DAY 4 ASSIGNMENT

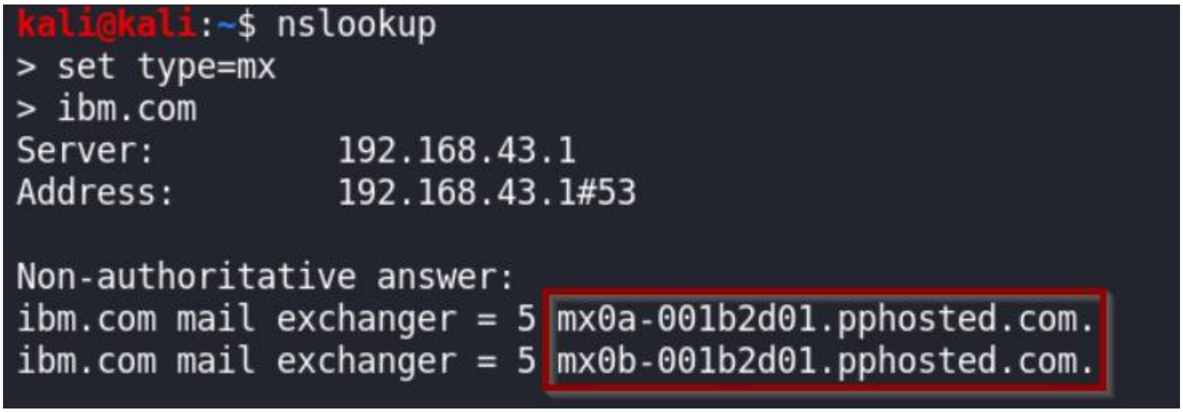
SUBMITTED BY- ADITYA SRIVASTAVA

Q1 FIND OUT THE MAIL SERVERS OF FOLLOWING DOMAIN

Ans: We will be using Kali Linux inbuild tool called nslookup for finding the mail servers. Power on your kali machine, login and open a terminal.

Type the command **nslookup** to launch an interactive interface, since the objective is to find mail server, the next command should filter out the mail servers, so use the command **set type=mx**, mx indicates Mail Servers, now we need domain name (the question does not mention sub-domains)

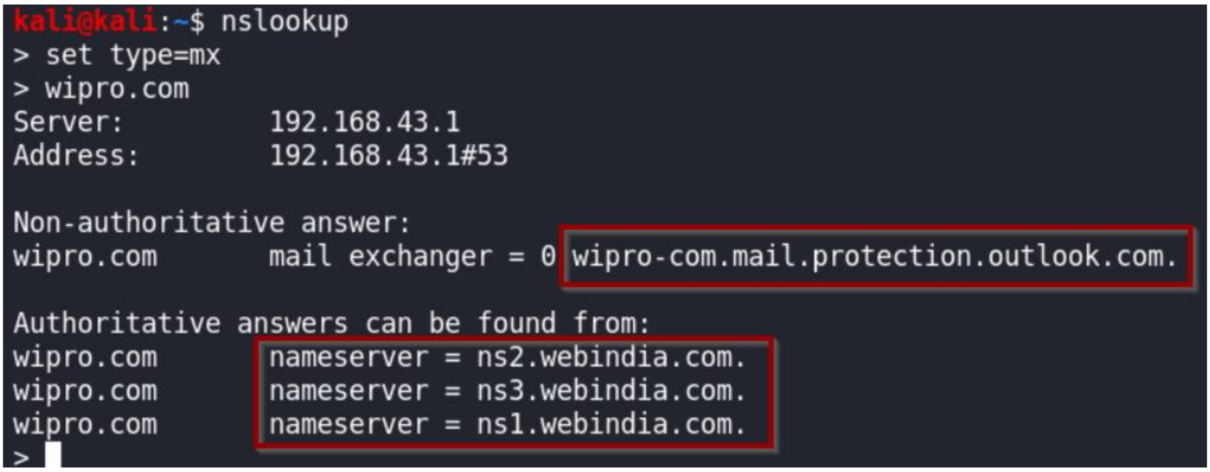
a) Ibm.com
   Type the domain name **ibm.com** and press enter.



```
kali@kali:~$ nslookup
> set type=mx
> ibm.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
ibm.com mail exchanger = 5 mx0a-001b2d01.pphosted.com.
ibm.com mail exchanger = 5 mx0b-001b2d01.pphosted.com.
```

