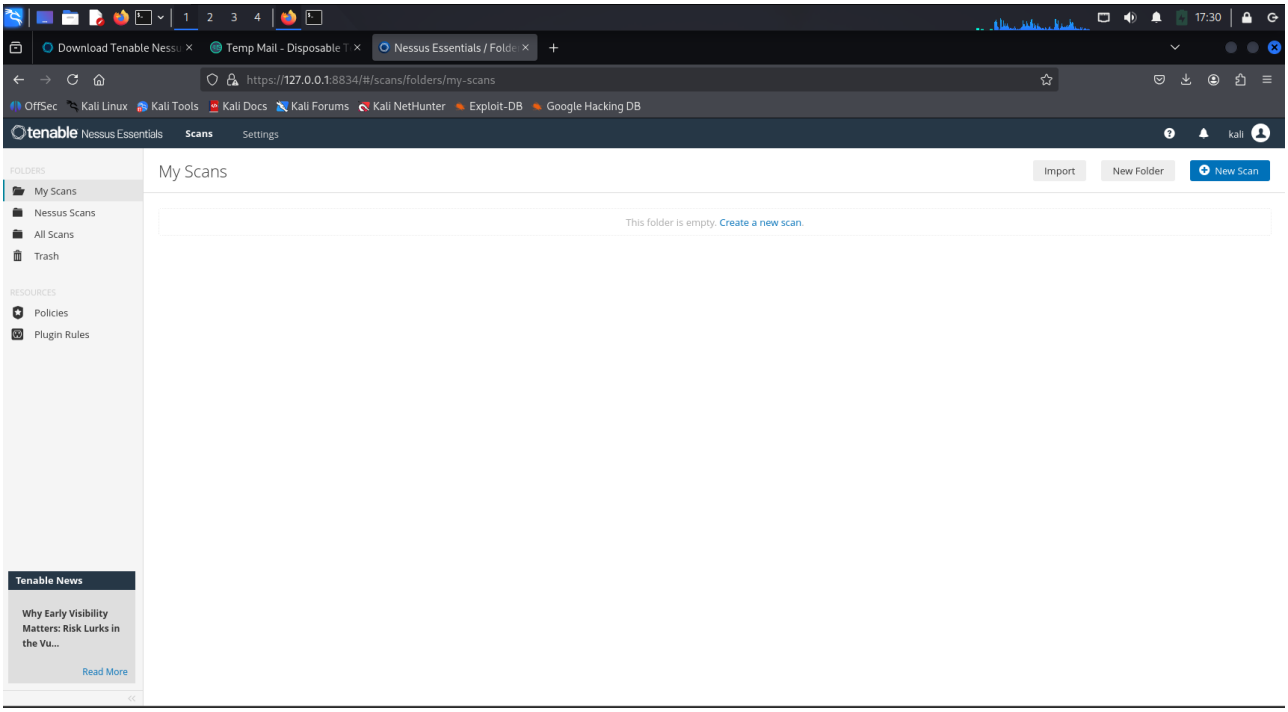
Task 3 : Perform a Basic Vulnerability Scan on Your PC.

Using Nessus for vulnerability scanning :-

The Vulnerable Metasploit machine I active and scanning it to get the whole vulnerabilities scans.

