Penetration Test Report

Pegasus Technical Services

March 24, 2022

Executive Summary

Background

Nicolas Meneses was contracted by Pegasus Technical Services to conduct a black-box penetration test on their new system to determine its exposure to an external attack from the internet. All activities were conducted in a manner that simulated a malicious actor engaged in a target attack against Pegasus Technical Services.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to organizational data. The attacks were conducted with the level of access that a general Internet user would have.

Overall Posture

Lack of password complexity rules and predictable usernames to log into the system are systemic issues. Some of the users with access to the system hold weak passwords that can be easily cracked via a brute force attack. Furthermore, information exposed on Pegasus Technical Service's website about employees could allow an attacker to easily guess login usernames. As a result of this, I was able to break into the system using one of the team members' accounts. In a real case scenario, an attacker could take advantage of these weak username and password combinations to get access to the system. Once inside, the attacker gets confidential information about the business's clients and employees. Additionally, this puts at risk the integrity and availability of the organization as information could be modified, or the services could be put down.

General Findings

1) Via Pegasus Technical Service's website, I was able to guess the username structure for all users (First initial + last name) by attempting to log in with probable combinations and weak passwords. As a result, I was able to get William Barker's credentials. Once in the system, I had access to all the usernames which allowed me to conduct further brute force attacks on the administrator's (Gregory Duffel) account. This led me to find the log-in information for the system administrator. Once in the administrator account, I had access to further information about the existing accounts which allowed me to also find the password for the webmaster user account.

2) The version of JQuery hosted on the remote web server is affected by multiple cross-site scripting vulnerabilities.

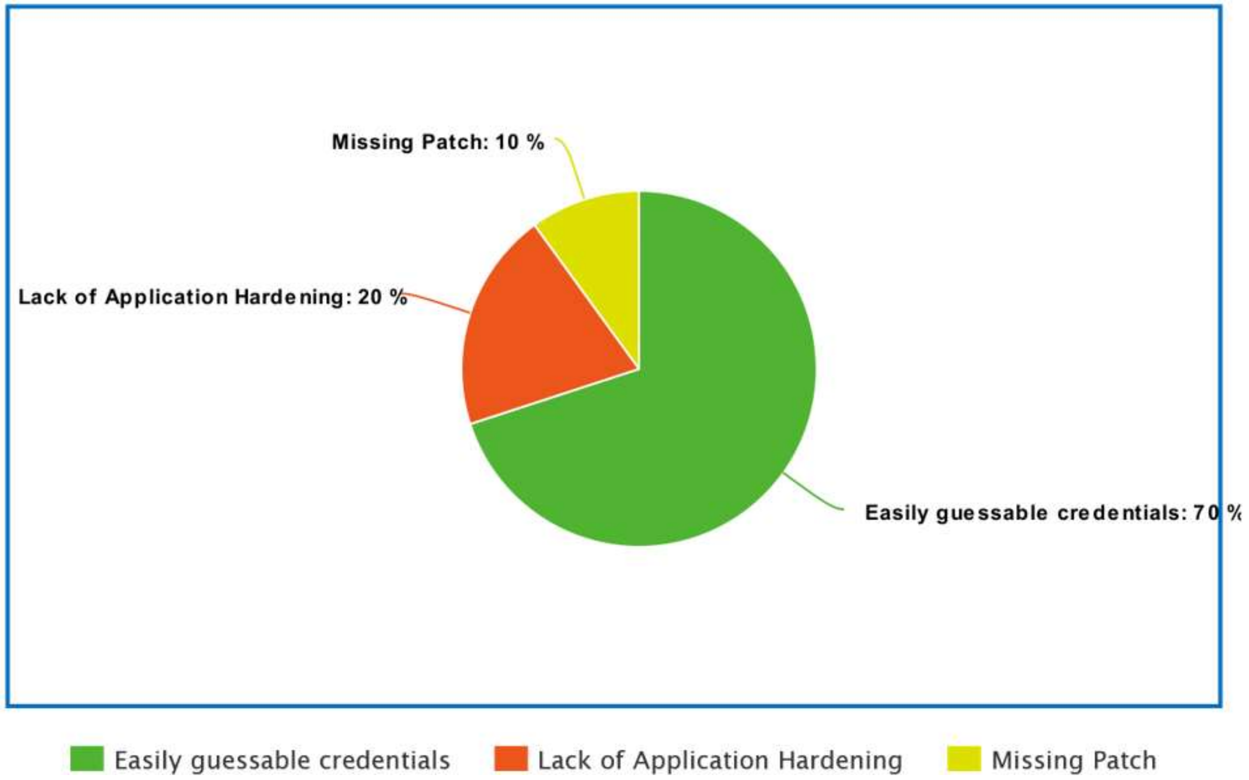
3) The version of the webserver (apache.2.4.25) has two common vulnerabilities and exposures with a risk score of 7.5.

