IDENTIFYING AND REMEDIATING VULNERABILITIES

MD IBTESAM HOSSAIN

TABLE OF CONTENTS

1. SUMMARY

Installed and configured Tenable Nessus to conduct vulnerability scanning on a Linux machine. Overall scan took 19 minutes. The scan yielded a total of 70 vulnerabilities across various severity levels, including Critical, High, Medium, and Informational vulnerabilities. Notably, Critical vulnerabilities with a CVSS score of 10.0 accounted for 11% of the total result, while High severity vulnerabilities with a CVSS score of 7.5 constituted 9%. Additionally, Medium severity vulnerabilities with a CVSS score ranging from 5.9 to 6.5 comprised another 11%. Following the vulnerability management life-cycle, I meticulously prioritized the top five vulnerabilities from the result. Subsequently, I created a comprehensive vulnerability report and provided actionable remediation recommendations for the identified vulnerabilities. This project exemplifies an enhanced approach to vulnerability management, leveraging Tenable Nessus for robust scanning and strategic remediation planning.

1.1. Project Motivation

According to NIST, a vulnerability is defined as "*A weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source*". As per the definition, it is crucial for the organizations to effectively identify, prioritize, mitigate, and report existing and potential vulnerabilities to reduce organizational risk level to an acceptance level that ensures the confidentiality, integrity, and availability of systems and data. One of the ways the CIA triad can be maintained is through Vulnerability Management, and vulnerability scanning is an essential part of this process. Through vulnerability scanning, this project identified existing vulnerabilities present in the target system. Demonstrated proficiency as a vulnerability analyst identifying and remediating vulnerabilities.

2. METHODOLOGIES

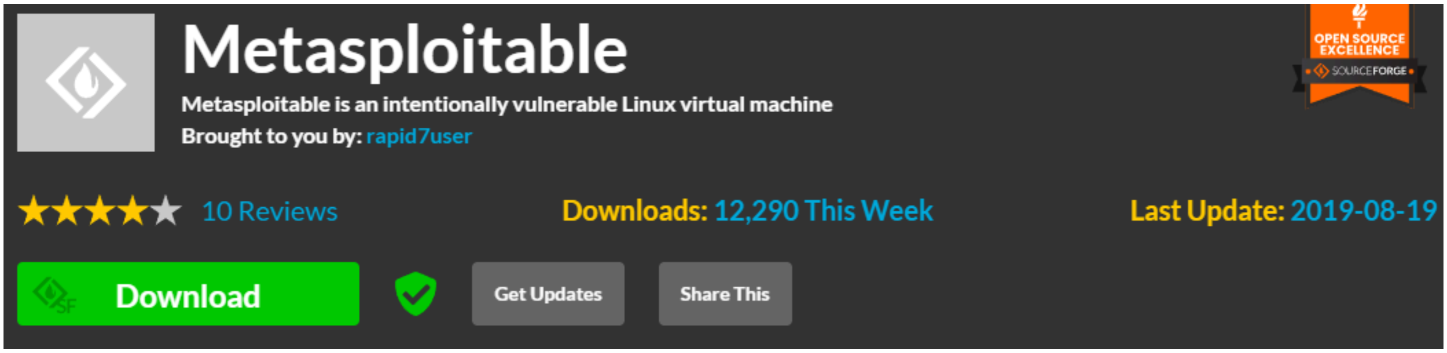
Overall project followed a step-by-step process from setting up the lab environment to installing and scanning with Nessus. These steps are given below.

1. Downloading and Launching Metasploitable 2 Linux Virtual Machine
2. Downloading and Installing Tenable Nessus in Kali Linux
3. Configuring Nessus for Vulnerability Scanning

2.1. Metasploitable 2 Setup

The target machine in this project is an intentionally vulnerable machine called "Metasploitable 2" provided by Rapid7. Information about the machine can be found at: https://docs.rapid7.com/metasploit/metasploitable-2/

Rapid7 provides the download link through Source forage and is downloaded from their site.



Metasploitable

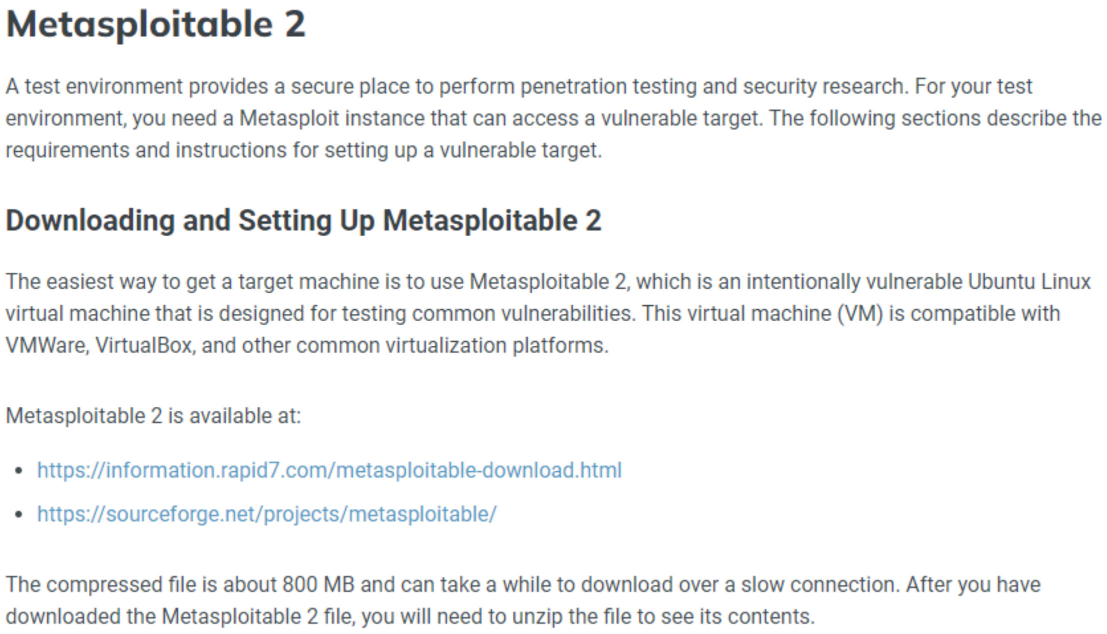
Metasploitable is an intentionally vulnerable Linux virtual machine

Brought to you by: rapid7user

★★★★★ 10 Reviews

Downloads: 12,290 This Week

Last Update: 2019-08-19



Metasploitable 2

A test environment provides a secure place to perform penetration testing and security research. For your test environment, you need a Metasploit instance that can access a vulnerable target. The following sections describe the requirements and instructions for setting up a vulnerable target.

Downloading and Setting Up Metasploitable 2

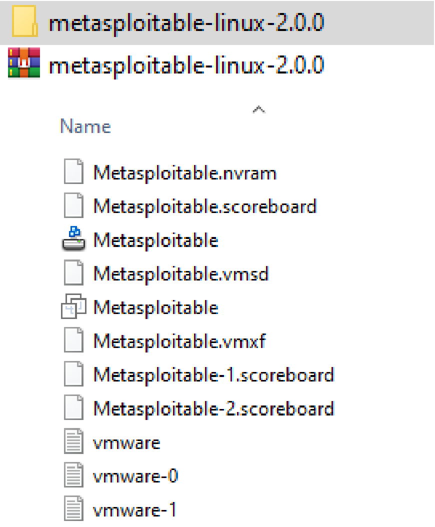
The easiest way to get a target machine is to use Metasploitable 2, which is an intentionally vulnerable Ubuntu Linux virtual machine that is designed for testing common vulnerabilities. This virtual machine (VM) is compatible with VMWare, VirtualBox, and other common virtualization platforms.

Metasploitable 2 is available at:

- https://information.rapid7.com/metasploitable-download.html
- https://sourceforge.net/projects/metasploitable/

The compressed file is about 800 MB and can take a while to download over a slow connection. After you have downloaded the Metasploitable 2 file, you will need to unzip the file to see its contents.

After it was downloaded, a metasploitable-linux-2.0.0 zip file was found and extracted. This was then loaded into the VMWare hypervisor to further configure the VM.

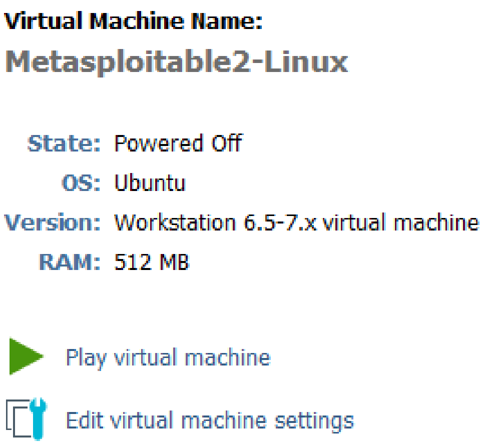


metasploitable-linux-2.0.0
metasploitable-linux-2.0.0

Name

Metasploitable.nvram
Metasploitable.scoreboard
Metasploitable
Metasploitable.vmsd
Metasploitable
Metasploitable.vmxf
Metasploitable-1.scoreboard
Metasploitable-2.scoreboard
vmware
vmware-0
vmware-1

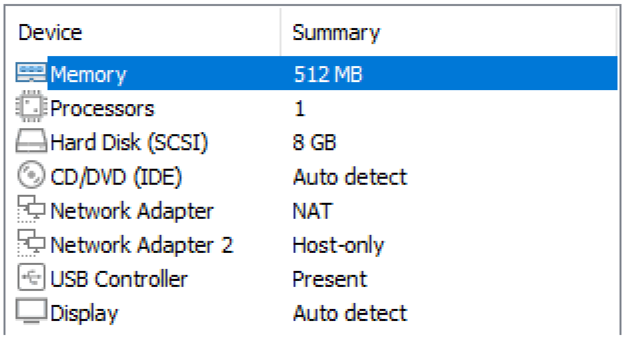
On the VMWare Player, clicked on the “Edit virtual machine settings” to open the configuration window for VM settings.



