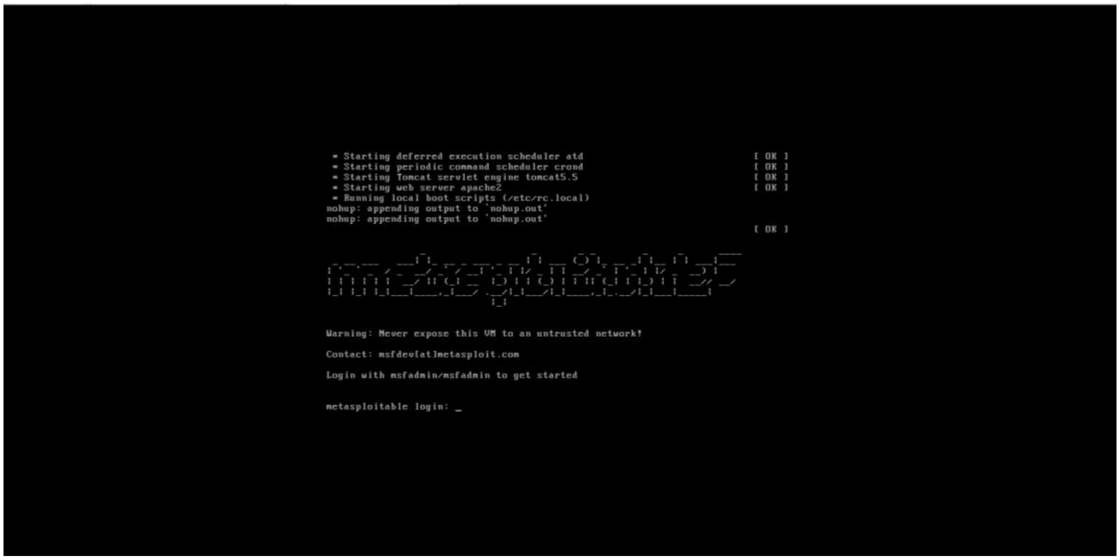
Vulnerability Management with Nessus

Install Vulnerable machine, I like to use Metasploitable2

Link to download: https://sourceforge.net/projects/metasploitable/

Link to configure Metasploitable: https://youtu.be/MY31DZiAPYA?si=CQjC5lco_IjhJXyb

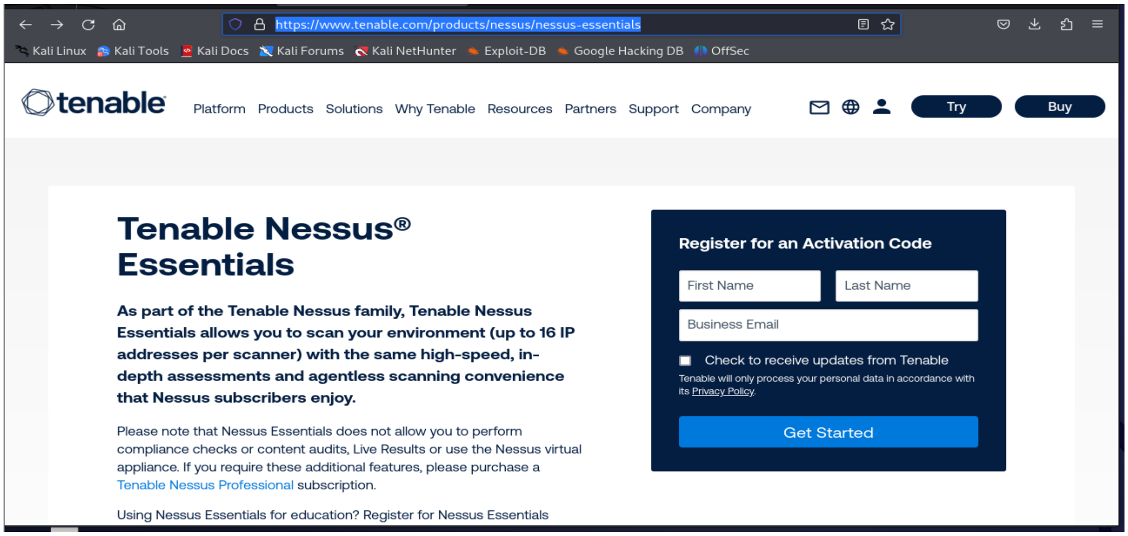


```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: _
```

Nessus Documentation for download in any OS: https://docs.tenable.com/nessus/Content/Search.htm?q=linux

In Kali Distribution:

