Security Blue Team – Introduction to Vulnerability Management

METASPLOITABLE 2 SETUP

You'll be setting up the intentionally vulnerable virtual machine Metasploitable 2, created by security firm Rapid7. This will be your test environment where you can practice vulnerability scanning, collecting results, and analysing them to produce vulnerability reports.

NESSUS SETUP

You'll install and explore the Nessus Essentials vulnerability scanner created by Tenable, in preparation for the final course challenge. You'll be walked through the GUI and conduct a scan against your own system, so that you're familiar with how to use this powerful tool, and understandscan results.

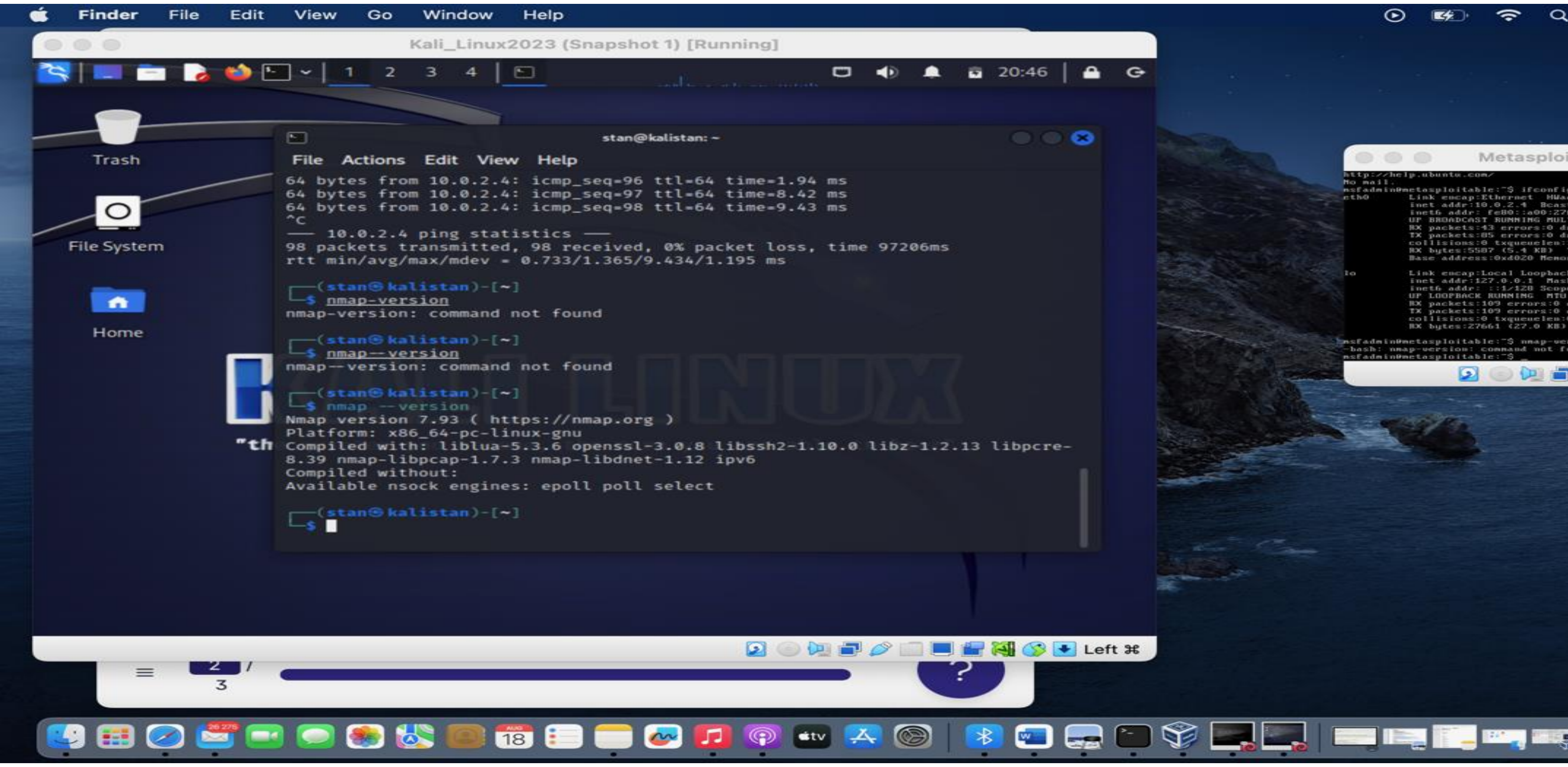
WPSCAN ANALYSIS

You'll be analysing real-world WPScan results to make sure you're familiar with the tool's output. and the security flaws that it can detect. In the future we will release a public lab where you can conduct your own scans.

