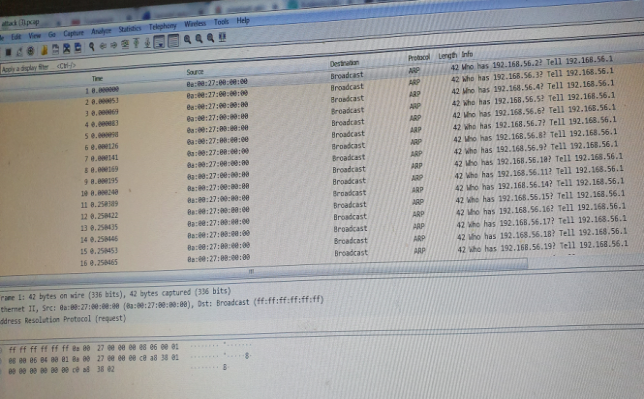
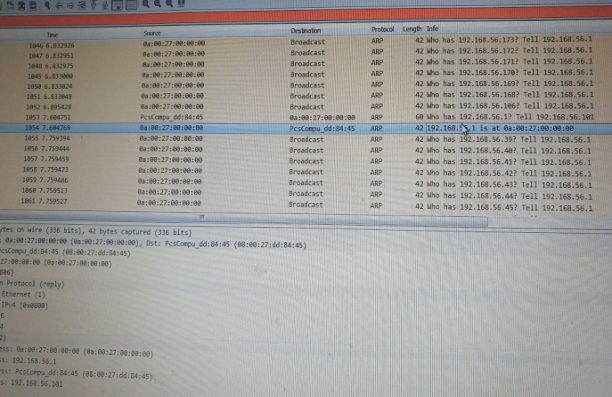
1. **How did the attacker find the vulnerability**

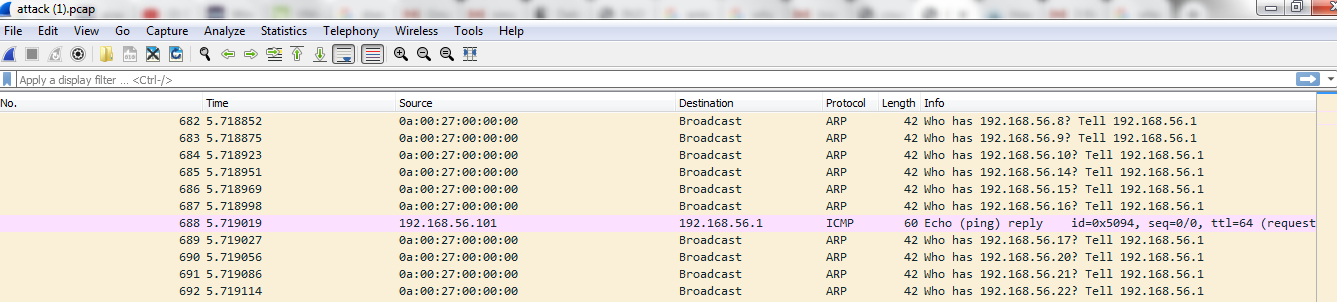
There were a variety of methods the attacker used to find the vulnerability some of the methods alongside the evidence have been indicated below. ARP stands for Address Resolution Protocol. When you try to ping an IP address on your local network, say 192.168.1.1, your system has to turn the IP address 192.168.1.1 into a MAC address. This involves using ARP to resolve the address, hence its name.

Systems keep an ARP look-up table where they store information about what IP addresses are associated with what MAC addresses. When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address. If there is a value cached, ARP is not used.