Virtual Machine Name:
Metasploitable2-Linux

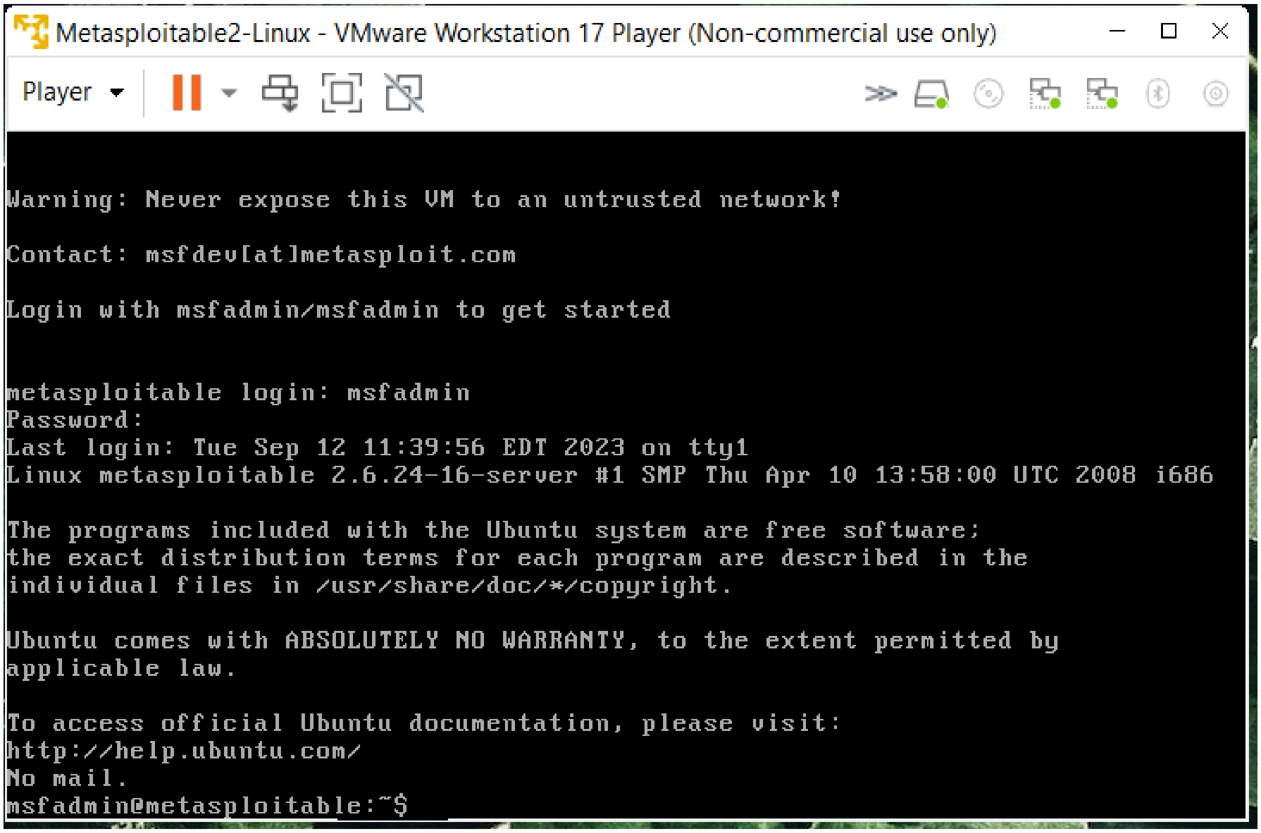
State: Powered Off
OS: Ubuntu
Version: Workstation 6.5-7.x virtual machine
RAM: 512 MB

This is a fairly light VM and does not require powerful system resources. Allocated 512 MB of memory, 1 processor, 8 GB of Disk space, and selected NAT as the Network Adapter.



Device	Summary
Memory	512 MB
Processors	1
Hard Disk (SCSI)	8 GB
CD/DVD (IDE)	Auto detect
Network Adapter	NAT
Network Adapter 2	Host-only
USB Controller	Present
Display	Auto detect

After all the settings were applied, the VM was launched using the green “Play Virtual Machine” button. Credentials provided by Rapid7 was msfadmin:msfadmin



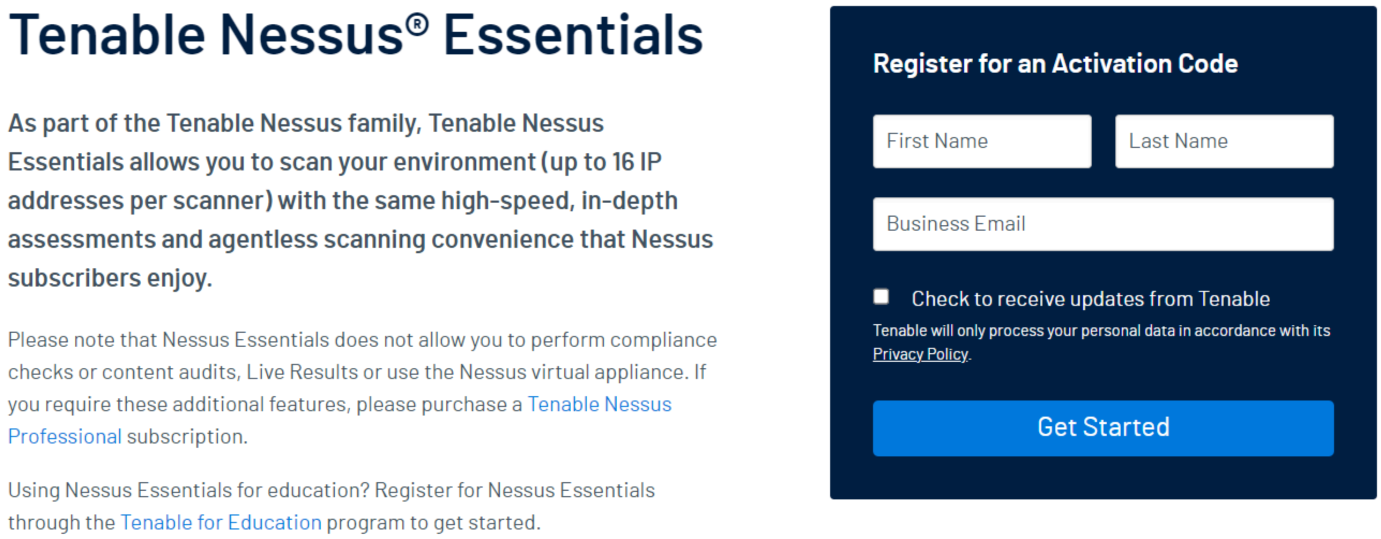
Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)
Player

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Tue Sep 12 11:39:56 EDT 2023 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

In addition, identified the IP Address by using the “ifconfig” command to later use in Nessus. The IP address was 192.168.96.129

2.2. Downloading and Installing Tenable Nessus

Tenable Nessus was downloaded from their official website:https://www.tenable.com/products/nessus to the Kali Linux virtual machine. Kali Linux is not required for Nessus however, it was the machine available at the time and used as a result. In this project, a free version of the software, Tenable Nessus Essentials was used.



Tenable Nessus® Essentials

As part of the Tenable Nessus family, Tenable Nessus Essentials allows you to scan your environment (up to 16 IP addresses per scanner) with the same high-speed, in-depth assessments and agentless scanning convenience that Nessus subscribers enjoy.

Please note that Nessus Essentials does not allow you to perform compliance checks or content audits, Live Results or use the Nessus virtual appliance. If you require these additional features, please purchase a Tenable Nessus Professional subscription.

Using Nessus Essentials for education? Register for Nessus Essentials through the Tenable for Education program to get started.

Register for an Activation Code

First Name

Last Name

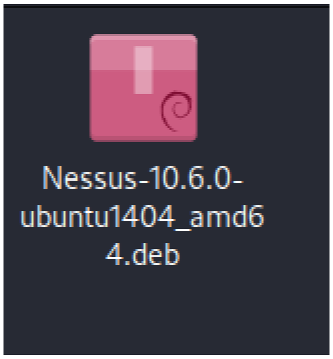
Business Email

□ Check to receive updates from Tenable

Tenable will only process your personal data in accordance with its Privacy Policy.

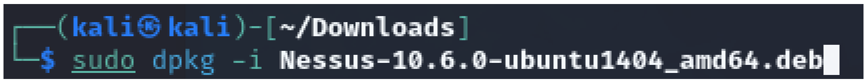
Get Started

After following the registration steps, nessus was downloaded into the Kali linux VM. Activation code saved for later use.



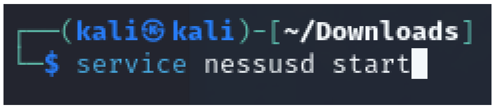
Nessus-10.6.0-ubuntu1404_amd64.deb

And finally installed using the command shown below.