COURSE CHALLENGE: VULNERABILITY ASSESSMENT

For the final challenge you'll be conducting a short and simple vulnerability assessment of the Metasploitable 2 system, by launching your own vulnerability scans using Nessus, and reporting on the vulnerabilities and flaws that are discovered.

Metasploitable 2



```
64 bytes from 10.0.2.4: icmp_seq=96 ttl=64 time=1.94 ms
64 bytes from 10.0.2.4: icmp_seq=97 ttl=64 time=8.42 ms
64 bytes from 10.0.2.4: icmp_seq=98 ttl=64 time=9.43 ms
^C
—— 10.0.2.4 ping statistics ——
98 packets transmitted, 98 received, 0% packet loss, time 97206ms
rtt min/avg/max/mdev = 0.733/1.365/9.434/1.195 ms

┌──(stan㉿kalistan)-[~]
└─$ nmap-version
nmap-version: command not found

┌──(stan㉿kalistan)-[~]
└─$ nmap—version
nmap—version: command not found

┌──(stan㉿kalistan)-[~]
└─$ nmap --version
Nmap version 7.93 ( https://nmap.org )
Platform: x86_64-pc-linux-gnu
Compiled with: liblua-5.3.6 openssl-3.0.8 libssh2-1.10.0 libz-1.2.13 libpcre-
8.39 nmap-libpcap-1.7.3 nmap-libdnet-1.12 ipv6
Compiled without:
Available nsock engines: epoll poll select

┌──(stan㉿kalistan)-[~]
└─$ 
```

```
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWad
          inet addr:10.0.2.4  Bcast
          inet6 addr: fe80::a00:27
          UP BROADCAST RUNNING MULT
          RX packets:43 errors:0 d
          TX packets:85 errors:0 d
          collisions:0 txqueuelen:
          RX bytes:5587 (5.4 KB)
          Base address:0xd020 Memor

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask
          inet6 addr: ::1/128 Scope
          UP LOOPBACK RUNNING  MTU
          RX packets:109 errors:0 
          TX packets:109 errors:0 
          collisions:0 txqueuelen:
          RX bytes:27661 (27.0 KB)

msfadmin@metasploitable:~$ nmap-ver
-bash: nmap-version: command not f
msfadmin@metasploitable:~$ 
```

Some of the questions in the course

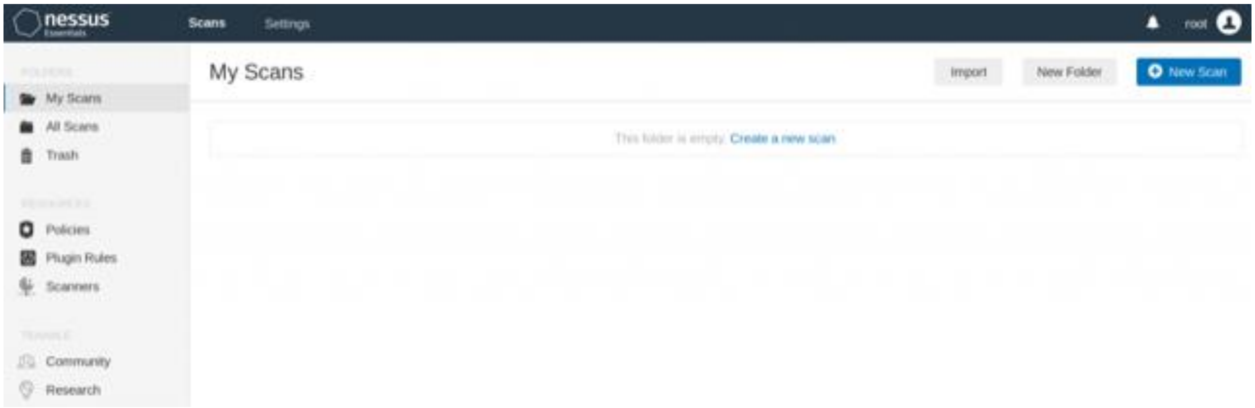
How many TCP ports are OPEN on MS2? (Use the -sT flag in Nmap).

How many UDP ports are OPEN on MS2? (Use the -sU flag in Nmap – this may take a while).