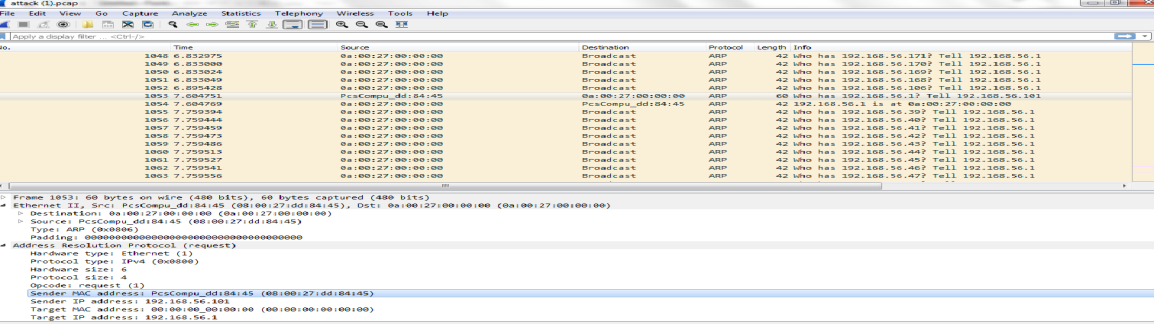
If the IP address is not found in the ARP table, the system will then send a broadcast packet to the network using the ARP protocol to ask "who has 192.168.1.1". Because it is a broadcast packet, it is sent to a special MAC address that causes all machines on the network to receive it. Any machine with the requested IP address will reply with an ARP packet that says e.g. "I am 192.168.1.1", and this includes the MAC address which can receive packets for that IP.

**Arp Broadcast / Storm**

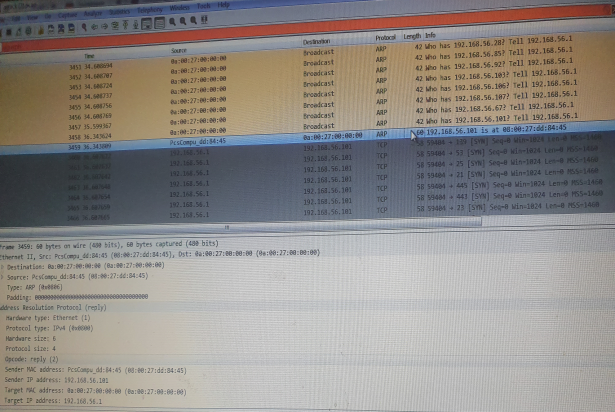
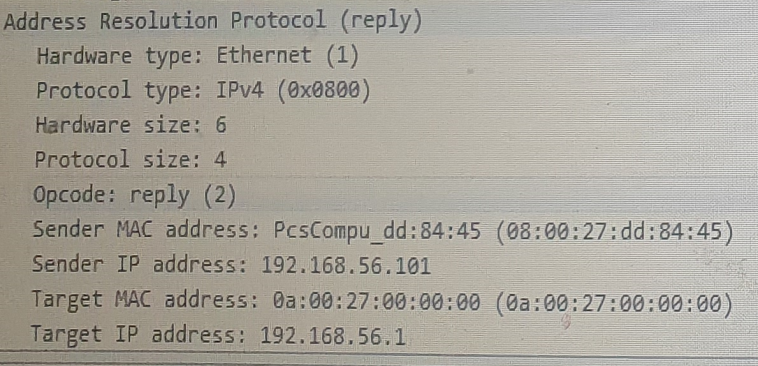
After careful analysing attack.pcap file, in order to find out vulnerability, the attacker having IP Address 192.168.56.1 has sent the ARP Broadcast packet to the whole network/subnet of 192.168.56.0 (all of hosts)so that intruder get the MAC address of the victim and by asking if this is his IP address, then the responder will reply with his respective MAC Address. In our case the responder 192.168.56.101 recognizes as its own IP and sends an ARP Reply back to the attacker. Attacker is sending more than 40 Arp requests per second. The purpose of sending ARP broadcast to potentially active hosts is to find out their Mac address (es) of the victim because it has a packet of data to deliver and to proceed with the conversation. In the below example sender sends a lot of broadcast which may cause the congestion in the network.

