Part 1

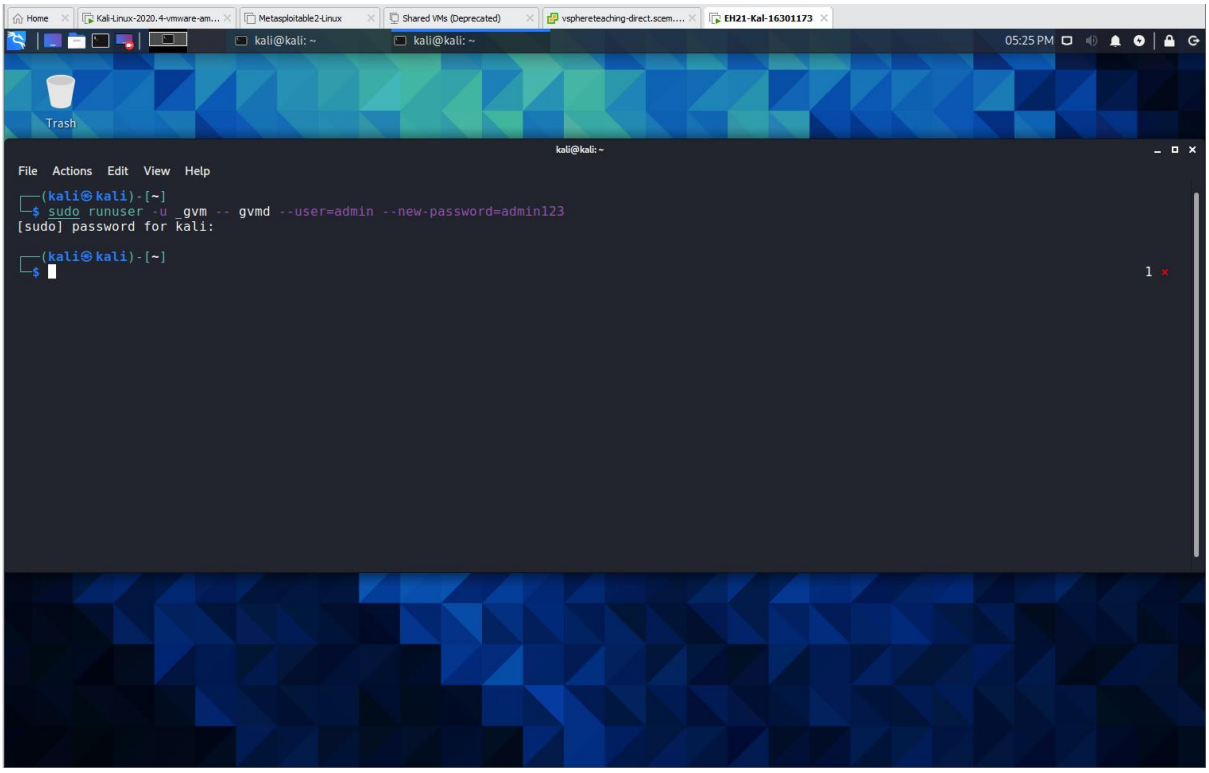
1.1 Use 'gvm-start' command to start GVM. After GVM is started, run the 'sudo ss -antp' command in a terminal. Based on the output of this command, explain which port the GSA daemon is listening on, and attach a screenshot as proof.

The daemon “gsad” is listening on port 9392

```
┌──(kali㉿kali)-[~]
└─$ sudo ss -antp                                                                                                  130 ×
State       Recv-Q   Send-Q                  Local Address:Port               Peer Address:Port   Process
LISTEN      0        128                         127.0.0.1:9392                    0.0.0.0:*       users:(("gsad",pid=1210,fd=5))
LISTEN      0        244                         127.0.0.1:5432                    0.0.0.0:*       users:(("postgres",pid=1154,fd=6))
TIME-WAIT   0        0                       192.168.1.102:55176            142.250.66.163:80
TIME-WAIT   0        0                       192.168.1.102:55174            142.250.66.163:80
TIME-WAIT   0        0                       192.168.1.102:49642             117.18.237.29:80
TIME-WAIT   0        0                       192.168.1.102:48142           162.247.243.147:443
ESTAB       0        0                       192.168.1.102:53328            35.244.181.201:443     users:(("firefox-esr",pid=1450,fd=40))
TIME-WAIT   0        0                       192.168.1.102:44668              13.35.145.47:443
ESTAB       0        0                       192.168.1.102:55738              44.238.3.246:443     users:(("firefox-esr",pid=1450,fd=150))
ESTAB       0        0                       192.168.1.102:36494            13.224.179.26:443      users:(("firefox-esr",pid=1450,fd=128))
TIME-WAIT   0        0                       192.168.1.102:43696            13.224.179.66:443
TIME-WAIT   0        0                       192.168.1.102:55662           216.58.203.106:443
TIME-WAIT   0        0                       192.168.1.102:59132            216.58.199.46:443
ESTAB       0        0                       192.168.1.102:49590             117.18.237.29:80      users:(("firefox-esr",pid=1450,fd=164))
LISTEN      0        244                                 [::1]:5432                  [::]:*       users:(("postgres",pid=1154,fd=5))
SYN-SENT    0        1           [fe80::250:56ff:fe94:300d]:52472      [2600:1901:0:38d7::]:80      users:(("firefox-esr",pid=1450,fd=118))
SYN-SENT    0        1           [fe80::250:56ff:fe94:300d]:52470      [2600:1901:0:38d7::]:80      users:(("firefox-esr",pid=1450,fd=41))
```

