PROJECT : - 1

Network Vulnerability Assessment

Objective: Scan network to identify and mitigate network vulnerabilities.

Network Assessment: A network vulnerability assessment reviews and analyzes an organization ' s network infrastructure to find cybersecurity vulnerabilities and network security loops .

How to performe :-

Network Setup:

- **Site Survey and Planning:** This involves physically inspecting the location where the network will be set up. Factors like building layout, structural considerations, and existing cabling infrastructure are assessed.
- **Design and Architecture:** Based on the site survey, a network architecture is designed. This includes decisions on the type of network (e.g., wired, wireless, or a combination), network devices (routers, switches, access points), and their placement.
- **Cabling and Hardware Installation:** Physical components like cables, routers, switches, and access points are installed according to the network design.
- **Configuration of Network Devices:** Each network device is configured with appropriate settings, such as IP addresses, routing tables, and security protocols.
- **Testing and Troubleshooting:** After installation, thorough testing is conducted to ensure all components are functioning properly. Any issues are identified and resolved.
- **Documentation:** Comprehensive documentation of the network setup, including configurations, IP addresses, and device details, is created. This is crucial for future troubleshooting and expansion.
-

Configuration:

- **IP Addressing:** Assigning unique IP addresses to each device on the network. This can involve static IP assignments or dynamic addressing using protocols like DHCP.
- **Subnetting and VLAN Configuration:** Segmentation of the network into smaller, more manageable subnetworks for security, traffic management, and organization.

PROJECT : - 1

- **Routing and Switching Configuration:** Determining how data packets are forwarded between different parts of the network.
- **Wireless Network Configuration:** Setting up wireless access points, securing them with encryption protocols, and optimizing signal strength and coverage.
- **Quality of Service (QoS):** Configuring QoS settings to prioritize certain types of traffic over others, ensuring critical applications get the bandwidth they need.
- **Network Services Configuration:** Configuring services like DNS (Domain Name System), DHCP, and NAT (Network Address Translation) as needed.

Security:

- **Firewall Setup:** Implementing firewalls to control incoming and outgoing traffic based on an applied rule set, thereby protecting the network from unauthorized access.
- **Intrusion Detection/Prevention Systems (IDS/IPS):** Setting up systems to monitor network traffic for suspicious activity and potentially block or alert on threats.
- **Antivirus and Anti-malware:** Deploying security software to protect against viruses, malware, and other malicious software.
- **Access Control and Authentication:** Implementing measures like user authentication, role-based access control, and multi-factor authentication to ensure only authorized users can access network resources.
- **Encryption:** Configuring protocols like SSL/TLS to secure data in transit and VPNs (Virtual Private Networks) for secure remote access.

Tools : -

Nmap (Network Mapper): A powerful network scanning tool used for discovering hosts and services on a computer network.

Metasploit Framework: A penetration testing framework that makes it easy to exploit known vulnerabilities in networks, servers, and applications.

Wireshark: A network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network.

Burp Suite: An integrated platform for performing security testing of web applications. It's particularly useful for finding and exploiting web application vulnerabilities.

Aircrack-ng: A suite of tools for assessing WiFi network security. It includes packet sniffing, password cracking, and other wireless network auditing tools.

PROJECT : - 1

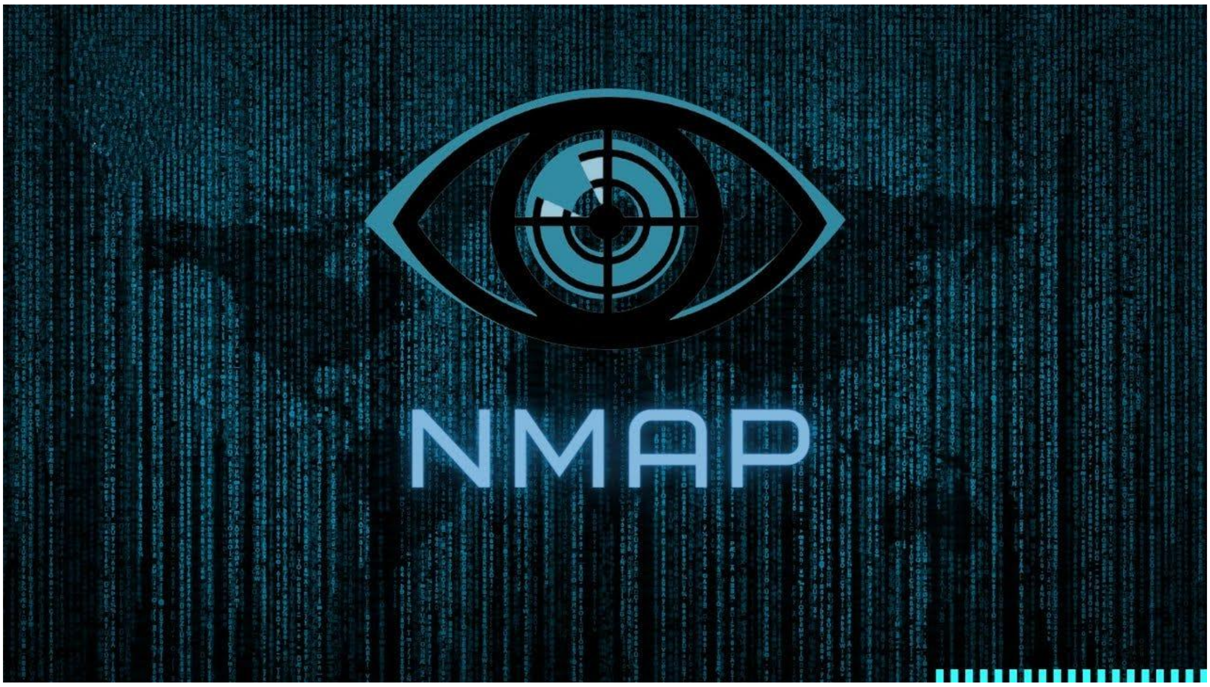
Hydra: A password-cracking tool that supports various protocols, including HTTP, HTTPS, FTP, and many others.

John the Ripper: Another password-cracking tool that can be used to identify weak passwords through brute-force attacks or dictionary attacks.

OpenVAS (Open Vulnerability Assessment System): A comprehensive vulnerability scanning tool that helps detect and classify vulnerabilities in computer systems and networks.

SQLMap: A powerful tool for automating the detection and exploitation of SQL injection vulnerabilities in web applications.

Nikto: A web server scanner that performs comprehensive tests against web servers for multiple items, including dangerous files/CGIs, outdated server software, and other potential vulnerabilities.



Nmap (Network Mapper): A powerful network scanning tool used for discovering hosts and services on a computer network

PROJECT : - 1

1. *Installation*: First, ensure Nmap is installed on your system. In Kali Linux, it's usually pre-installed, but you can also install it via the package manager if needed.

2. *Syntax*: Nmap commands follow a specific syntax. You typically start with the command nmap followed by various options and arguments to specify the target(s) and scan type.

3. *Target Specification*: Specify the target(s) you want to scan. This can be a single IP address, a range of IP addresses, a hostname, or even a CIDR notation for subnet scanning.

4. *Scan Types*: Choose the type of scan you want to perform. Common scan types include:

- *TCP SYN Scan (-sS)*: Stealthy scan that sends SYN packets to target ports and analyzes responses to determine if the port is open.
- *TCP Connect Scan (-sT)*: A full TCP connection is made to each port to check if it's open.
- *UDP Scan (-sU)*: Scans for open UDP ports.
- *Comprehensive Scan (-sC)*: Executes a series of scripts against the target, providing detailed information.

5. *Options and Flags*: Nmap offers numerous options and flags to customize the scan. These can include specifying port ranges, timing options, output formats, verbosity levels, and more.

