Christopher Bazyani

CYB 552

Advanced Hacking Prevention

Lab 10

Securing the Network with an Intrusion Detection System (IDS)

**Section 1: Hands-On Demonstration**

Part 1: Configure an Intrusion Detection System (IDS)

On the vWorkstation, double-click the Connections folder.

In the Connections folder, double-click on the SnortSSH shorcut to open a remote terminal window to the TargetIDS virtual machine.

At the command prompt, type sudo -i and press Enter to enable sudo privileges for the student user.

When prompted for the [sudo] password for student, type toor and press Enter to continue with root-level access.



Please note that Linux systems do not display password inputs on-screen for security reasons.

At the command prompt, type nsm\_sensor\_ps-start and press Enter to verify that Snort is running and check the configuration files, database rules, sensors, and other configuration options.

Text

Description automatically generated

At the command prompt, type cd /etc/nsm/SCO-eth0 and press Enter to change the working directory to the location of the Snort configuration files.



Note: The location /etc/nsm is the main directory for Snort and its configuration files; in this instance, the SCO-eth0 directory will contain a copy of the snort.conf file for the student profile. In the next steps, you will make some configuration changes to better tune Snort for this environment.

At the command prompt, type vi snort.conf and press Enter to open the Snort configuration file in the vi Editor.

Text

Description automatically generated

In the vi Editor, type i to open the edit (insert) mode, then use the arrow keys to locate the ipvar HOME\_NET line.

Text

Description automatically generated

This is where you can define the network addresses that Snort will protect.

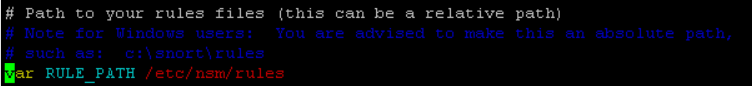
In the vi Editor, delete the 10.0.0.0/8 address and replace the 172.16.0.0/12 address with 172.30.0.0/24, as shown in the following figure.

Text

Description automatically generated

In the vi Editor, press Esc to leave edit mode.

In the vi Editor, use the arrow keys to locate the var RULE\_PATH /etc/nsm/rules line.



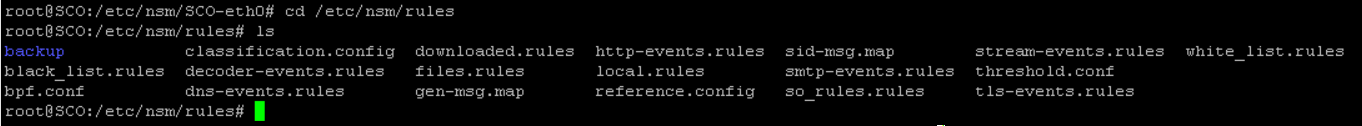
This is the location of all Snort rules files for all profiles. You will need this location later in the lab.

In the vi Editor, type :wq! and press Enter to save your changes, close the vi Editor, and return to the command prompt. If prompted, type y to confirm your changes.

At the command prompt, type cd /etc/nsm/rules and press Enter to change the working directory to the directory where the rules files are located.

At the command prompt, type ls and press Enter to list the contents of the directory.

Make a screen capture showing the contents of the /etc/nsm/rules directory and paste it into your Lab Report file.



At the command prompt, type cat reference.config and press Enter to display the contents of the reference.config file.

Text

Description automatically generated

The reference.config file includes links to web sites with information for all the alerts.

At the command prompt, type cat threshold.conf and press Enter to display the contents of the threshold.conf file.

**Text

Description automatically generated**

The threshold.conf file controls the Snort application in setting thresholds and suppression and allows you to control the number of events.

At the command prompt, type reboot and press Enter to reboot the Snort system, clearing all cache and forcing it to start with the new changes.

Text

Description automatically generated

You will need to reboot the Snort server after altering a configuration file in order for the changes to take effect.

Close the remote terminal window.

After any reboot, the terminal window will be deactivated. The reboot process takes up to 5 minutes to completely reset. Wait at least 3-5 minutes before continuing with the next step.

