Amerigo Industries LLC Vulnerabiltiy Report

Jalen Powell

Auburn University

Cyber Security: Threats and Countermeasures

As a result of my vulnerability testing on Amerigo Industries, I have learned of many risks and threats to their network security. I will share the vulnerabilities in this report and show how said weakness can be exploited. My first step was to identify my targets inside the subnet. The total number of IP addresses was 4,096. Next, I ran a host scan over the entire subnet to find any active IP addresses out of the possible 4096 targets. The host scan came back with only three active IP addresses. Those IP addresses being 172.31.60.169, 172.31.60.216, 172.30.60.217, and 172.31.53.92.

***IP #1: 172.31.60.169***

Text

Description automatically generated

Figure : Nmap stealth scan(Without Ping)

While running Nmap scans on this network, I encountered the four open TCP ports of 135, 139, 445, 3389. Scanning each port individually did not give me the desired answers to what I was searching for. I started to look for other vulnerability scanners like Metasploit and Netcat. The choice I made was to download Nessus as my secondary scanner.

After configuring Nessus, I ran a basic scan, which took around four minutes, and it gave me 13 vulnerabilities. Twelve of the vulnerabilities were informative with facts about traceroutes and SYN scanners. The one other weakness was a mixture of medium and informational. The main vulnerability is the “SMB signing not required” which states that the remote SMB server does not require signing. This flaw allows a remote attacker to exploit this as a man-in-the-middle attacker.

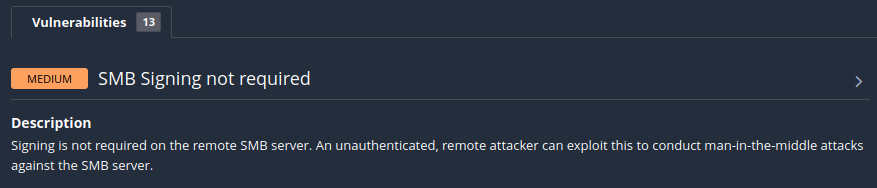


Figure : Nessus Basic Scan with medium weakness

Diagram

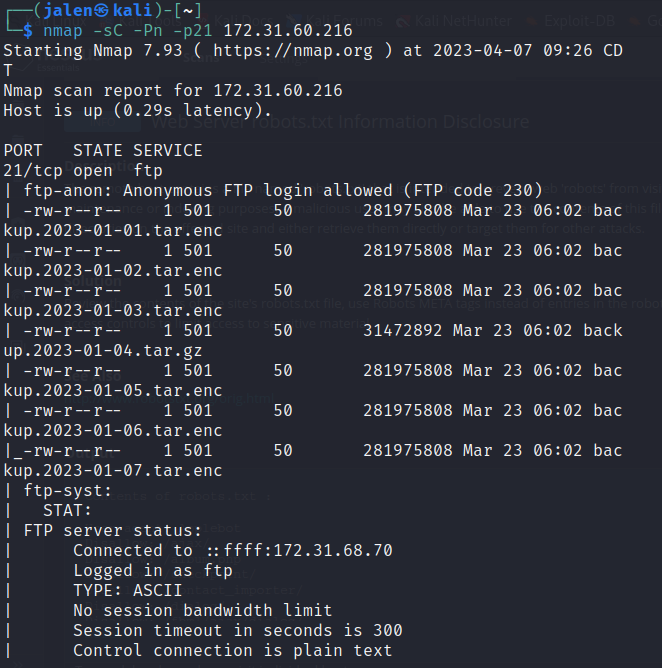
Description automatically generated

Figure : Man in the Middle image

A Man-in-the-Middle attack requires the attacker to place himself between two communicating parties and relaying messages for them, while the parties believe they are communicating with each other directly and securely.

A possible solution for this vulnerability would to be to enforce message signing in the host’s configuration. Policy options for Windows or Samba to show a message for signing.

***IP #2: 172.31.60.216***

Text

Description automatically generated

Figure 4: Nmap FTP port script scan Figure 5: FTP Anonymous Login and File Retrieval

Using Nmap on this IP address allowed me to see two open ports , one for ssh and one for ftp. FTP standing for File Transport Protocol allows files to transmit to other computers through a network. Most attackers can access these files quite easily with anonymous logins. The files in question are all tar files with only one being unencrypted.

Graphical user interface, text

Description automatically generated

Figure 6:Shadow file from Backup tar file

After opening the tar file, many encapsulated files flew down the screen. At the top of that list was two distinct files names. The shadow file and the security directory. The above image shows the inside of the shadow file. The many hashed passwords for users like “admin”, “alice”, and “dan” are all revealed. With the right tools, attackers can easily decrypt the hashes and use the passwords. The file below shows the “pwquality.conf” file which holds the password qualifications like “uppercase letters”or “more than 6 digits”. These signs can help attackers narrow down the possible number of passwords.

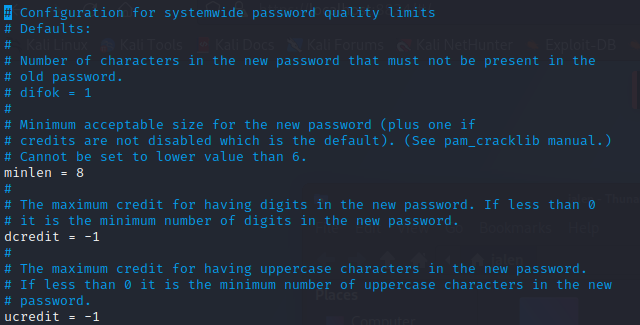


Figure : The pwquality.conf file

FTP can be in use by any company but it must be constantly checked and deactivated for when it is not being used. This will minimize the chances for attackers to gain access to this information.

***IP #3: 172.31.60.217***

After many Nmap scans and even a Nessus scan, I could not find any real vulnerablilities to show for. The host was up, but all the scanned ports were in ignored states

***IP #4: 172.31.53.92***

Text

Description automatically generatedText

Description automatically generated

On this IP address, there were TCP ports for HTTP that were open. Port 80 is shown to have a robots.txt file. That file is on to the right of the TCP scan figure up above. The Nessus vulnerability scans found only minor weakness. There is a web server on these ports is named Caddy. This is a remote server for the plugins to determine the type and version.

The robots.txt file can be dangerous in the wrong possession but are usually harmless. A malicious user can use the contents of the file to learn sensitive information on the affected site. A suggested solution would be to review the contents and adjust the access controls to limit viewing the material.

**Conclusion**

The number of vulnerabilities in the network of the Amerigo Industries is not world-ending. Most weakness live in the open ports of the active IP addresses. My task on this report was to view the surface-level vulnerabilities. These vulnerabilities have some very doable solutions if lessen or even eliminate the weaknesses. Amerigo should review and update their network to decrease ease of access as most of their IP addresses have ports accessible to almost anyone.