   We have 2 mail servers (marked in red rectangle).

b) Wipro.com
   Type the domain name **wipro.com** and press enter.



```
kali@kali:~$ nslookup
> set type=mx
> wipro.com
Server:         192.168.43.1
Address:        192.168.43.1#53

Non-authoritative answer:
wipro.com       mail exchanger = 0 wipro-com.mail.protection.outlook.com.

Authoritative answers can be found from:
wipro.com       nameserver = ns2.webindia.com.
wipro.com       nameserver = ns3.webindia.com.
wipro.com       nameserver = ns1.webindia.com.
>
```

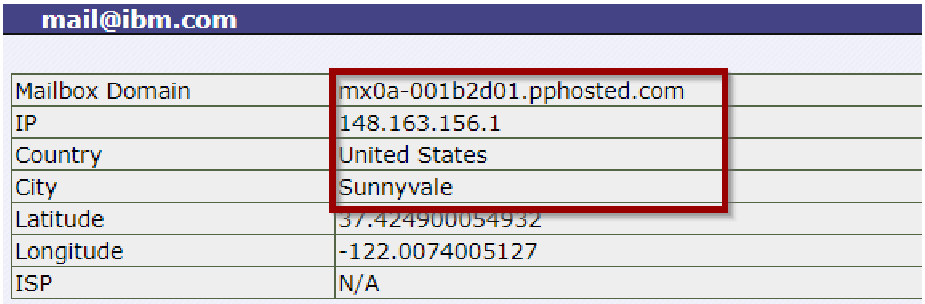
   We can see one non-authoritative and 3 authoritative servers for wipro.com

Q2 Find the locations where these email servers are located.

Ans: I went through a lot of sites for this one. Finally I found it here.

Now, it requires some logic to search.

First, I went for Ibm.com but it showed invalid, so instead of that I went to mail.ibm.com and I found a valid result.



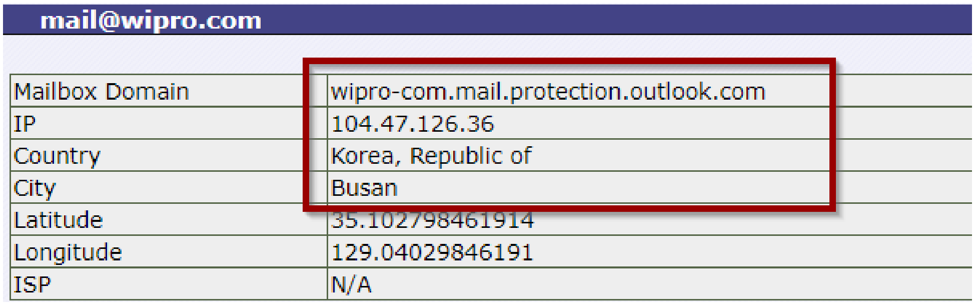
mail@ibm.com

Mailbox Domain	mx0a-001b2d01.pphosted.com
IP	148.163.156.1
Country	United States
City	Sunnyvale
Latitude	37.424900054932
Longitude	-122.0074005127
ISP	N/A

We can see the location to be Sunnyvale, US

Unfortunately, I could not figure out how to locate the second mail server.

Same for Wipro, search for mail.wipro.com



mail@wipro.com

Mailbox Domain	wipro-com.mail.protection.outlook.com
IP	104.47.126.36
Country	Korea, Republic of
City	Busan
Latitude	35.102798461914
Longitude	129.04029846191
ISP	N/A

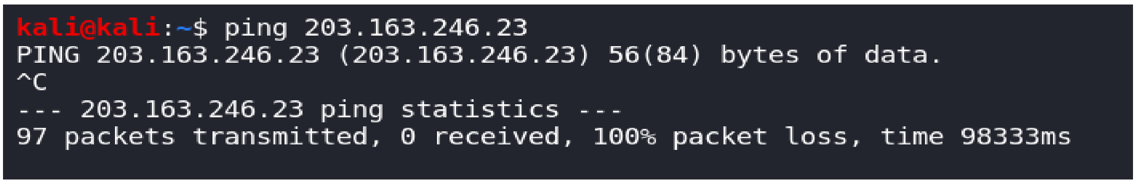
The location is Busan, Korea.

