ETHICAL HACKING
LAB SERIES

Lab 16: Evading IDS

Material in this Lab Aligns to the Following Certification Domains/Objectives
Certified Ethical Hacking (CEH) Domain
16: Evading IDS, Firewalls and Honeypots

Document Version: 2018-11-05

Contents

Introduction

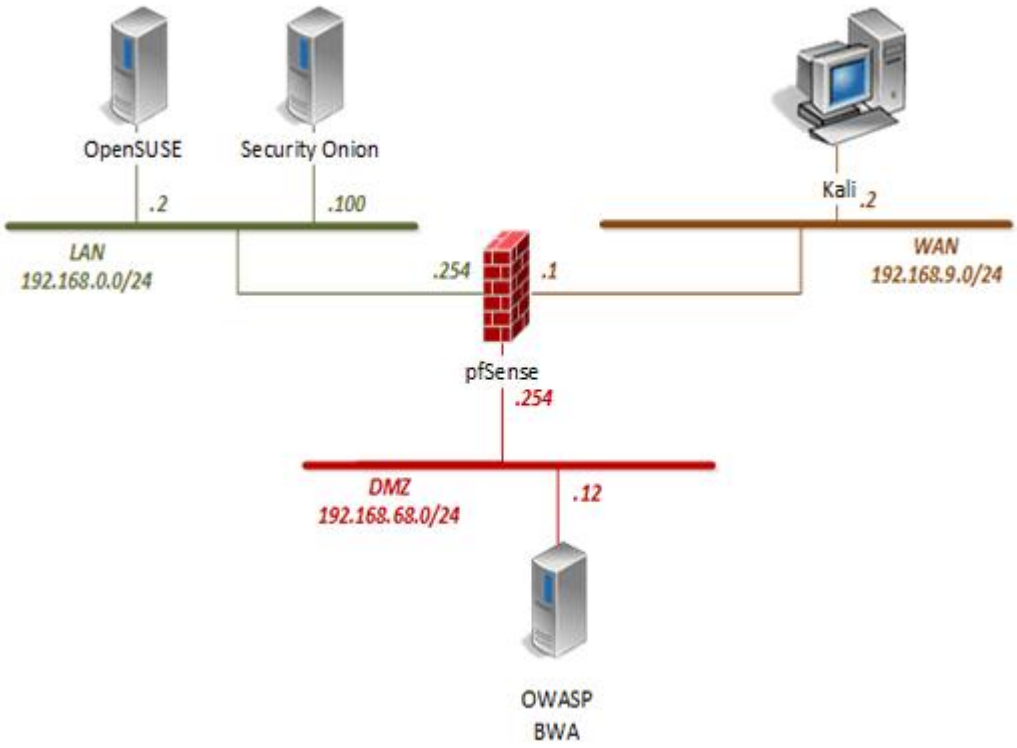
Different methods can be employed to attempt to thwart IDS detection. This lab explores the different methods that can be employed to hide from IDS systems.

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

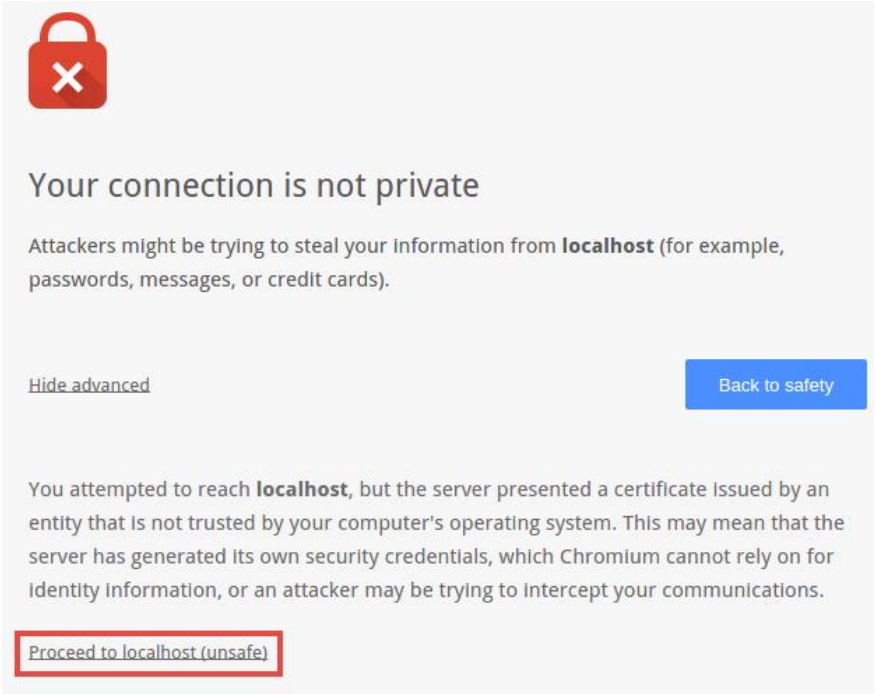
The information in the table below will be needed in order to complete the lab. The task sections below provide details on the use of this information.