**Figure 1 (Broadcast Request of Mac) Figure 2** **( ARP Reply)**

**192.168.56.101 is replying back to the 192.168.56.1**



**Figure 3 ( ARP Reply ) it sends the Mac Address**

****

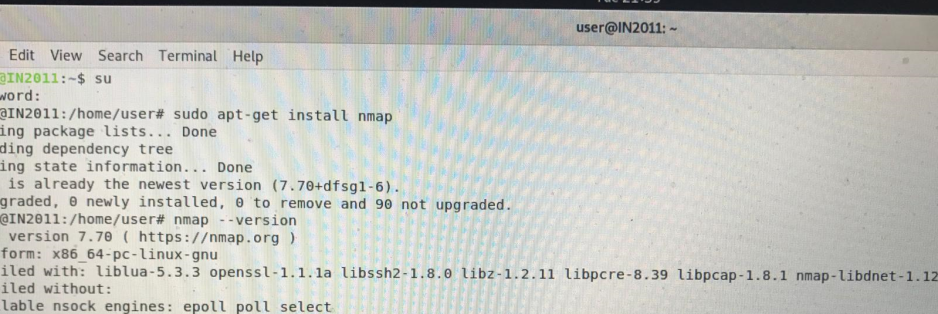
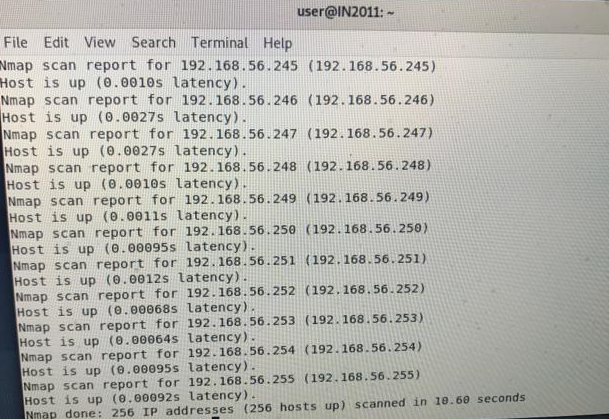
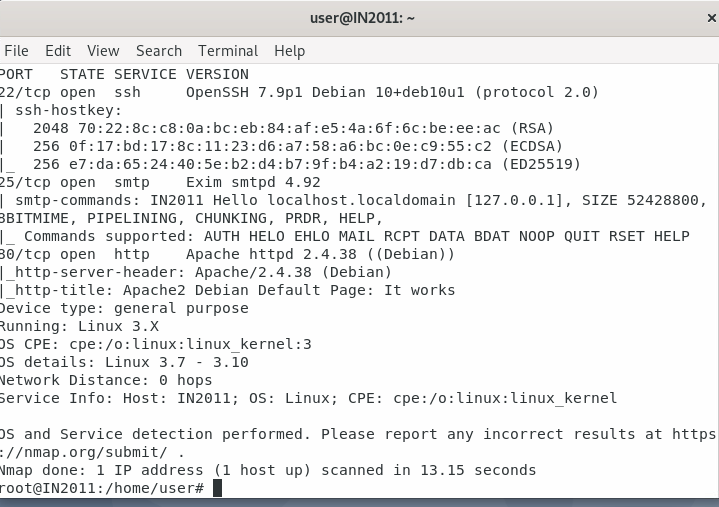
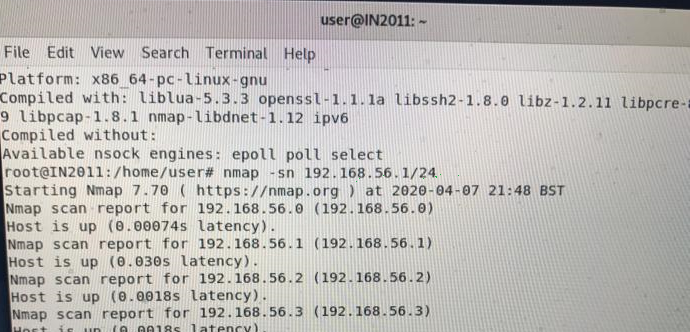
**In Figure 3 Explanation:-** In reply to the Broadcast messages sent to PcsCompu\_dd:84:85, PcsCompu\_dd:84:85 has displayed its mac address as 08:00:27: dd: 84:45 to Target IP address: 192.168.56.1 . So **In Packet 1053 ,1054** ARP spoofing and getting the Mac address of 192.168.56.101 is happening

