Nessus: A Security vulnerability Scanning tool

What is Nessus?

Nessus works as a remote security scanning tool. It aims to spot weaknesses that bad actors could use to break into computers on a network. This software runs more than 1,200 checks on a given computer. It evaluates if any of these possible attacks might compromise the system or cause damage.

Who would use a tool like this?

If you manage any computer or network linked to the internet, Nessus can help you out. It's a great tool to safeguard your systems from common weak spots that hackers and viruses often go after.

What Nessus is NOT

Nessus isn't a full security fix, but it plays a part in a bigger security plan. It doesn't stop attacks on its own; rather, it checks your computers to find weak spots that hackers might exploit. The system admin needs to patch these weak spots to keep things safe.

Why Nessus?

If you know about other network vulnerability scanners, you might want to know what makes Nessus stand out. Here are some key points:

Nessus doesn't guess about your server setup, unlike some scanners. For example, it won't just assume port 80 is open. This helps make sure real weak spots don't get missed.

- Nessus has great flexibility. It comes with a scripting language that lets you make tests just for your system as you get better at using the tool. It also has a plug-in interface. You can find many free plug-ins on the

Nessus plug-in site. People often design these to spot specific viruses or weak spots.

- Nessus gives you fresh info about new weak spots and attacks. The Nessus team updates the list of weak spots to check every day. This cuts down the time between when a new threat pops up and when you can spot it.
- Nessus is open-source. This means you can use it for free. You can also look at and change the source code if you need to.
- Help with patching: When Nessus spots a weak point, it suggests the best way to fix and reduce the problem.

How Nessus Works

To grasp how Nessus and other port-scanning security tools work, you need to understand how people access different services (like web servers, SMTP servers, FTP servers, etc.) on a remote server. Most high-level network traffic, including email and web pages, reaches a server through high-level protocols sent over a TCP stream. To keep different streams from interfering with each other, a computer splits its physical network connection into thousands of logical paths called ports. For instance, to talk to a web server on a specific machine, you connect to port 80 (the standard HTTP port). But to communicate with an SMTP server on the same machine, you'd connect to port 25.

Every computer has thousands of ports. These ports may or may not have services running on them. Services are servers for specific high-level protocols. Nessus checks each port on a computer to find out which service is active. It then evaluates that service to spot any weak points a hacker could use for harmful actions. People call Nessus a "remote scanner" because you don't need to put it on the computer you're checking. You can set it up on one machine and use it to test as many other computers as you want.

Scan Templates:

You have the ability to create custom policies for your organization using scan templates. Once you've done this, you can carry out scans based on Tenable's preset templates or the settings in your custom policies.

When you start to make a scan or policy in Tenable Nessus, you'll come across the Scan Templates or Policy Templates section. Tenable Nessus offers different templates for scanners and agents allowing you to choose the right sensor to match your scanning needs.

Tenable Nessus offers scanner templates that simplify scan setup and execution. These templates cater to various scanning requirements and objectives helping users to perform specific checks. Nessus includes several common scanner templates:

- The **Basic Network Scan** conducts a general network check to identify common vulnerabilities.
- The **Advanced Scan** allows users to customize options for detailed tailored checks.
- **Web Application Tests** search for vulnerabilities unique to web apps such as SQL injection or cross-site scripting (XSS).
- **Compliance Audits** verify if systems follow industry standards and regulations like PCI DSS, HIPAA, or CIS benchmarks.
- **Credentialed Scans** use login credentials to access systems for a thorough vulnerability examination.
- **Malware Scans** aim to detect harmful software on the network.
- **Host Discovery** identifies active devices without performing a complete vulnerability assessment.
- **Patch Management Audits** check whether systems have the latest security updates.

These templates streamline the scanning process enabling users to initiate scans that address their specific security needs.

There are three scanner Template categories:

Discovery: Tenable suggests discovery scans to identify hosts on your network and gather related details. These details might include IP addresses, FQDNs, operating systems, and open ports when available. Once you have a host list, you can select which ones to target in a specific vulnerability scan.