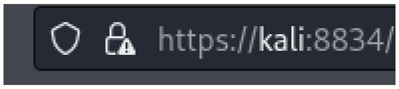
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.6.0-ubuntu1404_amd64.deb
```

To start Nessus after it was done installing, used command `service neesusd start`

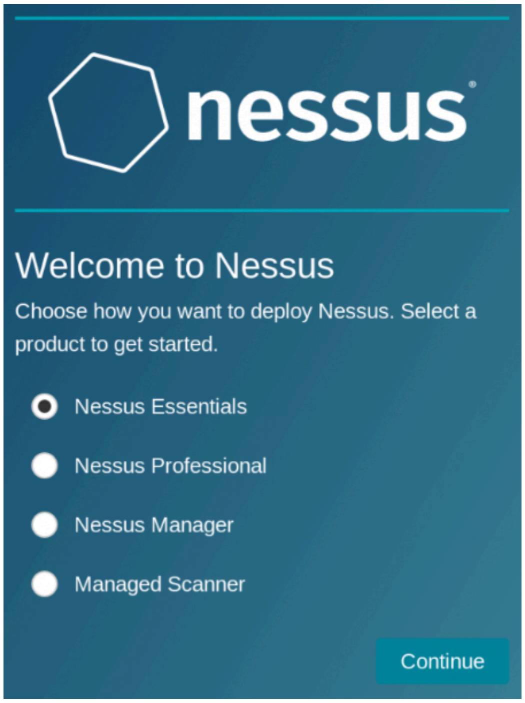