**2) How did they exploit the vulnerability to gain access?**

**1:- NMAP Port Scanning**

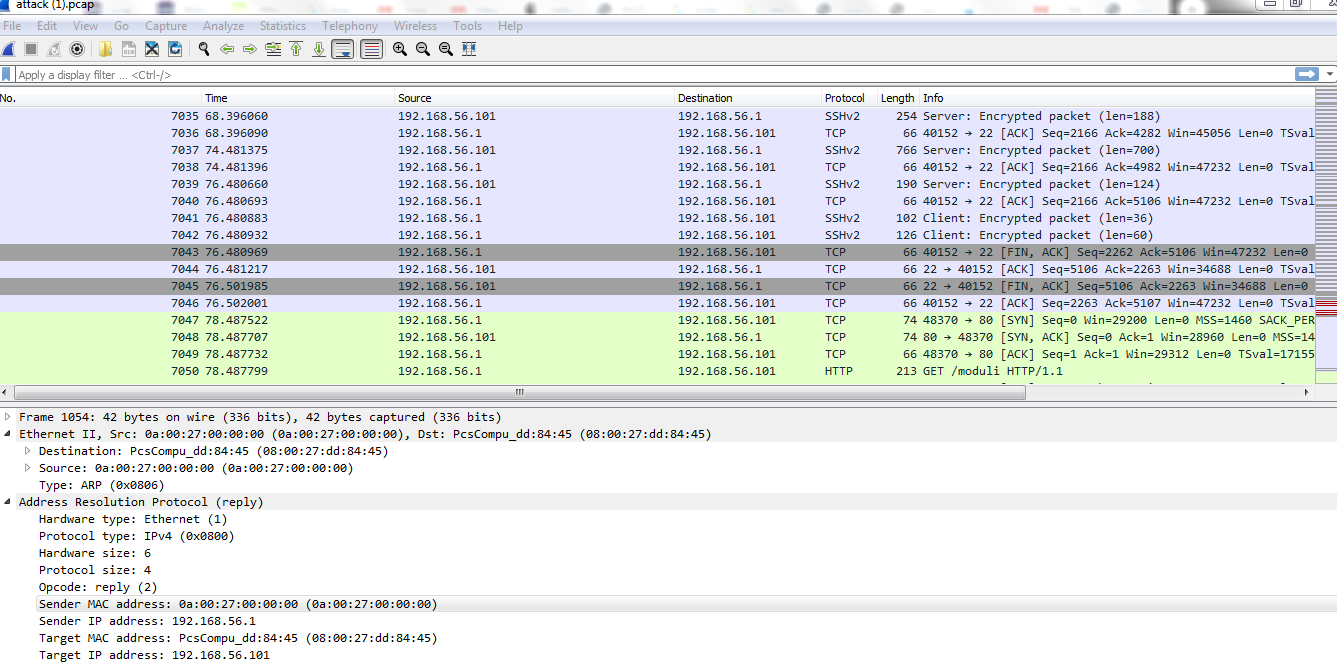
A **port scan** is a technique used in finding which ports on a network are open. As ports on a computer are the place where information is sent and received, port scanning can be compared to knocking on doors to see if someone is home. Running a port scan on a network or server reveals which ports are open and listening (receiving information), as well as revealing the presence of security devices such as firewalls that are present between the sender and the target. This technique is known as fingerprinting. It is also valuable for testing network security and the strength of the system’s firewall. Due to this functionality, it is also a popular reconnaissance tool for attackers seeking a weak point of access to break into a computer.

Attacker exploits the vulnerabilities and easily gains access once attacker is known to the Open Ports. Open ports are ports that are set up to accept arriving TCP connections. However, it can be quite dangerous to have too many **open ports** on your computer because these **ports** can easily be detected, and if found these **ports** are now open to vulnerabilities to third parties/attackers. Using the NMAP software on the Debian operating system (Linux 3.7) we’ve deduced using port scan hat ports 80 and 25 were open and thus can be exploited remotely by a hacker with malicious intent.

