



ETHICAL HACKING V2 LAB SERIES

Lab 07: Evading IDS

Document Version: **2020-08-24**

Material in this Lab Aligns to the Following	
Books/Certifications	Chapters/Modules/Objectives
All-In-One CEH Chapters ISBN-13: 978-1260454550	4: Sniffing and Evasion
EC-Council CEH v10 Domain Modules	12: Evading IDS, Firewalls, and Honeypots
CompTIA Pentest+ Objectives	4.1: Given a scenario, use Nmap to conduct information gathering exercises
CompTIA All-In-One PenTest+ Chapters ISBN-13: 978-1260135947	3: Network Scanning and Enumeration 7: Network-Based Attacks

Contents

Introduction	3
Objective	3
Pod Topology	4
Lab Settings	5
1 Initialize Network Monitoring Applications	6
2 Test IDS Results with Regular Nmap Scan	9
3 Test IDS Results with Decoy Scan	12
4 Test IDS Results with Spoofed MAC Scan	15

Introduction

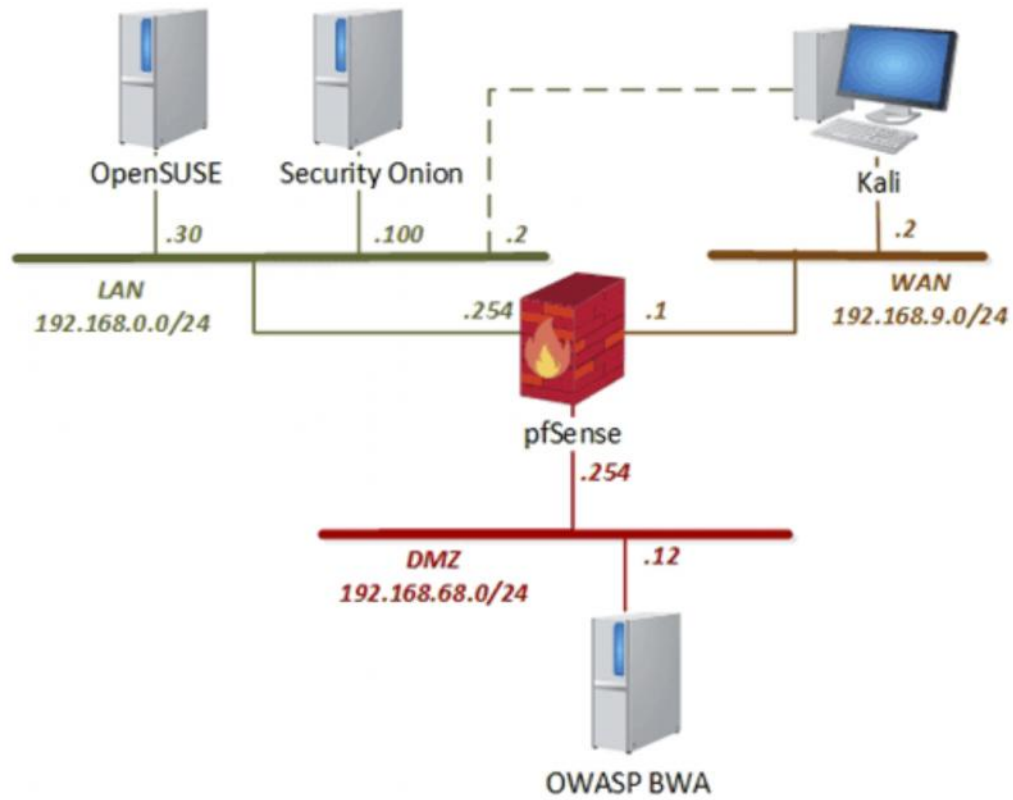
Different methods can be employed to attempt to thwart IDS detection. This lab explores the various methods that can be employed to hide from IDS systems.

Objective

In this lab, you will be conducting ethical hacking practices using various tools. You will be performing the following tasks:

1. Initialize Network Monitoring Applications
2. Test IDS Results with Regular Nmap Scan
3. Test IDS Results with Low MTU Scan
4. Test IDS Results with Decoy Scan
5. Test IDS Results with Spoofed MAC Scan