Virtual Machine	**IP Address**	**Account** (if needed)	**Password** (if needed)
Kali Linux	192.168.9.2	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	192.168.0.2	osboxes	osboxes.org
Security Onion	192.168.0.100	ndg	password123

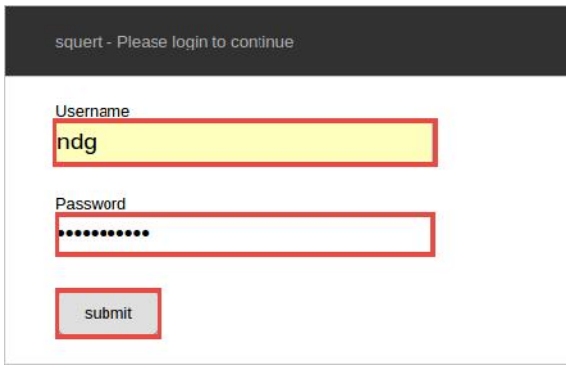
1 Initialize Network Monitoring Applications

1. Navigate to the *topology* page and click on the **Security Onion** VM icon.
2. At the login prompt, enter **ndg** as the *username*. 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 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**.

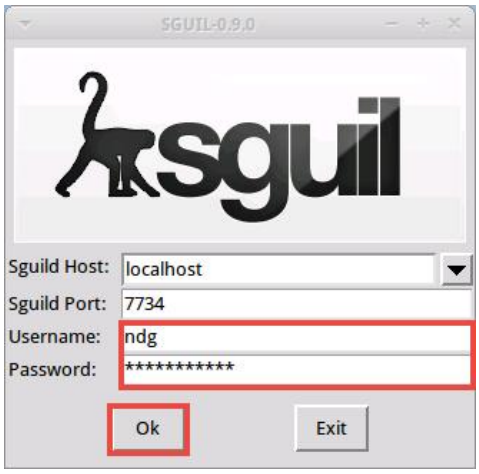


8. Navigate back to the **Desktop** and double-click on the **Snorby** icon.

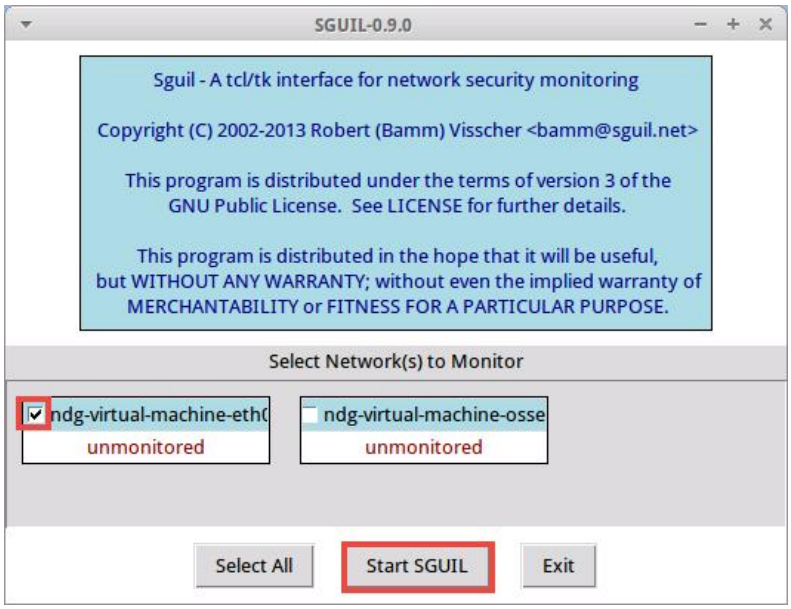
9. Log in to Snorby using the *email* **`ndg@ndg.com`** and *password* **`password123.`**