- Link: https://www.tenable.com/products/nessus/nessus-essentials



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

Register for an Activation Code

First Name

Last Name

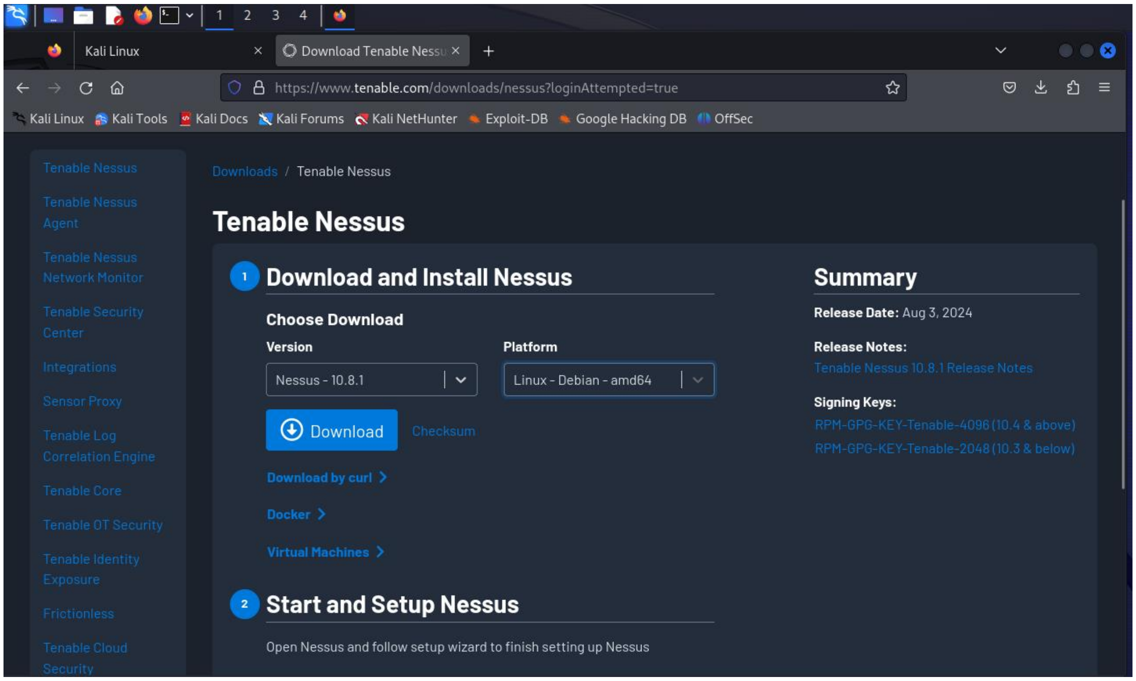
Business Email

□ Check to receive updates from Tenable

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

Get Started

- Nessus installation in Kali:



Downloads / Tenable Nessus

Tenable Nessus

1 Download and Install Nessus

Choose Download

Version: Nessus - 10.8.1

Platform: Linux - Debian - amd64

Download Checksum

Download by curl >

Docker >

Virtual Machines >

2 Start and Setup Nessus

Open Nessus and follow setup wizard to finish setting up Nessus

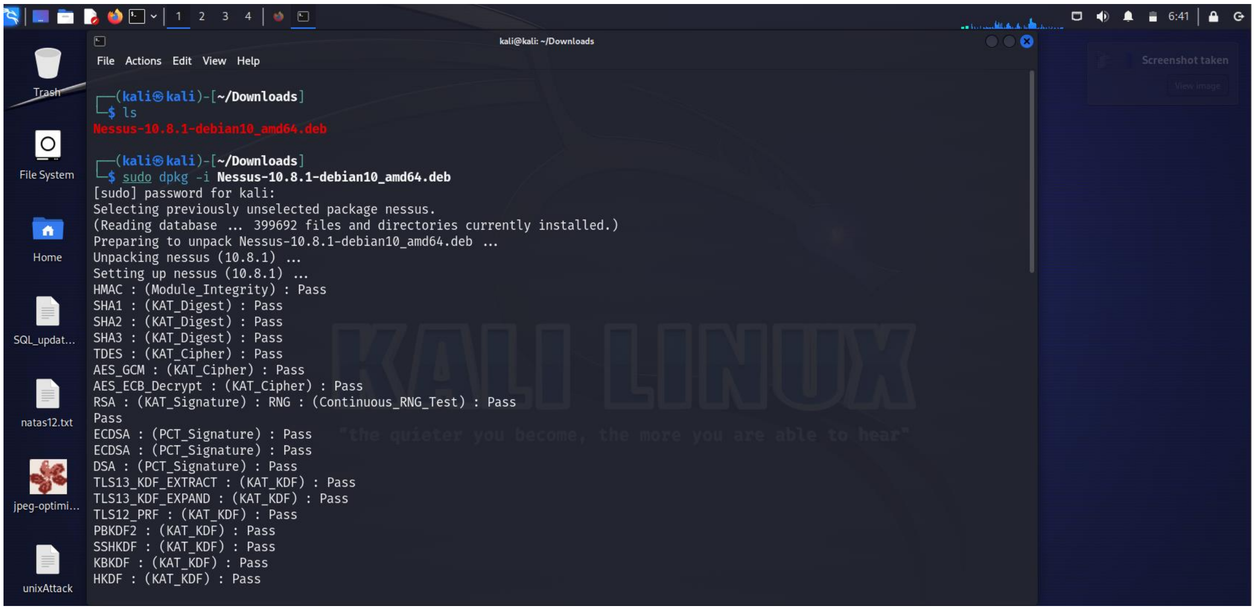
Summary

Release Date: Aug 3, 2024

Release Notes:
Tenable Nessus 10.8.1 Release Notes

Signing Keys:
RPM-GPG-KEY-Tenable-4096 (10.4 & above)
RPM-GPG-KEY-Tenable-2048 (10.3 & below)