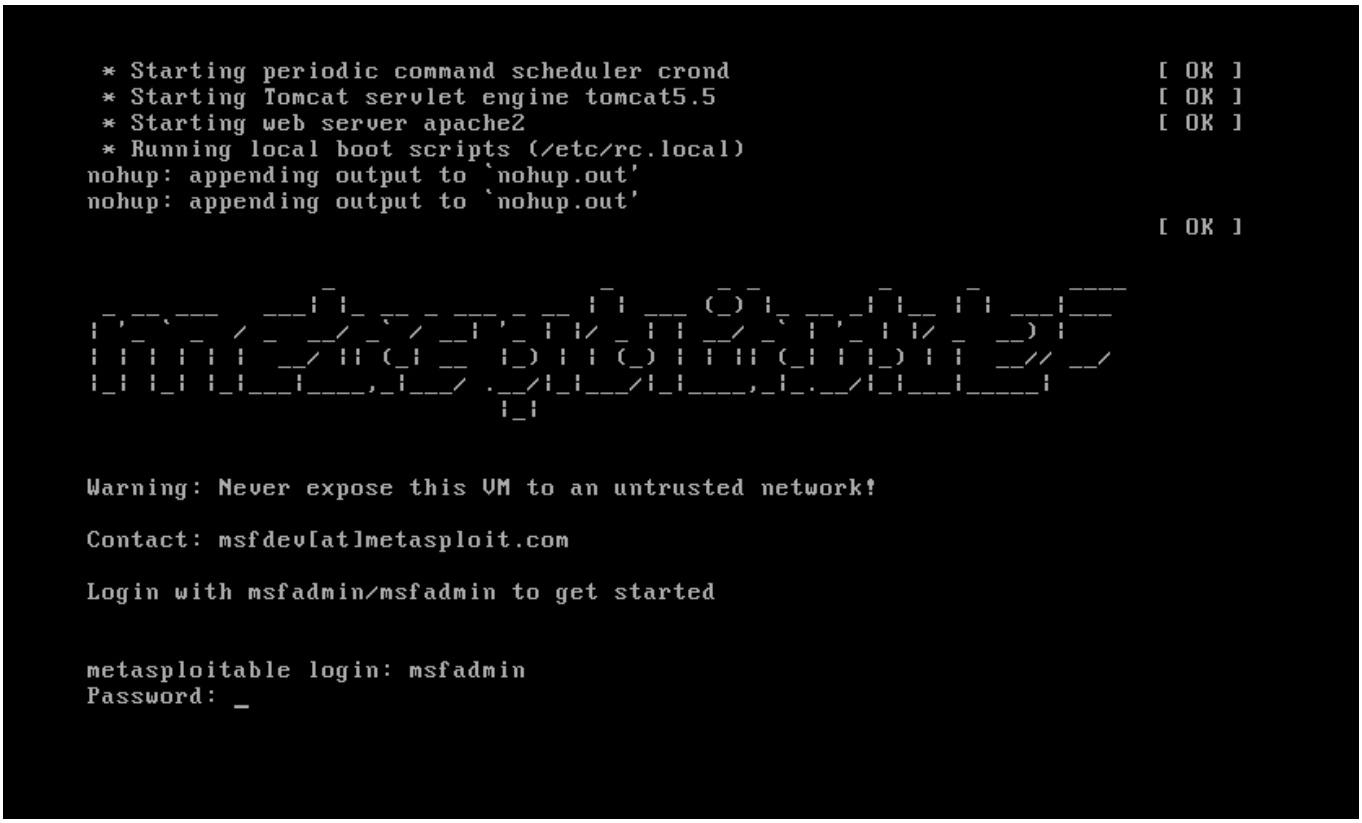
Step 1:-

Open the Nessus.



Step 2 :-

Starting the vulnerable lab and get the Ip address to scan it.