10. Navigate back to the **Desktop** and double-click on the **Sguil** icon.

11. In the *Sguil* login window, enter **ndg** as the *username* and **`password123`** as the *password*. Click **OK** to login.



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



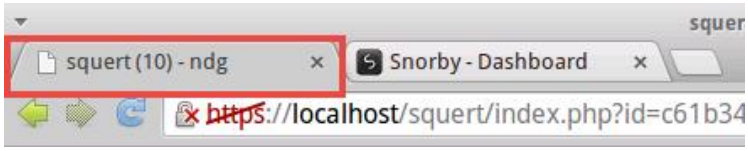
2 Test IDS Results with Regular Nmap Scan

1. Navigate to the **Topology** page and click on the **Kali** icon.
2. Click anywhere within the *Kali* console window and press **Enter** to display the login prompt.
3. Enter **`root`** as the *username*. Click **Next**.
4. Enter **`toor`** as the *password*. Click **Sign In**.
5. Open the *Terminal* by clicking on the **Terminal** icon located on the left panel.

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 192.168.0.2
```

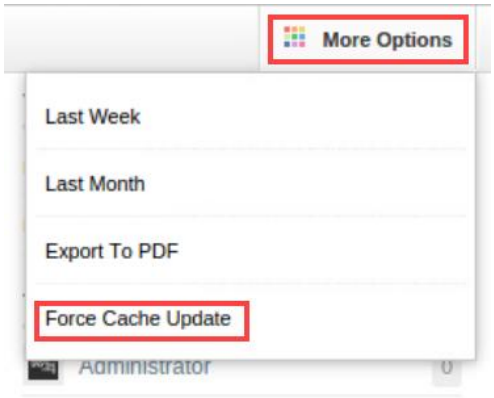
7. Once the scan successfully finishes, navigate back to the **Security Onion** VM.
8. Change focus to the **Chromium** browser and click the **squert** tab.



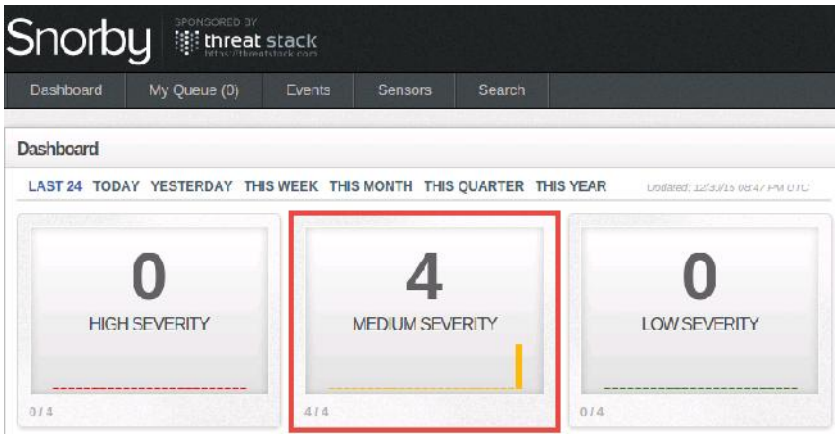
