CSCI 530: Security Systems
Lab 8: Intrusion Detection; Submission Due: November 22, 2024.

Name: Anne Sai Venkata Naga Saketh
USC Email: annes@usc.edu
USC ID: 3725520208

Question 1:

If node1 is a "man in the middle" then node4 is an "odd man out." In particular, node 4 was unaccounted for in section 3 "Recording actual address mappings." Later you arp poisoned node2 and node0 from node1; how about arp poisoning node 4 from node1? You accomplish poisoning by sending a crafted arp message to a node. Comment on the ways and means of poisoning node4 from node1.

Answer:

Implementing ARP poisoning between Node 1 and Node 4 presents a challenge due to their separation by a router (Node 0), as ARP requests are not permitted to cross subnet boundaries. Potential strategies for overcoming this obstacle include:

- Spoofing crafted ARP packets to deceive the router into forwarding requests to directly target Node 4 or simulating a scenario where Node 4 and Node 1 are on the same subnet.
- Poisoning the router's ARP cache to associate Node 4's IP address with Node 1's MAC address.

Cross-subnet ARP poisoning is inherently challenging due to the inherent blocking of ARP propagation by routers.

Question 2:

Answer the question at the end of section 6. Under the circumstances of that section, "How does traffic between node2 and node0 get from node2 to node0?"

Answer:

Since ARP spoofing is being employed to intercept traffic between nodes 2 and 0 using Ettercap, when node 2 (10.1.1.2) transmits a ping to node 0 (10.1.1.6), the initial communication appears normal. Executing the command tshark -c 4 -i enp0s3 icmp reveals a conventional request-reply pattern between the two nodes. However, since Ettercap positions node 1 (10.1.1.1) as a man-in-the-middle, the actual traffic flow discloses that the ping request initially traverses node 2 to node 1, which subsequently forwards it to node 0.

Upon receiving the response from node 0, the response is initially directed to node 1, which subsequently relays it back to node 2. Utilizing the command tshark -c 4 -i enp0s3 -T fields -e eth.src -e eth.dst -E header=yes icmp, we can observe that the hardware addresses indicate node 1's involvement. This transpires because both nodes 0 and 2 have been ARP poisoned, resulting in node 1's MAC address being associated with the

other's IP address. Consequently, all traffic between nodes 2 and 0 traverses' node 1, granting it the capability to monitor and manipulate the communication.

Question 3:

Answer the question at the end of section 7, "How?" Recall that node2 logged into ftp on node4 and somehow node1 figured out the user password given by node2. How?

Answer:

In the experiment, Node 2 successfully logged into an FTP server hosted on Node 4. Node 1 was able to decipher the user password provided by Node 2 due to Node 2 being ARP poisoned by Node 1. Utilizing ARP spoofing, Node 1 inserted itself into the communication path between Node 2 and Node 4, effectively executing a man-in-the-middle attack.

The tool Ettercap was configured with the command: ettercap -i eth0 -Tq -M arp:remote /10.1.1.2// /10.1.1.6//

This enabled Node 1 to intercept and monitor the traffic between Node 2 and Node 4. When Node 2 entered the FTP login credentials to access Node 4, the information was transmitted over the network in plaintext, as FTP does not encrypt communication, including usernames and passwords.

Consequently, Node 1, running Ettercap, captured and displayed the intercepted credentials in its output. The absence of encryption in FTP traffic facilitated Node 1's extraction of sensitive information, such as the username and password entered by Node 2 during the login process.

Question 4:

Imagine you run a web hosting company. The manager at one of your clients, a medium sized business, calls you in alarm and reports the apparent defacement of his website running on your host machine. Images on the site have all been replaced with various hacker images like the laughing skull. He heard about it from several of his employees, then saw it with his own eyes on their terminals. His website has fallen victim to the same mischief as the one on our node4. What is your course of action?

Answer:

In response to the defacement incident, the following actions would be taken

- Implement temporary site downtime or relocate the hosting to an alternative network to mitigate potential disruptions.
- Restart routers and switches to clear ARP caches and disrupt any ongoing spoofing attempts.
- Enhance network security by deploying intrusion detection systems and implementing static ARP usage to prevent future spoofing incidents.
- Enable HTTPS to encrypt website communication and enhance security.

- Conduct a comprehensive security audit to identify and address vulnerabilities, including outdated software and inadequate access controls.
- Perform a post-incident analysis to pinpoint the source of the attack and implement targeted preventive measures.
- Informing the clients about the security best practices