Pod Topology



Lab Settings

The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

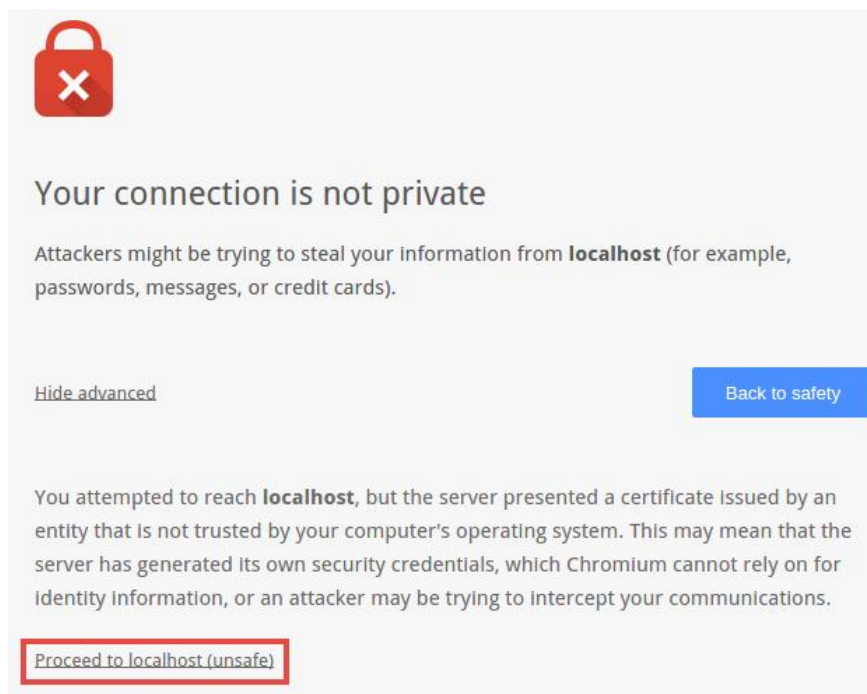
Virtual Machine	IP Address	Account (if needed)	Password (if needed)
Kali Linux	192.168.9.2 192.168.0.2	root	toor
pfSense	192.168.0.254 192.168.68.254 192.168.9.1	admin	pfsense
OWASP Broken Web App	192.168.68.12	root	owaspbwa
OpenSUSE	192.168.0.30	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

1 Initialize Network Monitoring Applications

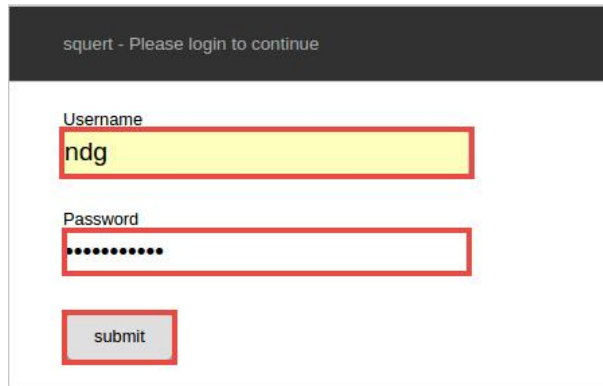
1. Click on the **Security Onion** tab.
2. At the login prompt, enter `ndg` as the *login*. Press **Enter**.
3. Enter `password123` as the *password*. Click **Login**.
4. Once logged in, double-click on the **Squert** icon to launch the application via a web browser.



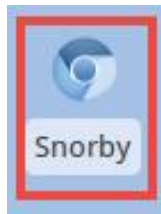
5. Once *Chromium* appears, notice the warning message. Click on the **Advanced** link for more options.
6. Click on the **Proceed to localhost (unsafe)** link.



7. On the *Squert* login page, enter **ndg** as the *username* and **password123** as the *password*. Click **submit**.



8. Navigate back to the **Desktop** and double-click on the **Snorby** icon.



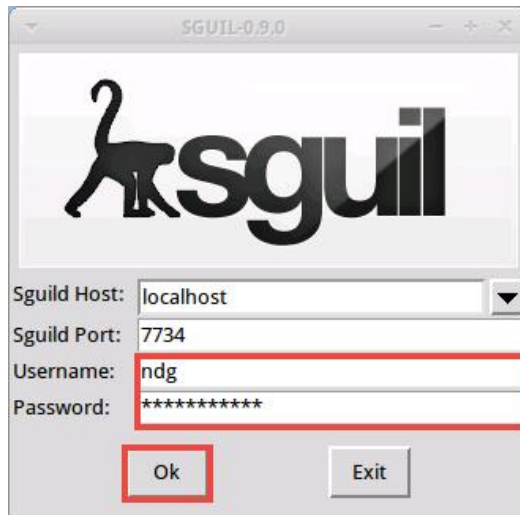
9. Log in to Snorby using the *email* **ndg@ndg.com** and *password* **password123**.