9. Click the **refresh** icon located in the top pane.

Notice a signature identified that the potential scan was detected by the system.

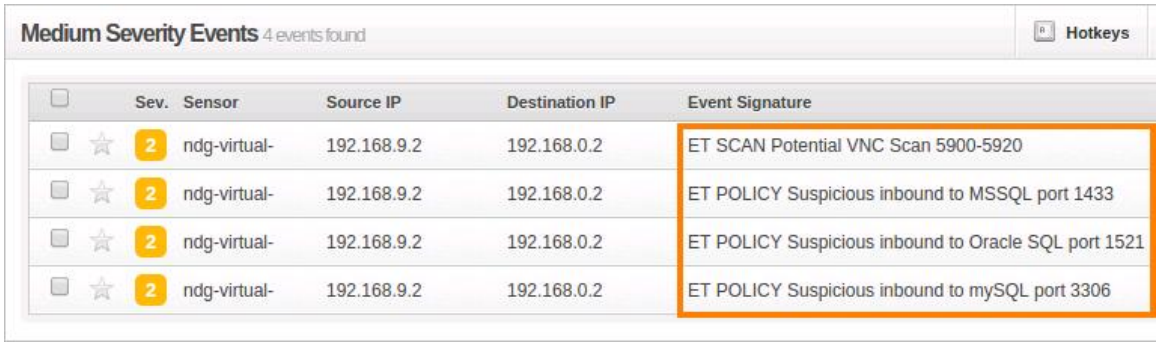
10. Click the **Snorby** tab.
11. Press the **F5** key to refresh the page. If that does not help refresh the dashboard, then click on the **More Options** icon and click on **Force Cache Update**. Wait until the forced update completes.



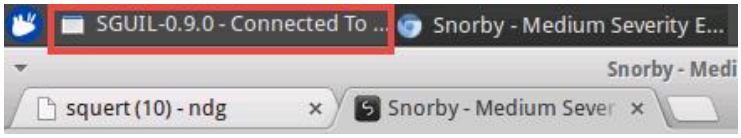
12. Notice the *Medium Severity* populates, click on its respective boxed icon.



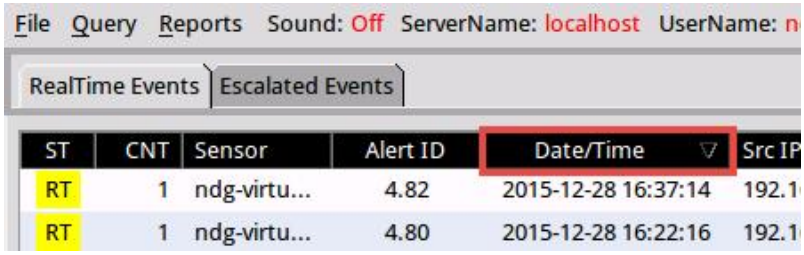
13. On the *Medium Severity Events* page, notice that the *Nmap* scan was detected.



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



15. Click on the **Date/Time** column to organize the events in a descending order.



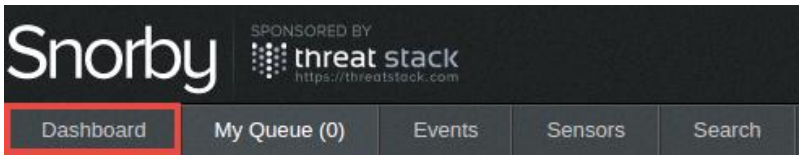
16. Notice that no results are given at this time with the *Sguil* application.

3 Test IDS Results with Low MTU 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 low *MTU* rate in attempt to be stealthier.