6. *Execution*: Once you've configured the scan type, target(s), and options, execute the Nmap command. Nmap will start scanning the specified target(s) according to the chosen scan type and options.

7. *Analysis*: As Nmap scans the target(s), it gathers information about open ports, services running on those ports, and potentially other details such as operating system detection and service version detection.

8. *Output*: After the scan completes, Nmap provides a summary of its findings. Depending on the options used, this can include detailed information about open ports, services, operating systems, and more. You can save the output to a file for further analysis if needed.

9. *Interpretation*: Analyze the results of the scan to identify potential vulnerabilities, misconfigurations, or security risks in the target network.

PROJECT : - 1

10. *Follow-up*: Depending on the purpose of your scan, you may take further actions such as exploiting discovered vulnerabilities (if authorized), providing recommendations for improving security, or conducting additional scans for deeper analysis.

Advantages of Nmap:

Comprehensive Network Scanning:

Nmap is a comprehensive network scanner that can be used to discover hosts on a network, identify open ports, and determine which services are running on those ports. It provides a detailed picture of a network's structure and the devices connected to it.

Platform Independence:

Nmap is platform-independent and supports various operating systems like Windows, Linux, macOS, and more. This cross-platform compatibility makes it a flexible and accessible tool for network administrators and security professionals across different environments.

Robust Port Scanning Options:

Nmap offers a wide range of scanning techniques, including TCP SYN scan, TCP connect scan, UDP scan, and more. These scanning options allow users to tailor their scans based on the specific requirements of the target network and optimize the scanning process.

Scriptable and Extensible:

Nmap comes with a scripting engine called NSE (Nmap Scripting Engine), which allows users to create and share custom scripts for specific tasks. This scripting capability enhances Nmap's functionality and adaptability for diverse network scanning needs.

Fast and Efficient:

Nmap is known for its speed and efficiency in scanning large networks. It can perform scans quickly and accurately, making it a valuable tool for network administrators looking to assess network security and identify potential vulnerabilities.

Disadvantages of Nmap:

Intrusive Scanning:

While Nmap is an excellent network mapping tool, its scanning techniques can be considered intrusive, especially on production networks. Certain scanning methods may trigger security alerts or cause disruptions on the network being scanned.

Complex User Interface:

Nmap's command-line interface can be intimidating for beginners and those less familiar with the tool. Understanding and configuring the various scanning options may require some learning and experimentation.

Limited Windows GUI:

Although Nmap provides command-line and graphical user interface (GUI) options, the Windows GUI version may not be as feature-rich as its command-line counterpart. Users who prefer a visual interface might find the GUI version lacking certain functionalities.

False Positives:

In some cases, Nmap may produce false positives, incorrectly identifying open ports or services due to firewalls, NAT devices, or other network configurations. This can lead to potentially misleading results if not interpreted correctly.

Ethical and Legal Considerations:

While Nmap is a legitimate security tool, using it without proper authorization to scan networks you do not own or manage may be illegal and considered unethical. It's essential to use Nmap responsibly and with appropriate permissions.

Conclusion:

In conclusion, Nmap is a powerful and valuable tool for network scanning and mapping, offering extensive features, platform independence, and robust scanning options ,

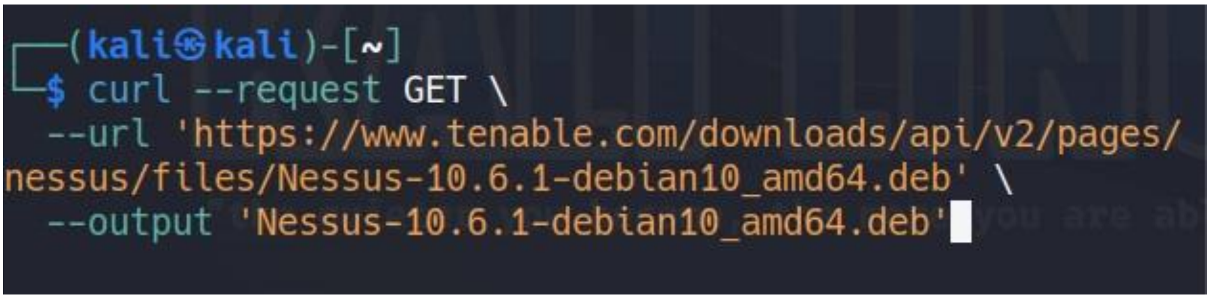
Tools Nessus : -

ABOUT NESSUS : -

PROJECT : - 1

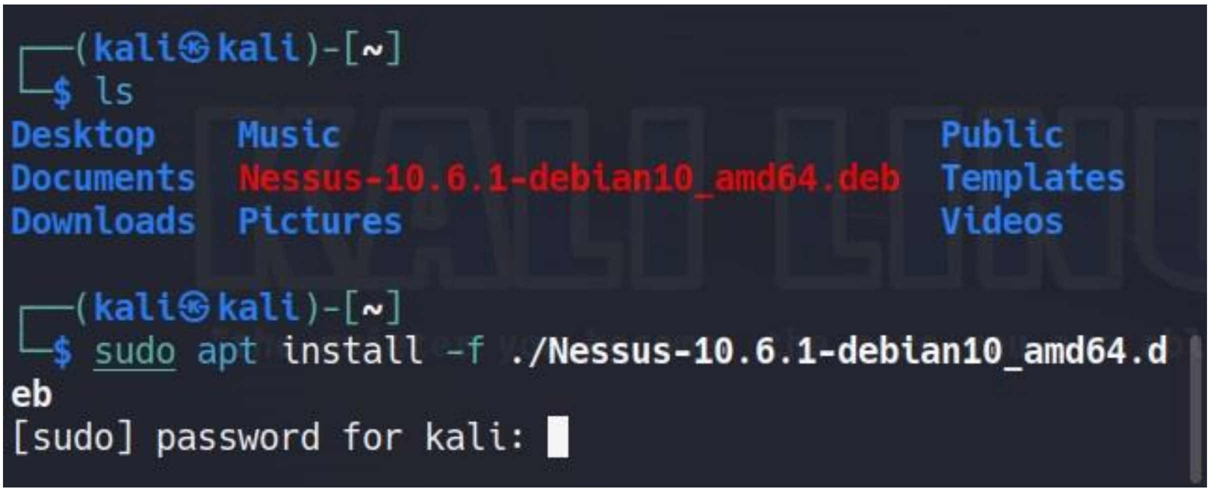
Nessus is a remote security scanning tool that checks for vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. It was originally released as an open source tool in 1998, and its enterprise edition became a commercial product in 2005. Nessus is known for its large plugin database, which is automatically compiled to improve scan performance Nessus is designed to be simple, intuitive, and portable. It has the following features: Vulnerability assessment Web application scans External attack surface scans Cloud infrastructure scans Pre-built policies and templates Customizable reporting Nessus is beginner-friendly and doesn 't require advanced knowledge of operating systems or command line tools .

HOW TO DOWNLOAD AND USE NESSUS : -



```
┌──(kali㉿kali)-[~]
└─$ curl --request GET \
  --url 'https://www.tenable.com/downloads/api/v2/pages/
nessus/files/Nessus-10.6.1-debian10_amd64.deb' \
  --output 'Nessus-10.6.1-debian10_amd64.deb'
```

Once the latest version of Nessus is downloaded, it can be installed as shown below.