******It opens up the 256 hosts along IP’s**

**Figure shows lists of IP addresses ( Hosts) are up** **Figure shows root login pass** **&version**

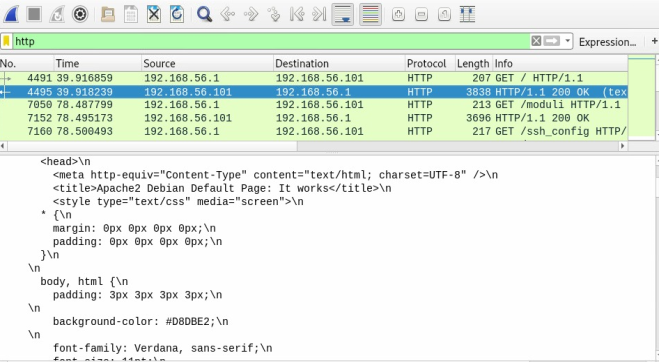
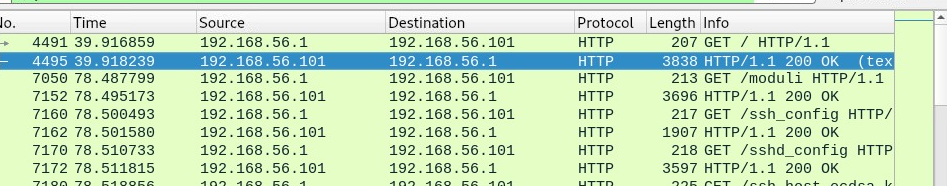
**Break into the SSH**



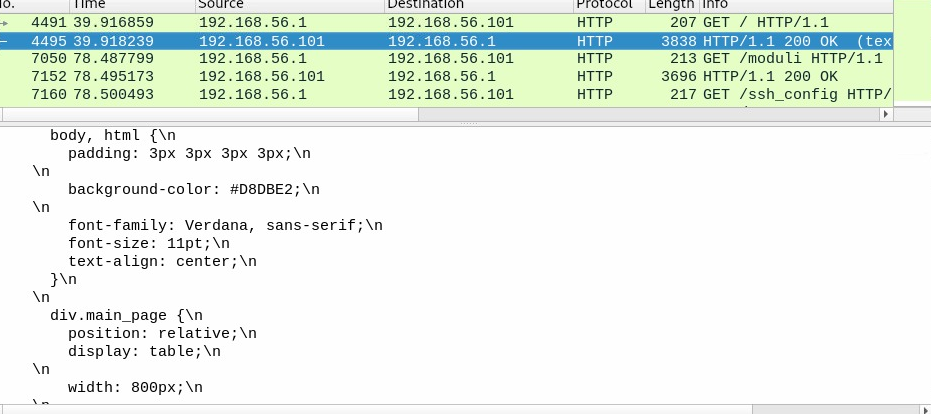
**Evidence**

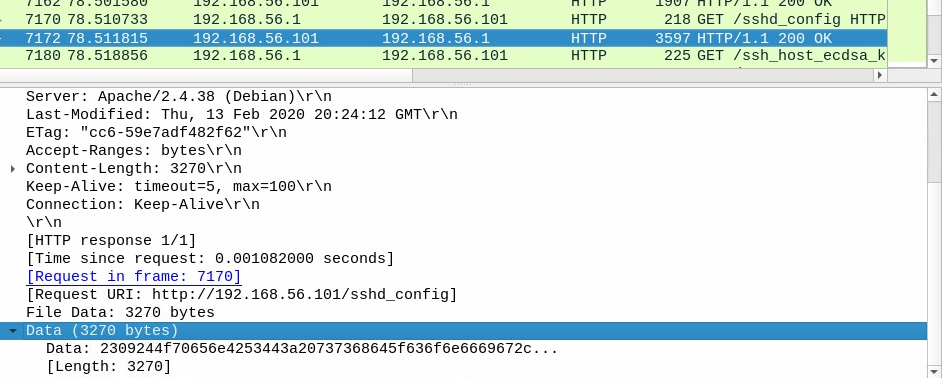
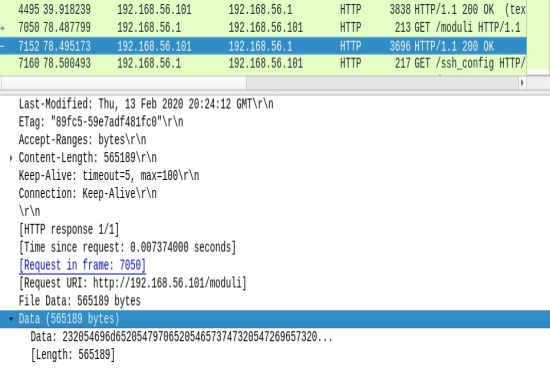
One of the vulnerability that attacker finds is the weak passwords and also the open ports while port scanning. Attackers breaks into the SSH. Evidence in the Wireshark is the blue colour traffic (SSH packets) just before the last green colour traffic (TCP Packets.) . It can be evident from all the conversation /communication with the random ports and ports 22. The main method in which the passwords were found can be explained by a method known as brute force attack and the type of brute force attack that was used a dictionary attack. There are a few methods of performing an SSH brute-force attack that will ultimately lead to the discovery of valid login credentials. A password dictionary attack is a brute-force hacking method used to break into a password-protected computer or server by systematically entering every word in a dictionary as a password. This attack method can also be employed as a means to find the key needed to decrypt encrypted files. While using words in the dictionary, as well as any derivatives of those words known as leetspeak (character replacement with alphanumeric and non-alphanumeric characters) is common, the dictionary in these types of attacks can also be a collection of previously leaked passwords or key phrases.