Q3 Scan and find out open port numbers for 203.163.246.23

Ans: Before scanning it is important to check if the machine is online or not.

We will use the **ping** command and provide it with an IP and check if the machine responds.

Use the command **ping 203.163.246.23**



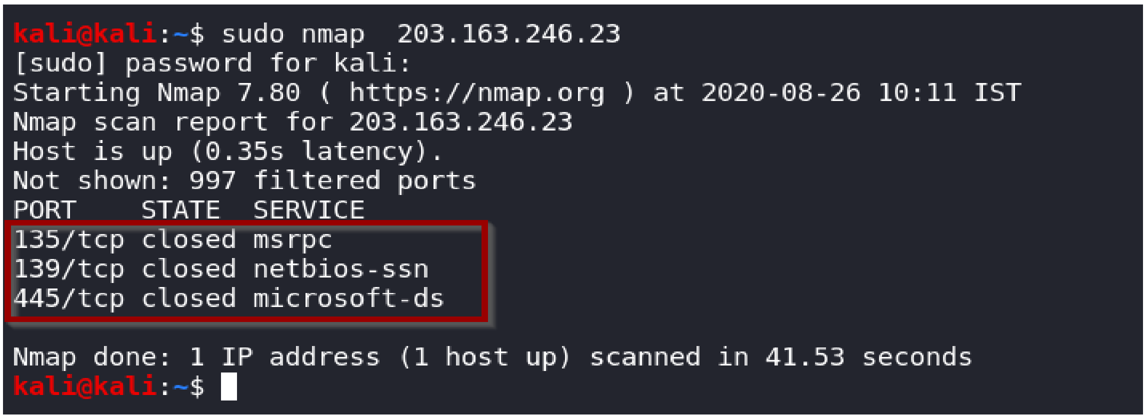
```
kali@kali:~$ ping 203.163.246.23
PING 203.163.246.23 (203.163.246.23) 56(84) bytes of data.
^C
--- 203.163.246.23 ping statistics ---
97 packets transmitted, 0 received, 100% packet loss, time 98333ms
```

We can packet gets lost, but we were able to send the packets, this can be due to firewall.

Let’s scan with a tool called nmap to see of the hosts is up.

Command is

nmap 203.163.246.23



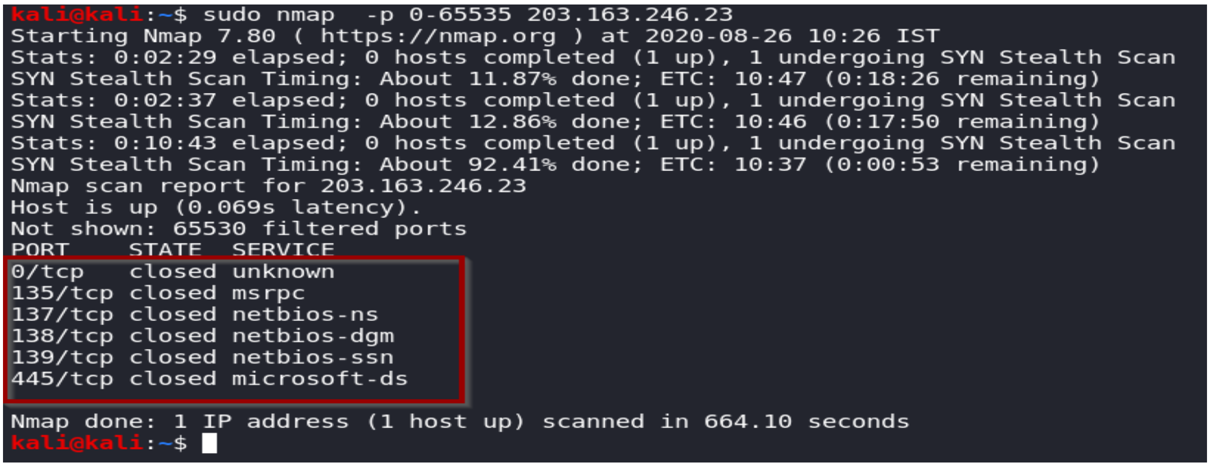
```
kali@kali:~$ sudo nmap  203.163.246.23
[sudo] password for kali:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 10:11 IST
Nmap scan report for 203.163.246.23
Host is up (0.35s latency).
Not shown: 997 filtered ports
PORT    STATE  SERVICE
135/tcp closed msrpc
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 41.53 seconds
kali@kali:~$ 
```