```
nmap --mtu 8 192.168.0.2
```

3. Once the scan finishes, navigate back to the **Security Onion** VM.
4. Change focus to the **Chromium** browser with the **Snorby** tab opened.
5. Click the **Dashboard** menu item.



6. Click on the **Medium Severity** box icon.
7. Notice that *Snorby* caught the recent *Nmap* scan.

If results are not being displayed, wait for 1-2 minutes and then refresh the page once more.

8. Click on the **Squert** tab.
9. Click the **refresh** icon located in the top pane.
10. Notice that *Squert* caught the recent *Nmap* scan.
11. Change focus to the **Sguil** application window.
12. Notice that *Sguil* was unable to capture any events from the *Nmap* scan.

4 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*.

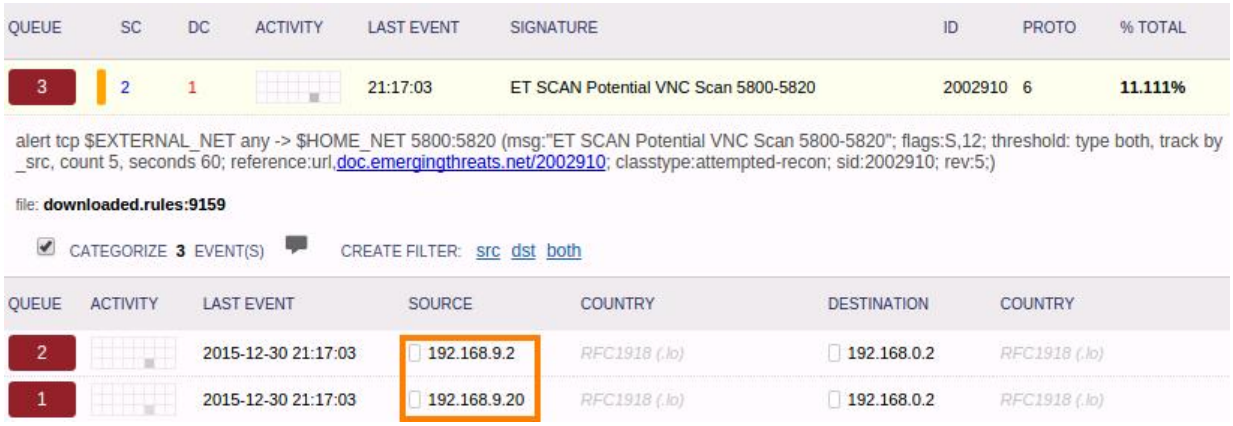
```
nmap –D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.2
```

```
root@Kali2:~# nmap -D 192.168.9.20 192.168.9.30 192.168.9.40 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-30 15:18 CST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.00090s 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 0.51 seconds
```

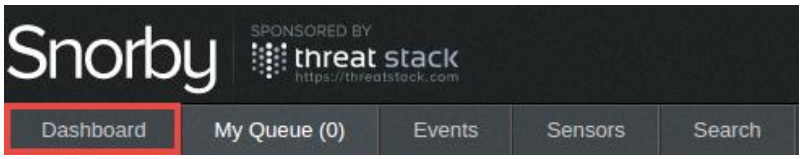
3. Once the scan finishes, navigate back to the **Security Onion** VM.
4. Change focus to the **Chromium** browser with the **squert** tab opened.
5. Click the **refresh** icon located in the top pane.
6. Notice that *Squert* caught the same recent *Nmap* scan. Click on the **QUEUE** event with **ET SCAN Potential VNC Scan 5X00-5X20** as its *Signature*.

QUEUE	SC	DC	ACTIVITY	LAST EVENT	SIGNATURE	ID	PROTO	% TOTAL
3	2	1		21:17:03	ET SCAN Potential VNC Scan 5800-5820	2002910	6	**11.111%**
4	2	1		21:17:03	ET SCAN Potential VNC Scan 5900-5920	2002911	6	**14.815%**
4	2	1		21:17:03	ET POLICY Suspicious inbound to Oracle SQL port 1521	2010936	6	**14.815%**
4	2	1		21:17:03	ET POLICY Suspicious inbound to mySQL port 3306	2010937	6	**14.815%**
3	2	1		21:17:03	ET POLICY Suspicious inbound to PostgreSQL port 5432	2010939	6	**11.111%**
7	7 1	1		21:13:53	[OSSEC] Received 0 packets in designated time interval (defined in ossec.conf). Please check interface, cabling, and tap/span!	111112	0	**25.926%**
2	1	1		21:03:18	ET POLICY Suspicious inbound to MSSQL port 1433	2010935	6	**7.407%**

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



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

5 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 0 192.168.0.2
```

```
root@Kali2:~# nmap -sT -PN -spoof-mac 0 192.168.0.2

Starting Nmap 6.49BETA5 ( https://nmap.org ) at 2015-12-30 15:35 CST
Spoofing MAC address 7E:98:AE:C8:62:E6 (No registered vendor)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
 Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.0.2
Host is up (0.0022s 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 0.14 seconds
```

3. Once the scan finishes, navigate back to the **Security Onion** VM.
4. Compare scan results with **Snorby**, **Squert**, and **Sguil**.
5. Close the **Security Onion** and **Kali** PC viewers.