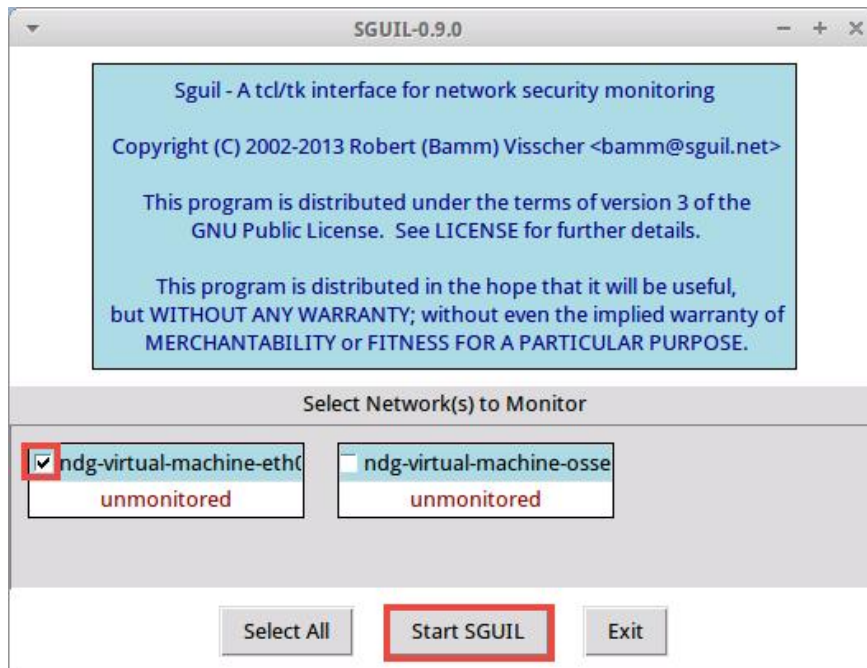
10. Click the **Welcome, Sign In** button.
11. Navigate back to the **Desktop** and double-click on the **Sguil** icon.



12. In the *Sguil* login window, enter **ndg** as the *username* and **password123** as the *password*. Click **OK** to log in.



13. Check the box for **ndg-virtual-machine-eth0** and click the **Start SGUIL** button.



2 Test IDS Results with Regular Nmap Scan

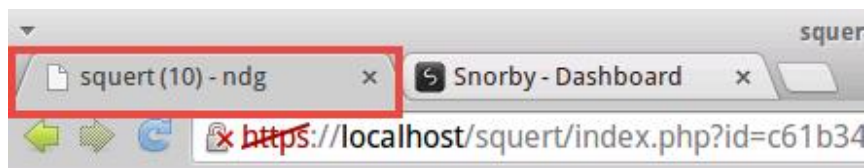
1. Click on the **Kali** tab.
2. Click within the console window, and press **Enter** to display the login prompt.
3. Enter `root` as the *username*. Press **Tab**.
4. Enter `toor` as the *password*. Click **Log In**.
5. Open a new terminal by clicking on the **Terminal** icon located at the top of the page if the terminal is not already opened.
6. Initiate a fragmented packet scan using the *Nmap* application. Using the *Terminal*, type the command below, followed by pressing the **Enter** key.

```
nmap -f 192.168.0.30
```

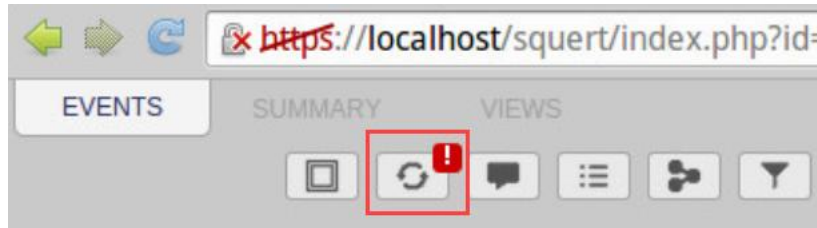
```
root@kali:~# nmap -f 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 16:35 EDT
Nmap scan report for 192.168.0.30
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
5801/tcp   open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
root@kali:~#
```

7. Once the scan successfully finishes, navigate back to the **Security Onion VM**.
8. Change focus to the **Chromium** browser and click the **squert** tab.



