

Metasploitable Analysis Report

Services Running: After running a Nmap scan of the machine we can see what services the machine is running. The screenshot below shows cases that scan and the result of the services.

```
(kali㉿kali)-[~]
$ nmap -sV 192.168.56.105
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-1
2 12:44 EDT
Nmap scan report for 192.168.56.105
Host is up (0.028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              vsftpd 2.3.4
22/tcp    open  ssh              OpenSSH 4.7p1 Debian 8ubuntu
1 (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 (workgr
oup: WORKGROUP)
445/tcp   open  netbios-ssn      Samba smbd 3.X - 4.X (workgr
oup: WORKGROUP)
512/tcp   open  exec             netkit-rsh rshcd
513/tcp   open  login            Netkit rshd
514/tcp   open  shell            GNU Classpath grmiregistry
1099/tcp  open  java-rmi         Metasploitable root shell
1524/tcp  open  bindshell        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            PostgreSQL DB 8.3.0 - 8.3.7
5432/tcp  open  postgresql       VNC (protocol 3.3)
5900/tcp  open  vnc              (access denied)
6000/tcp  open  X11              UnrealIRCd
6667/tcp  open  irc              Apache Jserv (Protocol v1.3)
8009/tcp  open  ajp13            Apache Tomcat/Coyote JSP eng
8180/tcp  open  http
ip: 1.1
```

Architecture: With the list of services, we can determine how the machines are laid out. First, the web services that are being used are Apache and Tomcat. The databases in use are MySQL and PostgreSQL. The file system services in place are Samba, FTP, and NFS. Lastly, the network services are SSH, HTTP, HTTPS, and Netcat.

External Connections: Upon reviewing the website, the only connections being made are the local storage database. From here the website obtains information for users and resources needed. With that being said there doesn't appear to be any external connections being made it outside services.

Password Storage: The passwords are stored on the local database, i.e., MySQL. The majority of passwords are encrypted with hash algorithms. The metasploitable databases use MySQL and PostgreSQL to store information about the user's information, including

their passwords. For the most part the passwords stored are done in plain text, however there are a few that are stored using hashing algorithms.

Recommendations: While searching for passwords I was able to find passwords that were not protected. To remedy this situation an overview of the passwords used needs to be done and upon finding unprotected passwords, either remove them from text files or use hashing and salting techniques to make them unreadable. Regular audits of passwords are also a good practice to ensure the security of the system and protect against unauthorized access to passwords.