```
┌──(kali㉿kali)-[~/Downloads]
└─$ service nessusd start
```

According to the documentation provided by Tenable, Nessus starts in port 8834. Accessed Nessus by visiting https://kali:8834 in the web browser. Bypassing the SSL warning, Nessus was accessed successfully.



https://kali:8834/



Welcome to Nessus

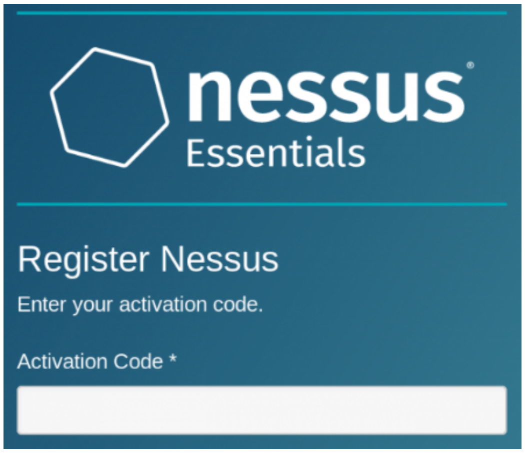
Choose how you want to deploy Nessus. Select a product to get started.

● Nessus Essentials

○ Nessus Professional

○ Nessus Manager

○ Managed Scanner

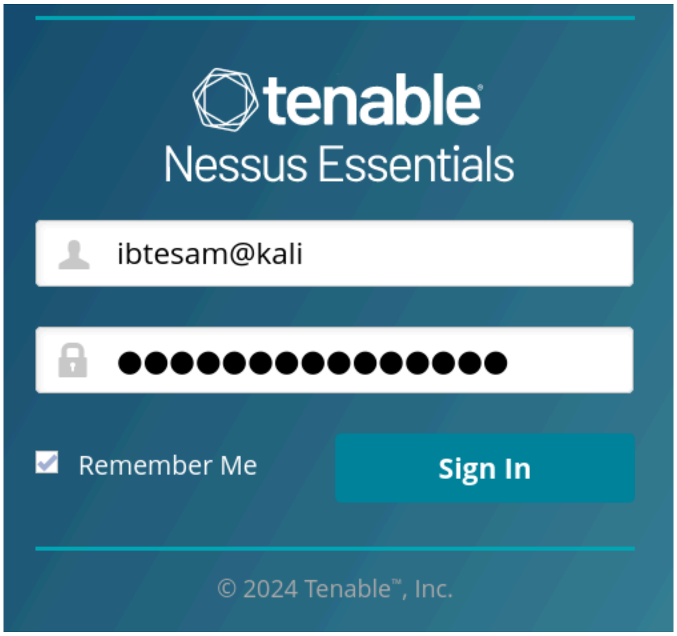


Register Nessus

Enter your activation code.

Activation Code *

Registered for an account and used the activation code generated from earlier steps to finish registration and logged in to Nessus.



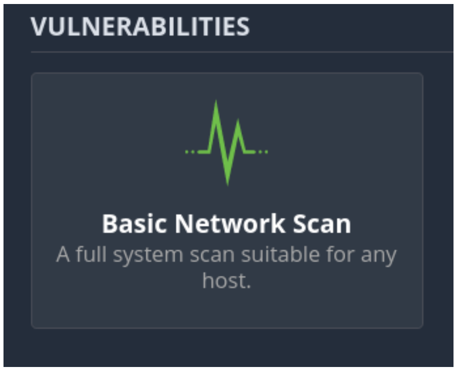
ibtesam@kali

●●●●●●●●●●●●●●●

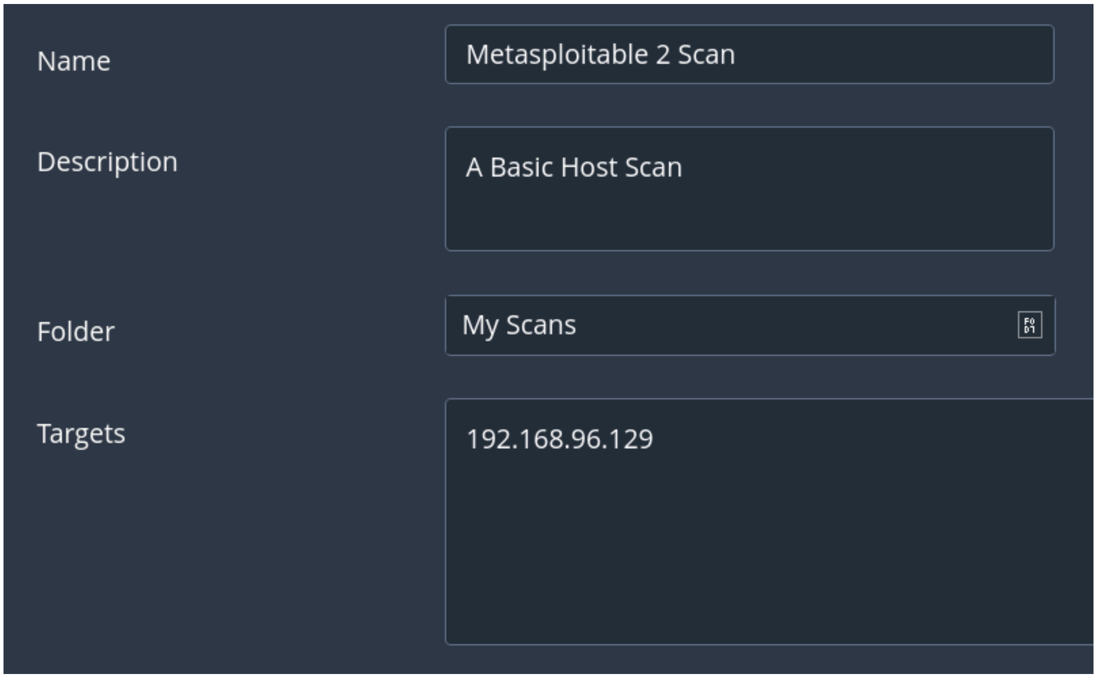
☑ Remember Me

2.3. Configuring Nessus to Start Scanning

Nessus takes quite a long time to download and compile necessary plugins. Nessus also provides multiple scanning templates to choose. In this project, a basic host scan option was selected.



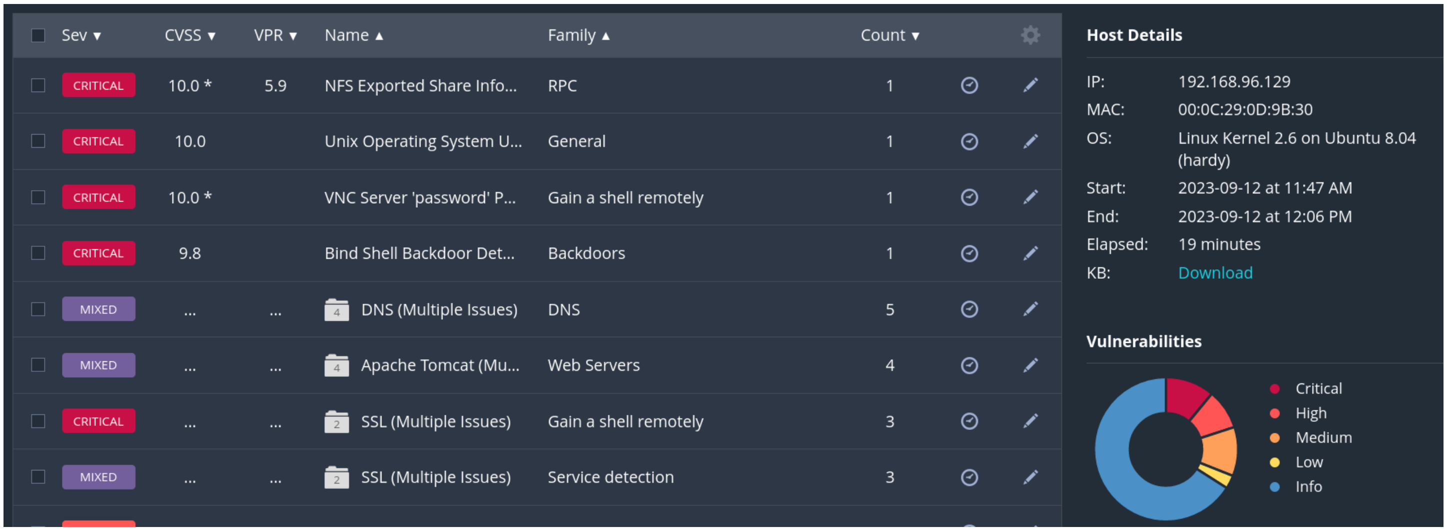
It does a full system scan and is perfect for the test environment. In a production environment, it is necessary to properly implement plans and procedures before conducting vulnerability scanning as it can cause DoS events and disrupt critical business operations. As this was a test environment, went ahead with the scanning without any prior preparation.



Name	Metasploitable 2 Scan
Description	A Basic Host Scan
Folder	My Scans
Targets	192.168.96.129

Before a scan could take place it needs to be configured with some parameters including the name, description, folder and targets. This scan was given a name of “Metasploitable 2 Scan” and used the target VM’s IP address. All other settings related to type of scans and port number selection were kept at default option. Finally pressed save and started scanning.

3. ANALYSIS



□ Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		
□ CRITICAL	10.0 *	5.9	NFS Exported Share Info...	RPC	1	⊘	✎
□ CRITICAL	10.0		Unix Operating System U...	General	1	⊘	✎
□ CRITICAL	10.0 *		VNC Server 'password' P...	Gain a shell remotely	1	⊘	✎
□ CRITICAL	9.8		Bind Shell Backdoor Det...	Backdoors	1	⊘	✎
□ MIXED	...	...	4 DNS (Multiple Issues)	DNS	5	⊘	✎
□ MIXED	...	...	4 Apache Tomcat (Mu...	Web Servers	4	⊘	✎
□ CRITICAL	...	...	2 SSL (Multiple Issues)	Gain a shell remotely	3	⊘	✎
□ MIXED	...	...	2 SSL (Multiple Issues)	Service detection	3	⊘	✎

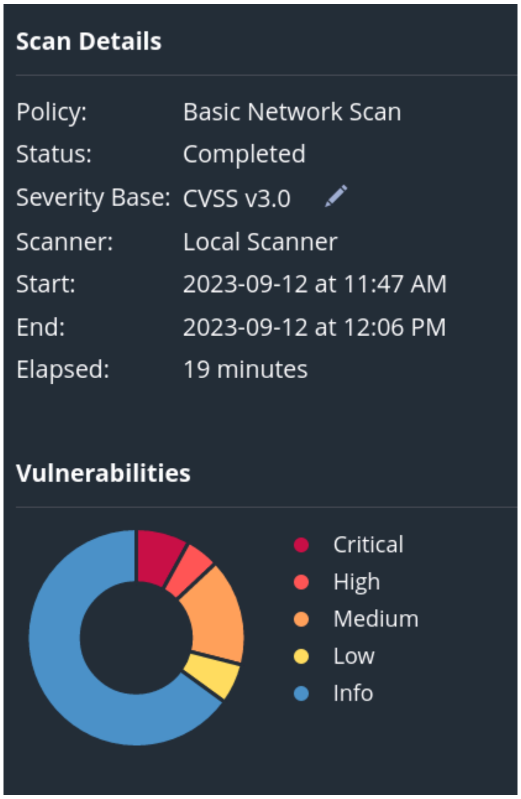
Host Details

IP:	192.168.96.129
MAC:	00:0C:29:0D:9B:30
OS:	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start:	2023-09-12 at 11:47 AM
End:	2023-09-12 at 12:06 PM
Elapsed:	19 minutes
KB:	Download

Vulnerabilities

3.1. Scan Details

The scan took 19 minutes to complete. As from the image below, it was seen that the scan comprised Critical, High, Medium, Low, and Informational Vulnerabilities.

