**CIS 8088 Project**

**By:**

**Swati M. Radia**

**Jeremiah Warren**

**Kaustuv Dutta**

**Zaki Khan**

Graphical user interface

Description automatically generated

***Table of Contents***

[**Problem Description** 3](#_Toc116129464)

[**Network Diagram** 4](#_Toc116129465)

[**System Configuration** 4](#_Toc116129466)

[**Establishing A Connection** 5](#_Toc116129467)

[**Attacks** 6](#_Toc116129468)

[**Intrusion Detection** 11](#_Toc116129469)

[**Our Thoughts** 13](#_Toc116129470)

[**References** 15](#_Toc116129471)

# 

# **Problem Description**

After evaluating several attacks, we decided to demonstrate network enumeration, a man-in-the middle attack, a syn flood attack, and a backdoor attack. We thought it would be important to demonstrate and understand network enumeration, because hackers use network scans to identify their targets and to detect potential vulnerabilities. We thought network enumeration would help us grow more comfortable with Nmap scans and to learn how to better interpret the results. We chose ARP spoofing as our man-in-the-middle attack to illustrate the ease in which this protocol can be exploited by malicious actors. Additionally, our group wanted to be able to observe the corrupted network traffic generated by this attack in Wireshark. Through a syn flood attack, we hoped to learn more about denial-of-service attacks and to observe the incomplete three-way handshake in Wireshark. For the backdoor attack, we wanted to exploit vulnerable software and to access private files. Finally, we wanted to learn if our attacks would create any alerts in our Intrusion Detection System or if they would go undetected.

# **Network Diagram**

**A picture containing diagram

Description automatically generated**

# **System Configuration**

Our group chose the Windows 10 virtual machine as our client machine. For our server, we chose the Metasploitable 2 Machine. We decided to use the Kali 2019 machine as our attacker. After we set up Security Onion, we chose the Squert web interface as our Intrusion Detection System. Squert is used to better visualize IDS (Intrusion Detection System) alerts from the Sguil database.

# **Establishing A Connection**

To establish a connection between the host and server, our group decided to use the ping command. From the Windows 10 machine, we pinged the Metasploitable 2 machine with IP address 192.168.64.145. Our packets were sent and received with no loss. We performed the same process in the Metasploitable machine, pinging the Windows 10 machine IP address of 192.168.64.137. This was also successful. In our attacking Kali 2019 machine, we successfully pinged both the Windows 10 machine and the Metasploitable 2 machine. Now that we have established a connection between all our machines, we are ready to begin our attacks.

# **Attacks**

**1. Enumeration – Identification of Target & Reconnaissance**

We began this phase of the attack by discovering our IP address through the ifconfig utility. On the Kali 2019 terminal, we ran ifconfig -a, which displays all our network interfaces. In this case, our Kali 2019 machine had an IP address of 192.168.64.138. Now that we have this information, we are ready to discover all the hosts on our subnet.

For network enumeration, our group decided to use Zenmap, the graphical user interface for network scanner Nmap. We found the GUI made it easier to classify hosts and to visually map our network. After launching the program by typing Zenmap into the Kali terminal, we needed to supply Zenmap with a target. We entered our previously discovered IP address and then added /24, which searches all 256 IP addresses on our subnet. The last step before beginning our network scan is to decide how we want to scan the network. On our initial scan, we added parameters to treat all hosts as online, to search the top 1,000 ports, and to enable operating system discovery.

Our scan discovered eleven hosts on our subnet. Several of these hosts had open ports, including one host with twenty-three open ports. To execute the additional phases of our attack, we needed to understand which version of the service was running on each open port, so we ran a service scan targeting all hosts. Armed with this information, we were ready to begin the next phase of our operation.

**2. Man-in-the-Middle Attack – Intrusion**

Address Resolution Protocol (ARP) is used to discover MAC addresses and map them to associated IP addresses. In a Man-in-the-Middle attack, the attacker sends specifically crafted ARP messages to the victim machine pretending to be the default server or a gateway. The idea is to poison the victim's ARP cache and trick it into listing the hacker’s address as the web server or default gateway. So, the host places the MAC address of the web server or default gateway with the MAC address of the hacker machine. Now, when the victim machine wants to send a message to the web server/default gateway, it looks up its ARP cache and sends the message. But now the message goes to the attacker machine since the MAC address listed is that of the attacker machine. The hacker can snoop and sniff the messages before sending it to the actual destination.