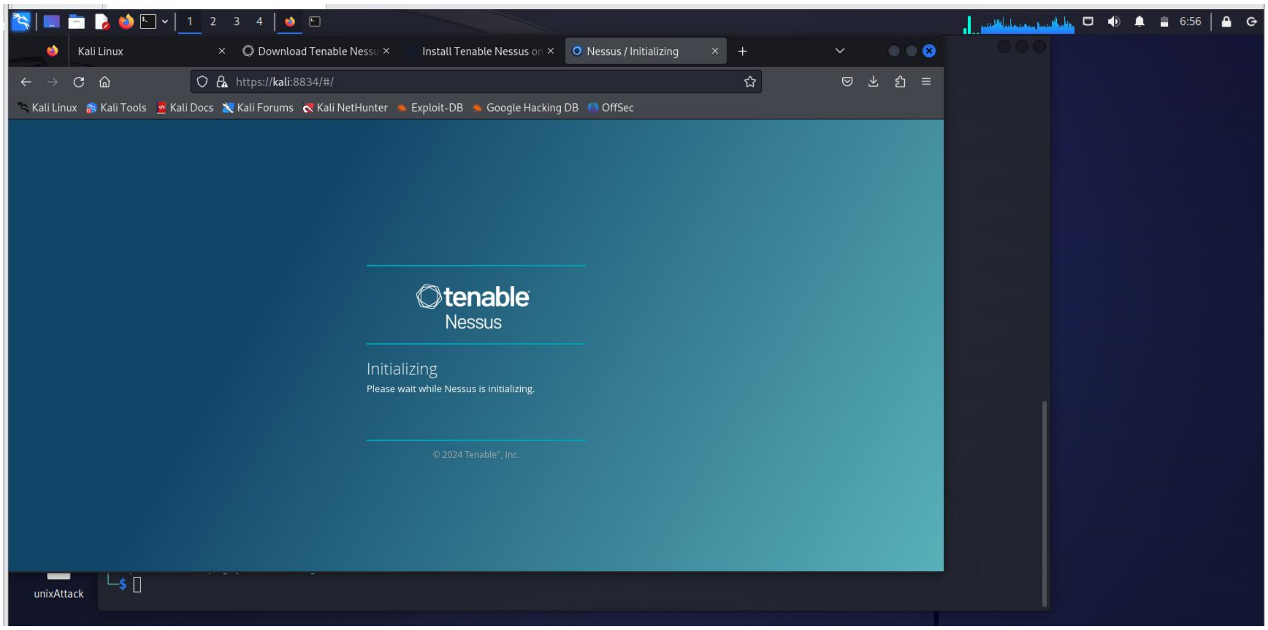
- Terminal: sudo dpkg -i Nessus-10.8.1-debian10_amd64.deb



```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Nessus-10.8.1-debian10_amd64.deb

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.8.1-debian10_amd64.deb
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 399692 files and directories currently installed.)
Preparing to unpack Nessus-10.8.1-debian10_amd64.deb ...
Unpacking nessus (10.8.1) ...
Setting up nessus (10.8.1) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
```