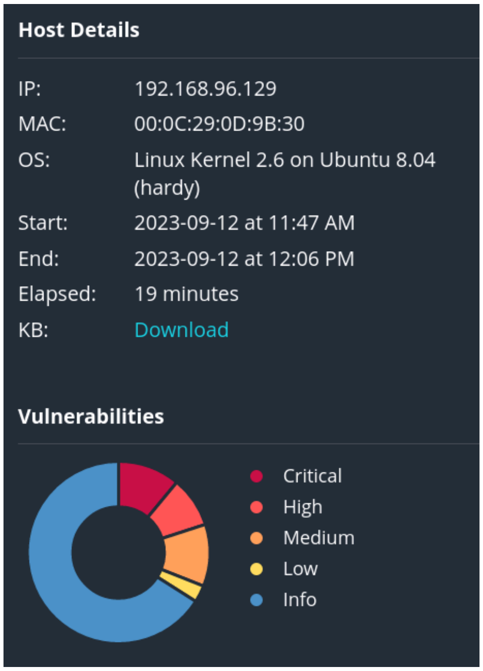


Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: 2023-09-12 at 11:47 AM
End: 2023-09-12 at 12:06 PM
Elapsed: 19 minutes

Vulnerabilities

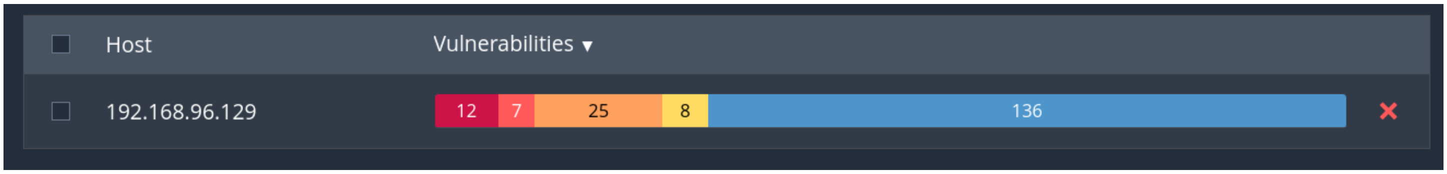
3.2. Host Details



Host Details

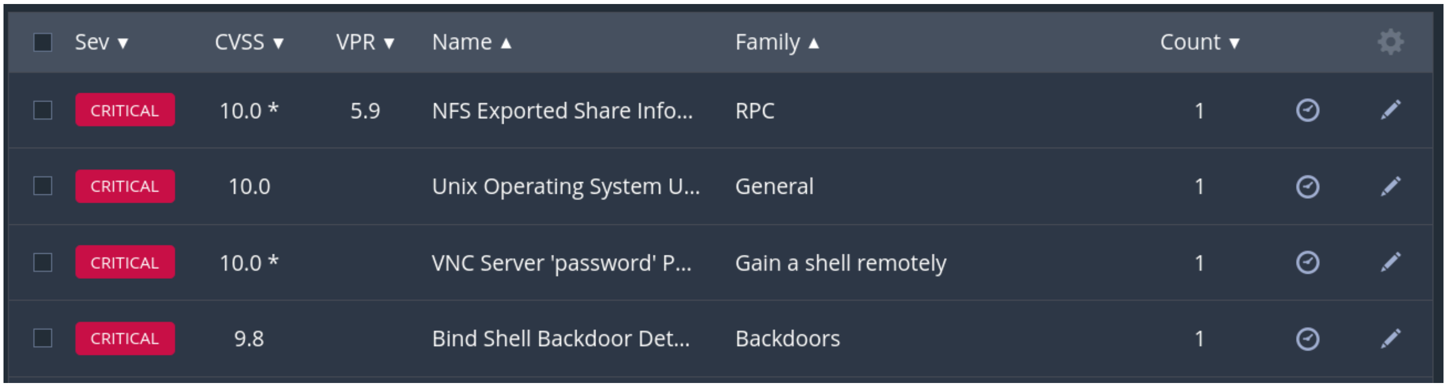
IP: 192.168.96.129
MAC: 00:0C:29:0D:9B:30
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: 2023-09-12 at 11:47 AM
End: 2023-09-12 at 12:06 PM
Elapsed: 19 minutes
KB: Download

Vulnerabilities

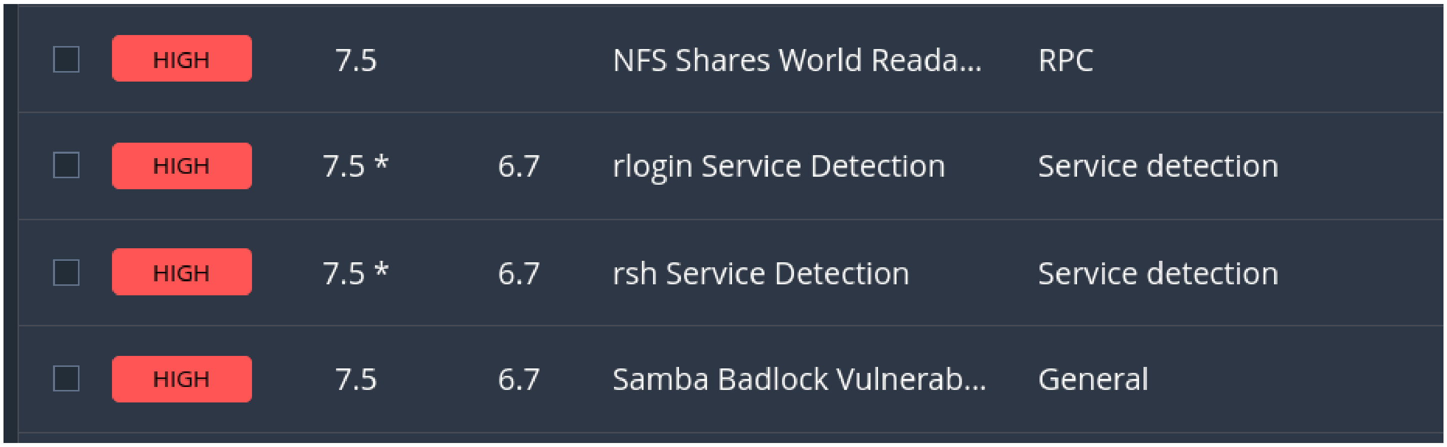


□	Host	Vulnerabilities ▾	
□	192.168.96.129	12 7 25 8 136	✕

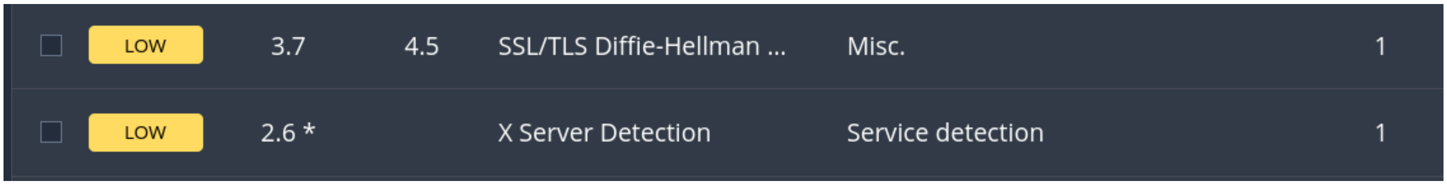
Nessu also showed the target system had 12 Critical, 7 High, 25 Medium, and 8 Low severity vulnerabilities.



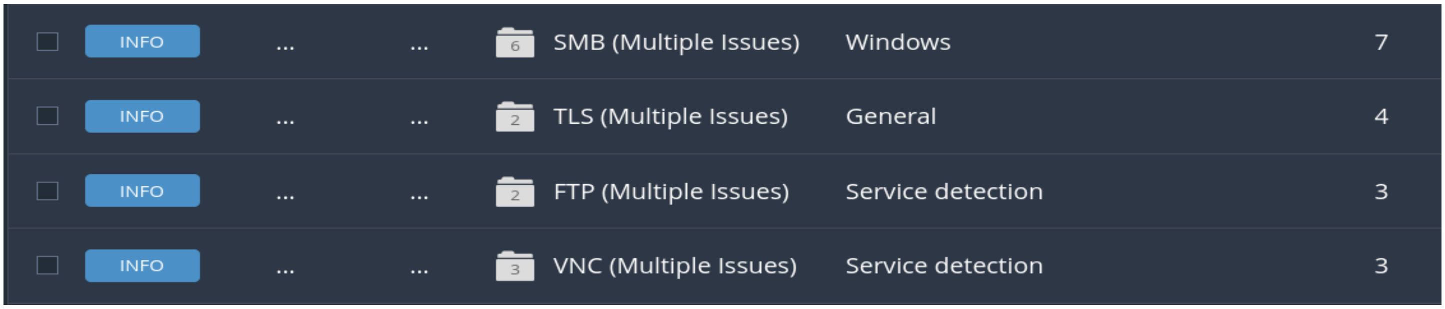
□	Sev ▾	CVSS ▾	VPR ▾	Name ▴	Family ▴	Count ▾		⚙
□	CRITICAL	10.0 *	5.9	NFS Exported Share Info...	RPC	1	⊘	✎
□	CRITICAL	10.0		Unix Operating System U...	General	1	⊘	✎
□	CRITICAL	10.0 *		VNC Server 'password' P...	Gain a shell remotely	1	⊘	✎
□	CRITICAL	9.8		Bind Shell Backdoor Det...	Backdoors	1	⊘	✎



□	HIGH	7.5		NFS Shares World Reada...	RPC
□	HIGH	7.5 *	6.7	rlogin Service Detection	Service detection
□	HIGH	7.5 *	6.7	rsh Service Detection	Service detection
□	HIGH	7.5	6.7	Samba Badlock Vulnerab...	General



□	LOW	3.7	4.5	SSL/TLS Diffie-Hellman ...	Misc.	1
□	LOW	2.6 *		X Server Detection	Service detection	1



□	INFO	...	...	6 SMB (Multiple Issues)	Windows	7
□	INFO	...	...	2 TLS (Multiple Issues)	General	4
□	INFO	...	...	2 FTP (Multiple Issues)	Service detection	3
□	INFO	...	...	3 VNC (Multiple Issues)	Service detection	3

3.3. Prioritizing Vulnerabilities

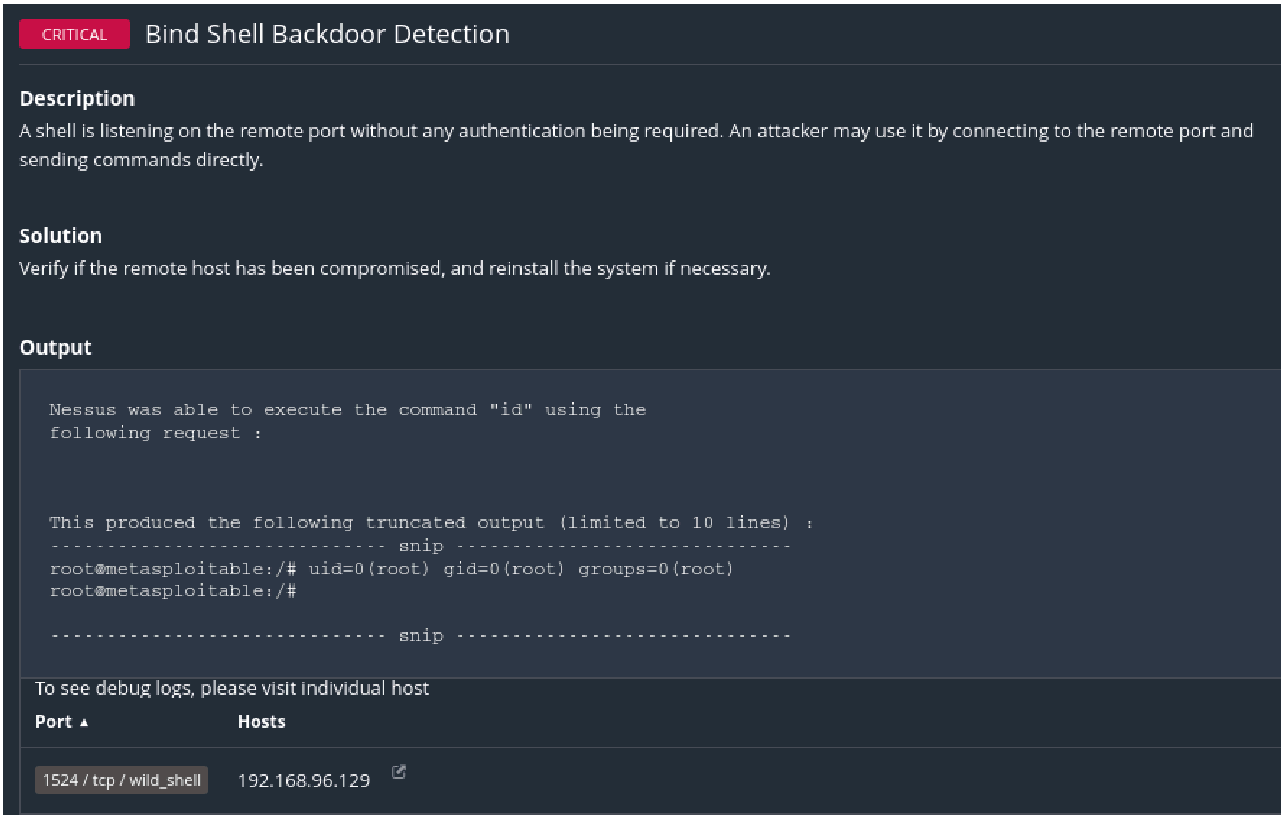
According to Vulnerability Management Lifecycle, not all vulnerabilities are prioritized equally and nor is it the mission to eliminate all of the identified vulnerabilities. Depending on the business operations, risk assessment, and ease of exploitation, some vulnerabilities are prioritized higher than others. In the scan result, it can be seen that there are multiple Critical severity vulnerabilities however, decisions need to be made to select which Critical vulnerability should be remediated first. Furthermore, each selected vulnerability should be examined first whether the vulnerability really exists or it is a false positive.

Top five vulnerabilities selected are given below:

1. Bind Shell Backdoor Detection

CRITICAL Bind Shell Backdoor Detection

A shell is a computer program that exposes operating system's services to a human or other programs. The scanned system has a shell running without any authentication. Attackers can use this shell to connect to our system and exploit it. This is a top priority. Immediate action needs to be taken to identify whether the system had already been compromised.



CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

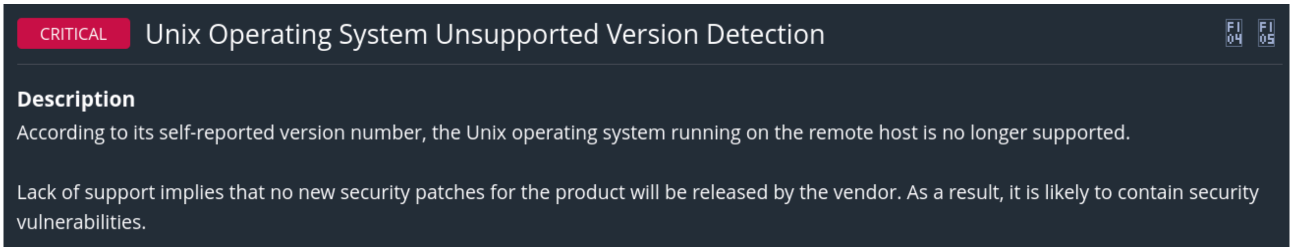
Output