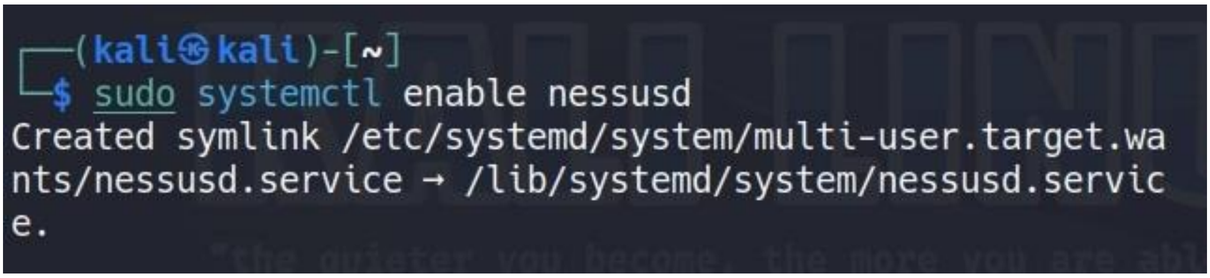


```
┌──(kali㉿kali)-[~]
└─$ ls
Desktop    Music                             Public
Documents  Nessus-10.6.1-debian10_amd64.deb  Templates
Downloads  Pictures                          Videos

┌──(kali㉿kali)-[~]
└─$ sudo apt install -f ./Nessus-10.6.1-debian10_amd64.d
eb
[sudo] password for kali: 
```

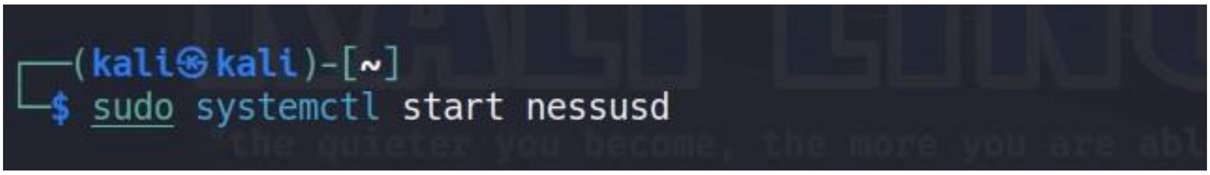
Once the installation is finished, enable nessus as shown below.

PROJECT : - 1



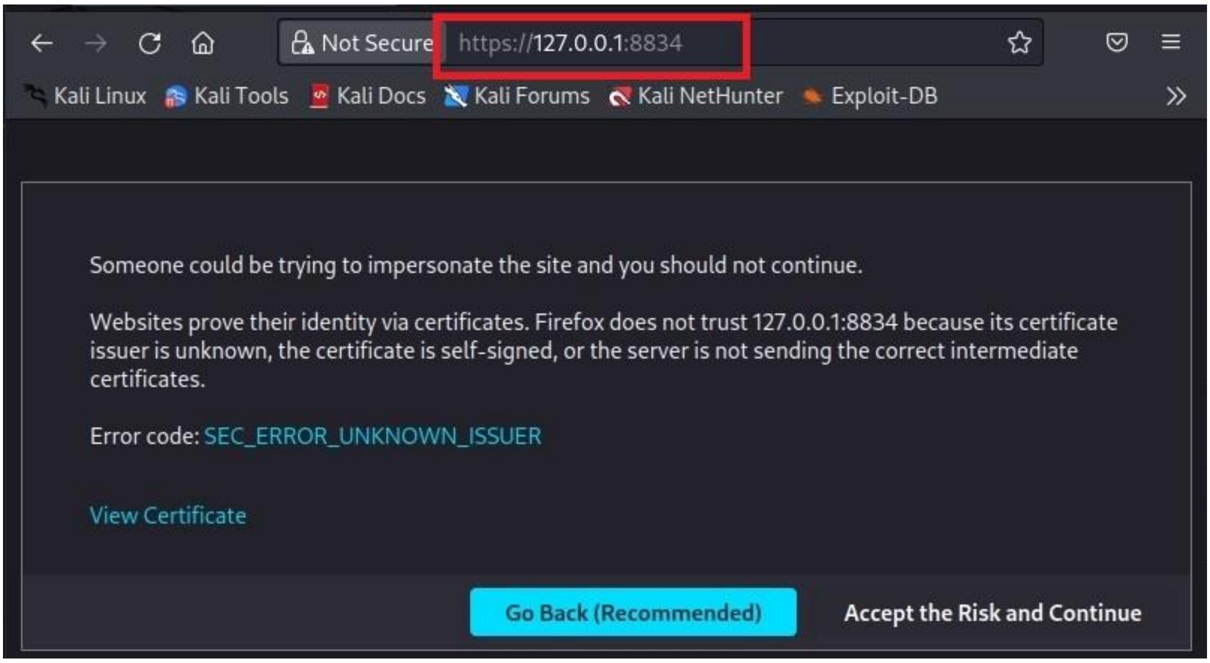
```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl enable nessusd
Created symlink /etc/systemd/system/multi-user.target.wa
nts/nessusd.service → /lib/systemd/system/nessusd.servic
e.
```

Then start nessus as shown below



```
┌──(kali㉿kali)-[~]
└─$ sudo systemctl start nessusd
```

Nessus runs on port 8834 by default. It can be viewed in browser



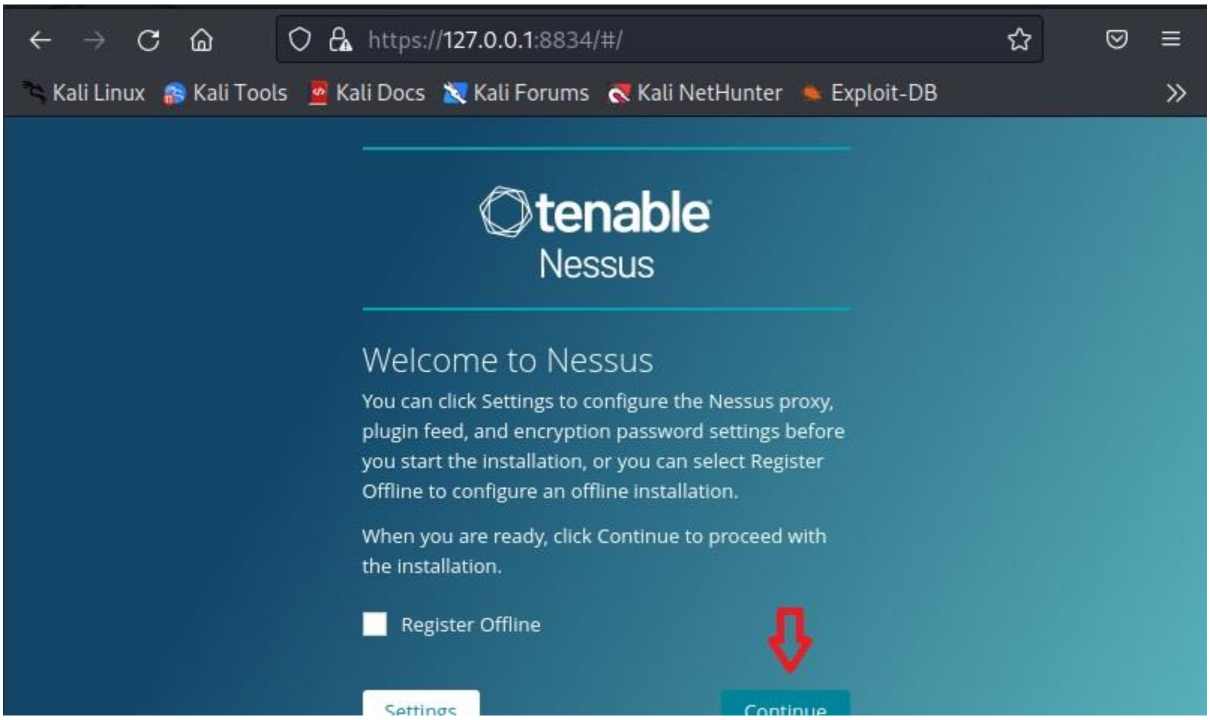
Someone could be trying to impersonate the site and you should not continue.