Vulnerabilities: Tenable recommends using vulnerability scan templates for most of your organization's regular scanning needs. Tenable also provides specialized vulnerability scan templates. These templates let you scan your network to find specific vulnerabilities or groups of vulnerabilities. Tenable continues to update the Nessus scan template library with new templates. These new templates help detect the latest known vulnerabilities such as Log4Shell.

Compliance: Tenable recommends configuration scan templates to check if host setups follow different industry standards. These checks, which people also call compliance scans, make sure systems follow specific rules. To get more info about what these compliance scans can examine, check out the Compliance and SCAP Settings.

Installation

Step 1: To Download Nessus click on the following link

https://www.tenable.com/downloads/nessus?loginAttempted=true

```
┌──(root㉿kali)-[/home/kali]
└─# ls
15285.c           cyber.xml       JD.gnmap                              Pass.txt
192.168.174.129   Desktop         JD.html                               Pictures
192.168.174.130   DJ.gnmap        JD.nmap                               poo.html
33321.c           DJ.nmap         JD.xml                                pre.apk
69phisher         DJ.xml          john.xml                              prerna.html
Alice.txt         GgZwRvvf.jpeg   lol.pcap                              PRERNA.nmap
and.apk           house           Music                                 prerna.txt
cacert.der        ink             nano.21462.save                       prerna.xml
cup.apk           IP.TXT          Nessus-10.4.2-ubuntu1404_amd64.deb    PRERNA.xml
```

Step 2: Installing Nessus

Go to your kali or Downloads and then install Nessus and run the Nessus.

$ dpkg -i Nessus-10.4.2-ubuntu1404_amd64.deb

```
┌──(root㉿kali)-[/home/kali]
└─# dpkg -i Nessus-10.4.2-ubuntu1404_amd64.deb
(Reading database ... 406689 files and directories currently installed.)
Preparing to unpack Nessus-10.4.2-ubuntu1404_amd64.deb ...
Unpacking nessus (10.4.2) over (10.4.2) ...
Setting up nessus (10.4.2) ...
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
```

Step 3: To start the nessus copy and paste /bin/systemctl start nessusd.server

$ /bin/systemctl start nessusd.service

```
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner


┌──(root㉿kali)-[/home/kali]
└─# /bin/systemctl start nessusd.service
```