9. Click the **refresh** icon located in the top pane.



INTERVAL: 2020-07-27 00:00:00 -> 2020-07-27 23:59:59 (+00:00) FILTERED BY OBJECT: NO FILTERED BY SENSOR: 100.0%

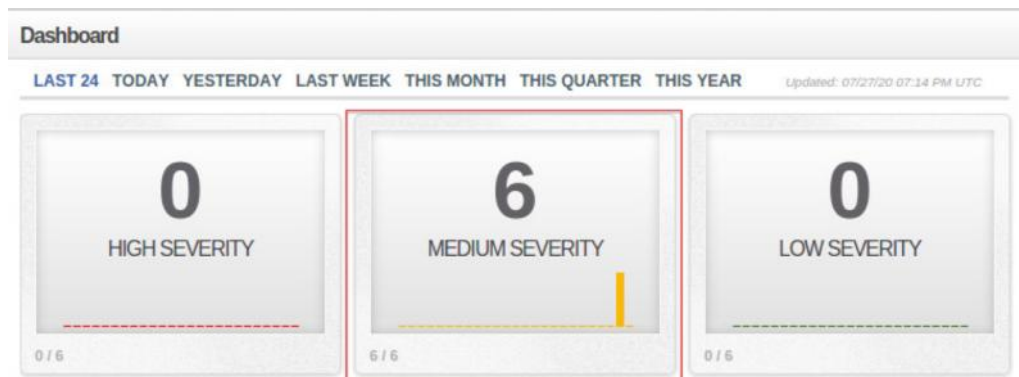
queue only	1	1	1	20:35:08	ET SCAN Potential VNC Scan 5800- 5820	2002910	6	16.667%
grouping	1	1	1	20:35:08	ET SCAN Potential VNC Scan 5900- 5920	2002911	6	16.667%
SUMMARY								
queued events	6				ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	16.667%
total events	6	1	1	20:35:08	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	16.667%
total signatures	6				ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	16.667%
total sources	-							
total destinations	-	1	1	20:35:08				
COUNT BY PRIORITY								
high	1	1	1	20:35:08				
medium	-							
6 (100.0%)								

WELCOME ndg | LOGOUT UTC 2 0:9:39

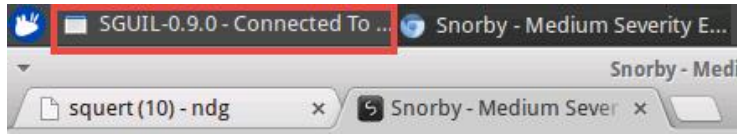
Notice Squert has found potential threats.

10. Click the **Snorby** tab.
11. Press the **F5** key to refresh the page.

Notice the medium severity is not at 6.



12. Change focus to the **Sguil** window.



13. Click on the **Date/Time** column to organize the events in descending order and scroll to the top.

File Query Reports Sound: Off ServerName: localhost UserName: n						
RealTime Events Escalated Events						
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	
RT	1	ndg-virtu...	4.82	2015-12-28 16:37:14	192.1	
RT	1	ndg-virtu...	4.80	2015-12-28 16:22:16	192.1	

Notice that no results are given at this time with the Sguil application.

3 Test IDS Results with Decoy Scan

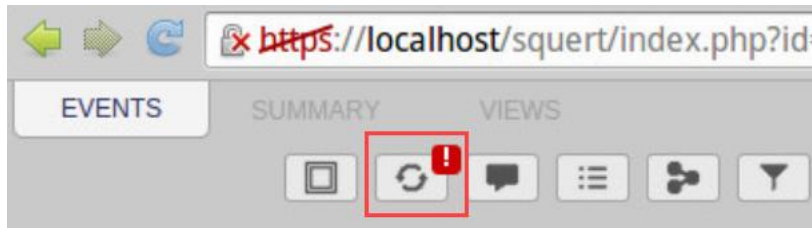
1. Navigate back to the **Kali** VM.
2. Using the *Terminal*, enter the command below to initiate another *Nmap* scan, but this time with a decoy type scan to hide the source IP address from the *IDS*.

```
nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.30
```

```
root@kali:~# nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 17:22 EDT
Nmap scan report for 192.168.0.30
Host is up (0.00013s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
5801/tcp  open  vnc-http-1

Nmap done: 3 IP addresses (1 host up) scanned in 2.68 seconds
root@kali:~#
```


3. Once the scan finishes, navigate back to the **Security Onion** VM.
4. Change focus to the **Chromium** browser with the **squert** tab opened.
5. Click the **refresh** icon located in the top pane.