Websites prove their identity via certificates. Firefox does not trust 127.0.0.1:8834 because its certificate issuer is unknown, the certificate is self-signed, or the server is not sending the correct intermediate certificates.

Error code: SEC_ERROR_UNKNOWN_ISSUER

Click on “Accept the risk and continue”.

PROJECT : - 1



Welcome to Nessus

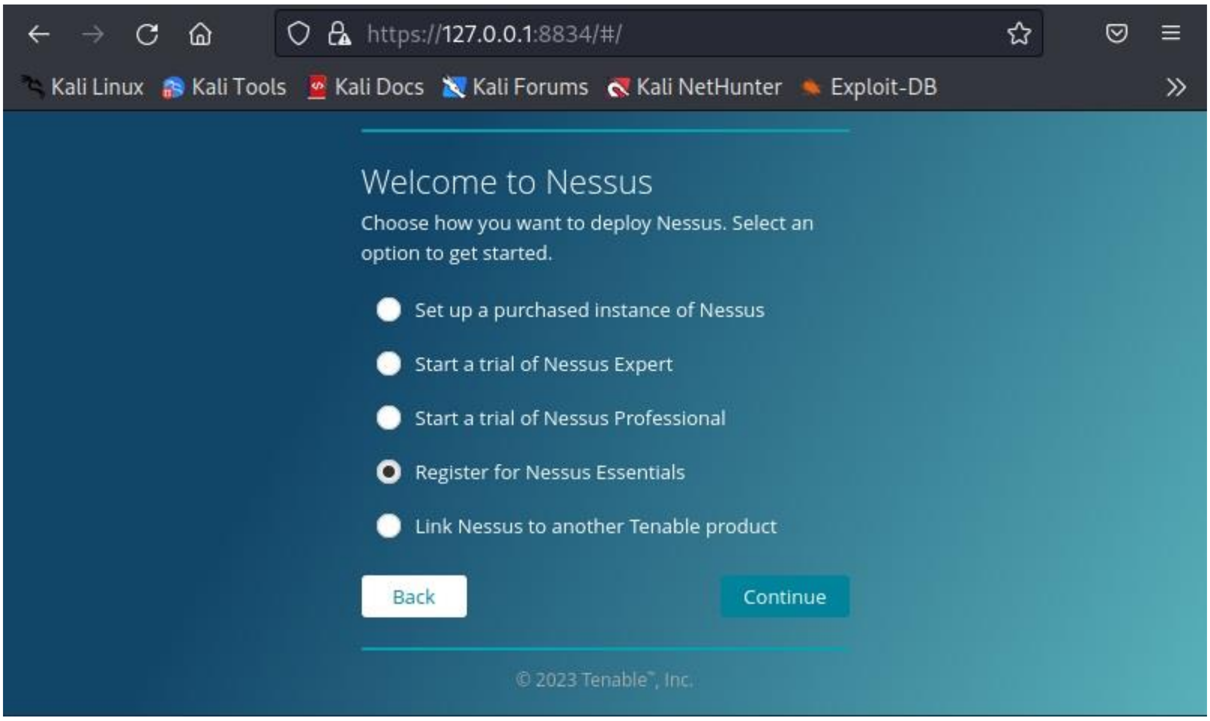
You can click Settings to configure the Nessus proxy, plugin feed, and encryption password settings before you start the installation, or you can select Register Offline to configure an offline installation.

When you are ready, click Continue to proceed with the installation.

□ Register Offline

Click on “Continue”. Select the type of Nessus install you want. Since we are using a Free version of Nessus for this tutorial we select “Register for Nessus Essentials”. Click on “continue”.

PROJECT : - 1

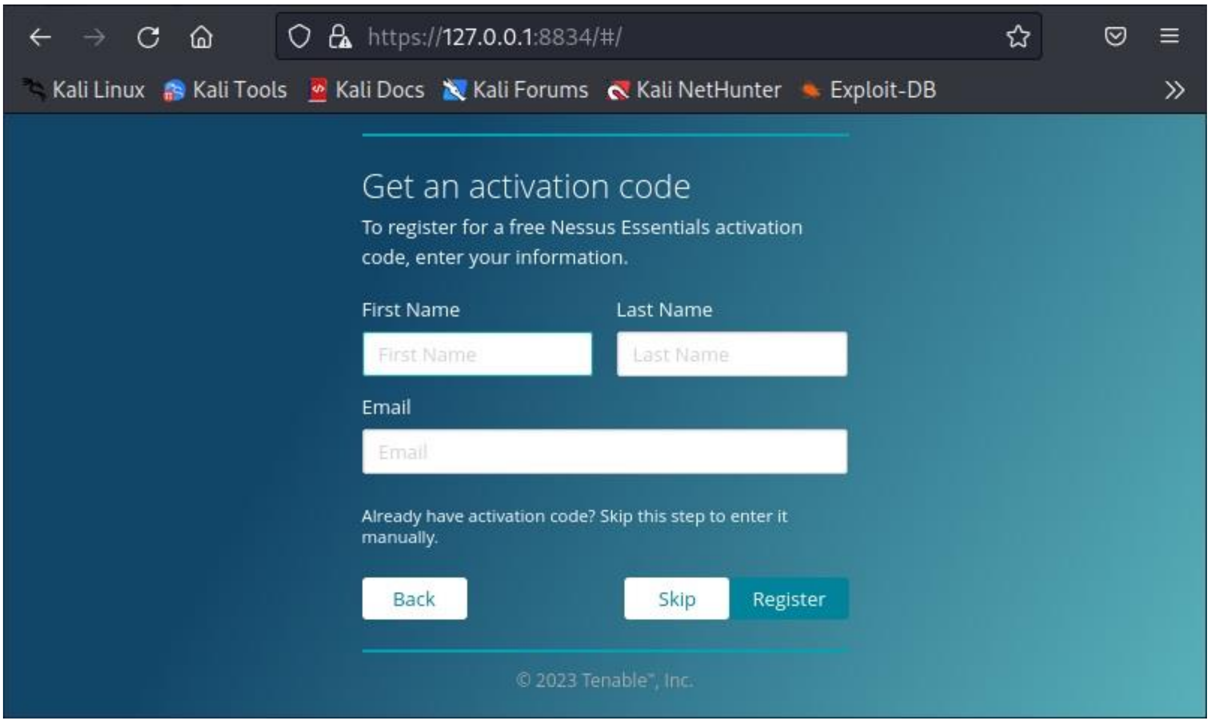


Welcome to Nessus

Choose how you want to deploy Nessus. Select an option to get started.

○ Set up a purchased instance of Nessus
○ Start a trial of Nessus Expert
○ Start a trial of Nessus Professional
● Register for Nessus Essentials
○ Link Nessus to another Tenable product

To run Nessus Essentials, you need an activation code. Get the activation code by entering the following details