4) The version of the SSH protocol (OpenSSH 7.4) has a low-risk bug that was fixed in version 7.6.

5) The version of the FTP protocol (vsftpd 3.0.3) is vulnerable to a Remote Denial of Service.

6) The system allows unlimited remote log in attempts into their services which let attackers to brute force credentials.

Security Risk Origin



Overall Risk Score

Damage Potential: 10

Reproducibility: 7

Exploitability: 6

Affected Users: 10

Discoverability: 5

Risk Rating: High

Recommendation Summary

Employees’ usernames should not be easily guessable and should not follow a common pattern. Instead, they should be generated with some randomness on them. Furthermore, the system administrator should enforce password complexity by requiring numbers, special characters, and capital/lowercase combinations. Employees should be trained in this matter so that they take real care of their credentials.

The system should not allow multiple log-in attempts and scans coming from the same IP address. Filters should be placed to monitor and block this behavior; this can be easily done with software tools like snort.

Software running the web server, FTP, and SSH connections should be updated to the latest versions.

Strategic Roadmap

User credentials should be renewed as soon as possible, and password complexity must be enforced. This should be a short-term goal since the current credentials are easily guessable by attackers. Failing to do so puts at risk the entire system as attackers can steal or modify information and/or put services down if they manage to steal an employee’s account.

After this, the system administrator should get the required tools to monitor the network activity and block strange behavior that could be an attacker performing scans and/or attempting brute force attacks on the system. This should be a short-term goal as well; failing to do so makes it easier for an attacker to find a way into the system.

The services running in the system should be constantly updated and/or patched when required. These should be a long-term goal; failing to do so might allow attackers to find exploits and common vulnerabilities in outdated applications which could result in data breaches, loss of data, or make resources unavailable.

Technical Report

Introduction

Nicolas Meneses was contracted by Pegasus Technical Services to conduct a black-box penetration test on their new system to determine its exposure to an external attack from the Internet. All activities were conducted in a manner that simulated a malicious actor engaged in a target attack against Pegasus Technical Services. The scope of the test is limited to network attacks and the objective is to make a comprehensive analysis of the security of the company and how vulnerable they are to Internet attacks.

Information Gathering

Using Netscan I was able to get the server IP of the target. Then, using a network scanning tool I found the following open ports in the target machine:

- Apache Web Server in port 80
- Secure Shell Protocol in port 22
- File Transfer Protocol in port 21

The company is called Pegasus Technical Services and was founded in 2019. The company's president is Everett Griffin and some of their employees are Pat Patrick (Project Manager), Ben Benedict (Project Manager), Erin Nire (Project Manager), Gregory Duffel (System Administrator), and William Barker (Intern Technician). This information is public and can be found on the Company's website.

With further use of scanning tools, I found the version of the webserver is Apache 2.4.25 (Debian) which was first built in 2018. Additionally, the software in charge of FTP is vsftpd 3.0.3 and the software in charge of SSH is OpenSSH 7.4. The operating system of the machine is Linux.

Vulnerability Assessment

1) The names and roles of the company's employees are public. This information might be used to guess usernames and perform brute force attacks on those employees who might have a server account (based on their role in the company).
2) There is no intrusion System prevention that blocks malicious network activity. This makes brute force attacks and scans over the network possible.