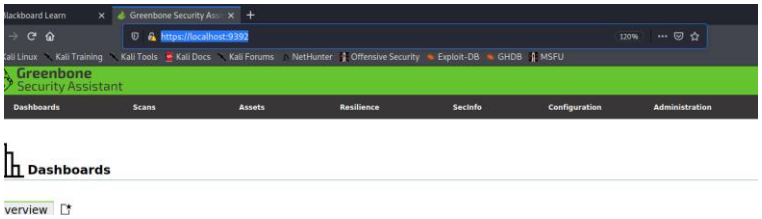
1.2 Change the password of the GSA user 'admin' to be 'admin123'. Write your command line into your lab report, and attach a screenshot to prove that it is executed without errors.

sudo runuser -u _gvm -- gvmd --user=admin --new-password=admin123



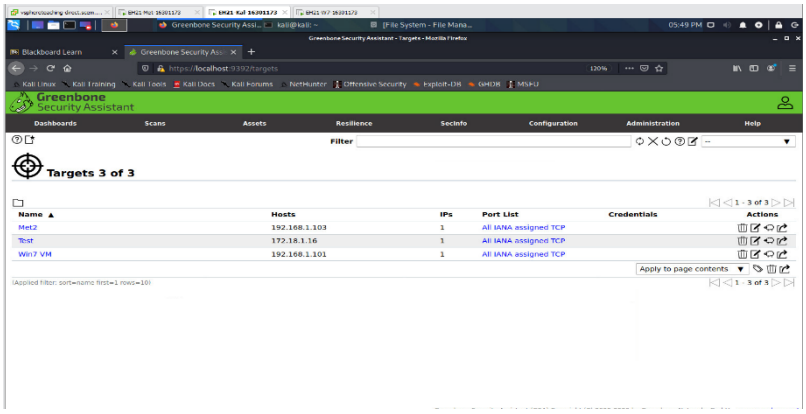
1.3 What’s the URL for Firefox to access the GVM web interface?

https://localhost:9392/ or https://127.0.0.1:9392



Part 2

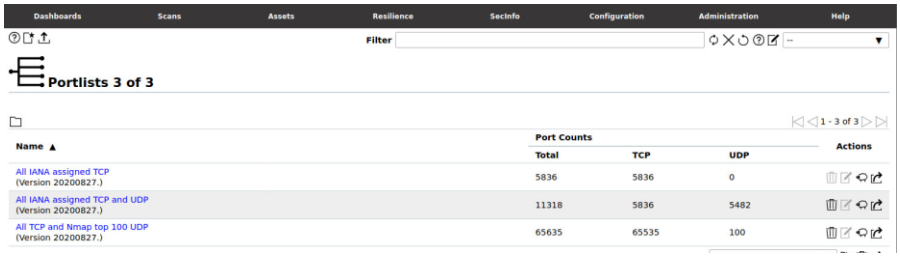
2.1 Create targets for Win7 VM and Metasploitable2 VM respectively. You should choose options according to our lecture slides. Include a screenshot for each target creation into your lab report.



2.2 Explore the GSA web interface to find out the following:

a) How many TCP ports will be scanned if the port list 'All IANA assigned TCP' is used?