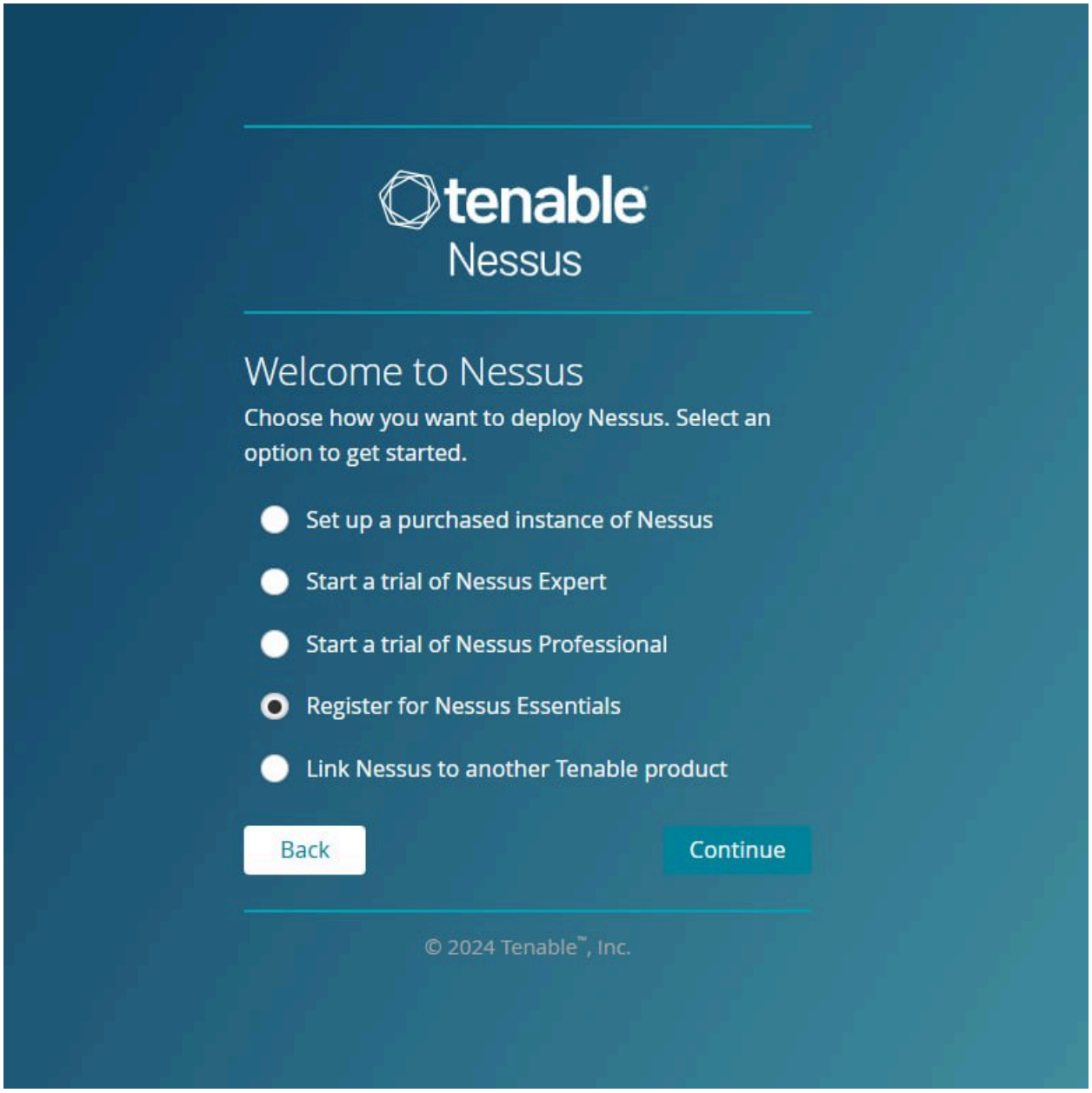
Step 4: To Nessus go to your browser and paste