Based on the analysis of the vulnerability scanning results from Nikto, Legion, and Nessus the following vulnerabilities were found.

1) The version of JQuery hosted on the remote web server is affected by multiple cross site scripting vulnerabilities. However, these vulnerabilities have no security impact on PAN-OS running devices.
2) The version of the web server (Apache 2.4.25) has two critical vulnerabilities. a) There is a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value (CVE-2017-7668) and b) mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port (CVE-2017-3169).
3) The version of the SSH protocol (OpenSSH 7.4) has a low-risk bug that does not properly prevent write operations in read only mode, which allows attackers to create zero-length files.
4) The version of the FTP protocol (vsftpd 3.0.3) is vulnerable to a Remote Denial of Service; there exists an exploit for this vulnerability in the exploit database (EDB-ID: 49719).

Risk Score for each vulnerability

1) JQuery (CVE-2020-11023):

Confidentiality Impact: Low

Integrity Impact: Partial

Availability Impact: Low

Score: 6.0

2) Apache 2.4.25 (CVE-2017-7668):

Confidentiality Impact: Partial (There is considerable informational disclosure.)

Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)

Score: 7.5

3) Apache 2.4.25 (CVE-2017-3169):

Confidentiality Impact: Partial (There is considerable informational disclosure.)

Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact: Partial (There is reduced performance or interruptions in resource availability.)

Score: 7.5

4) OpenSSH 7.4 (CVE-2017-15906):

Confidentiality Impact: None (There is no impact to the confidentiality of the system.)

Integrity Impact: Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)

Availability Impact: None (There is no impact to the availability of the system.)

Score: 5.0

5) vsftpd 3.0.3 (EDB-ID: 49719):

Confidentiality Impact: None

Integrity Impact: None

Availability Impact: Partial

Score: 7.0

6) No introduction detection system and public full names of employees:

Confidentiality Impact: High

Integrity Impact: Partial

Availability Impact: Partial

Score: 8.0

Post Exploitation

Confirm vulnerabilities: Lack of IPS and public release of employee names allowed me to perform multiple brute force attacks via FTP and get access to the machine.