```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

To see debug logs, please visit individual host

Port ▲	Hosts
1524 / tcp / wild_shell	192.168.96.129

2. Unix Operating System Unsupported Version Detection



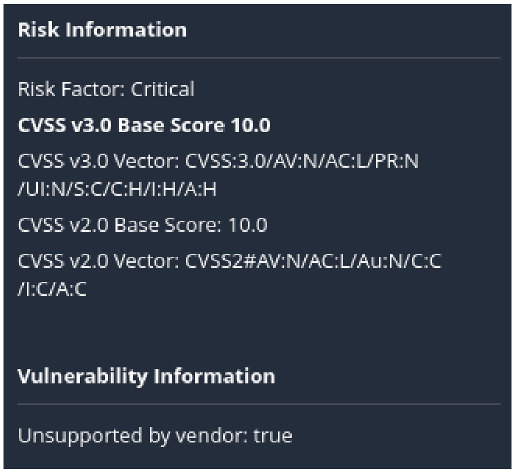
CRITICAL Unix Operating System Unsupported Version Detection

Description

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.

This is another top priority vulnerability. All the applications and services run on top of the Operating System. If the OS is not supported by the vendor then no update or security patch is available. This opens up multiple attack vectors for an adversary to compromise the system.



Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 10.0

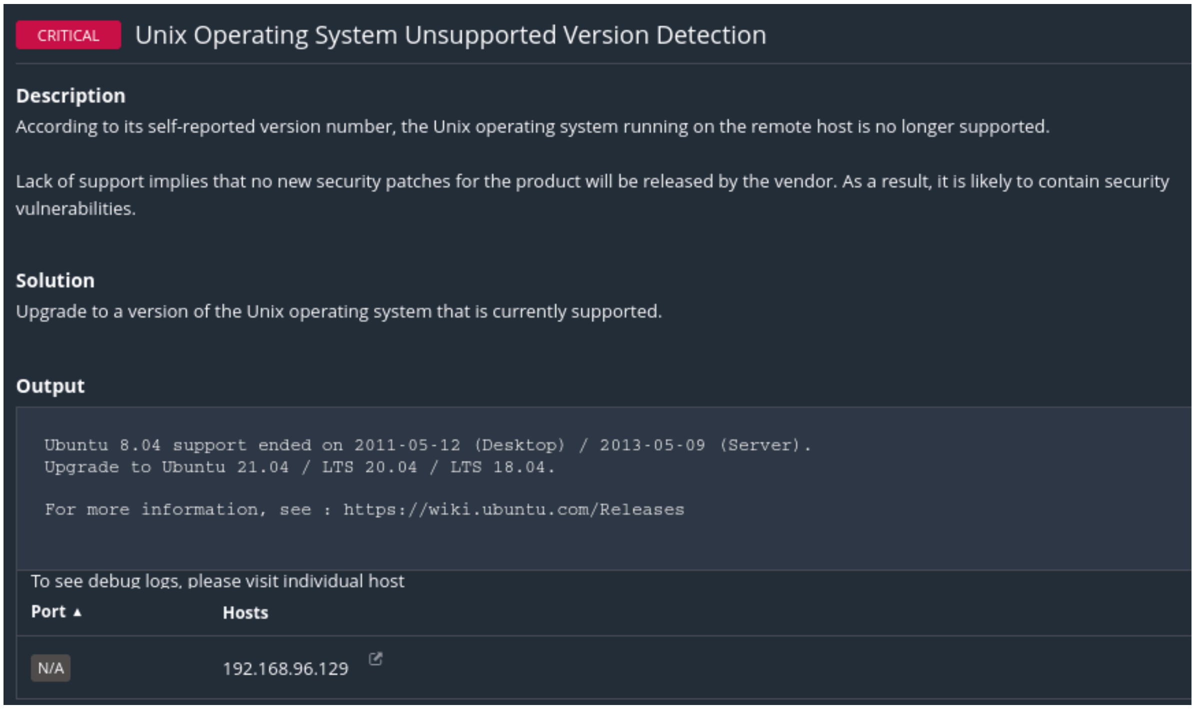
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Unsupported by vendor: true



CRITICAL Unix Operating System Unsupported Version Detection

Description

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.

Solution

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 21.04 / LTS 20.04 / LTS 18.04.

For more information, see : https://wiki.ubuntu.com/Releases
```

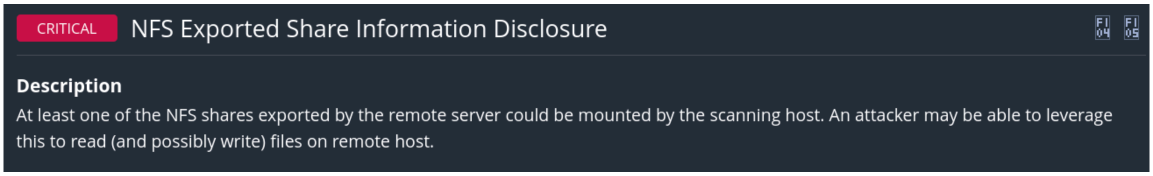
To see debug logs, please visit individual host

Port ▲	Hosts
N/A	192.168.96.129

Nessus successfully detects the version running on the system as Ubuntu 8.04 and the vendor support ended on 2011-05-12 for Desktop, 2013-05-09 for Server edition.

Some additional details provided by Nessus was that the Risk Factor is Critical with a base score of 10.0 in both CVSS v3.0 and v2.0 scoring system.

3. NFS Exported Share Information Disclosure

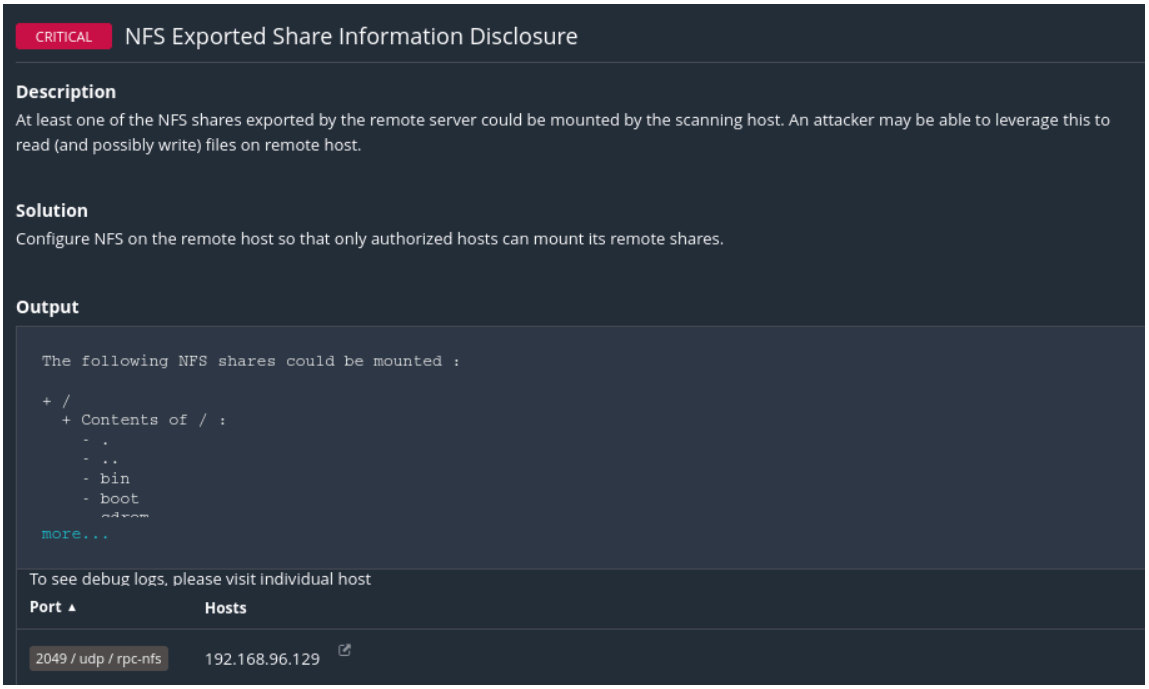


CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

NFS stands for Network File System which allows users to read, write and view data on a remote system as if it is a local system. Right now anyone can mount remote shares. If a threat actor mounts these remote shares, they can read and possibly write files on this remote host compromising the confidentiality and integrity.



CRITICAL NFS Exported Share Information Disclosure

Description

At least one of the NFS shares exported by the remote server could be mounted by the scanning host. An attacker may be able to leverage this to read (and possibly write) files on remote host.

Solution

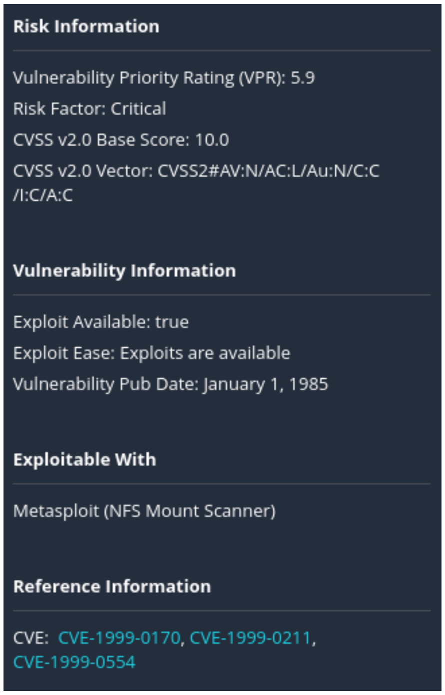
Configure NFS on the remote host so that only authorized hosts can mount its remote shares.

Output