$ https://kali:8834

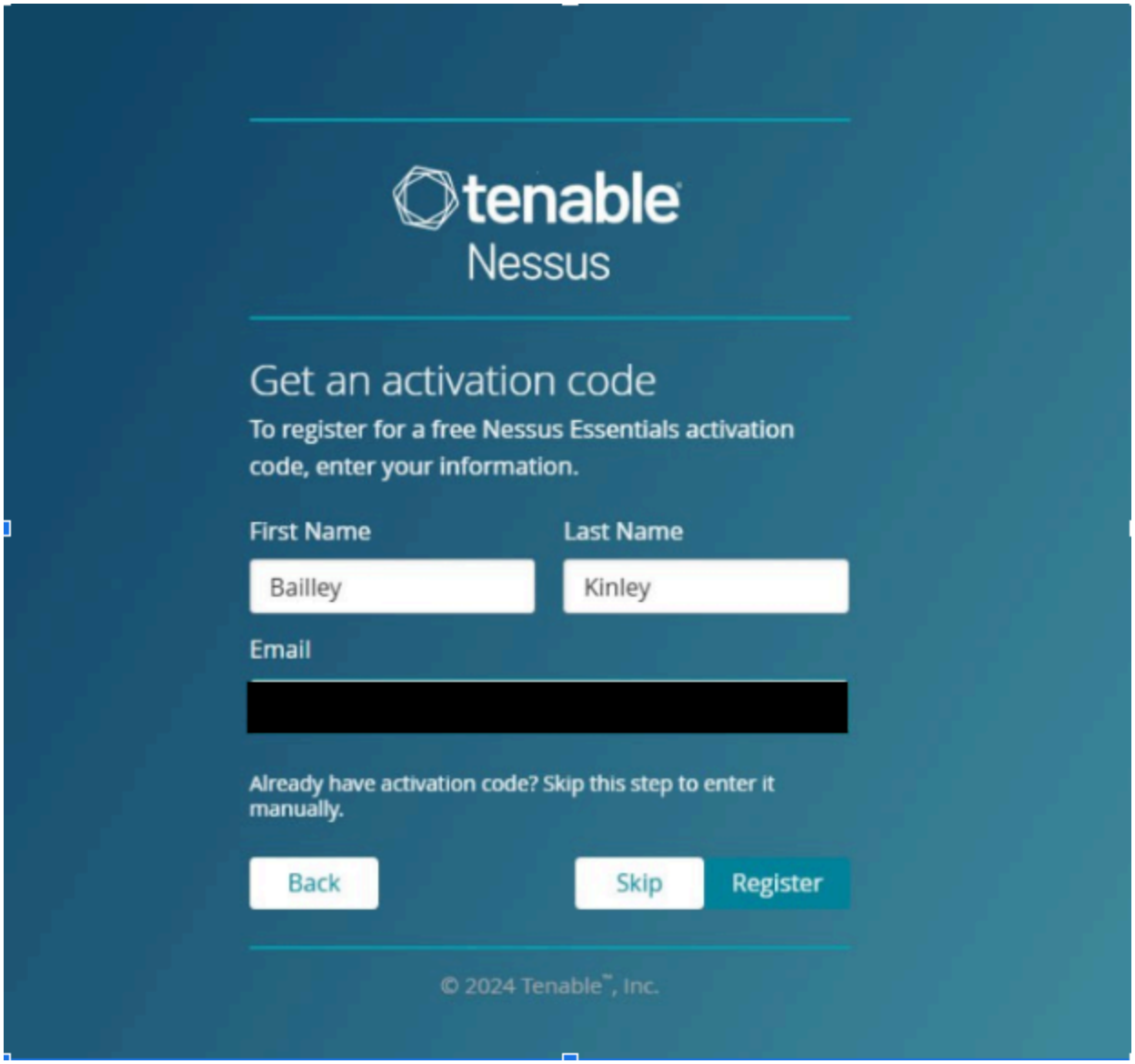
```
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://kali:8834/ to configure your scanner
```

Step 5: Click on Register for Nessus Essentials.