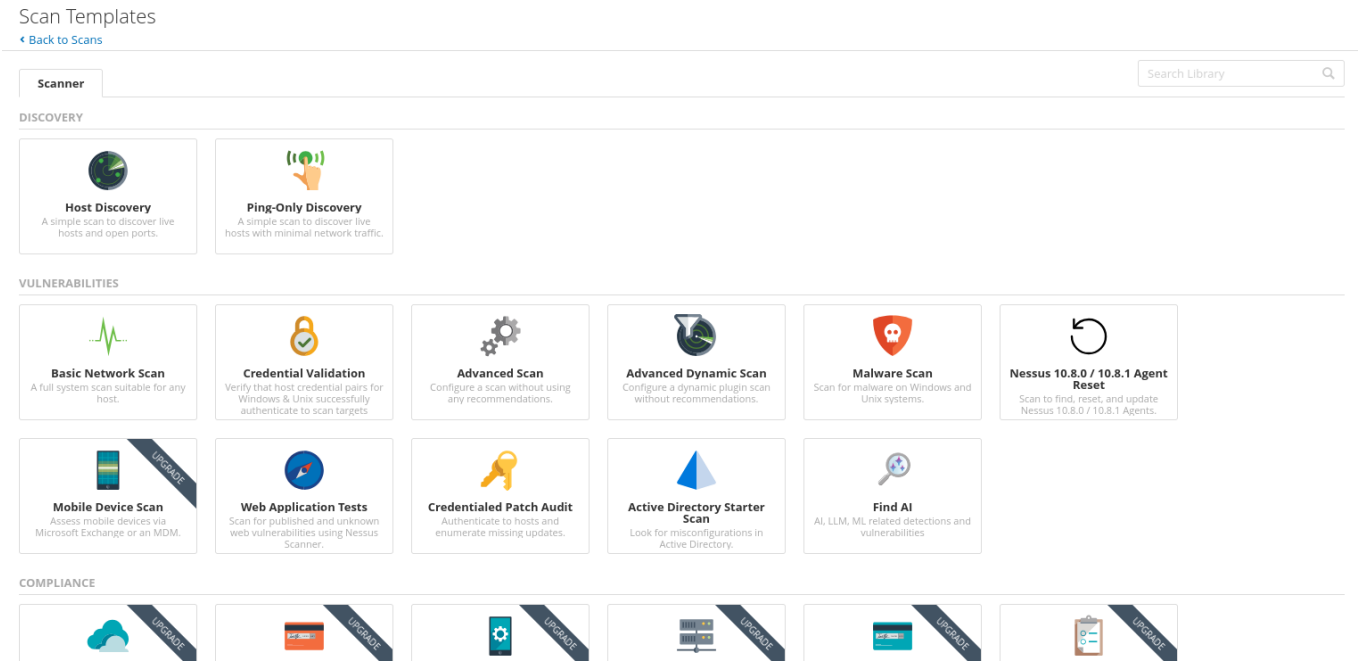
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:[redacted]
          inet addr:192.168.[redacted]  Bcast:192.[redacted]  Mask:255.[redacted]
          inet6 addr: fe80:[redacted]Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:38 errors:0 dropped:0 overruns:0 frame:0
          TX packets:65 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4588 (4.4 KB)  TX bytes:6826 (6.6 KB)
          Interrupt:17 Base address:0x2000

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:91 errors:0 dropped:0 overruns:0 frame:0
          TX packets:91 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19301 (18.8 KB)  TX bytes:19301 (18.8 KB)