What port is running a Metasploitable Root Shell? (Use the -sV flag in Nmap).
What non-standard port is FTP running on? (NOT p21) (Use the -sT flag in Nmap)

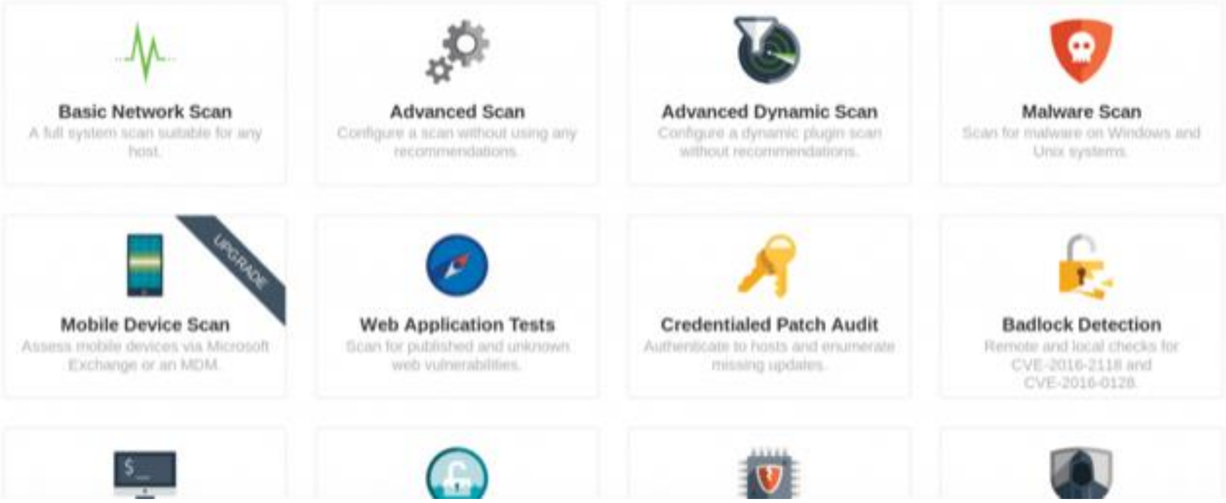
What version of FTP is running on the non-standard port? (Use the -sV flag in Nmap).

Nessus



My Scans

This folder is empty. Create a new scan



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.

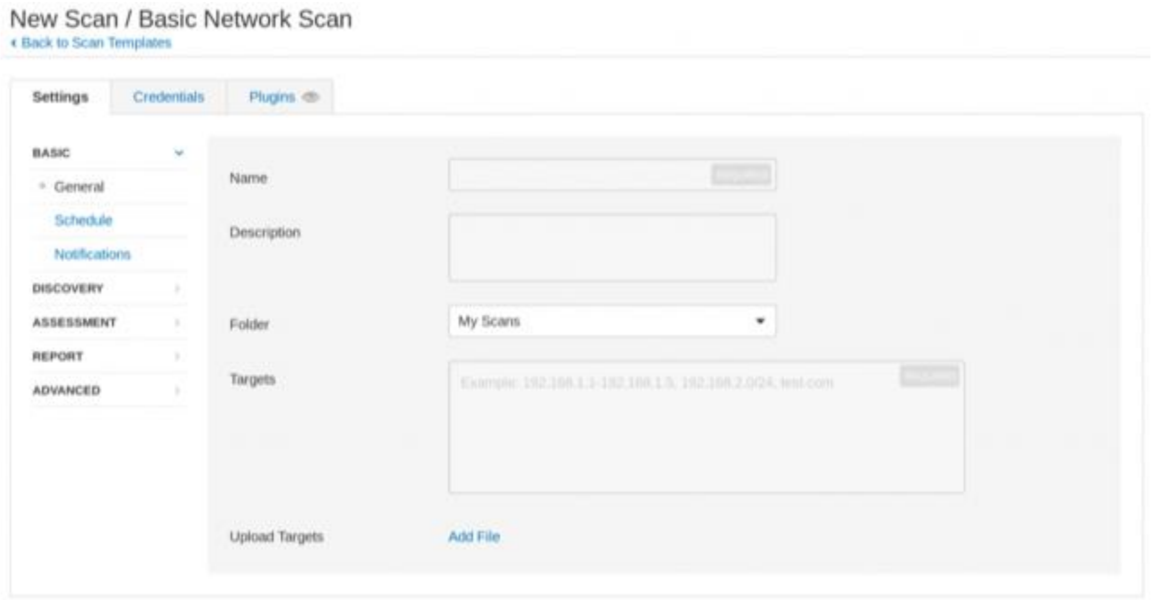
Malware Scan
Scan for malware on Windows and Unix systems.