(I ran this command with sudo privileges)

The scan shows that the host is up.

But none of the ports are open.

Note: This command scanned only the first 1000 ports. To scan all ports, add the module -p- or -p 0-65535 as shown below.



```
kali@kali:~$ sudo nmap  -p 0-65535 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-26 10:26 IST
Stats: 0:02:29 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 11.87% done; ETC: 10:47 (0:18:26 remaining)
Stats: 0:02:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 12.86% done; ETC: 10:46 (0:17:50 remaining)
Stats: 0:10:43 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.41% done; ETC: 10:37 (0:00:53 remaining)
Nmap scan report for 203.163.246.23
Host is up (0.069s latency).
Not shown: 65530 filtered ports
PORT    STATE  SERVICE
0/tcp   closed unknown
135/tcp closed msrpc
137/tcp closed netbios-ns
138/tcp closed netbios-dgm
139/tcp closed netbios-ssn
445/tcp closed microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 664.10 seconds
kali@kali:~$ 
```

Though there are more ports shown but all are closed.

Q4 Install Nessus in VM and scan your computer or desktop/laptop for CVE.

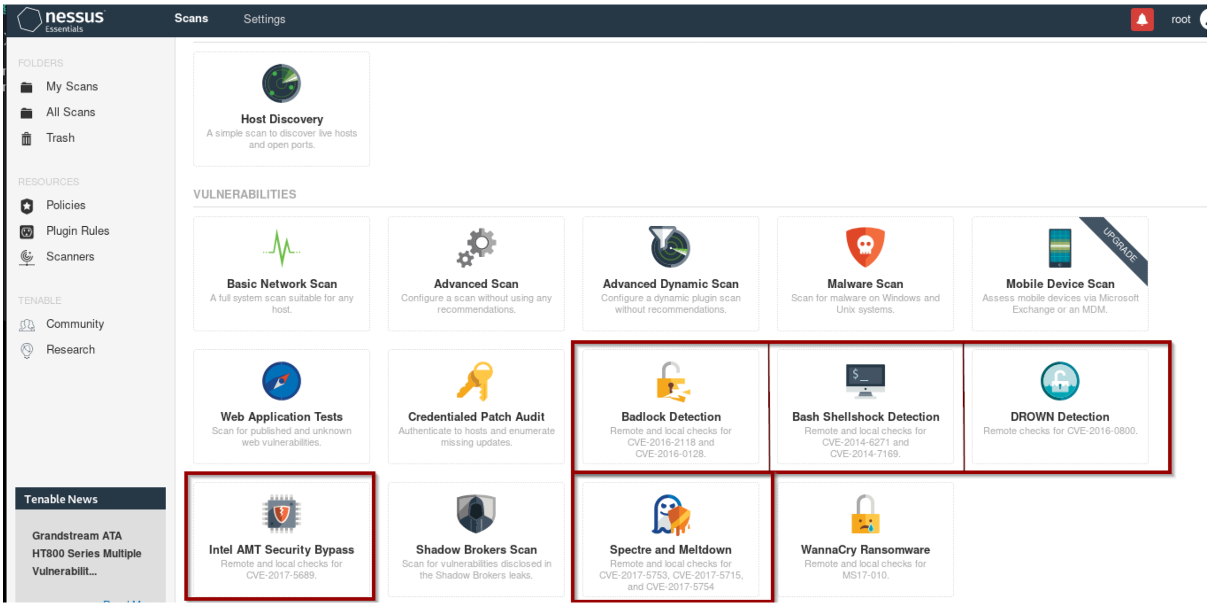
Ans: Nowadays, Nessus comes preinstalled in kali (free version), if its now there install it from the official site in zip file, use the command

dpkg -i <package_name_of_nessus>

And now follow the commands given there to launch it, register yourself and you should be ready to go.