To proceed with the Man-in-the-Middle attack, we got the IP address of the victim machine. Here we targeted Metasploitable 2 and Windows 10 machines. We began the attack by running a Nmap scan on the Kali 2019 machine, which we are using as the attacker. After running the Nmap scan, we knew the IP address and MAC address of the victim machines. We ran the following command in Nmap: nmap-T4-A-v.

To perform an ARP snooping attack, we used the tool Ettercap. We launched the tool by typing in ettercap -G in our Kali terminal. The GUI of Ettercap opened, and we set the network interface to eth0. Then we listed all the hosts, by clicking on the Hosts option on the menu bar and then clicked on Host list. We found the Metasploitable-2 and Windows 10 IP addresses and added them to Target 1 and Target 2, respectively.

Once our targets were added, we began the ARP poisoning by selecting the ARP poisoning option under Mitm (Man-in-the-Middle) menu on the menu bar. After this was done, we saw that on the bottom screen of Ettercap the ARP poisoning was running. We ran Wireshark on the attacker machine to see that ARP traffic. By expanding the ARP protocol section, we saw that the IP addresses of both victim machines had the attacker machine's MAC address.

To check if any messages sent between the two machines were first sent to the attacker machine, we sent a ping ICMP echo request from Windows 10 to Metasploitable 2. Checking the ICMP traffic on Wireshark, we saw that the MAC address of the attacker machine was also listed as the destination. Therefore, our ARP poisoning was successful.

**3. Syn Flood – Doing Damage**

TCP uses the 3-way handshake mechanism to establish a connection. The client and server machine send synchronization and acknowledgment messages to establish a connection before beginning communication. The client who wants to initiate a connection sends an SYN message and waits for the server to respond. The server receives the SYN message and sends back the SYN+ACK message. The client receives this message and responds with an ACK message. This way the two machines establish a connection.

The connection is established only when these 3 steps are completed. In a SYN flood attack, the attacker machine only sends SYN message and does not respond back after receiving a SYN+ACK message. The server keeps waiting for the ACK message and waits for a certain period before the timeout. When the attacker machine sends SYN messages in a series the victim machine becomes overwhelmed and uses all its resources to wait for ACK message which it never receives back. This results in DOS attack (Denial of service).

We used Kali 2019 as the attacker machine and Metasploitable 2 as the victim machine. We began by consulting the Nmap scan of the Metasploitable 2 machine. The result helped us to find all the open ports available on the victim machine. We picked port 22, the SSH port. On the Kali terminal, we started the postgresql service database to run in the background. We ran the msfconsole command, and after the Metasploit framework launched, we searched for syn flood. We located the syn flood exploit in Metasploit. We entered use and then the path for the command we found in Metasploit to select this attack. Once this was completed, we used the show options command to check what values were set for RPORT and RHOST. We set the RHOST and RPORT to the Metasploitable 2 machine’s IP address and the open port 22. Once these values were set, we ran the exploit command.

In Wireshark, we noted that our attacking machine was continuously sending SYN packets to our victim machine, and the victim machine was responding back with SYN+ACK packets. However, we did not see any ACK packets being sent from our attacker to the victim, confirming that we had successfully conducted a syn flood attack.

**Enhancement**

**1.** **VSFTPD 2.3.4 Backdoor – Intrusion & Doing Damage**

After running the service and version network scan, we needed to decide on our target and our method of attack. We decided to target the host with twenty-three open ports (IP address of 192.168.64.145), and we determined the File Transfer Port (FTP) on this host looked vulnerable. Since we knew which version of the service was being used on this port, we needed to locate an exploit for this specific version.

Using the searchsploit command on our Kali machine to search Kali’s exploit database, we located a backdoor command execution for VSFTPD v2.3.4. Digging into the history of this exploit a little more, we learned that a backdoor which opens a shell on port 6200 was added to the VSFTPD download archive between June 30th and July 1st of 2011. It was removed two days later. This outdated VSFTPD version made our target vulnerable, and now we knew how to exploit this vulnerability.

Before beginning our attack, we had to make sure we could reach our target on our attacking machine. We pinged our target and successfully transmitted and received the set number of packets. Next, we ran the traceroute command to ensure that we were only one hop away from our target. Both tests were successful.

Having established a connection with our target, we launched the Metasploit framework console from our Kali terminal. We searched for the previously identified VSTFPD exploit in the system and chose this exploit as the exploit we were going to use. Then we set the RHOSTS to our target IP address. We utilized the show options command to check that we had the exploit configured correctly. Now we are ready to begin our intrusion.

