Tasks no - 4

Name: Noman Masood Khan
Roll Number: 211042
Course: CY243L - Penetration Testing - Lab
Date: 26/10/2023
Total Questions: 4
Attempted Questions: 4

---

1. What service is running on port 2049.

The service running on the port 2049 is **nfs(Network File System).**

This service allows file transfer among the computers running the windows server and Unix operating System. The user can access files over the computer network just like the local network.

```
22  2049/tcp  open  nfs
23  2121/tcp  open  ccproxy-ftp
24  3306/tcp  open  mysql
```

Exploitation of nfs service

A nfs service has vulnerability which is **improper handling of NFSv4 requests**. A remote attacker can exploit this vulnerability by sending the **malicious RPC calls** to a target server. Successful exploitation of the service can allow the attacker for the **arbitrary code execution**.

---

2. What service is running on the port 3632

The service running on the **port 3632** is **distccd.** A tool for speeding up the compilation time by using the distributed computing over the networking. It takes

advantage of the free computers. distccd can reduce the compilation time for the project.

```
25  3632/tcp  open  distccd
26  5432/tcp  open  postgresql
27  5900/tcp  open  vnc
```

Exploitation of distccd service.

CVE 2004-2687; distcc 2.x when not configured to restrict access to the server port, allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

---

3. What service is running on the port 5900

The service running on the port 5900 VNC **(Virtually Network Computing).** This protocol allows connect with the remote user and control their screen and work on their computer over the internal or over the network. The user can use his own mouse and keyboard on the remote computer.

```
27  5900/tcp  open  vnc
28  6000/tcp  open  X11
29  6667/tcp  open  irc
```

Exploitation of vnc service

Exposing the vnc over the internet allowing the attacker to connect to the service remotely. Attacker tries for the password log-in through the brute forcing. Which in turn allow the attacker to make changes to the server or allow the remote code execution.

---

4. Service running on the port 6000

The service running on the port 600 is **X11.** The X11 protocol is responsible for the delivering the data between the client and server either on the localy or remotely.

Exploitation

Multiple vulnerabilities allow a local or remote, unprivileged user to execute arbitrary code with root privileges on the Solaris X11 display server from XHost [1] or XAuth [1] to access arbitrary memory and X server address space and crash the X11 display server process. Vulnerabilities have been found in Xorg X11 Server, Windows, and the system software of unknown versions.

It is also possible for an attacker to take a screenshot of the remote machine and exploit it for malicious purposes. For example, a cyber attacker can connect to the X11 server to listen to the keyboard and mouse events of a user using the remote machines. This allows the attacker to gain access to the username and password of the user logging into the host.