5836 TCP total ports of these.

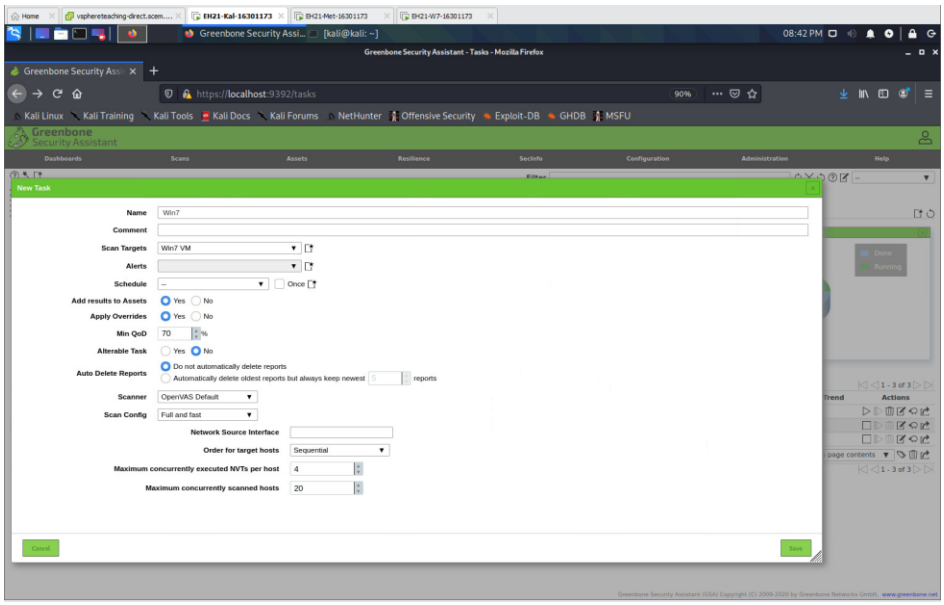


b) Will the TCP port '4' be scanned if this port list is used?

No.

Part 3

3.1 Create a task to scan Win7 VM. Name this task 'Win7', and choose 'Full and Fast' for Scan Config. Include a screenshot of the task configuration into your lab report.



3.2 After the scan is done, download the GVM report in PDF. The report should be saved to the folder '/home/kali/Downloads'. Then, execute 'cd /home/kali/Downloads' and 'ls -l'. Based on the output of 'ls -l', what's the size of your GVM report for Win7 VM?

130238 bytes

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 9348
-rw-r--r--  1 kali kali 9433996 Mar 16 20:12 Lab3-Supplement-treasure.zip
-rw-r--r--  1 kali kali  130238 Mar 22 19:08 report-cd79c875-616c-419e-9150-2763f690a7ff.pdf
drwxr-xr-x 52 kali kali    4096 Mar 14  2019 treasure
```

3.3 Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.

mv report-cd79c875-616c-419e-9150-2763f690a7ff.pdf win7-report.pdf