After you login it, click on **new scan** (present at right side of screen).

We have to perform scans related to CVE, there are multiple options available but the procedure is same.



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.

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

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

Bash Shellshock Detection – Remote and local checks for CVE-2014-6271 and CVE-2014-7169.

DROWN Detection – Remote checks for CVE-2016-0800.

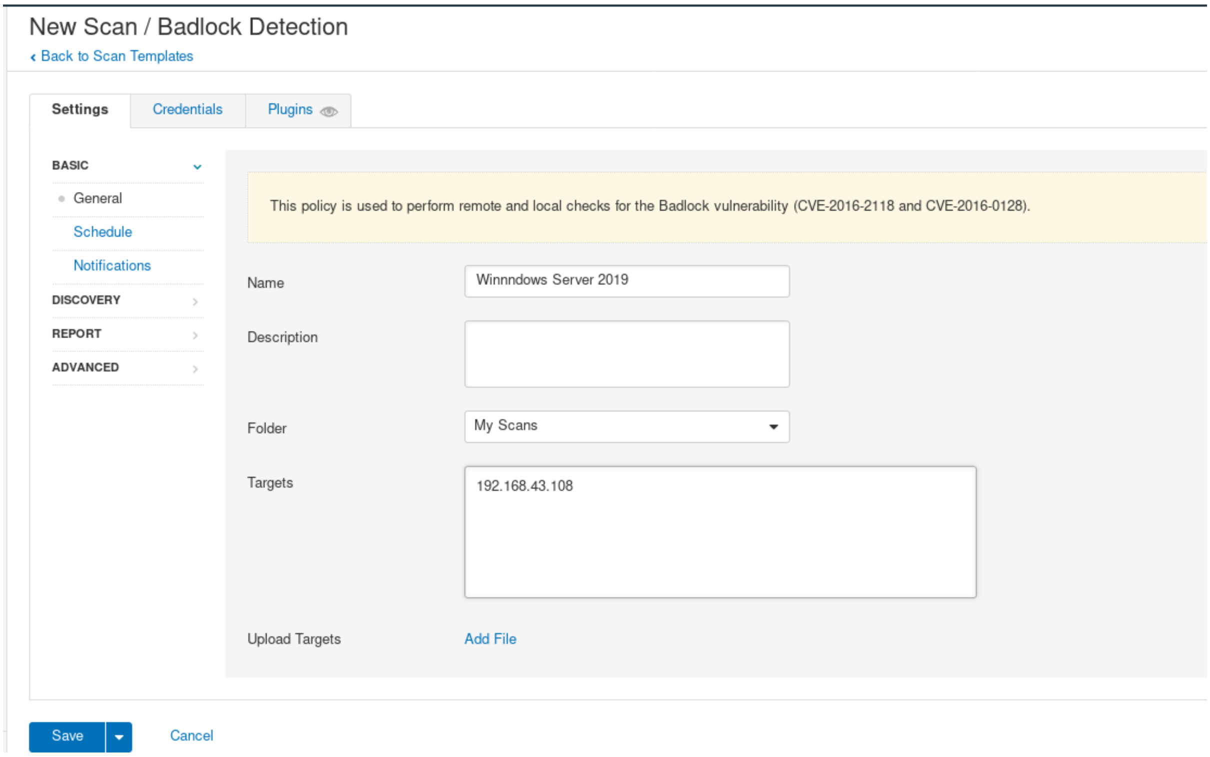
Intel AMT Security Bypass – Remote and local checks for CVE-2017-5689.

Shadow Brokers Scan – Scan for vulnerabilities disclosed in the Shadow Brokers leaks.

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.

