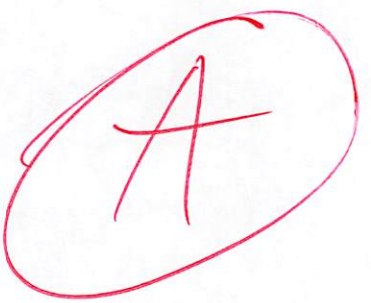
COMP5830 Midterm Report

Melvin Moreno



I. Introduction

We would like to express our gratitude to Amerigo Industries LLC for choosing our company to continue forward with your cybersecurity engagement. In this report we will outline the following: Vulnerabilities within the network, recommendations/controls to implement, and conclusive findings. We look forward to your review and feedback.

II. Vulnerabilities within the Network

1.1. TCP Connection Scan

Missed Win Server

A TCP connection scan conducts a three-way TCP handshake process to determine if ports are open or closed. When we conducted this scan on your network, we found the following:

```
┌──(mem0282㉿kali)-[~]
└─$ nmap -sT 172.31.48.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 12:46 CDT
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 0.37% done
Nmap scan report for 172.31.53.92
Host is up (0.052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE
80/tcp   open  http
8000/tcp open  http-alt
8080/tcp open  http-proxy

Nmap scan report for 172.31.60.216
Host is up (0.057s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap scan report for 172.31.63.217
Host is up (0.038s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE    SERVICE
22/tcp filtered ssh
23/tcp open     telnet

Nmap done: 4096 IP addresses (3 hosts up) scanned in 444.47 seconds
```

Why here if just going to explain immediately?

From this we can draw which ports are open and connect to them using a tool like netcat or perform a more comprehensive search on them using our penetration tools. One of the open ports that is worth investigating is 172.31.53.92 port 80 since it is an open HTTP webserver. We expand on this further in the report. 172.31.60.216 port 21 is also worth looking into as it is a file-transfer-protocol port. Finally, 172.31.63.217 port 23 telnet port is worth debriefing. We'll start by conducting a more in-depth search of the HTTP webserver.

1.2. Running a Dirbuster search

Dirbuster brute forces directories and file names on web/application servers. It will find different openings on a website. Here were our findings after running dirb on the open HTTP port on the IP 172.31.53.92.

Why not put in appendix?

```
┌──(mem0282㉿kali)-[~]
└─$ dirb http://172.31.53.92:80 /usr/share/dirb/wordlists/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Mar 28 15:20:07 2023
URL_BASE: http://172.31.53.92:80/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://172.31.53.92:80/ ----
+ http://172.31.53.92:80/api (CODE:308|SIZE:41)
+ http://172.31.53.92:80/index.html (CODE:200|SIZE:1342)
+ http://172.31.53.92:80/legal (CODE:308|SIZE:43)
+ http://172.31.53.92:80/resources (CODE:308|SIZE:47)
+ http://172.31.53.92:80/robots.txt (CODE:200|SIZE:20587)
+ http://172.31.53.92:80/specs (CODE:308|SIZE:43)

-----------------
END_TIME: Tue Mar 28 15:22:13 2023
DOWNLOADED: 4612 - FOUND: 6
```

We found the above websites open and navigable. We conducted a search on all of them and found *http://172.31.53.92:80/robots.txt* to be the most useful as it displays which websites disallow crawling traffic. This raises a red-flag for us to see which pages may have vulnerable and sensitive information. We were able to find one specifically that piqued our interests:

```
User-agent: THREATS-AND-COUNTERMEASURES-STUDENTS
Disallow: /webserver-backups/
```

From there we can infer that http://172.31.53.92/webserver-backups/ is something the web server does not want publicly accessible. We can also deduce that this contains a backup of your webserver. We navigated to the website and found encrypted backup files and one unencrypted file named **backup.2023-01-06.tar.gz.** We untarred this file and found a **password policy** file and a **shadow** file.