```
┌──(kali㉿kali)-[~/Downloads]
└─$ mv report-cd79c875-616c-419e-9150-2763f690a7ff.pdf win7-report.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Lab3-Supplement-treasure.zip  treasure  win7-report.pdf
```

3.4 Use Firefox to visit uni email to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Compare your GVM report for Win7 with the sample one provided

to you on vUWS. Focus on the ‘Results Overview’ section of both reports. According to this section,

a) How many results of severity ‘High’ are reported in your report totally?

3

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.101	3	4	1	0	0
Total: 1	3	4	1	0	0

b) How many results of severity ‘High’ are reported in the sample report totally?

There are 3 in my one (above), and 2 in the sample lab report online.

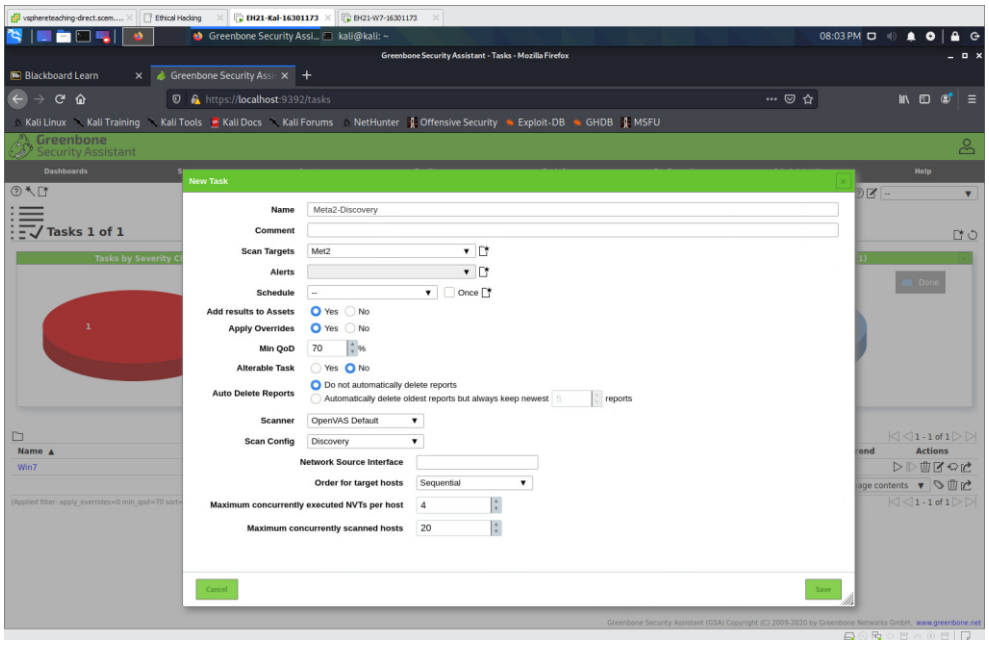
Sample:

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.76.134	2	4	1	0	0
Total: 1	2	4	1	0	0

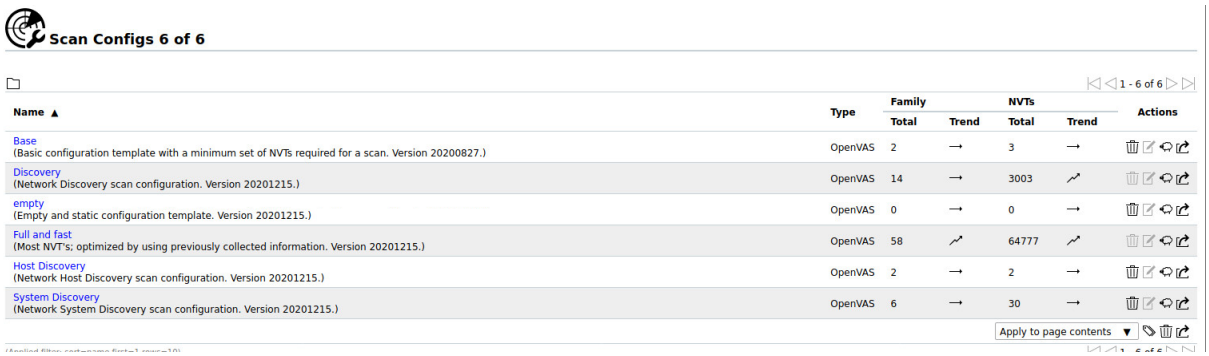
Part 4

4.1 Create a task to scan Metasploitable2 VM. Name this task 'Meta2-Discovery', and choose 'Discovery' as Scan Config. Include a screenshot of the task configuration into your lab report.



4.2 Explore the GSA web interface to find out how many NVTs will be executed under the 'Discovery' Scan Config?

3003



Scan Configs 6 of 6

1 - 6 of 6

Name	Type	Family Total	Family Trend	NVTs Total	NVTs Trend	Actions
Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)	OpenVAS	2	→	3	→	
Discovery (Network Discovery scan configuration. Version 20201215.)	OpenVAS	14	→	3003	↗	
empty (Empty and static configuration template. Version 20201215.)	OpenVAS	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.)	OpenVAS	58	↗	64777	↗	
Host Discovery (Network Host Discovery scan configuration. Version 20201215.)	OpenVAS	2	→	2	→	
System Discovery (Network System Discovery scan configuration. Version 20201215.)	OpenVAS	6	→	30	→	

Apply to page contents

4.3 After the scan is done, download the GVM report in PDF. Then, run 'cd /home/kali/Downloads' and 'ls -l'. Based on the output of 'ls -l', what's the time of your GVM report for Metasploitable2 being saved?

March 23 20:26

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 9400
-rw-r--r--  1 kali kali 9433996 Mar 16 20:12 Lab3-Supplement-treasure.zip
-rw-r--r--  1 kali kali   50901 Mar 23 20:26 report-50370b6c-9aa2-4199-b6b2-5d3df6a70316.pdf
drwxr-xr-x 52 kali kali    4096 Mar 14  2019 treasure
-rw-r--r--  1 kali kali  130238 Mar 22 19:08 win7-report.pdf
```

4.4 Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.