We typed execute into the Kali terminal, and Metasploit began its attack. Success! We were able to create the backdoor service and a command shell session was launched. To confirm that we were in the target directory, we used the list command to list all files and directories. Then we used the print working directory command to ensure that we were in the root directory. Finally, we used the whoami command to confirm that we were logged in as root. All searches were successful. Inside the system we accessed the secret files folder in the root directory.

# **Intrusion Detection**

For each of our attacks, we observed event data through Squert and network traffic through Wireshark when appropriate. Below is a summary of our observations.

*Establishing A Connection*

In this phase of our operation, we used the ping command to send ICMP echo requests to several hosts on our network. The ping commands generated an ICMP Info Ping notification in Squert, and we were able to see the source IP and the destination IP for the request. In Wireshark, we captured the ICMP echo requests and were able to observe the source and destination of these requests.

*Network Enumeration*

After running our scans on Nmap, we returned to Squert to see if our IDS picked up our activities. For the first scan, Squert created notifications for an Nmap OS Detection Probe and located suspicious activity around several ports. The service scan generated notifications for an Nmap Scripting Agent and additional suspicious inbound and outbound activity on several ports.

*Man-in-the-Middle*

Interestingly, this attack did not generate any notifications in our IDS. This makes sense, as our IDS system was only configured to observe behavior at Level 3 and higher. Since ARP-Spoofing is a Level 2 attack, our intrusion detection system would not be able to detect this form of attack. As previously mentioned, we used Wireshark to observe that the MAC addresses of our victims were changed to the MAC address of our attacker.

*Syn Flood*

This attack produced potential SSH scan notifications in Squert. It discovered that our syn flood attack was targeting the SSH port on the Metasploitable machine, but it did not notify us that we were under a DOS attack. Therefore, we used Wireshark to better observe the network traffic created by this attack. As previously mentioned, we were able to observe the attacking machine sending SYN packets, the victim machine responding with SYN+ACK, and the attacking machine failing to respond with an ACK message to complete the three-way handshake.

*VSFTPD 2.3.4 Backdoor*

During this attack, the IDS system alerted us that a backdoor exploit for VSFTPD was used. Under this alert, it showed us that a backdoor was created after logging in with a smiley face. It also created an alert that the attacker had logged into our Metasploitable machine as root.

# **Our Thoughts**

Implementing different attacks and trying to search through different websites and YouTube videos really helped us to learn a lot more. We learned how vulnerabilities or loopholes in the system can be used to attack the system. Having ports open on any system makes it very susceptible to attacks. It’s important to make sure that unnecessary ports need to be closed and very common ports like FTP or SSH which are assigned to ports 21 and 22 respectively can be set to different ports to make it a bit difficult or the attacker. Updating the system and having good antivirus that has a firewall, and IDS are also crucial in keeping the system safe from any sort of attacks.

While trying to perform attacks on Windows 10 system we faced difficulties as the system wasn’t responding to ping commands from any other machine. After doing a bit of research, we found that it was because of the firewall in place, which was trying to keep the system secure. We then turned off the firewall from settings and were then able to perform attacks. This was a good learning experience.

The virtual environment setup was good and helped us learn about the different operating systems and their features. The only disadvantage was that it wasn’t connected to the internet. This limited us to performing only a certain set of attacks, as few of the other attacks we researched needed pulling the latest patches. Overall, the setup seems well structured to learn and perform attacks.

Next time, we would like to conduct more sophisticated attacks. We want to explore new attack vectors, which will help us learn more about system vulnerabilities and how they can be protected. Performing more complicated attacks will allow us to learn more about networks, operating systems, and network devices. During our attacks, we want to learn how to do more damage so we can truly simulate the experience of being a hacker. Overall, this experience provided us with a solid foundation of network security and hacking, and we hope to continue to build on it in the future.

# 

# **References**

**Network Enumeration -** [**https://www.youtube.com/watch?v=Xfh5a6fRsD4**](https://www.youtube.com/watch?v=Xfh5a6fRsD4)

**ARP Spoofing -** [**https://openmaniak.com/ettercap\_arp.php**](https://openmaniak.com/ettercap_arp.php)

**SYN Flood -** [**https://www.youtube.com/watch?v=7bHQtpcfZ8U**](https://www.youtube.com/watch?v=7bHQtpcfZ8U)

**Windows 10 Firewall turning on/off -** [**https://www.youtube.com/watch?v=dlBgoVMXIWo**](https://www.youtube.com/watch?v=dlBgoVMXIWo)

**VSFTPD Backdoor -** [**https://www.youtube.com/watch?v=YriYszGRCaI**](https://www.youtube.com/watch?v=YriYszGRCaI)