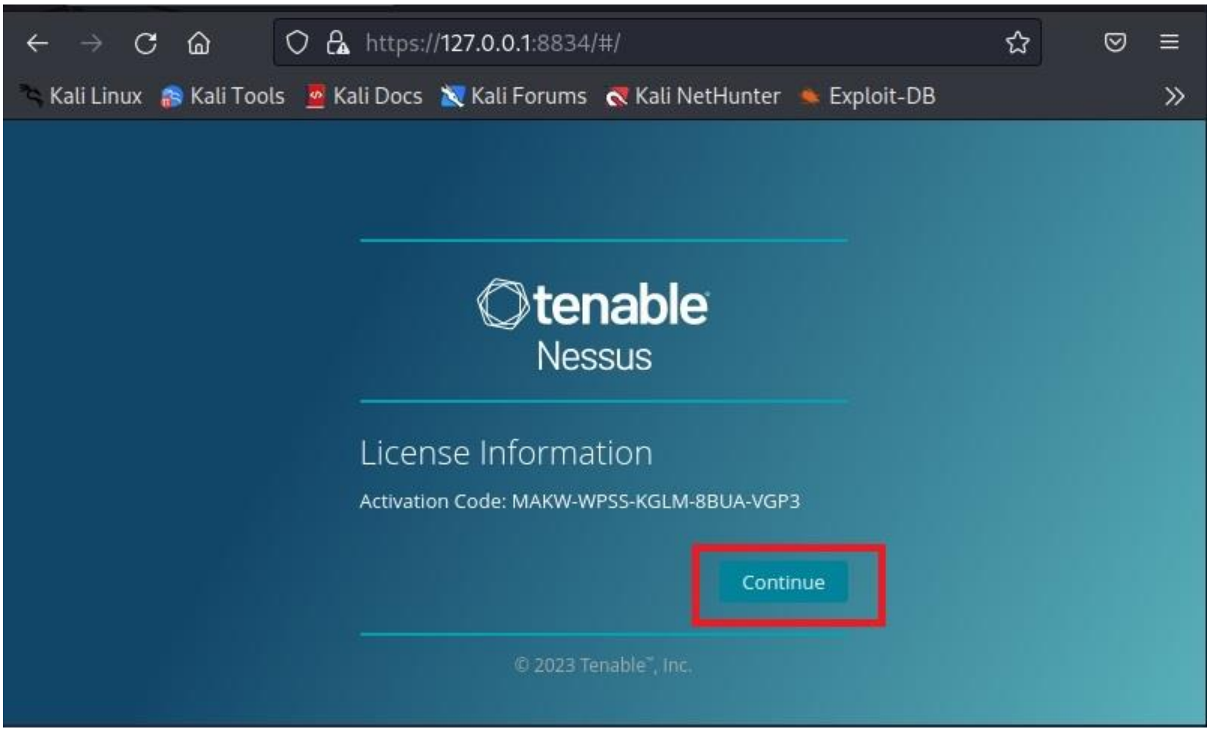
Get an activation code

To register for a free Nessus Essentials activation code, enter your information.

First Name: First Name
Last Name: Last Name
Email: Email

Already have activation code? Skip this step to enter it manually.

PROJECT : - 1

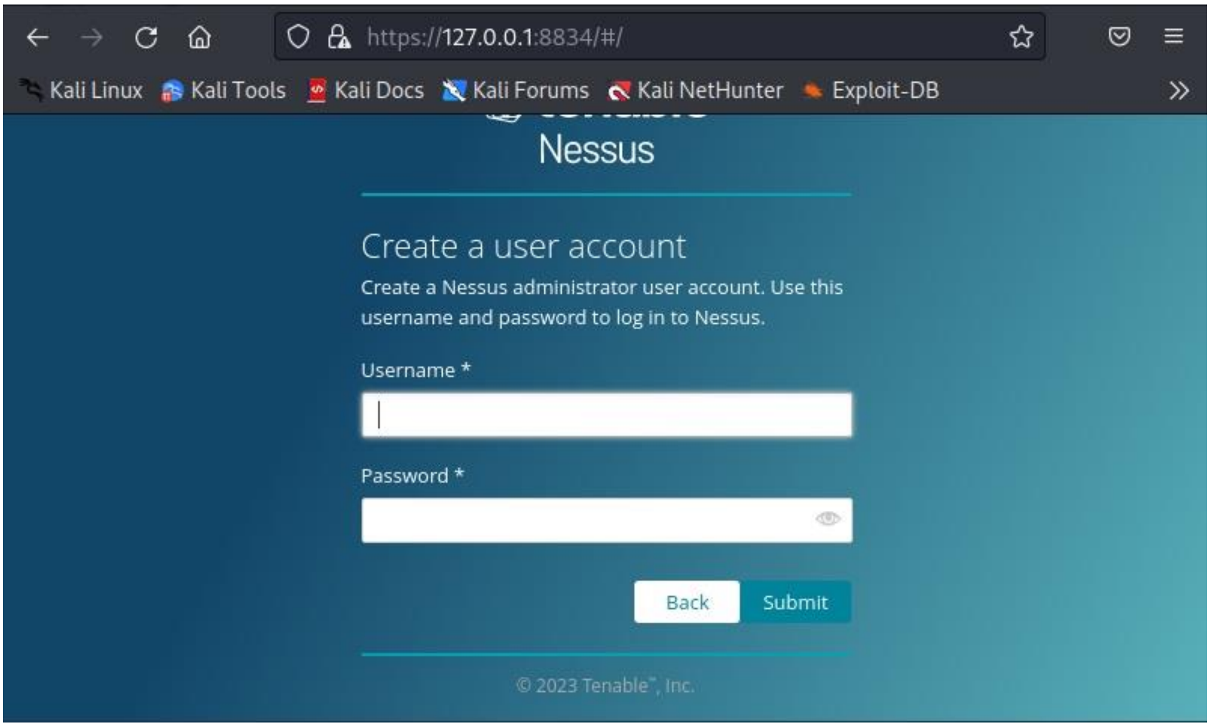


License Information

Activation Code: MAKW-WPSS-KGLM-8BUA-VGP3

You need a user account to login into Nessus. Create an account and most importantly remember the user account information.

PROJECT : - 1



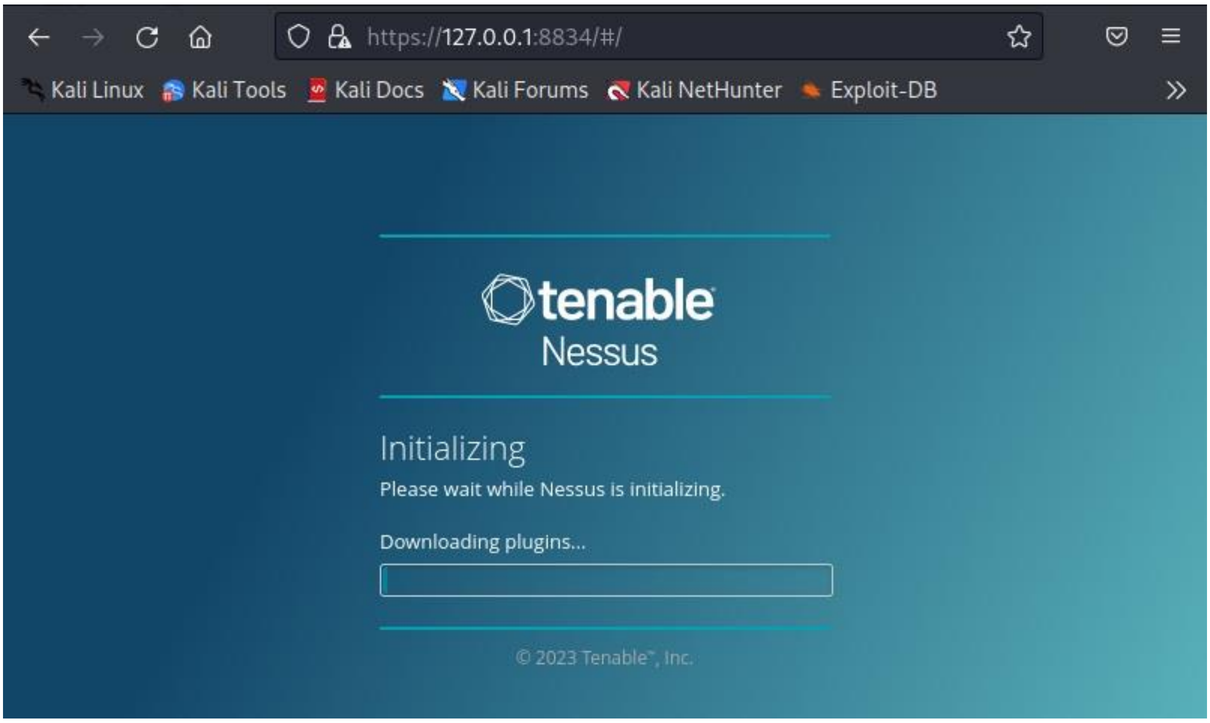
Create a user account

Create a Nessus administrator user account. Use this username and password to log in to Nessus.