- To start and authenticate Nessus in your system: # systemctl start nessusd

- Access The Nessus through web browser: https://<System_IP>:8834/

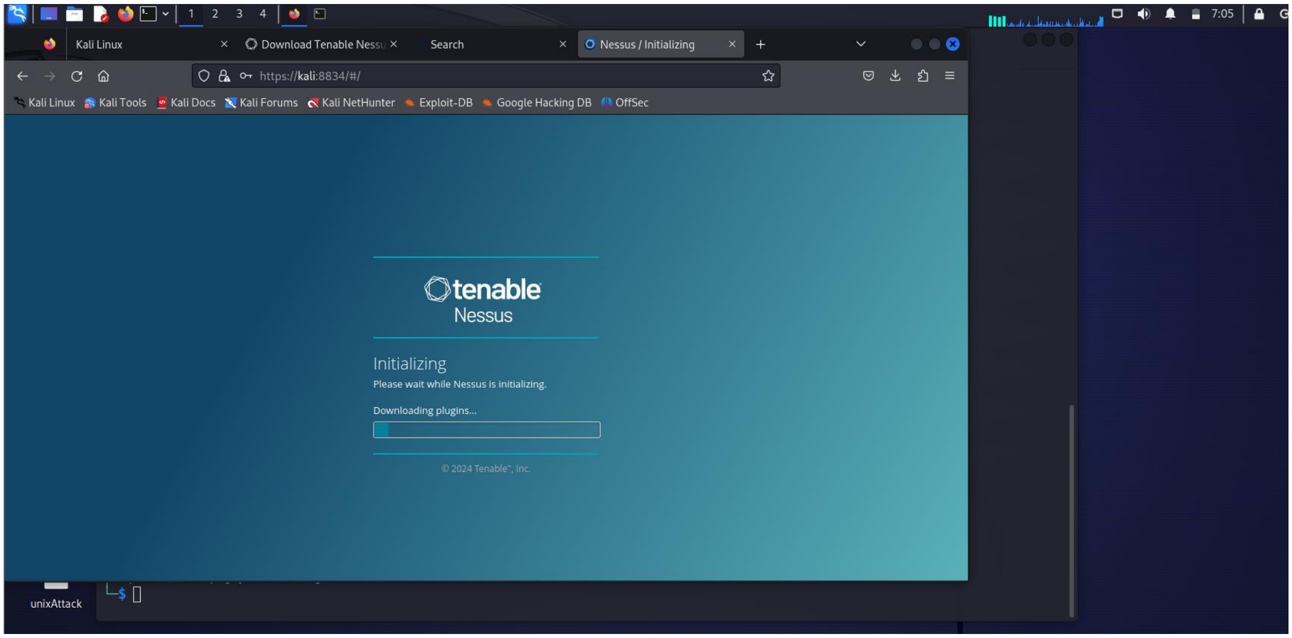


Initializing

Please wait while Nessus is initializing.

© 2024 Tenable™, Inc.

- Create an account by selecting **Register in Nessus Essential**, enter the details, and enter the activation key received via email.
(And wait for the plugin installation)



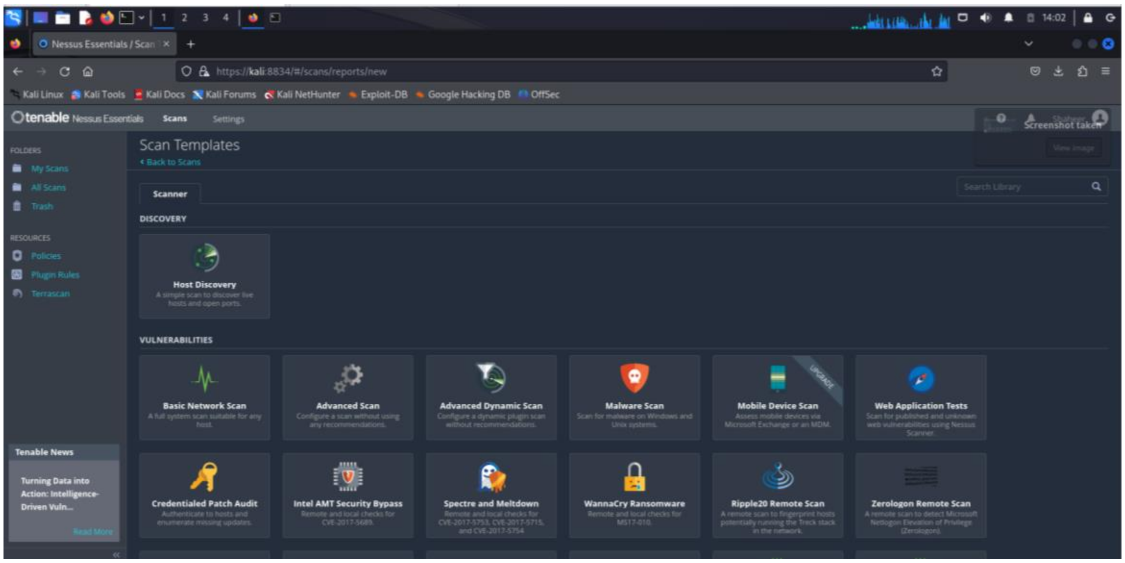
Initializing

Please wait while Nessus is initializing.

Downloading plugins...

© 2024 Tenable™, Inc.

- Go to new scan -> Basic network scan



https://kali:8834/#/scans/reports/new

Scan Templates

‹ Back to Scans

Turning Data into Action: Intelligence-Driven Vuln...

DISCOVERY

Host Discovery: A simple scan to discover live hosts and open ports.

VULNERABILITIES

Basic Network Scan: A full system scan suitable for any host.

Advanced Scan: Configure a scan without using any recommendations.

Advanced Dynamic Scan: Configure a dynamic plugin scan without recommendations.

Malware Scan: Scan for malware on Windows and Unix systems.

Mobile Device Scan: Assess mobile devices via Microsoft Exchange or an MDM.

Web Application Tests: Scan for published and unknown web vulnerabilities using Nessus Scanner.

Credentialed Patch Audit: Authenticate to hosts and enumerate missing updates.

Intel AMT Security Bypass: Remote and local checks for CVE-2017-5689.