Tools used: Hydra, John, rockyou.txt

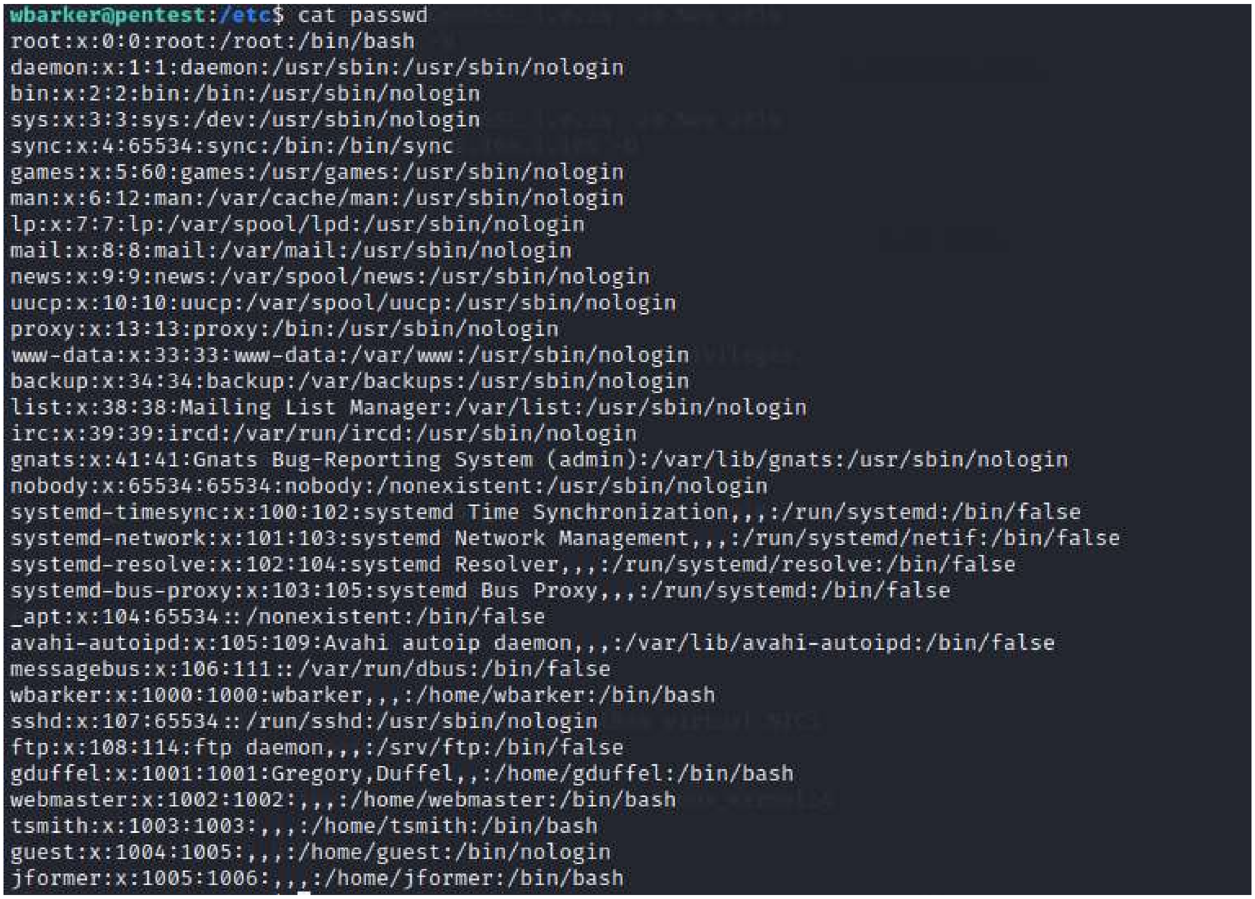
Technique: Brute force attacks, privilege escalation.

Steps:

Using the names of all employees I crafted a list of possible usernames to log into the server. Then I used hydra with the option -e nsr to try to log in using my crafted list in combination with three possible passwords: username, username backward, none. By doing this I was able to find the intern technician password to log into the system.

user: William Barker, username: wbarker, password: wbarker.