Username *

Password *

Then, Nessus will download all the required plugins. This may take some time (a bit long time sometimes).



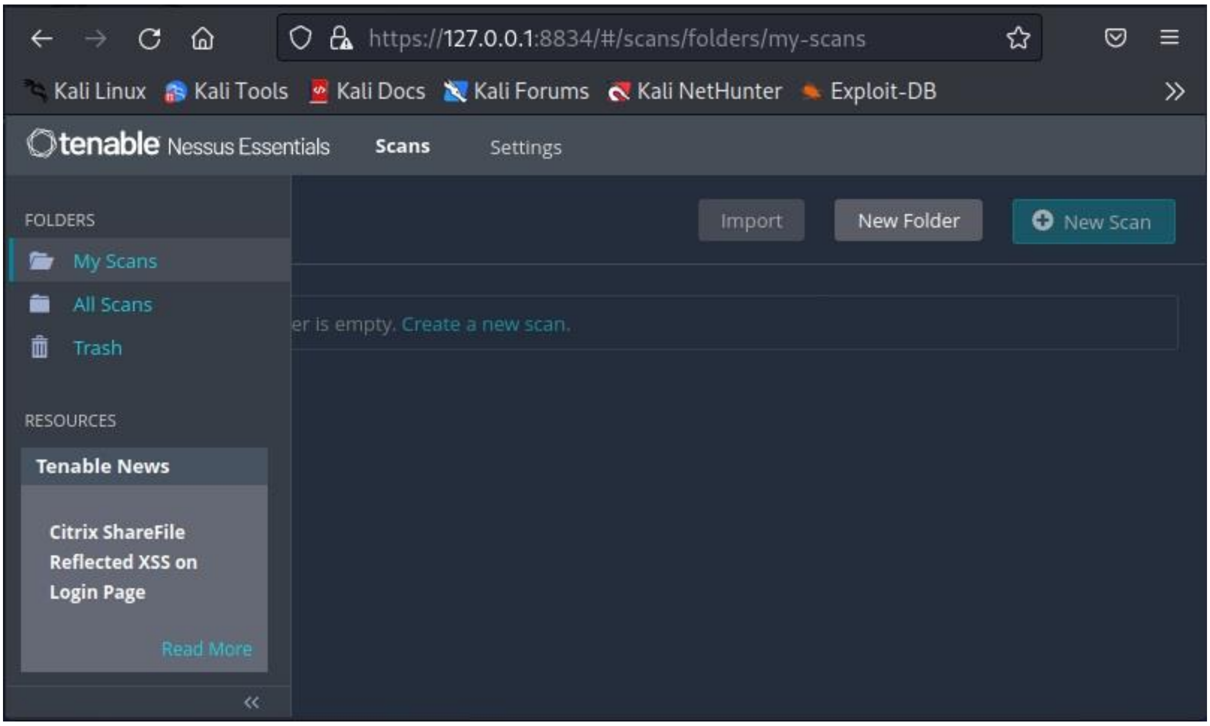
Initializing

Please wait while Nessus is initializing.

Downloading plugins...

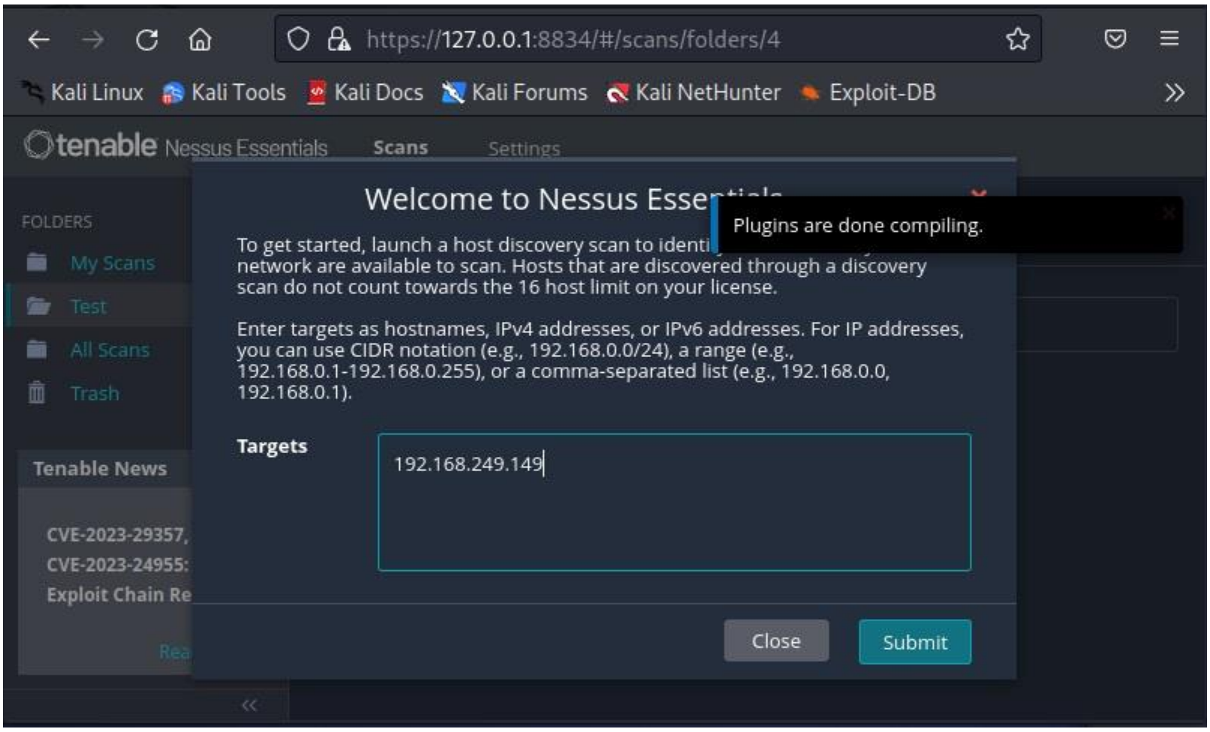
Once all the plugins are finished downloading, you should see this.

PROJECT : - 1



er is empty. Create a new scan.

The installation is finished. Now, it’s time to start scanning with Nessus. Click on “New scan”. A new popup opens. Assign a target.