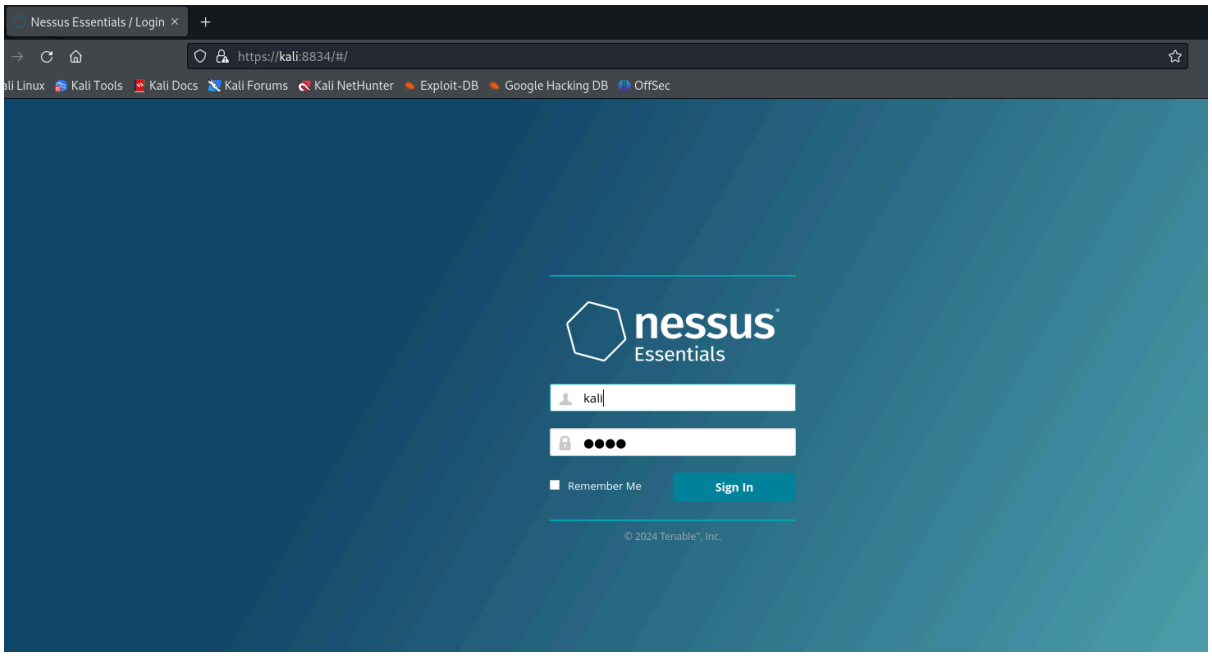


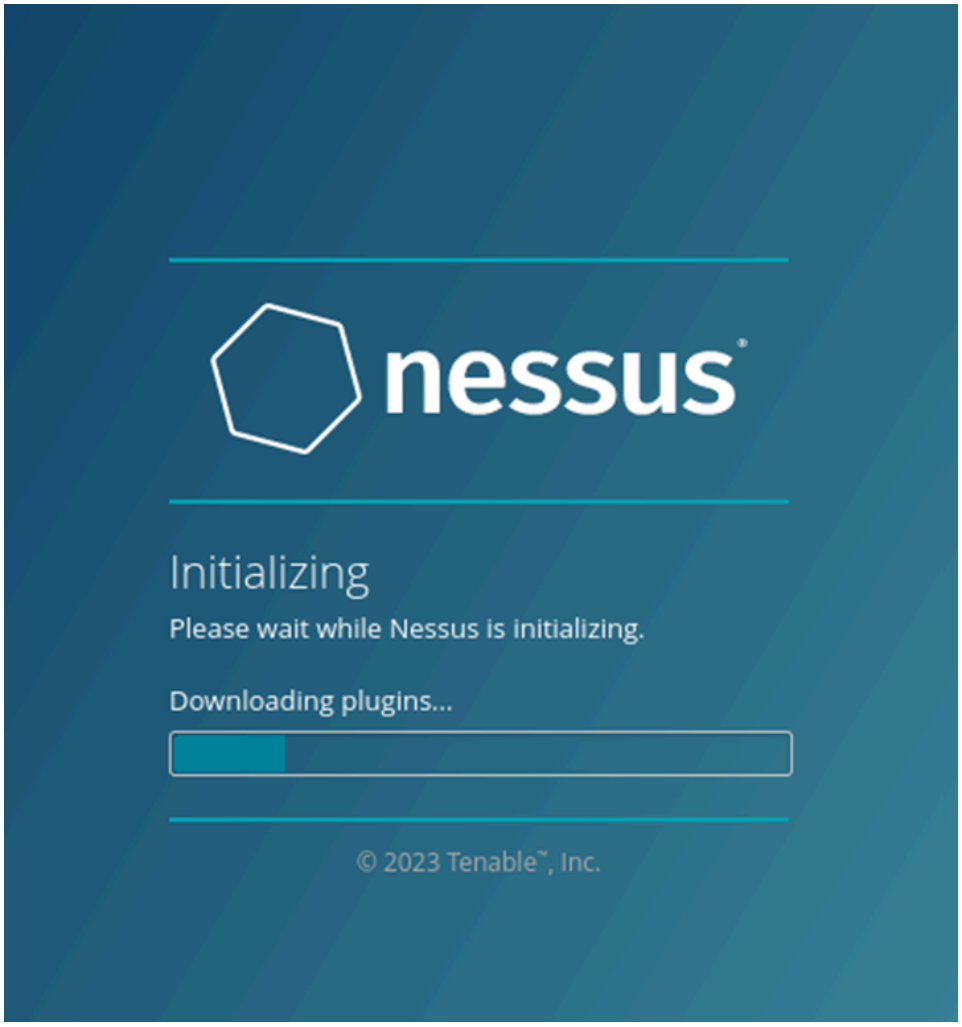
Step 6: To get an activation code register yourself in it and get the activation code in your email.



