

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 | 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? | |
| 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

Results of Vsftpd exploit attempt on target

```
[0m[36m[0m          #####          #
          #####          #
          #####          #
          #####          #
```

END OF REPORT