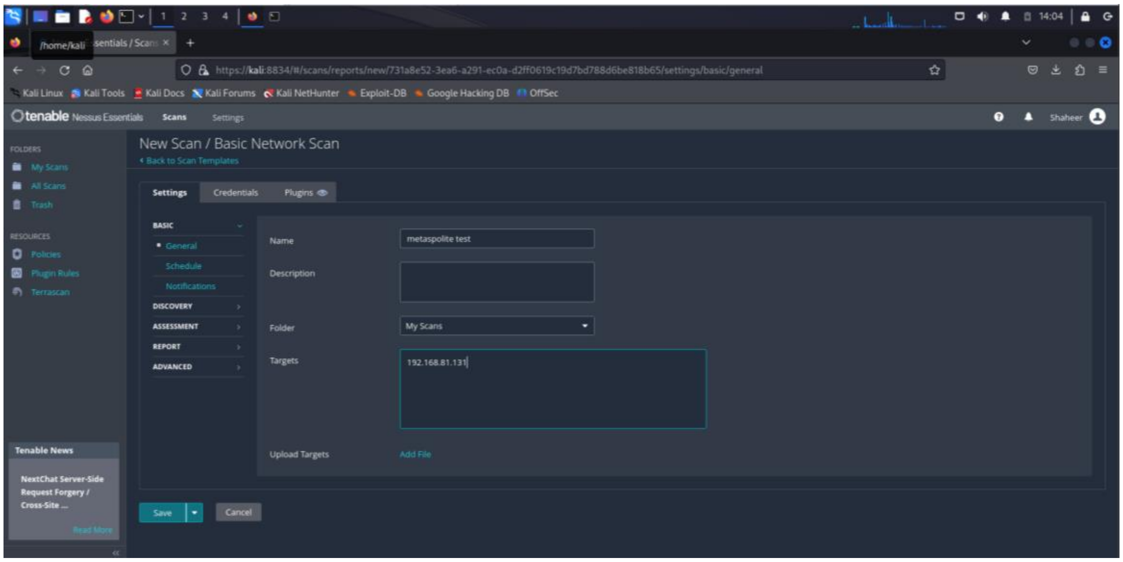
Spectre and Meltdown: Remote and local checks for CVE-2017-5753, CVE-2017-5715, and CVE-2017-5754

WannaCry Ransomware: Remote and local checks for MS17-010.

Ripple20 Remote Scan: A remote scan to fingerprint hosts potentially running the Treck stack in the network.

Zerologon Remote Scan: A remote scan to detect Microsoft Netlogon Elevation of Privilege (Zerologon).

- Add your metaspoliteable2 IP:



https://kali:8834/#/scans/reports/new/731a8e52-3ea6-a291-ec0a-d2ff0619c19d7bd788d6be818b65/settings/basic/general

New Scan / Basic Network Scan

‹ Back to Scan Templates

NextChat Server-Side Request Forgery / Cross-Site ...

Name: metaspolite test

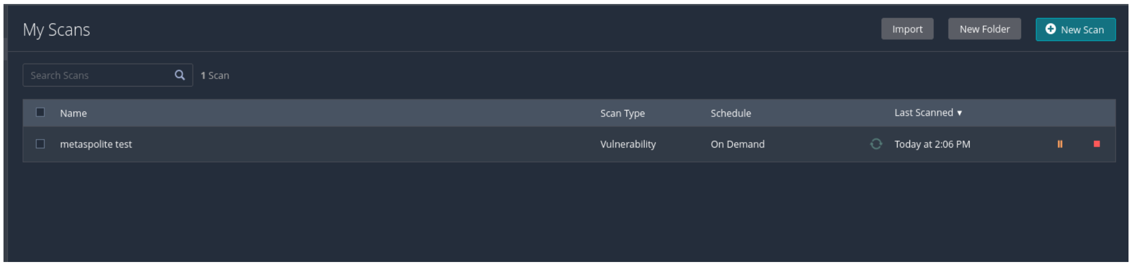
Description:

Folder: My Scans

Targets: 192.168.81.131

Upload Targets: Add File

- And start attack:

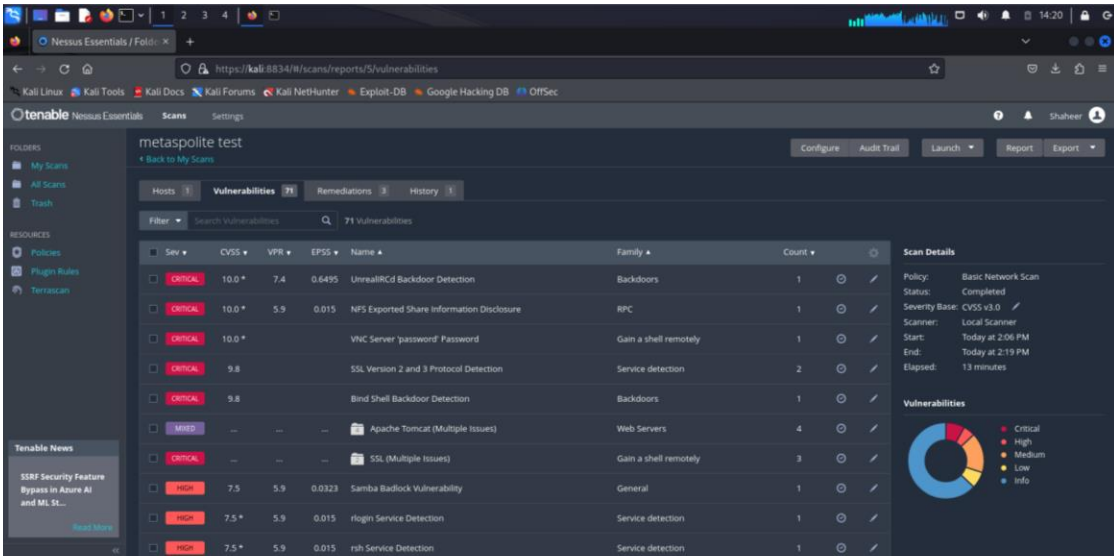


My Scans

1 Scan

Name	Scan Type	Schedule	Last Scanned ▾
metaspolite test	Vulnerability	On Demand	Today at 2:06 PM