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

Web Application Tests
Scan for published and unknown web vulnerabilities.

Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.

Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.

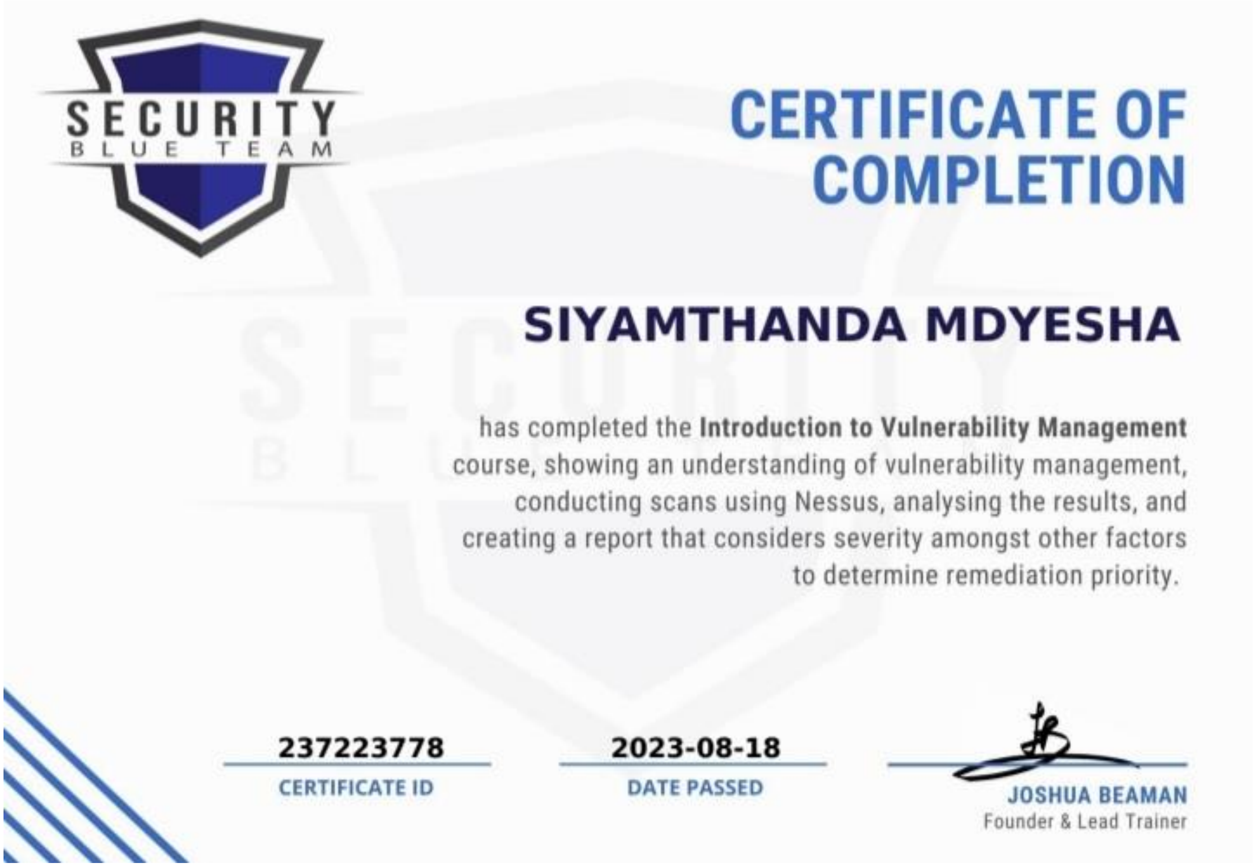


New Scan / Basic Network Scan

Folder: My Scans

The course also included OpenVAS and WPScan with activities…

Completion Certificate



SECURITY BLUE TEAM

CERTIFICATE OF COMPLETION

SIYAMTHANDA MDYESHA

has completed the **Introduction to Vulnerability Management** course, showing an understanding of vulnerability management, conducting scans using Nessus, analysing the results, and creating a report that considers severity amongst other factors to determine remediation priority.

237223778	2023-08-18	
CERTIFICATE ID	DATE PASSED	JOSHUA BEAMAN Founder & Lead Trainer