```
The following NFS shares could be mounted :

+ /
  + Contents of / :
    - .
    - ..
    - bin
    - boot
    - cdrom
more...
```

To see debug logs, please visit individual host

Port ▲	Hosts
2049 / udp / rpc-nfs	192.168.96.129



Risk Information

Vulnerability Priority Rating (VPR): 5.9

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Exploit Available: true

Exploit Ease: Exploits are available

Vulnerability Pub Date: January 1, 1985

Exploitable With

Metasploit (NFS Mount Scanner)

Reference Information

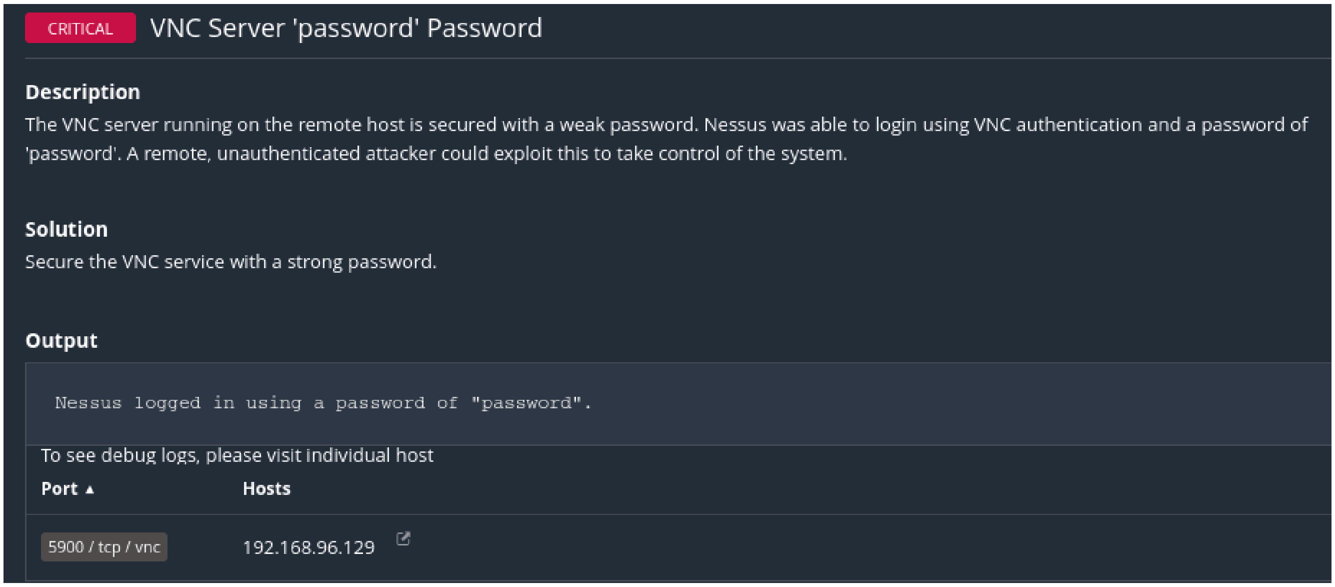
CVE: CVE-1999-0170, CVE-1999-0211, CVE-1999-0554

Nessus provided Risk Factor is labeled as Critical. And it also showed there is a Metasploit exploit available to take advantage of this vulnerability. This vulnerability is identified in multiple CVEs including CVE 1999-0170, CVE 1999-0211, and CVE 1999-0554.

4. VNC Server “password” Password

CRITICAL VNC Server 'password' Password

The VNC server which stands for Virtual Network Computing is a graphical desktop-sharing system to remotely control another computer. This server has an authentication system where only those who have the authorized access to the server can use it. However, in this case the password was set to default password as ‘password’ which is an extremely risky password and threat actors can easily take control of the system. Because of how easy it is to exploit this vulnerability this should be among the top priorities selected.



CRITICAL VNC Server 'password' Password

Description

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

Solution

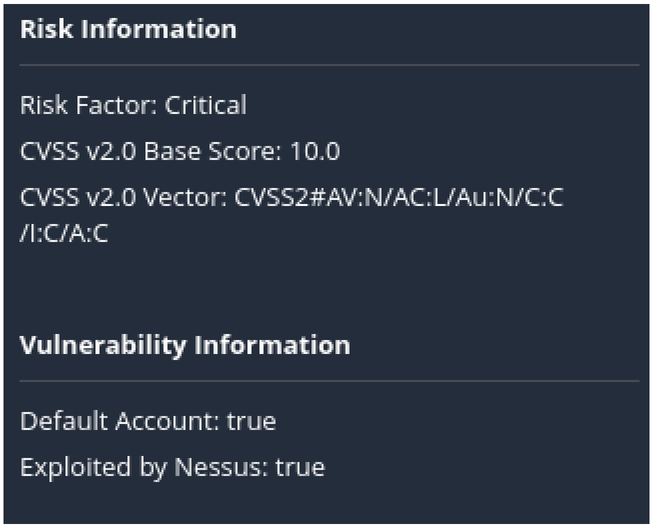
Secure the VNC service with a strong password.

Output

```
  Nessus logged in using a password of "password".
```

To see debug logs, please visit individual host

Port ▲	Hosts
5900 / tcp / vnc	192.168.96.129



Risk Information

Risk Factor: Critical

CVSS v2.0 Base Score: 10.0

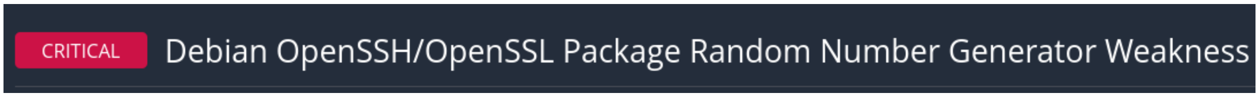
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerability Information

Default Account: true

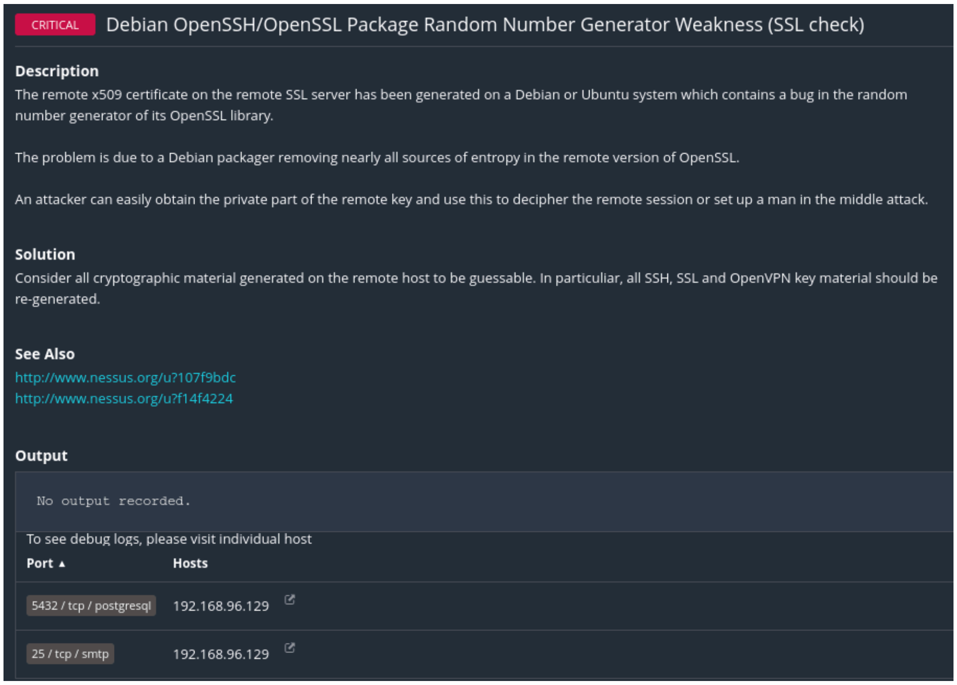
Exploited by Nessus: true

5. Debian OpenSSH/OpenSSL Random Number Generator Weakness



CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

OpenSSL is the library that implements the actual encryption and authentication. The issue was the OpenSSL library present on the system had a bug in its random number generator which is used to create an encryption. An attacker as a result can easily obtain the private part of the remote key used for encryption and set up a man in the middle attack. Meaning, the attacker can intercept and relay messages between two parties who believe they are communicating directly with each other. This compromises both the Confidentiality and Integrity of data-in-transit.



CRITICAL Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)

Description

The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library.

The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL.

An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.

Solution

Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

See Also

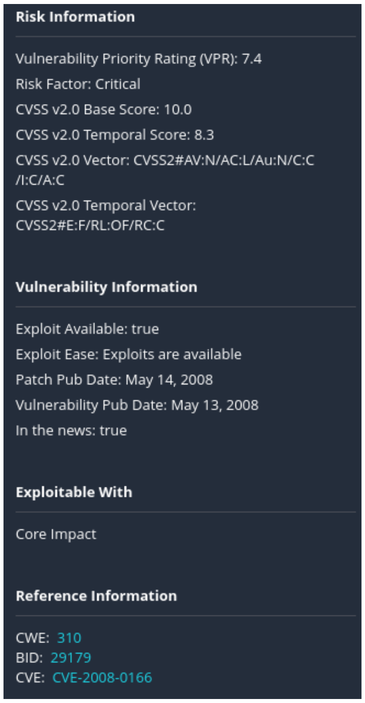
http://www.nessus.org/u?107f9bdc
http://www.nessus.org/u?f14f4224

Output