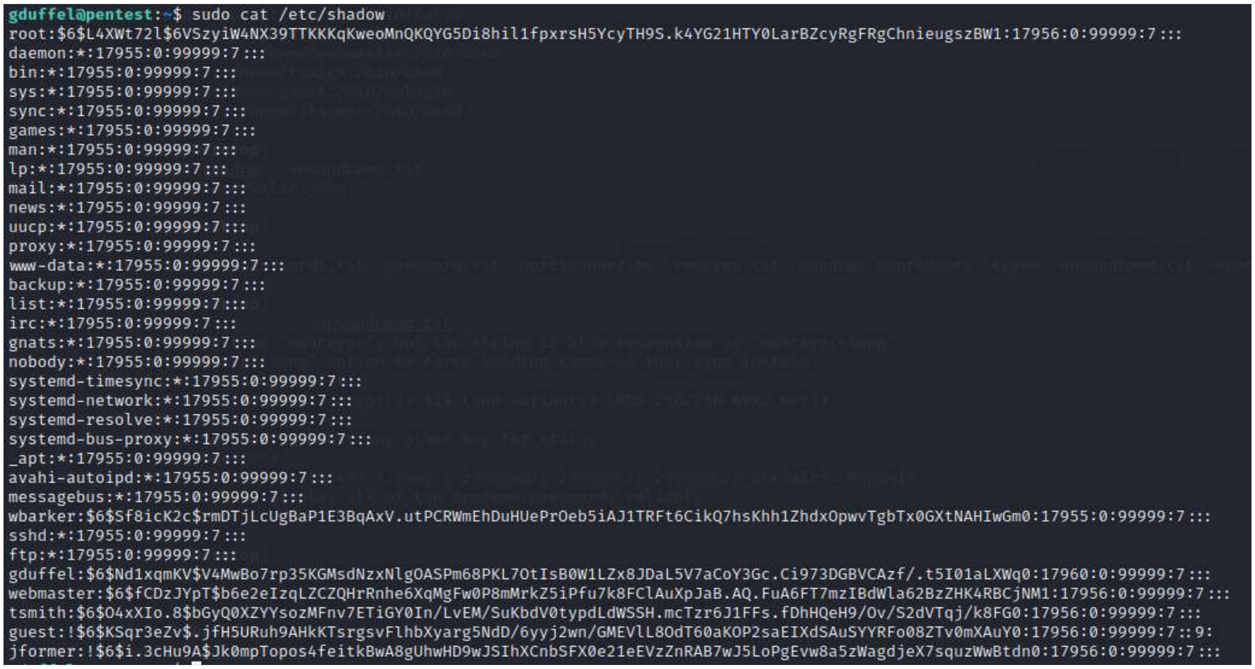
Once I got into the system using the interns' account, I downloaded the /etc/passwd to see all available usernames.



```
wbarker@pentest:/etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
avahi-autoipd:x:105:109:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
messagebus:x:106:111::/var/run/dbus:/bin/false
wbarker:x:1000:1000:wbarker,,,:/home/wbarker:/bin/bash
sshd:x:107:65534::/run/sshd:/usr/sbin/nologin
ftp:x:108:114:ftp daemon,,,:/srv/ftp:/bin/false
gduffel:x:1001:1001:Gregory,Duffel,,:/home/gduffel:/bin/bash
webmaster:x:1002:1002:,,,:/home/webmaster:/bin/bash
tsmith:x:1003:1003:,,,:/home/tsmith:/bin/bash
guest:x:1004:1005:,,,:/home/guest:/bin/nologin
jformer:x:1005:1006:,,,:/home/jformer:/bin/bash
```

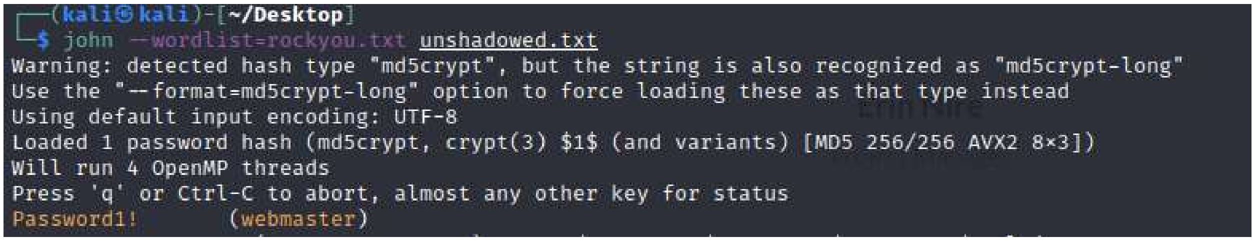
Then, I used hydra against one of the users with root privileges (the system administrator, Gregory Duffel) along with the dictionary rockyou.txt via ftp. After a day hydra was able to get a match for the password.