Welcome to Nessus Esse

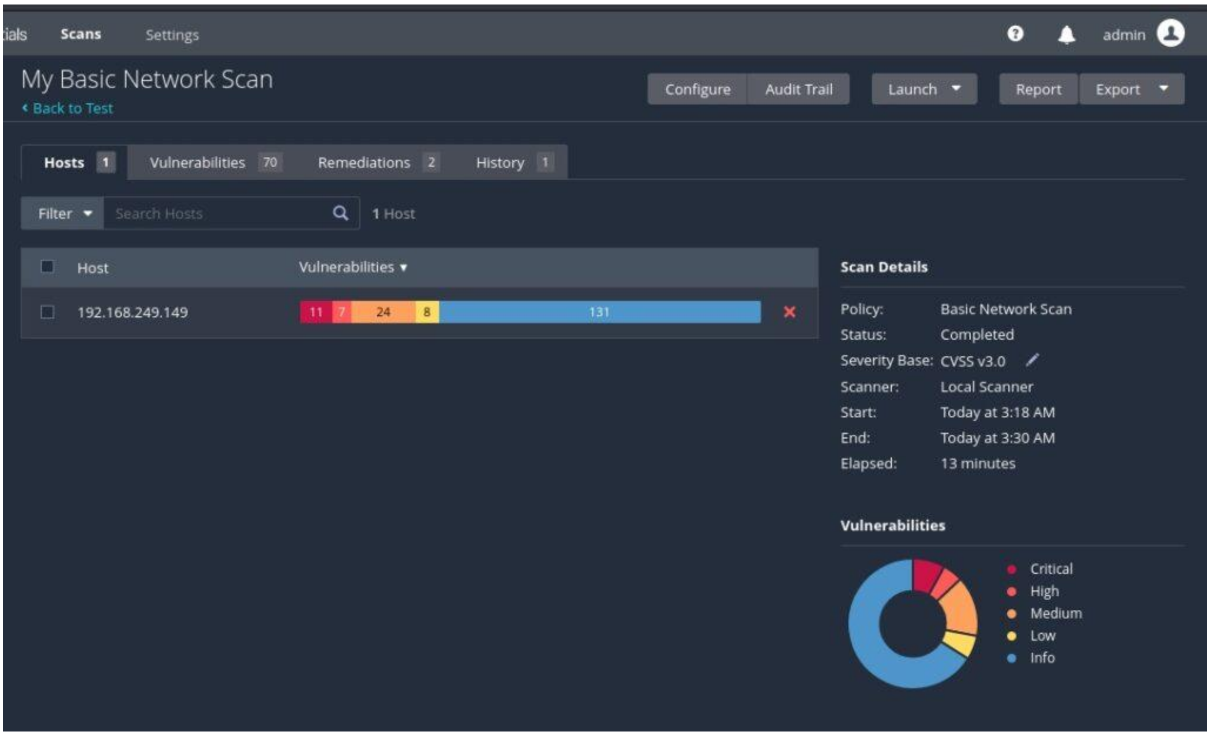
Plugins are done compiling.

To get started, launch a host discovery scan to identi network are available to scan. Hosts that are discovered through a discovery scan do not count towards the 16 host limit on your license.

Enter targets as hostnames, IPv4 addresses, or IPv6 addresses. For IP addresses, you can use CIDR notation (e.g., 192.168.0.0/24), a range (e.g., 192.168.0.1-192.168.0.255), or a comma-separated list (e.g., 192.168.0.0, 192.168.0.1).

Targets: 192.168.249.149

The scan will start and take some time to finish



My Basic Network Scan

‹ Back to Test

Host	Vulnerabilities ▾
192.168.249.149	11 7 24 8 131

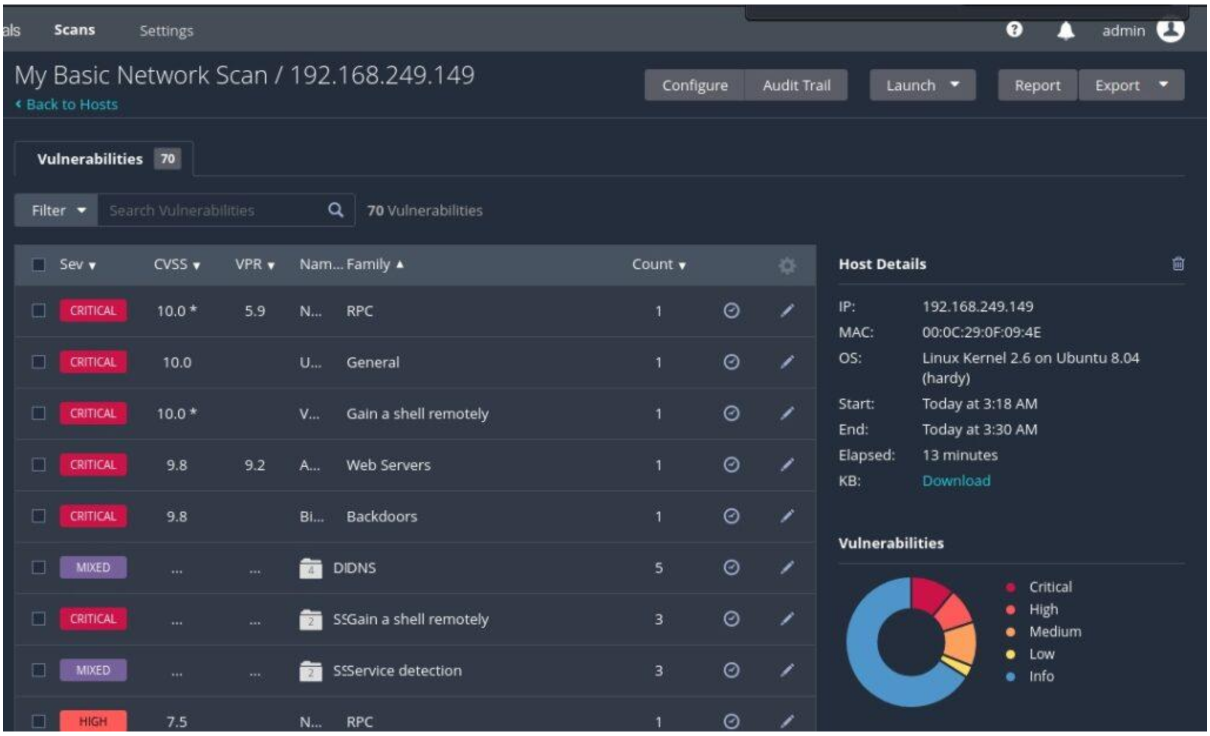
Scan Details

Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 3:18 AM
End: Today at 3:30 AM
Elapsed: 13 minutes

Vulnerabilities

The vulnerabilities are classified into five categories by Nessus. They are Critical, High, Medium, Low and Information. You can view detailed information about the detected vulnerabilities by clicking on them.

PROJECT : - 1



My Basic Network Scan / 192.168.249.149

70 Vulnerabilities

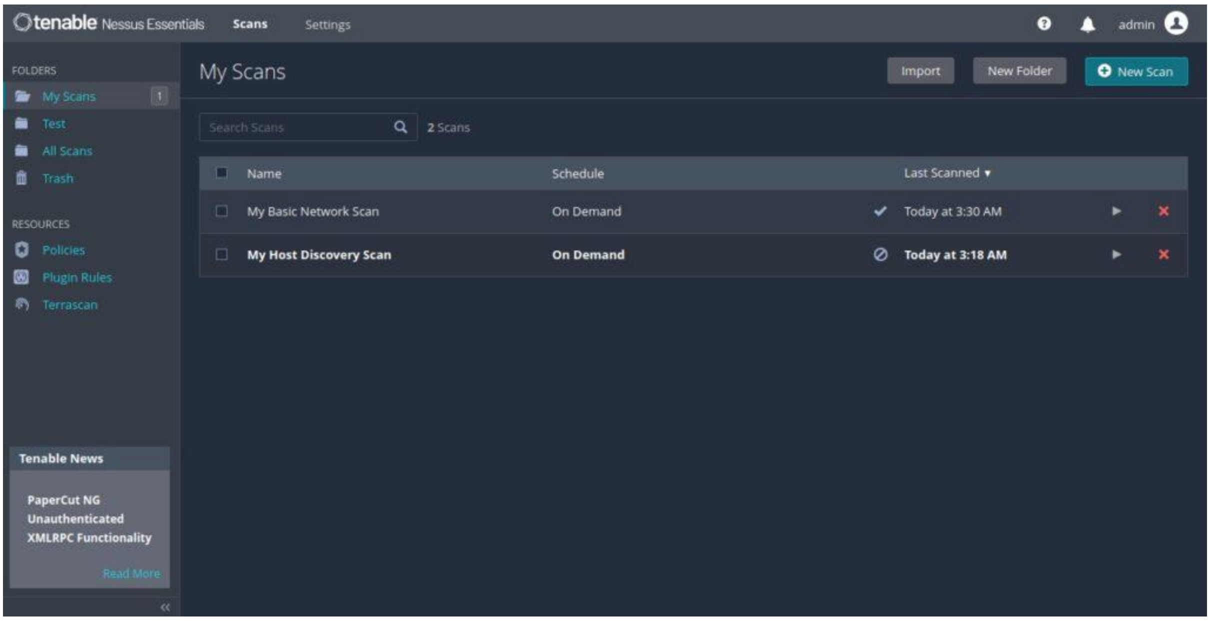
Sev	CVSS	VPR	Nam...	Family	Count
CRITICAL	10.0 *	5.9	N...	RPC	1
CRITICAL	10.0		U...	General	1
CRITICAL	10.0 *		V...	Gain a shell remotely	1
CRITICAL	9.8	9.2	A...	Web Servers	1
CRITICAL	9.8		Bi...	Backdoors	1
MIXED	...	...	4	DIDNS	5
CRITICAL	...	...	2	SSGain a shell remotely	3
MIXED	...	...	2	SSService detection	3
HIGH	7.5		N...	RPC	1