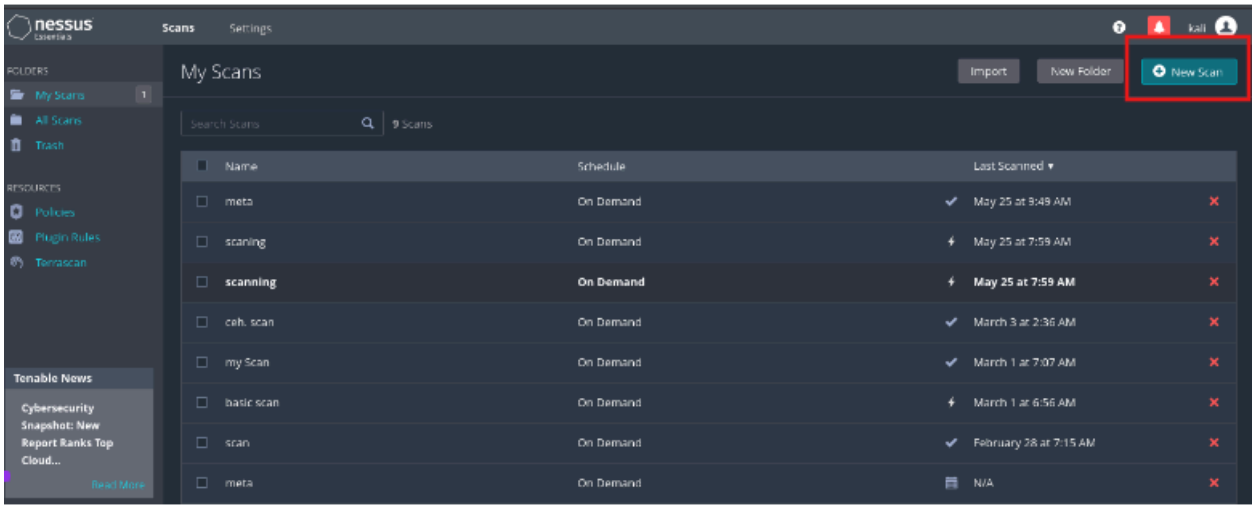
Step 7: Once you get the activation code write the code you get in the email and press continue.

Step 8: Create an Account in Nessus, and start initializing it.