msfadmin@metasploitable:~$ _
```

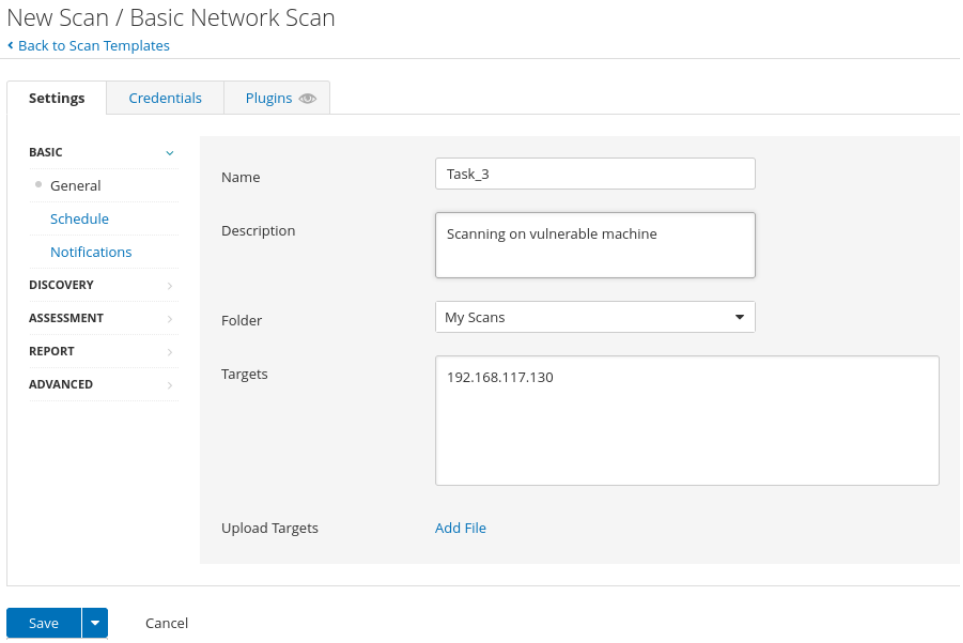
Step 3 :-

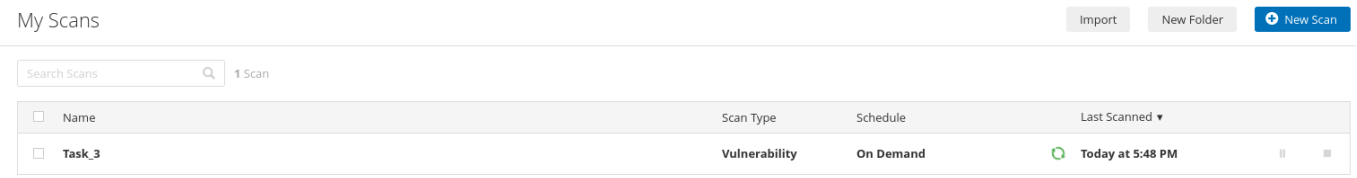
Now, scan the Ip address using Nessus tool.



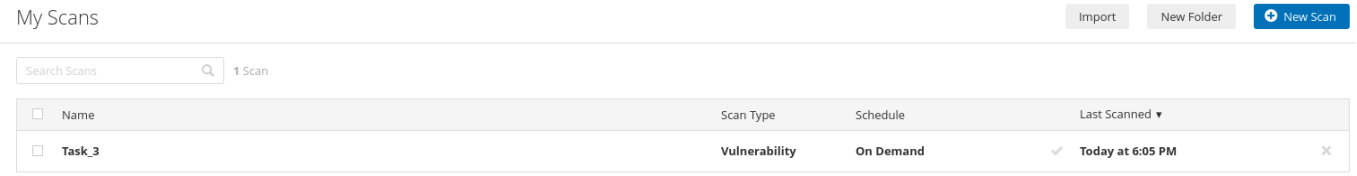
Step 4 :-

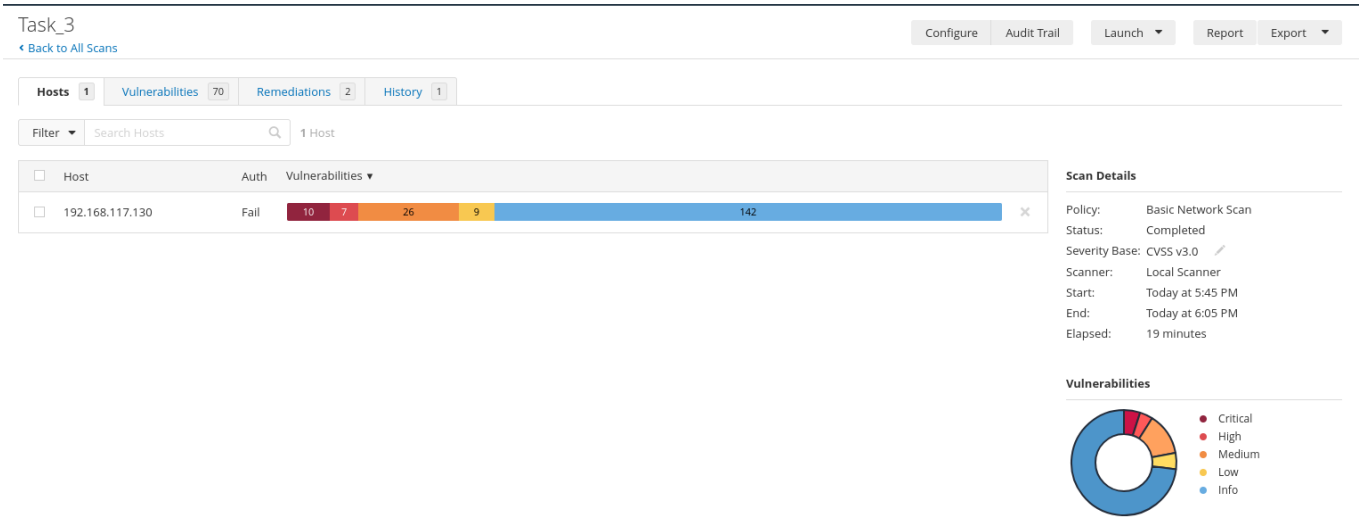
We will use Basic Scan to find vulnerabilities.





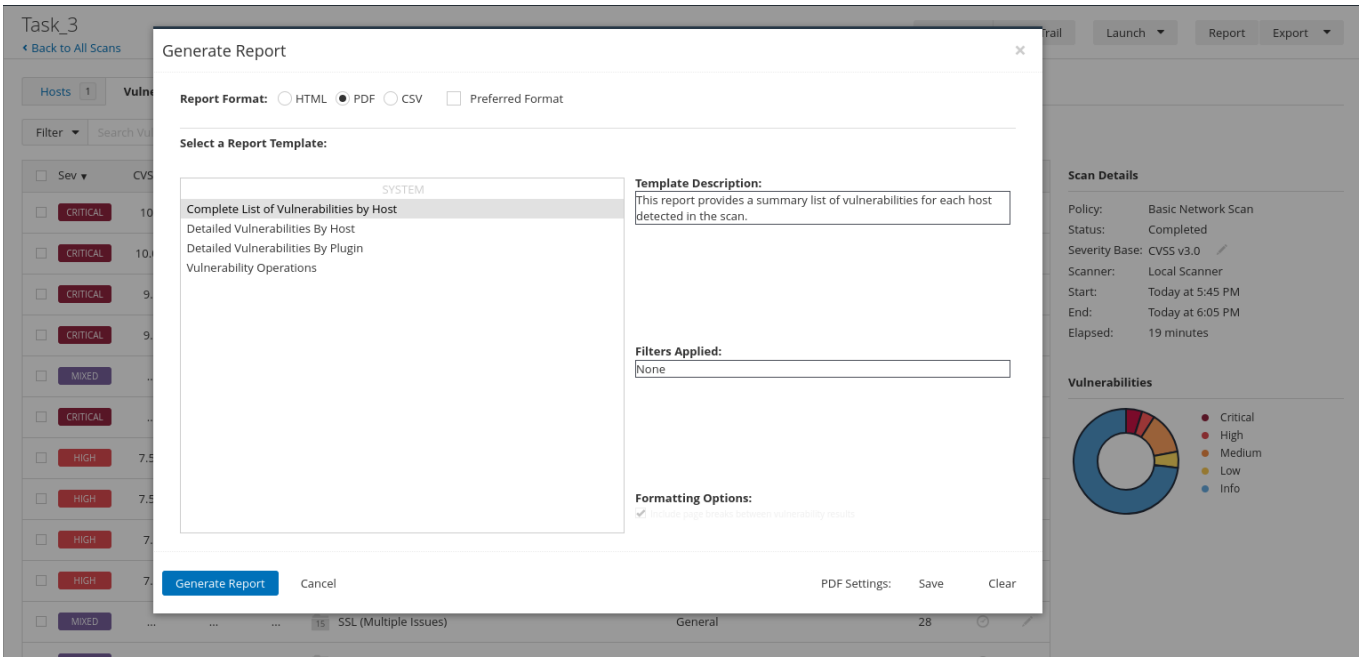
Now, its time to check the result





Step 5 :-

Let's generate the Report



Step 6 :-

Analyse the report and find the critical vulnerabilities.

CRITICAL	9.8	8.9	0.9447	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	-	-	201352	Canonical Ubuntu Linux SEoL (8.04.x)
CRITICAL	10.0*	5.1	0.0165	32314	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness
CRITICAL	10.0*	5.1	0.0165	32321	Debian OpenSSH/OpenSSL Package Random Number Genera Weakness (SSL check)
CRITICAL	10.0*	-	-	61708	VNC Server 'password' Password

Step 7 :-

Give some solutions to these critical vulnerabilities that are found.

1. **134862 - Apache Tomcat AJP Connector Request Injection (Ghostcat) :-**
   Solution :- Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.
2. **171340 - Apache Tomcat SEoL (<= 5.5.x) :-**
   Solution :- Upgrade to a version of Apache Tomcat that is currently supported.

3. **51988 - Bind Shell Backdoor Detection :-**
   Solution :- Verify if the remote host has been compromised, and reinstall the system if necessary.
4. **201352 - Canonical Ubuntu Linux SEoL (8.04.x) :-**
   Solution :- Upgrade to a version of Canonical Ubuntu Linux that is currently supported.
5. **32314 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness :-**
   Solution :- Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.
6. **32321 - Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) :-**
   Solution :- Consider all cryptographic material generated on the remote host to be guessable. In particular, all SSH, SSL and OpenVPN key material should be re-generated.
7. **20007 - SSL Version 2 and 3 Protocol Detection :-**
   Solution :- Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
8. **61708 - VNC Server 'password' Password :-**
   Solution :- Secure the VNC service with a strong password.