Host Details

IP: 192.168.249.149
MAC: 00:0C:29:0F:09:4E
OS: Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
Start: Today at 3:18 AM
End: Today at 3:30 AM
Elapsed: 13 minutes
KB: Download

Vulnerabilities

All the scans you perform are located in “My scans” section.



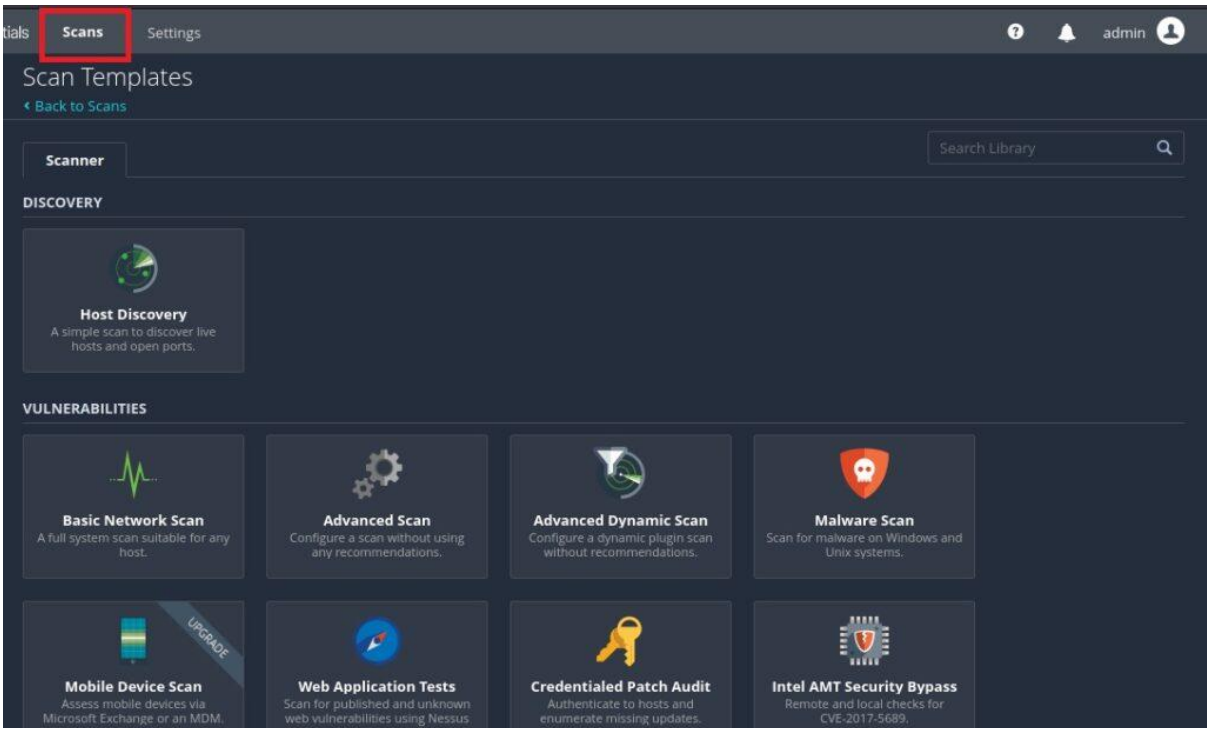
My Scans

2 Scans

Name	Schedule	Last Scanned
My Basic Network Scan	On Demand	✓ Today at 3:30 AM
My Host Discovery Scan	On Demand	Today at 3:18 AM

Nessus allows different types of scans. All the scans that can be performed using Nessus can be viewed from “All scans” section.

PROJECT : - 1



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

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

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

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

What are the Benefits of Nessus?

Some of the major benefits are as follows;

- **Scalable Architecture:** It is designed to handle large-scale environments, making it suitable for organizations of all sizes. It can efficiently scan thousands of hosts simultaneously, enabling comprehensive vulnerability assessments even in complex and expansive network infrastructures.
- **Advanced Scanning Capabilities**: It offers advanced scanning options such as credentialed scanning, which allows for authenticated scans to gain deeper insights into the configuration and security of the target systems. This enhances the accuracy and reliability of vulnerability assessments.
- **Vulnerability Prioritization:** It provides a risk-based approach to vulnerability management. It assigns severity levels to identified vulnerabilities, allowing organizations to prioritize remediation efforts based on the potential impact on the business and the likelihood of exploitation.
- **Customization and Flexibility:** It allows users to customize scans based on specific requirements. It offers the flexibility to select specific targets, configure scan parameters, and customize reporting formats, enabling organizations to tailor vulnerability assessments to their unique needs.

- **Threat Intelligence Integration:** It integrates with threat intelligence platforms, enabling organizations to enrich vulnerability data with real-time threat information. This integration enhances the context of vulnerability assessments, allowing security teams to prioritize remediation based on the current threat landscape.
- **Remediation Workflow Integration:** It facilitates the remediation process by integrating with ticketing and workflow management systems. This enables seamless collaboration between security teams and IT departments, streamlining the vulnerability remediation workflow and ensuring timely resolution of identified issues.
- **Regulatory Compliance Reporting:** It simplifies compliance reporting by providing built-in templates for various regulatory frameworks, such as PCI DSS, HIPAA, and GDPR. It helps organizations demonstrate adherence to security standards and streamline the compliance reporting process.
- **API and Automation Capabilities:** It offers an extensive API that allows for integration with other security tools and systems. This enables automation of vulnerability scanning, data retrieval, and reporting, enhancing efficiency and enabling seamless integration with existing security infrastructure.
- **Continuous Innovation:** It is developed by Tenable, a leading provider of cybersecurity solutions. Tenable consistently invests in research and development, ensuring that Nessus remains at the forefront of vulnerability assessment technology, incorporating the latest advancements and industry best practices.

Conclusion

Nessus is a powerful and versatile vulnerability assessment tool that helps organizations proactively manage their security risks. With comprehensive coverage, advanced scanning techniques, and compliance auditing capabilities, it provides accurate vulnerability detection. Its scalability, customization options, and integration capabilities make it suitable for organizations of all sizes. By automating processes and offering continuous monitoring, it saves time and resources while ensuring ongoing security vigilance. With a strong user community and continuous innovation, it remains at the forefront of vulnerability assessment technology. Overall, it empowers organizations to strengthen their security, achieve compliance, and protect critical assets.

THANKS EXTION INFOTECH

Submitted by – RAHUL SAHU

Email – rahulsahurs403@gmail.com