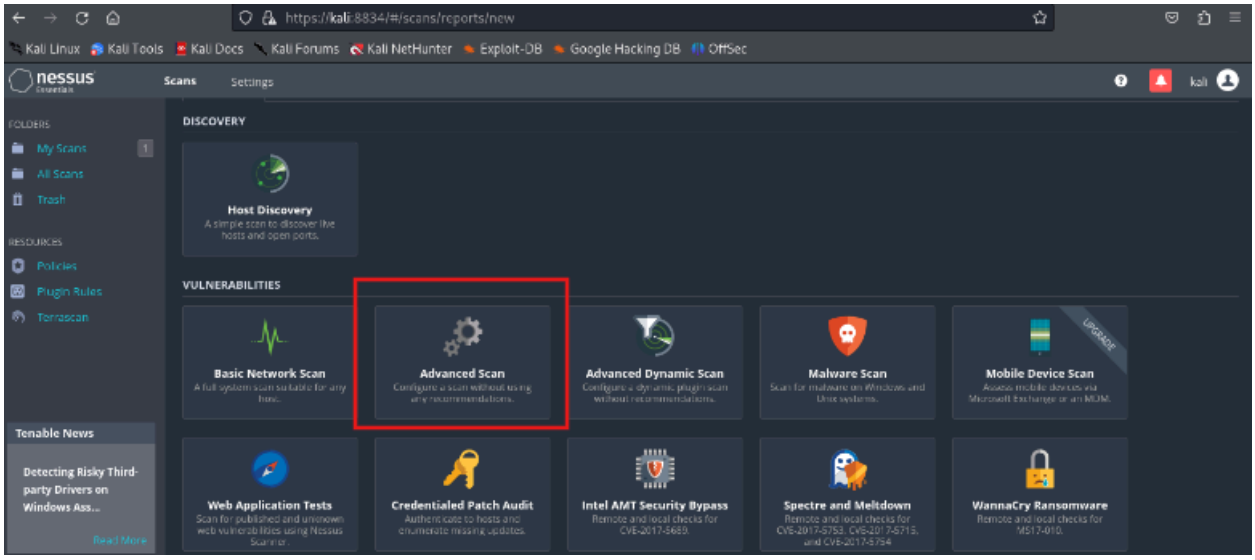




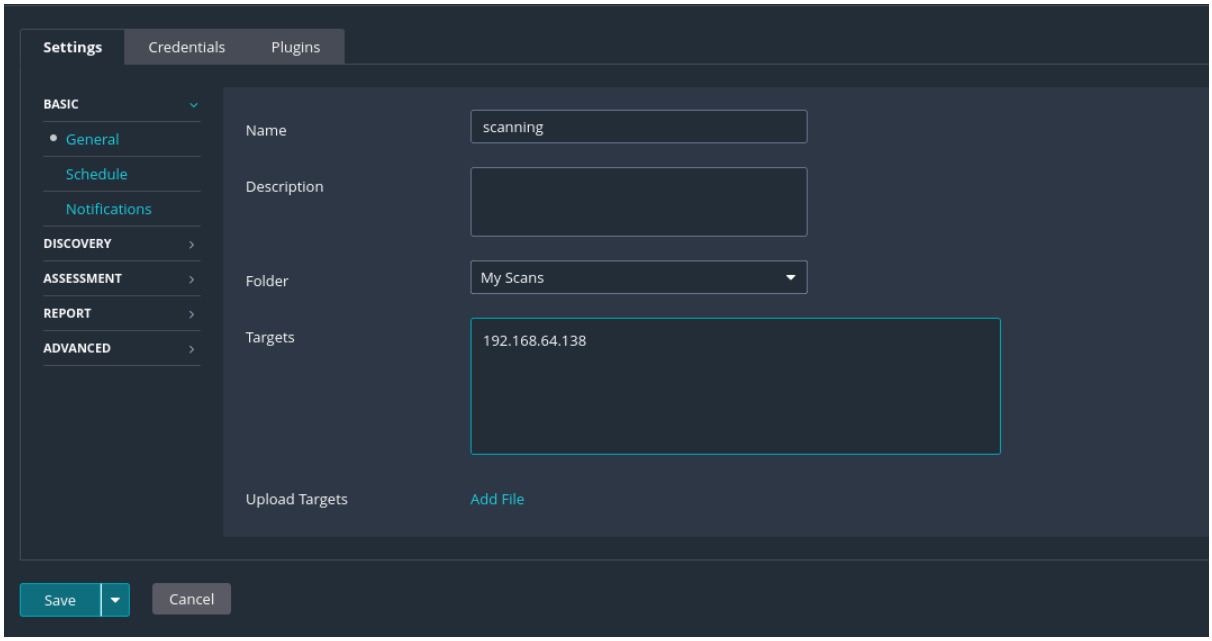
Step 9: Login to Nessus and Start the scanning by pressing the new scan.



$ Click on Advanced Scan



Step 10: Put the details of the target in the section given below.



$ Save the details and Start the Scan.

Step 11: Run the scan and analyze the vulnerabilities which are present in the target.