mv report-50370b6c-9aa2-4199-b6b2-5d3df6a70316.pdf met2-report.pdf

```
┌──(kali㉿kali)-[~/Downloads]
└─$ mv report-50370b6c-9aa2-4199-b6b2-5d3df6a70316.pdf met2-report.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ ls -l
total 9400
-rw-r--r--  1 kali kali 9433996 Mar 16 20:12 Lab3-Supplement-treasure.zip
-rw-r--r--  1 kali kali   50901 Mar 23 20:26 met2-report.pdf
drwxr-xr-x 52 kali kali    4096 Mar 14  2019 treasure
-rw-r--r--  1 kali kali  130238 Mar 22 19:08 win7-report.pdf
```

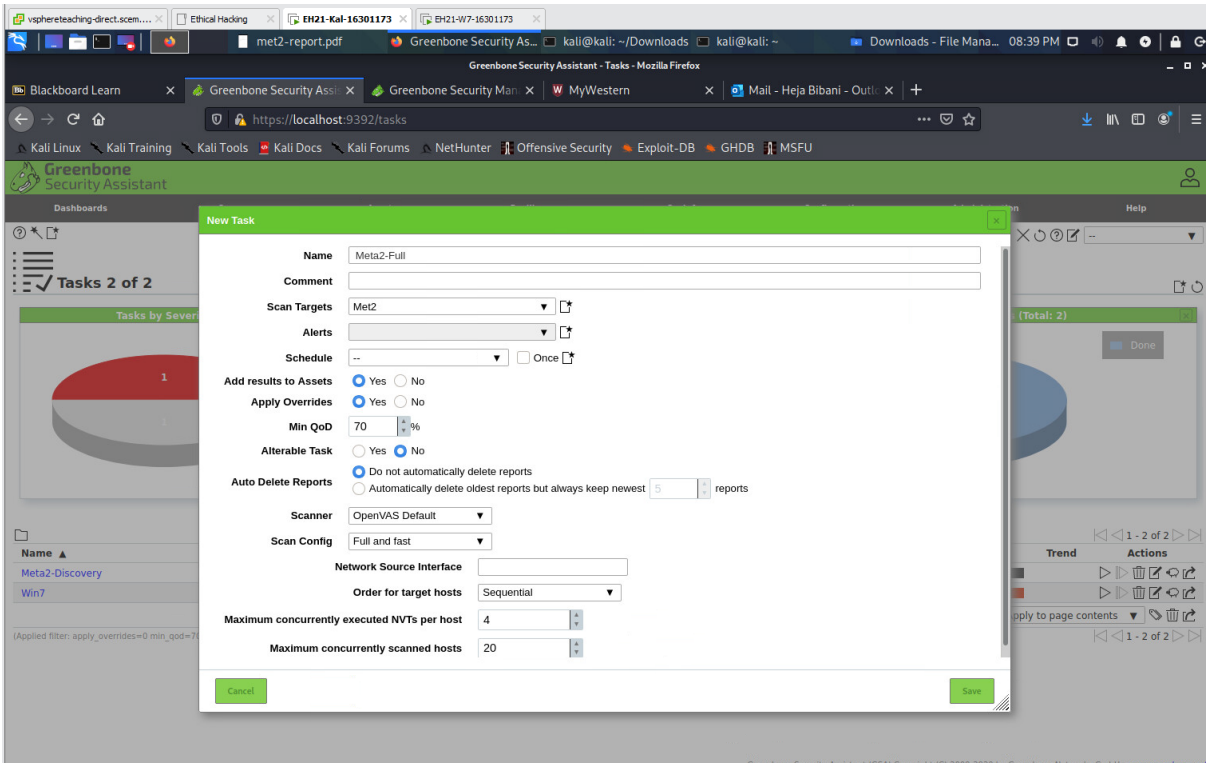
4.5 Use Firefox to visit uni email webpage to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Look at the ‘Results Overview’ section of this report. According to this section, how many results of severity ‘High’ are reported totally?

“0”

1 Result Overview

Host	High	Medium	Low	Log	False Positive
Total: 0	0	0	0	0	0

4.6 Create a second task to scan Metasploitable2 VM. Name this task 'Meta2-Full', and choose 'Full and Fast' as Scan Config. Include a screenshot of the task configuration into your lab report.