```
No output recorded.
```

To see debug logs, please visit individual host

Port ▲	Hosts
5432 / tcp / postgresql	192.168.96.129
25 / tcp / smtp	192.168.96.129



Risk Information

Vulnerability Priority Rating (VPR): 7.4
Risk Factor: Critical
CVSS v2.0 Base Score: 10.0
CVSS v2.0 Temporal Score: 8.3
CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C
CVSS v2.0 Temporal Vector: CVSS2#E:F/RL:OF/RC:C

Vulnerability Information

Exploit Available: true
Exploit Ease: Exploits are available
Patch Pub Date: May 14, 2008
Vulnerability Pub Date: May 13, 2008
In the news: true

Exploitable With

Core Impact

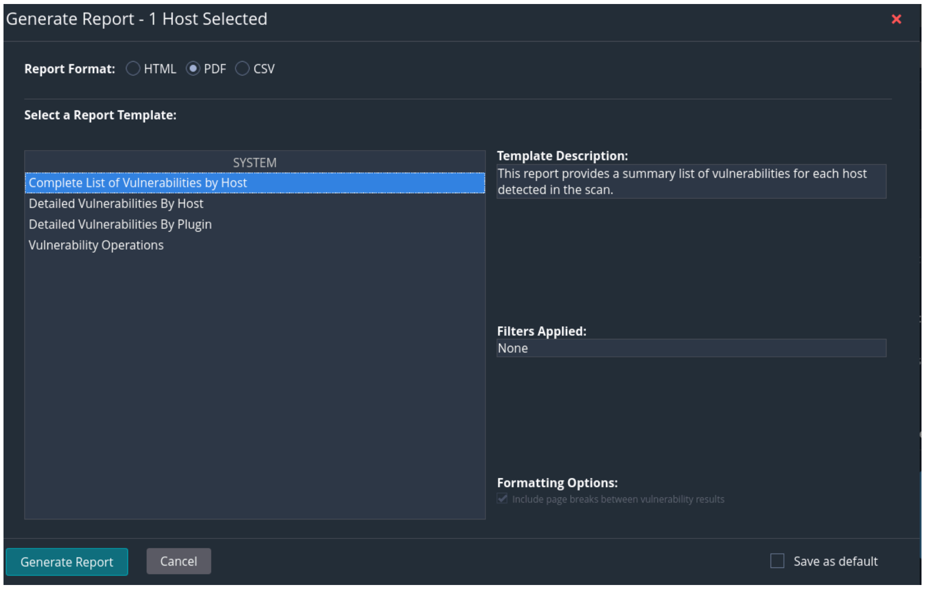
Reference Information

CWE: 310
BID: 29179
CVE: CVE-2008-0166

Risk Factor is Critical with a base score of 10.0 and exploits are available for anyone to take advantage and compromise system and data. The CVE related to this vulnerability is CVE 2008-0166.

3.4. Generating Report

A full report comprising all the vulnerabilities was generated using Nessus' report generation tool. Reports can be generated in HTML, PDF, or CSV format. Reporting feature also has options to choose whether to include only a list of findings or a detailed report. In this case generated a report using "Complete List of Vulnerabilities by Host" option.



Generate Report - 1 Host Selected

Report Format: ○ HTML ● PDF ○ CSV

Select a Report Template:

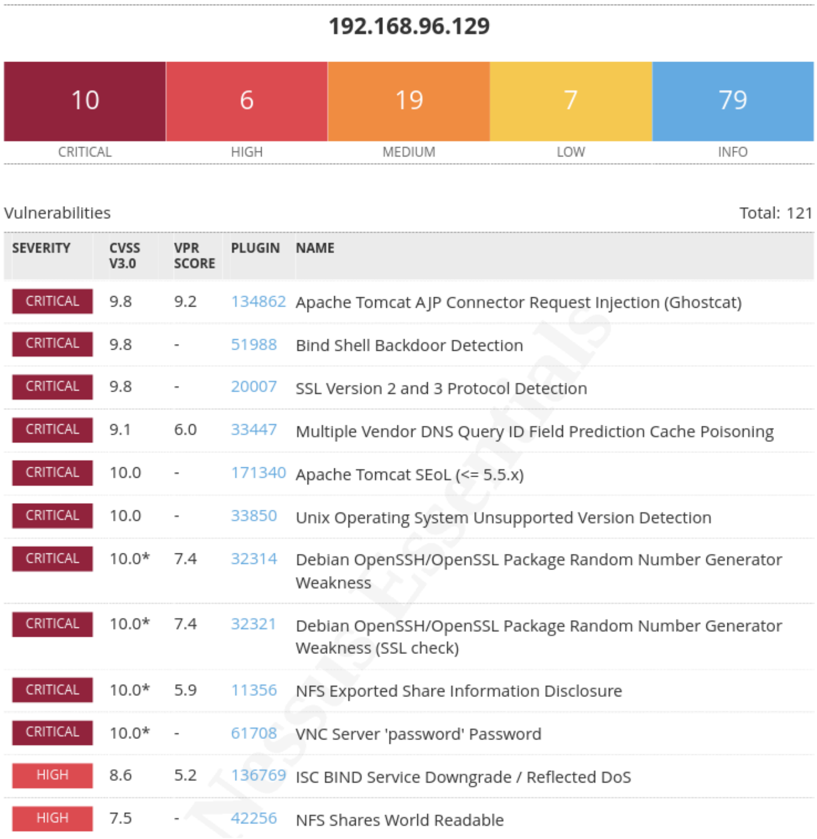
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

Template Description:
This report provides a summary list of vulnerabilities for each host detected in the scan.

Filters Applied:
None

Formatting Options:
☑ Include page breaks between vulnerability results

Here is a preview of the generated report



192.168.96.129

10	6	19	7	79
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 121

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
CRITICAL	9.8	9.2	134862	Apache Tomcat AJP Connector Request Injection (Ghostcat)
CRITICAL	9.8	-	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	-	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	9.1	6.0	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoning
CRITICAL	10.0	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0	-	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0*	7.4	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	10.0*	7.4	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	10.0*	5.9	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	42256	NFS Shares World Readable

4. REMEDIATIONS

The remediation steps for each of the identified and selected vulnerabilities is presented below.

1. Bind Shell Backdoor Detection

Please verify whether the system is already compromised and re-install the system. If the system is already compromised, it is fruitless to try and install patches as adversaries may have already installed persistent backdoors such as a “RootKit”.

2. Unix Operating System Unsupported Version Detection

The remediation step for an unsupported operating system version is to update the operating system to the latest version released from the vendor. This will have all the latest security patches required to create a secure OS. However, specific versions of the latest vendor supported image can be selected depending on current legacy applications. A patch management system is recommended so that new updates can be tested for business operations before implementing new updates.

3. NFS Exported Share Information Disclosure

To remediate this issue where anyone can mount remote shares we need to configure the NFS with a proper authentication system. This will make sure that only authorized personnel are able to mount its remote shares. Identity and Access Management can play a crucial role in creating a robust authentication and authorization framework.

4. VNC Server “password” Password

   Solution for this is to set a strong password containing alphanumeric characters so that it is not easy to guess and thus cannot be easily accessible to threat actors. Also, consider implementing password policies that include password complexity, history, and expiry.

5. Debian OpenSSH/OpenSSL Random Number Generator Weakness

   Consider that all the cryptographic material generated and present on the system is compromised and re-generate all of them. Update to the latest patch to resolve this vulnerability. This will ensure confidentiality and integrity of all the data at-rest, in-use, or in-transit.

After taking all the recommended steps to remediate vulnerabilities, it is essential to verify that the vulnerabilities are no longer present in the system. If complete remediation is not possible, businesses might take measures to mitigate which lowers risks to an acceptance level.

5. CONCLUSION

In conclusion, any organization that wants to understand the security threats posed by the technology should implement a vulnerability management program. A vulnerability scan is at the heart of this program. This project shows the importance of finding vulnerabilities present in the system. The project also demonstrates my ability to implement systems and perform vulnerability analysis to safeguard organization’s data and infrastructure.