We will see the scan for Badlock Detection and the rest are similar to it.



New Scan / Badlock Detection

‹ Back to Scan Templates

This policy is used to perform remote and local checks for the Badlock vulnerability (CVE-2016-2118 and CVE-2016-0128).

Name: Winnndows Server 2019

Description:

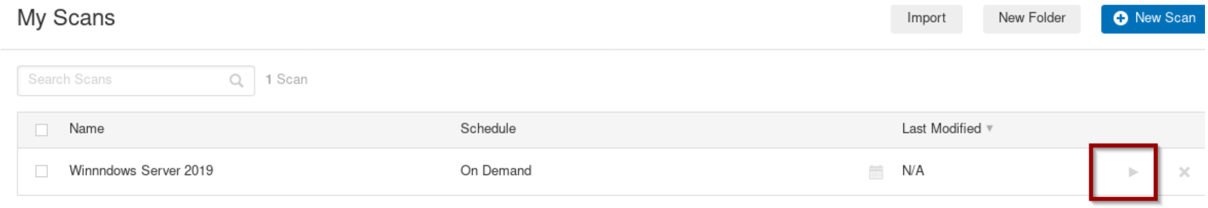
Folder: My Scans

Targets: 192.168.43.108

Upload Targets: Add File

Fill the details here, I am scanning my Windows Server 2019

Save it.



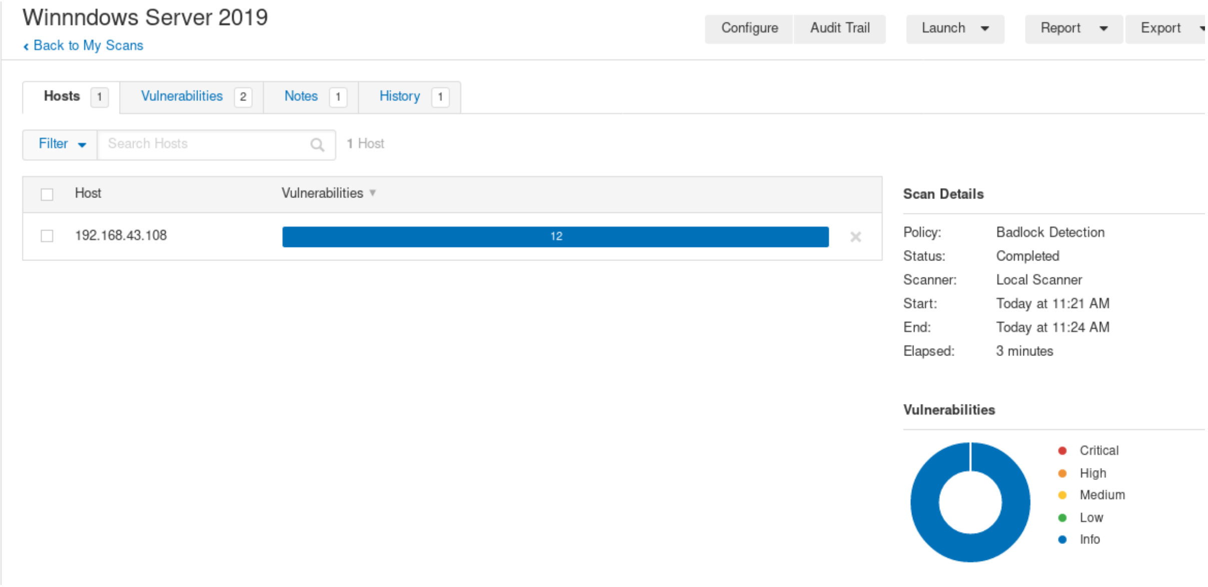
My Scans

1 Scan

□	Name	Schedule	Last Modified ▾
□	Winnndows Server 2019	On Demand	N/A

To start the scan, press the start button.

After the scanning is finished open it.



