5:54
5. What is the MAC address of the hacker's device? 00:0c:29:1d:b3:b1
6. What negative impact might this type of attack have? The traffic is rerouted to the attackers device.

Part 2: DHCP Attacks

Continue in the same PCAP.

1. Filter by DHCP packets.
2. Review the packets captured, and explain in simple terms what is taking place. There are many DHCP requests asking for IPs.
3. What type of attack is this? DHCP starvation
4. Why is the destination IP `255.255.255.255` for all packets? This is a broadcast
5. What negative impact might this type of attack have? The server can run out of IPs for new devices resulting in a DoS attack.

Part 3: TCP Attacks

Continue in the same PCAP.

1. Filter by TCP packets.
2. Review the packets captured, and explain in simple terms what is taking place. There are many SYN requests to the various ports.
3. What type of attack is this? SYN scan
4. Is this type of activity always an attack? In other words, can a security professional benefit from what is taking place? Yes an analyst can use these to determine if any ports need to be closed.
5. What negative impact might this type of attack have? They gather intel to determine if there are any vulnerabilities in the open ports.

Part 4: Wireless Attacks

Answer the following questions:

1. What are the different security types available for wireless communications? List them in order from least to most secure. WEP, WPA1, WPA2, WPA3
2. What is 802.11? Wireless network standard
3. What is an SSID? Service set identifier. Name of the network
4. What is the name of the signal a WAP sends out identifying its SSID? Beacon
5. If a user has WEP-encrypted wireless, what is a potential negative outcome? An attacker can easily decrypt the traffic to steal sensitive data.

Part 5: Email Attacks

Open email_reviews.pdf.

1. Review the two emails and their headers and determine if the emails are legitimate or spoofed.
2. Document your findings and summarize why you believe the emails are legitimate or spoofed.

The first email is likely legitimate. The names match, the SPF passed, the IP matches the record on arin.

The second email is likely not legitimate. The names do not match, the SPF failed, the IP is not associated with Fedex.