1. **What did they do once they had access?**

****

192.168.56.1 is trying to get the information of 192.168.56.101 and in reply 192.168.56.101 web site content is clearly reflected as in the content of the html code and CSS code that is visible and can easily be seen in the line based text data part of the Wireshark window . It is noted **that the file size was 10701 bytes altogether.**

In the picture HTML/CSS coding ( content ) of the page is clearly visible (white part).



After analysing 3096 HTTP/1.1 200 OK , it is evident from the above screen shot that File data has been changed to 565189 bytes now. Looking at 3597 HTTP/1.1 200 OK output, It is evident from the above screen shot that now that File data has been changed to 3270 bytes , so right after analysing every four packets the file size (payload) gets changed . It may be because of the files have been moved.

1. **Solution to protect the network from Hackers**

In order to prevent network/System from attacker to do port scanning is to implement a good firewall and intrusion prevention system (IPS) in the network. The main purpose of the firewall use in the network to block unwanted and unauthorized traffic and to filter out the traffic. However the purpose of the IPS implemented in the network is to provide solution so that IPS can detect the viruses signatures or attack by its signature and consequently alert system/network administrator there and then. The reality is that if you have a server facing the internet, there are going to be loads of SSH brute-force attempts daily, many of which are [automated](https://null-byte.wonderhowto.com/how-to/automate-brute-force-attacks-for-nmap-scans-0184132/). But don't fret, there are some simple solutions to help protect against this and cut down on the number of login attempts. Perhaps one of the easiest things to do is change the port number which SSH operates on. Although this will dissuade the most rudimentary brute-force attempts, it is trivial to scan for SSH running on alternate ports. How to Prevent an ARP Spoofing Attack: ARP spoofing attacks appear quite complex on the surface but the methods you can use to prevent them are actually quite simple. Using a combination of VPNs, anti ARP spoofing tools and packet filtering is key to keeping these attacks at bay: **Use a Virtual Private Network**(**VPN**) – Using a VPN will allow you to keep your traffic protected via encryption. This means that even if your network falls victim to ARP spoofing the attacker won’t be able to access any of your data because it has been encrypted. **Anti ARP Spoofing Tools**– You can also download an anti ARP spoofing tool. Anti ARP spoofing tools can help to detect and fight off incoming ARP attacks. Tools like ARP AntiSpoofer and shARP are two popular anti-spoofing tools. **Packet Filtering** – Packet filtering is used to filter incoming packets and prevent compromised packets from questionable sources. This means that if someone attempts to launch an ARP attack you will be able to fight it off.

Narrative- The narrative of the attack could be due to the attacker wanting to sell to third parties for profit. Moreover, they could have done the attack to alter important information for their own reasons. Lastly, another malicious reason for the attack could be related to blackmail by gaining access to sensitive information this can be used to get people to things they otherwise wouldn’t have.

# Bibliography

<https://www.tummy.com/articles/networking-basics-how-arp-works/>

<https://ritwiksharmaneo.blogspot.com/2017/07/performing-arp-attacks.html>

<https://www.coursehero.com/file/p6tkb5n/If-the-IP-address-is-not-found-in-the-ARP-table-the-system-will-then-send-a/>

<https://osqa-ask.wireshark.org/questions/8029/counting-incoming-tcp-open-http-get-requests-to-a-web-server>

<https://heimdalsecurity.com/blog/home-wireless-network-security/>