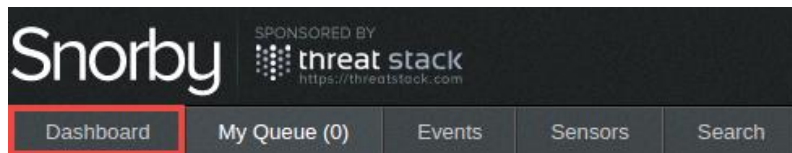
6. Notice that *Squert* caught the same recent *Nmap* scan. Click on the **QUEUE** event with **ET SCAN Potential VNC Scan 5800-5820** as its *Signature*.

3	2	1		21:22:52	ET SCAN Potential VNC Scan 5800- 5820	2002910 6	16.667%
alert tcp \$EXTERNAL_NET any -> \$HOME_NET 5800:5820 (msg:"ET SCAN Potential VNC Scan 5800-5820"; flags:S,12; threshold: type both, track by_src, count 5, seconds 60; reference:url, doc.emergingthreats.net/2002910 ; classtype:attempted-recon; sid:2002910; rev:5;)							
file: downloaded.rules:9159							
<input checked="" type="checkbox"/> CATEGORIZE 3 EVENT(S) <input type="checkbox"/> CREATE FILTER: src dst both							
QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY	
2		2020-07-27 21:22:52	192.168.9.2	RFC1918 (.lo)	192.168.0.30	RFC1918 (.lo)	
1		2020-07-27 21:22:52	192.168.9.20	RFC1918 (.lo)	192.168.0.30	RFC1918 (.lo)	

7. Notice that the scan successfully created a decoy *IP address* along with the real IP address of the *Kali VM*.

QUEUE	ACTIVITY	LAST EVENT	SOURCE	COUNTRY	DESTINATION	COUNTRY
2		2020-07-27 21:22:52	<input type="checkbox"/> 192.168.9.2	RFC1918 (.lo)	<input type="checkbox"/> 192.168.0.30	RFC1918 (.lo)
1		2020-07-27 21:22:52	<input type="checkbox"/> 192.168.9.20	RFC1918 (.lo)	<input type="checkbox"/> 192.168.0.30	RFC1918 (.lo)
3		21:22:52	ET SCAN Potential VNC Scan 5900- c000	2002911	6	16.667%

8. Click on the **Snorby** tab.
9. Click the **Dashboard** menu item.



10. Click on the **Medium Severity** box icon.



11. Notice that *Snorby* caught the recent *Nmap* scan with different source IPs.

Medium Severity Events 18 events found

<input type="checkbox"/>	Sev.	Sensor	Source IP	Destination IP
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.20	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.2	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.20	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.2	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.20	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.2	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.20	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.2	192.168.0.30
<input type="checkbox"/>	★ 2	ndg-virtual-	192.168.9.20	192.168.0.30

12. Change focus to the **Sguil** application window.
13. Notice that *Sguil* was able to identify intrusion but only displays the decoy IP address. You may need to scroll to the top.

ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP	DPort
RT	1	ndg-virtu...	3.797	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	3306
RT	1	ndg-virtu...	3.799	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	5904
RT	1	ndg-virtu...	3.801	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	5432
RT	1	ndg-virtu...	3.803	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	1521
RT	1	ndg-virtu...	3.805	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	5801
RT	1	ndg-virtu...	3.807	2020-07-27 21:22:52	192.168.9.20	49730	192.168.0.30	1433
RT	1	ndg-virtu...	4.104	2019-12-19 18:36:25	192.168.0.20	49812	8.252.116.126	80
RT	1	ndg-virtu...	4.101	2019-12-19 18:18:48	192.168.0.100	40609	104.17.201.89	80
RT	1	ndg-virtu...	4.100	2019-12-19 18:18:48	192.168.0.100	60694	192.168.0.254	53

4 Test IDS Results with Spoofed MAC Scan

1. Navigate back to the **Kali** VM.
2. Using the *Terminal*, enter the command below to initiate another *Nmap* scan, but this time with a spoofed MAC address.

```
nmap -sT -PN -spoof-mac 0 192.168.0.30
```

```
root@kali:~# nmap -sT -PN -spoof-mac 0 192.168.0.30
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-27 17:34 EDT
Spoofing MAC address 11:4E:26:C6:6D:9D (No registered vendor)
You have specified some options that require raw socket access.
These options will not be honored for TCP Connect scan.
Nmap scan report for 192.168.0.30
Host is up (0.00021s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
5801/tcp  open  vnc-http-1

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
root@kali:~#
```

3. Once the scan finishes, navigate back to the **Security Onion** VM.
4. Compare scan results with **Snorby**, **Squert**, and **Sguil**.
5. You may now end your reservation.