Vuln: Backups accessible
Vuln: Unencrypted backup
Vuln: Shadow ~~config~~ file accessible

1.3. Password Cracking

Given the password policy file and shadow file, it would be relatively easy for someone to perform password-cracking on the shadow file shown here:

```
admin:$y$j9T$d.2a4wTF4uoL2cqQbfS6g.$kP8Vimi2pFK8I687kI0GqnqPbBPV6VrSREqyCP4QTc7:19439:0:99999:7:::
alice:$y$j9T$g5nY.HyHD7XqlsX5qhrGk/$zUkRdY0Bkb7p9OjSG6NCPWODkzJUsu63879XX44lsE/:19439:0:99999:7:::
bob:$y$j9T$vDBbu9JC/BSYAWxtHE6jW.$ZID5ZfJyn5aVVC9OEWpXFOx.90GEUvCdRdi6pzgZEp.:19439:0:99999:7:::
charlie:$y$j9T$eIQqgmzA6sNdAQxJ2WclB0$z3YflfhORkMLZ6WvOJZ3tWNNyLYZOMv5w76zFR8BPkD:19439:0:99999:7:::
dan:$y$j9T$bnkz0s98SdMOIUD1y6tfd1$BvSWmOXTmGBrNgF5SrhNA6t7Th1yCWOgKXHpuXbB5l5:19439:0:99999:7:::
```

As we can see, users *admin, alice, bob, charlie,* and *dan* are all at risk. Tools like John the Ripper could utilize the information from the password policy to crack these hashed passwords. John the Ripper can take flags such as minimum/maximum password lengths which can be found in the password policy list. This raises the possibility of a potential hacker cracking their passwords relatively easily.

2.1. FTP Vulnerabilities

Moving on, we can look at vulnerabilities the FTP server mentioned earlier can pose. Host 172.31.60.216 has a running FTP server on port 21 that allows anonymous login. This raises multiple security concerns. Anonymous login means that anyone can access the server without having to provide any credentials. An attacker can then send arbitrary commands. This increases the risk of command injection attacks, where an attacker can inject malicious commands into the server and execute them with the privileges of the FTP server. The server also displays detailed information about itself and its capabilities which provides useful information to attackers trying to exploit the server.

```
┌──(mem0282㉿kali)-[~]
└─$ nc 172.31.60.216 21
220 (vsFTPd 3.0.5)
USER anonymous
331 Please specify the password.
PASS
230 Login successful.
pwd
257 "/" is the current directory
help
214-The following commands are recognized.
 ABOR ACCT ALLO APPE CDUP CWD  DELE EPRT EPSV FEAT HELP LIST MDTM MKD
 MODE NLST NOOP OPTS PASS PASV PORT PWD  QUIT REIN REST RETR RMD  RNFR
 RNTO SITE SIZE SMNT STAT STOR STOU STRU SYST TYPE USER XCUP XCWD XMKD
 XPWD XRMD
214 Help OK.
```

3.1 Outdated Software Vulnerabilities

It's worth noting that the server is running an old version of vsFTPd (version 3.0.5 shown above). Upon further research, we discovered there are no known vulnerabilities for this version of vsFTPd, but it is important to keep all server software up to date to mitigate the possibility of an attack. We ran a software version scan on the entire host address and came up with the

following results.

```
┌──(mem0282㉿kali)-[~]
└─$ nmap -sV 172.31.48.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-27 12:57 CDT
Nmap scan report for 172.31.53.92
Host is up (0.059s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Caddy httpd
8000/tcp open  http    Caddy httpd
8080/tcp open  http    Caddy httpd

Nmap scan report for 172.31.60.216
Host is up (0.065s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 172.31.63.217
Host is up (0.065s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE    SERVICE VERSION
22/tcp filtered ssh
23/tcp open     ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4096 IP addresses (3 hosts up) scanned in 178.76 seconds
```

What is outdated? You say vsFTPd but why?