- Scanned vulnerabilities (71 Vulnerabilities found):



metaspolite test

Back to My Scans

71 Vulnerabilities

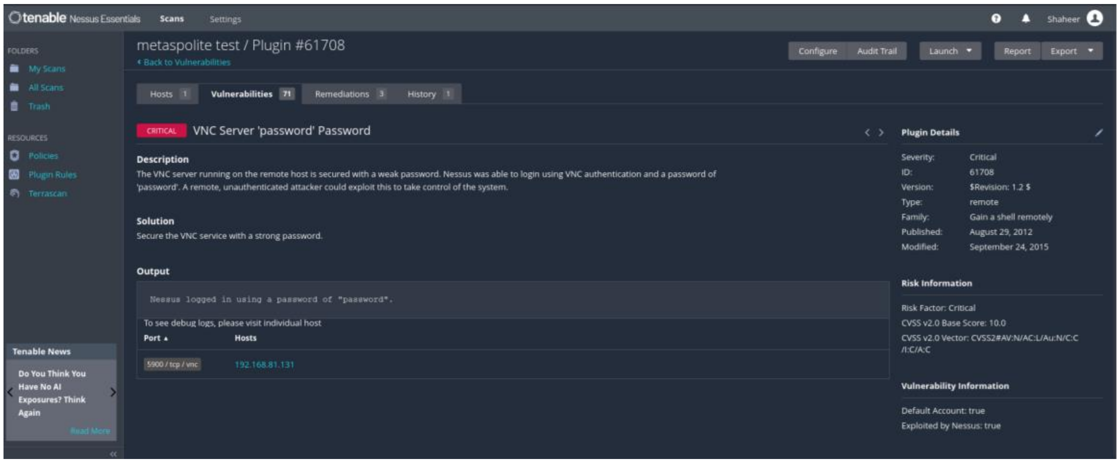
Sev	CVSS	VPR	EPSS	Name	Family	Count
CRITICAL	10.0 *	7.4	0.6495	UnrealIRCd Backdoor Detection	Backdoors	1
CRITICAL	10.0 *	5.9	0.015	NFS Exported Share Information Disclosure	RPC	1
CRITICAL	10.0 *			VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8			SSL Version 2 and 3 Protocol Detection	Service detection	2
CRITICAL	9.8			Bind Shell Backdoor Detection	Backdoors	1
MIXED	...	...	...	Apache Tomcat (Multiple Issues)	Web Servers	4
CRITICAL	...	...	...	SSL (Multiple Issues)	Gain a shell remotely	3
HIGH	7.5	5.9	0.0323	Samba Badlock Vulnerability	General	1
HIGH	7.5 *	5.9	0.015	rlogin Service Detection	Service detection	1
HIGH	7.5 *	5.9	0.015	rsh Service Detection	Service detection	1

Scan Details

Policy:	Basic Network Scan
Status:	Completed
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 2:06 PM
End:	Today at 2:19 PM
Elapsed:	13 minutes

Vulnerabilities

- Exploit anyone of vuln: i.e. VNC default password:



metaspolite test / Plugin #61708

Back to Vulnerabilities

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	192.168.81.131

Plugin Details

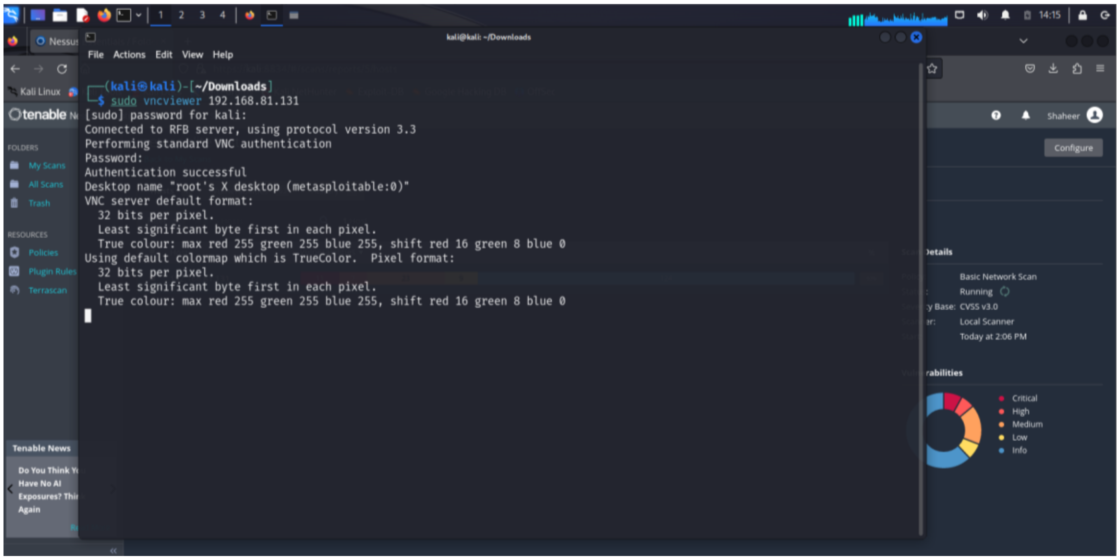
Severity:	Critical
ID:	61708
Version:	$Revision: 1.2 $
Type:	remote
Family:	Gain a shell remotely
Published:	August 29, 2012
Modified:	September 24, 2015