Winnndows Server 2019

‹ Back to My Scans

1 Host

□	Host	Vulnerabilities ▾
□	192.168.43.108	12

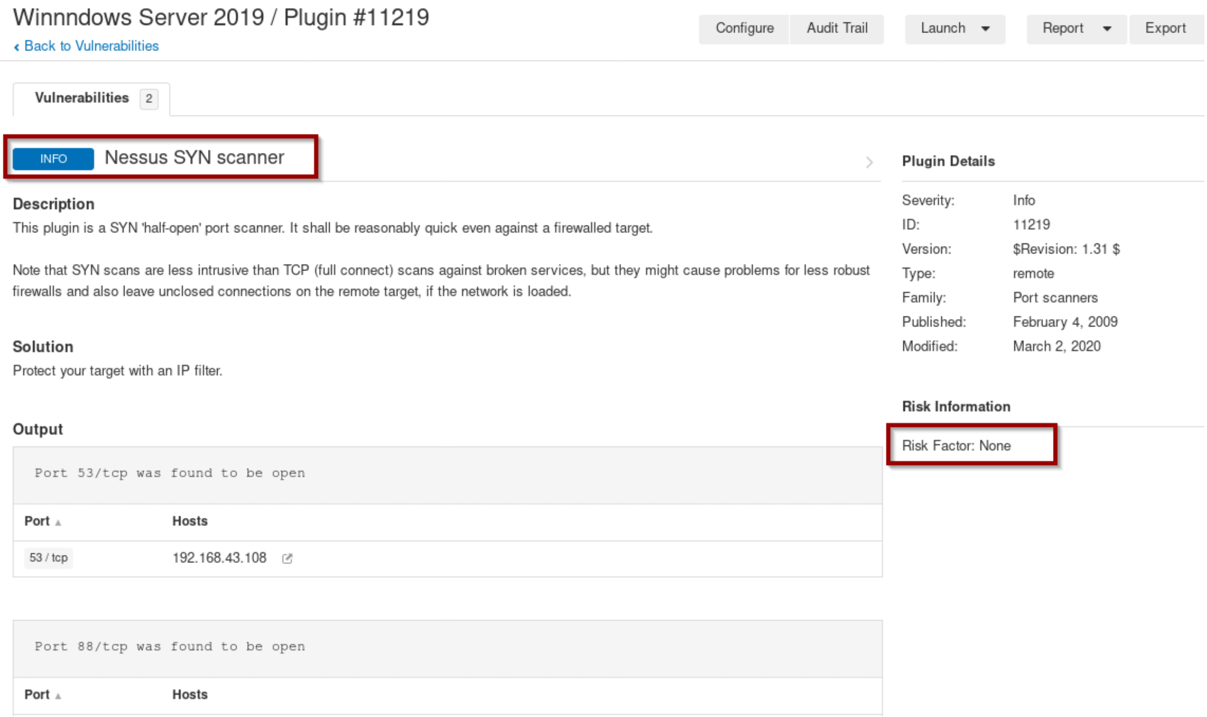
Scan Details

Policy:	Badlock Detection
Status:	Completed
Scanner:	Local Scanner
Start:	Today at 11:21 AM
End:	Today at 11:24 AM
Elapsed:	3 minutes

Vulnerabilities

The scan will tell you various vulnerabilities present.

Go into vulnerability section and have a look.



Winnndows Server 2019 / Plugin #11219

‹ Back to Vulnerabilities

Nessus SYN scanner

Description

This plugin is a SYN 'half-open' port scanner. It shall be reasonably quick even against a firewalled target.

Note that SYN scans are less intrusive than TCP (full connect) scans against broken services, but they might cause problems for less robust firewalls and also leave unclosed connections on the remote target, if the network is loaded.

Solution

Protect your target with an IP filter.

Output

```
Port 53/tcp was found to be open
```

Port ▴	Hosts
53 / tcp	192.168.43.108

```
Port 88/tcp was found to be open
```

Port ▴	Hosts

Plugin Details

Severity:	Info
ID:	11219
Version:	$Revision: 1.31 $
Type:	remote
Family:	Port scanners
Published:	February 4, 2009
Modified:	March 2, 2020

Risk Information

Risk Factor: None

The risk factor is shown and in similar manner see all other.

I am not posting all the scans and details (due to my busy schedule, as well as my privacy), hope you understand.