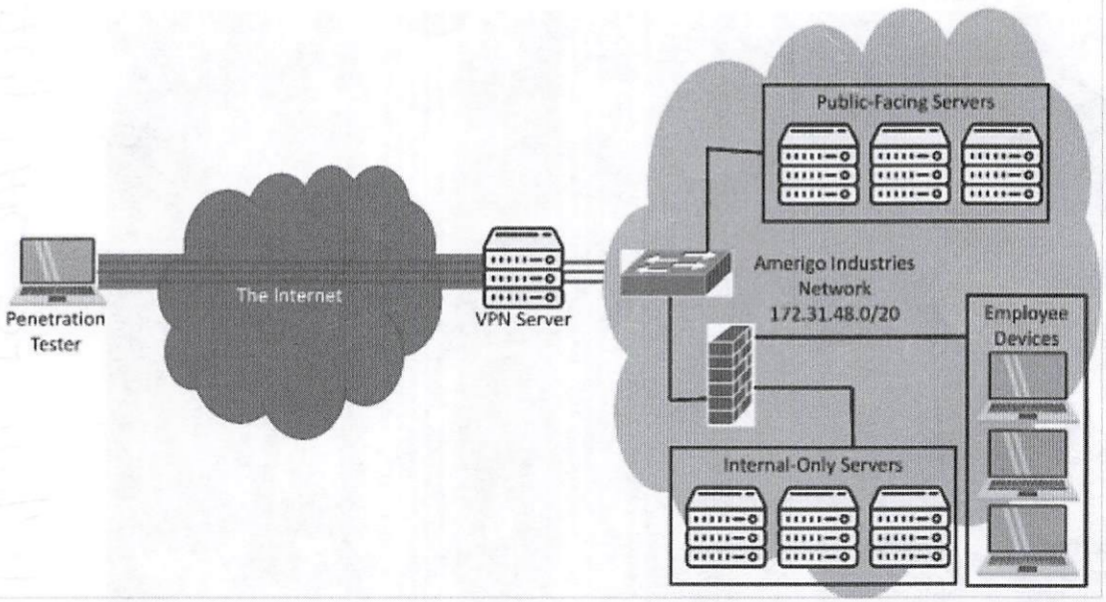
3.2 OpenSSH Software Version

We are able to determine that the ssh service is using OpenSSH version 8.9p1 and running on Ubuntu Linux. We were able to find various old vulnerabilities for this service, but none that are applicable to 8.9p1. We would still recommend reviewing the website *https://www.cvedetails.com/vulnerability-list/vendor_id-97/product_id-585/Openbsd-Openssh.html* for any new vulnerabilities that may appear. ← put in "references"

III. Recommendations/Controls to Implement

1. *Encryption:* Within the webserver-backups directory there is an unencrypted backup file called **backup.2023-01-06.tar.gz.** We recommend reviewing all files on your web server and encrypting all files that contain crucial and sensitive information. why share at all?
2. *Disallowing Anonymous Login within FTP:* Your FTP server allows for anonymous login. This is a security vulnerability as it allows anyone to log-in and perform potentially malicious activities. Creating an authentication process like a username/password login would allow your company to maintain an audit log of all processes committed with this work environment.
3. *Maintaining Software:* Software vulnerabilities are constantly being found and reported on different applications. We recommend periodically updating all of your software to mitigate the risk of these vulnerabilities.
4. *Revaluation of Network Architecture:* After reviewing the network architecture you provided us, we have determined there is a need to review it as such. Below is the diagram we have been provided.

"your documentation is wrong"



In the above diagram there is a firewall in the WAN-to-LAN domain. We found none and were able to enter into your internal-only servers. We recommend implementing firewalls and other intrusion detection systems to help prevent unallowed actors from entering your system.

awkward phrasing

IV. Conclusion

We would once again like to thank Amerigo Industries LLC for accepting our contract to perform the initial network test. We look forward to your review and feedback. If there are any more comprehensive or in-depth tests that Amerigo Industries would like us to conduct, we would be more than happy to work with you again in the future.

- Missed Windows server entirely
- Only 1 cite/reference

Best Regards,

Melvin Moreno
Auburn University '23
Computer Science | ISMN
(256) 324-9491 | mem0282@auburn.edu