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

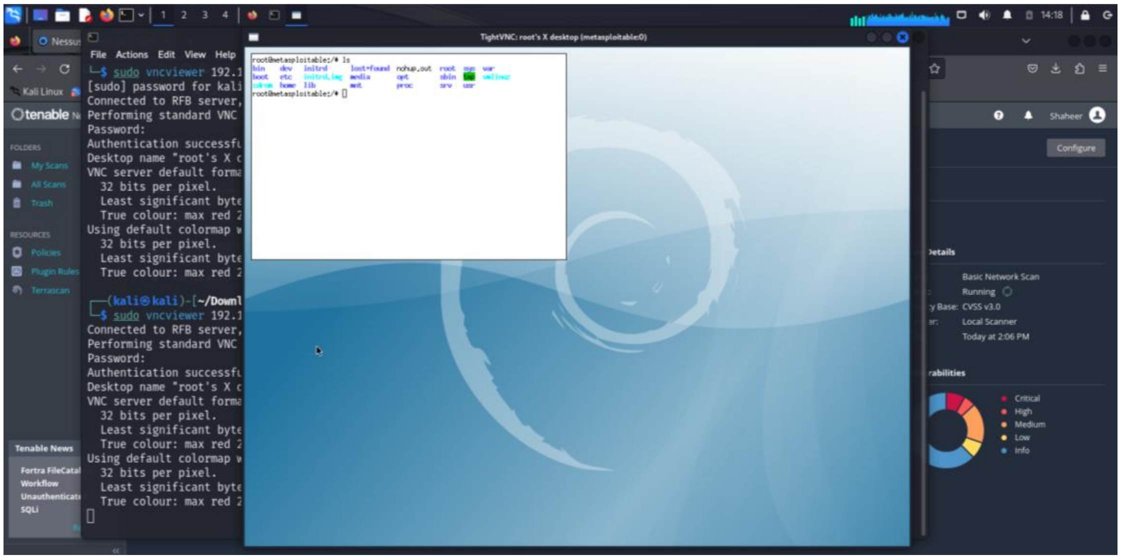
Vulnerability Information

Default Account: true
Exploited by Nessus: true



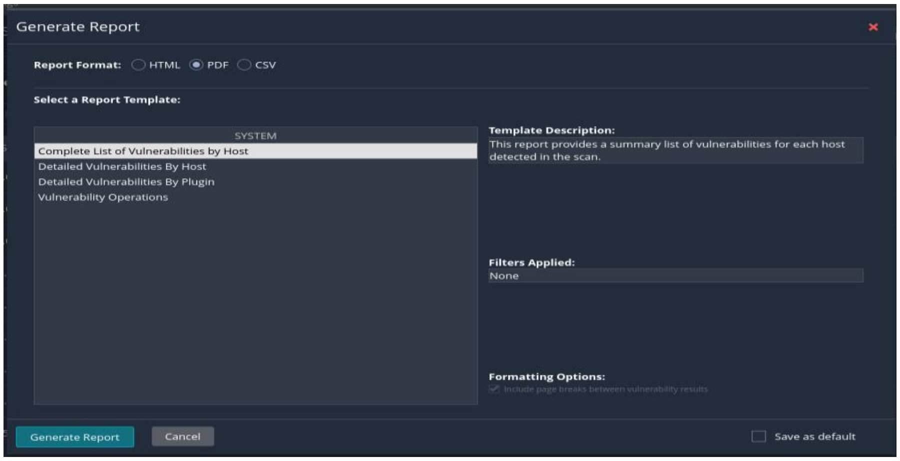
```
┌──(kali㉿kali)-[~/Downloads]
└─$ sudo vncviewer 192.168.81.131
[sudo] password for kali:
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

Remote access:


TightVNC: root's X desktop (metasploitable:0)
File Actions Edit View Help
Tenable News
Fortra FileCatalyst Workflow Unauthenticated SQLi
14:18