4.7 Explore the GSA web interface to find out how many NVTs will be executed under the 'Full and Fast' Scan Config?

64777

Scan Configs 6 of 6

Name	Type	Family Total	Family Trend	NVTs Total	NVTs Trend	Actions
Base (Basic configuration template with a minimum set of NVTs required for a scan. Version 20200827.)	OpenVAS	2	→	3	→	
Discovery (Network Discovery scan configuration. Version 20201215.)	OpenVAS	14	→	3003	↗	
empty (Empty and static configuration template. Version 20201215.)	OpenVAS	0	→	0	→	
Full and fast (Most NVT's; optimized by using previously collected information. Version 20201215.)	OpenVAS	58	↗	64777	↗	
Host Discovery (Network Host Discovery scan configuration. Version 20201215.)	OpenVAS	2	→	2	→	
System Discovery (Network System Discovery scan configuration. Version 20201215.)	OpenVAS	6	→	30	→	

(Applied filter: sort=name first=1 rows=10)

4.8 After the scan is done, download the GVM report in PDF. Rename this GVM report to a more meaningful name using the 'mv' command. Write your command line into the lab report.

mv report-47167e04-f45d-40d0-a6c4-4ee97a6b2d58.pdf met2-Full-report.pdf

```
┌──(kali㉿kali)-[~/Downloads]
└─$ mv report-47167e04-f45d-40d0-a6c4-4ee97a6b2d58.pdf met2-Full-report.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
Lab3-Supplement-treasure.zip  met2-Full-report.pdf  met2-report.pdf  treasure  win7-report.pdf

┌──(kali㉿kali)-[~/Downloads]
└─$
```

4.9 Use Firefox to visit uni email webpage to email this GVM report to you, or you can use other means to transfer this report out of the virtual lab environment. Look at the 'Results Overview' section of this report. According to this section, how many results of severity 'High' are reported totally?

23

1 Result Overview

Host	High	Medium	Low	Log	False Positive
192.168.1.103	23	34	2	0	0
Total: 1	23	34	2	0	0

Part 5

5.1 Look at your GVM report for Win7.

a) How many results have severity 'Medium' according to the 'Results Overview' section?

4

Host	High	Medium	Low	Log	False Positive
192.168.1.101	3	4	1	0	0
Total: 1	3	4	1	0	0

b) In the 'Results per host' section, under the TCP port 445, there should be one result with severity 'High'. What is the name of the NVT that detect this result?

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

2.1.2 High 445/tcp

High (CVSS: 9.3)
NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

c) Study the details of the result mentioned in b) above. Answer the following questions in your lab report.

i) What is the solution recommended for this vuln?

VendorFix: By performing a patch or an update that has been released by the vendor.

Solution
Solution type: VendorFix
The vendor has released updates. Please see the references for more information.

ii) What are the affected OSes listed for this vuln?

Affected Software/OS
- Microsoft Windows 10 x32/x64
- Microsoft Windows Server 2012
- Microsoft Windows Server 2016
- Microsoft Windows 8.1 x32/x64
- Microsoft Windows Server 2012 R2
- Microsoft Windows 7 x32/x64 Service Pack 1
- Microsoft Windows Vista x32/x64 Service Pack 2
- Microsoft Windows Server 2008 R2 x64 Service Pack 1
- Microsoft Windows Server 2008 x32/x64 Service Pack 2

iii) What are the related CVE IDs and BIDs for this vuln?

```
cve: CVE-2017-0143
cve: CVE-2017-0144
cve: CVE-2017-0145
cve: CVE-2017-0146
cve: CVE-2017-0147
cve: CVE-2017-0148
bid: 96703
bid: 96704
bid: 96705
bid: 96707
bid: 96709
bid: 96706
url: https://support.microsoft.com/en-in/kb/4013078
url: https://technet.microsoft.com/library/security/MS17-010
url: https://github.com/rapid7/metasploit-framework/pull/8167/files
cert-bund: CB-K17/0435
dfn-cert: DFN-CERT-2017-0448
```

5.2 Look at your GVM report from task 'Meta2-Full' for Metasploitable2.

a) How many results have severity 'Medium' according to the ‘Results Overview’ section?

34

Host	High	Medium	Low	Log	False Positive
192.168.1.103	23	34	2	0	0
Total: 1	23	34	2	0	0

b) Study the details of the result "Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability". What are the summary and the solution listed for this vuln?

Summary: Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Solution: The solution type is a "work around" which specifies to disable class-loading.

High (CVSS: 10.0)
NVT: Java RMI Server Insecure Default Configuration Remote Code Execution Vulnerability

Summary
Multiple Java products that implement the RMI Server contain a vulnerability that could allow an unauthenticated, remote attacker to execute arbitrary code on a targeted system with elevated privileges.

Solution
Solution type: Workaround
Disable class-loading.