user: Gregory Duffel, username: gduffel, password: whispering.



```
gduffel@pentest:~$ sudo cat /etc/shadow
root:$6$L4XWt72l$6VSzyiW4NX39TTKKKqKweoMnQKQYG5Di8hil1fpxrsH5YcyTH9S.k4YG21HTY0LarBZcyRgFRgChnieugszBW1:17956:0:99999:7:::
daemon:*:17955:0:99999:7:::
bin:*:17955:0:99999:7:::
sys:*:17955:0:99999:7:::
sync:*:17955:0:99999:7:::
games:*:17955:0:99999:7:::
man:*:17955:0:99999:7:::
lp:*:17955:0:99999:7:::
mail:*:17955:0:99999:7:::
news:*:17955:0:99999:7:::
uucp:*:17955:0:99999:7:::
proxy:*:17955:0:99999:7:::
www-data:*:17955:0:99999:7:::
backup:*:17955:0:99999:7:::
list:*:17955:0:99999:7:::
irc:*:17955:0:99999:7:::
gnats:*:17955:0:99999:7:::
nobody:*:17955:0:99999:7:::
systemd-timesync:*:17955:0:99999:7:::
systemd-network:*:17955:0:99999:7:::
systemd-resolve:*:17955:0:99999:7:::
systemd-bus-proxy:*:17955:0:99999:7:::
_apt:*:17955:0:99999:7:::
avahi-autoipd:*:17955:0:99999:7:::
messagebus:*:17955:0:99999:7:::
wbarker:$6$Sf8icK2c$rmDTjLcUgBaP1E3BqAxV.utPCRWmEhDuHUePrOeb5iAJ1TRFt6CikQ7hsKhh1ZhdxOpwvTgbTx0GXtNAHIwGm0:17955:0:99999:7:::
sshd:*:17955:0:99999:7:::
ftp:*:17955:0:99999:7:::
gduffel:$6$Nd1xqmKV$V4MwBo7rp35KGMsdNzxNlgOASPm68PKL7OtIsB0W1LZx8JDaL5V7aCoY3Gc.Ci973DGBVCAzf/.t5I01aLXWq0:17960:0:99999:7:::
webmaster:$6$fCDzJYpT$b6e2eIzqLZCZQHrRnhe6XqMgFw0P8mMrkZ5iPfu7k8FClAuXpJaB.AQ.FuA6FT7mzIBdWla62BzZHK4RBCjNM1:17956:0:99999:7:::
tsmith:$6$O4xXIo.8$bGyQ0XZYYsozMFnv7ETiGY0In/LvEM/SuKbdV0typdLdWSSH.mcTzr6J1FFs.fDhHQeH9/Ov/S2dVTqj/k8FG0:17956:0:99999:7:::
guest:!$6$KSqr3eZv$.jfH5URuh9AHkKTsrgsvFlhbXyarg5NdD/6yyj2wn/GMEVlL8OdT60aKOP2saEIXdSAuSYYRFo08ZTv0mXAuY0:17956:0:99999:7::9:
jformer:!$6$i.3cHu9A$Jk0mpTopos4feitkBwA8gUhwHD9wJSIhXCnbSFX0e21eEVzZnRAB7wJ5LoPgEvw8a5zWagdjeX7squzWwBtdn0:17956:0:99999:7:::
```

After this, I owned the machine and had access to all its information. For instance, I was able to download the /etc/shadow file and used john to crack some other credentials.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ john --wordlist=rockyou.txt unshadowed.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1!       (webmaster)
```

user: webmaster, username: webmaster, password: Password1!

Remediation:

It is fundamental to make new usernames for all employees. These usernames must not follow a predictable structure. Furthermore, there should be some type of password complexity policy to make brute force attacks hard. In addition to this, the system administrator should install some type of network monitoring tool and block IP’s that are showing a weird behavior (possible attacker scans and/or brute force attempts).

Risk/Exposure

The lack of a network monitoring system and having weak credentials to log into the system represent a huge risk to the company. An attacker getting access to any of these accounts represents a confidentiality problem as there might be private information about clients, and employees. Additionally, if an attacker manages to get root access, he could wipe all the data in the server or make the company's website unavailable. Any of these scenarios could cost a lot of money to the company and therefore must be addressed as soon as possible.

Conclusion

Nicolas Meneses was contracted by Pegasus Technical Services to conduct a black-box penetration test over the network. During the test, several vulnerabilities were found for the software running SSH and FTP connections. Additionally, the complete names of employees and the lack of a network intrusion detection tool allowed scan and brute force attacks over FTP. As a result of this, I was able to get login credentials for an account without root privileges. Then, I could perform a second brute force attack, this time using the username of an account with root privileges, to get root access. To mitigate these risks, Pegasus Technical Services should change their login credential policies, install a network monitoring tool to block intruders, and update their SSH and FTP software to the latest release available.