```
root@metasploitable:/# ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# 
```

- Report generation (Choose template):



Generate Report

Report Format: ○ HTML ● PDF ○ CSV

Select a Report Template:

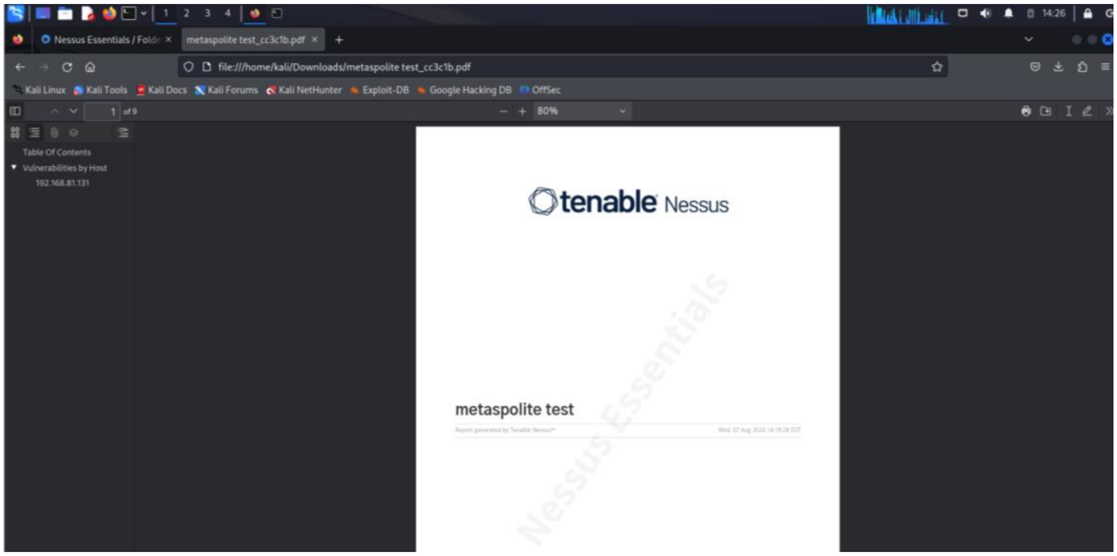
SYSTEM
Complete List of Vulnerabilities by Host
Detailed Vulnerabilities By Host
Detailed Vulnerabilities By Plugin
Vulnerability Operations

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

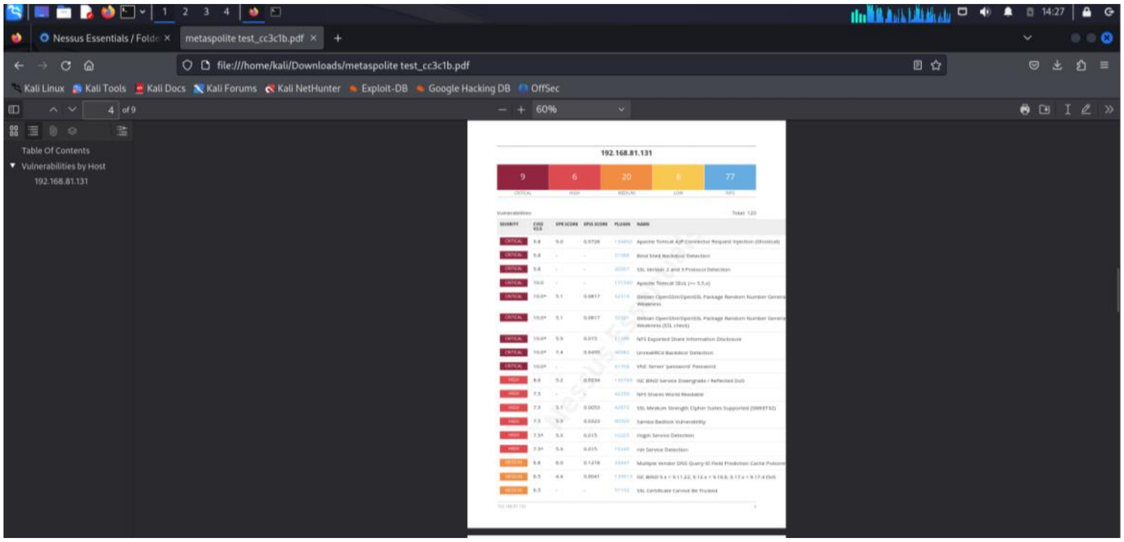
The report will be downloaded in your download section:



tenable Nessus

metaspolite test

Report generated by Tenable Nessus™



192.168.81.131

CRITICAL	HIGH	MEDIUM	LOW	INFO
9	6	20	8	77

Vulnerabilities Total: 120

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
CRITICAL	9.8	9.0	0.9728	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	10.0	-	-	171340	Apache Tomcat SEoL (<= 5.5.x)
CRITICAL	10.0*	5.1	0.0817	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0817	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	5.9	0.015	11356	NFS Exported Share Information Disclosure
CRITICAL	10.0*	7.4	0.8495	46882	UnrealIRCd Backdoor Detection
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password
HIGH	8.6	5.2	0.0234	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	-	-	42256	NFS Shares World Readable
HIGH	7.5	6.1	0.0053	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	5.9	0.0423	90509	Samba Badlock Vulnerability
HIGH	7.5*	5.9	0.015	10205	rlogin Service Detection
HIGH	7.5*	5.9	0.015	10245	rsh Service Detection
MEDIUM	6.8	6.0	0.1218	33447	Multiple Vendor DNS Query ID Field Prediction Cache Poisoni
MEDIUM	6.5	4.4	0.0041	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted

192.168.81.131

Happy Hacking ☺