In the Connections folder, double-click the SnorbyWWW Internet Shortcut to open the Snorby tool in a new browser window.

If prompted with a security certificate warning, click Continue to this website (not recommended) to continue. This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate.

At the Snorby log-in screen, type the following credentials and press Enter to continue.

Username: student@securelabsondemand.com

Password: student

If prompted to save the password, click Not for this site.

A screenshot of a computer

Description automatically generated with medium confidence

Explore the tabs and links on this page to familiarize with the features of Snorby.

Graphical user interface, website

Description automatically generated

Note: Snorby is a web-based front-end to other applications, such as Snort. When Snort captures and examines IP packets, it does not save every IP packet. Rather, it is looking for specific IP packet traffic patterns and abnormal traffic attempting to enter a network. The IDS maintains logs and alerts and alarms when certain IP packet traffic patterns are identified inbound to the organization’s network. Alerts or alarms can be automated to send information to a network or security operations help desk. Should you receive an IDS alert about a port scan detected from the same IP on a subnet, this is one of the first signs of a possibly compromised machine. An attacker may have remote access to a workstation and enabled a vulnerability assessment scan from within your organization. The results of his scan will be sent back to the attacker, unnoticed by your organization.

Note: Your organization’s security policies should define acceptable and unacceptable protocols, applications, and services running on your network. Performing a network traffic baseline definition analysis will provide you with information about what protocols and traffic behavior patterns are normal. Using this as a baseline, the IDS can be configured to recognize abnormal digital signatures or IP traffic patterns, which helps harden the LAN-to-WAN domain at the Internet ingress/egress point.

Minimize the Snorby window.

You will return to the Snorby interface later in the lab.

Part 2: Conduct a Vulnerability Scan

In the Connections folder, double-click the TargetWindows02 RDP shortcut to open a remote connection to the TargetWindows02 machine.

If prompted, type the following credentials and click OK to open the remote connection.

The remote desktop opens with the IP address of TargetWindows02 (172.30.0.10) in the title bar at the top of the window.

From the TargetWindows02 taskbar, click the Windows Start button and select Tenable Network Security > Nessus Web Client from the menu.

Graphical user interface

Description automatically generated

If prompted with a security certificate warning, click Continue to this website (not recommended) to continue. This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate.

At the Nessus log-in screen, type the following credentials and press Enter to open the Nessus web client.

Username: administrator

Password: P@ssw0rd!

Graphical user interface

Description automatically generated

If prompted to save the password, click Not for this site.

In the upper-left corner of the Scans page, click the New Scan button to open the Scan Library of preconfigured network scans, then click the Basic Network Scan option.

In the New Scan / Basic Network Scan form, type the following information:

Name: yourname\_S1\_ScanIDS, replacing yourname with your own name

Description: TargetIDS scan

Folder: My Scans

Target: 172.30.0.8

At the bottom of the form, click the Save button to save the new configuration and open the My Scans page.

Graphical user interface

Description automatically generated

On the My Scans page, click the yourname\_S1\_ScanIDS checkbox to select your Basic Scan.

In the upper-right corner of the My Scans page, click the More menu and select Launch to launch your Basic Scan.

Graphical user interface, application

Description automatically generated

When prompted, click Launch again to confirm the launch of the scan.

Graphical user interface, text, application, email

Description automatically generated

From the Remote Connection title bar for TargetWindows02, click the Restore Down button to make the vWorkstation desktop visible.

From the vWorkstation taskbar, restore the Snorby browser window, then click TODAY in the top navigation pane and arrange the windows so you can see both the Nessus scan and the Snorby dashboard, as shown in the following figure.

Graphical user interface, website

Description automatically generated

The Nessus scan will take 20-25 minutes to complete. As the Nessus scan continues to run in the TargetWindows02 window, you should periodically refresh your browser window on the vWorkstation. You will notice that the Snorby Dashboard recognizes the Nessus scan, and catalogs the network traffic according to threat severity. Scan results will vary, so your results may not reflect what you see in the following figure.

Part 3: View the Scan Results

When the Nessus scan has completed, maximize the Snorby window.

On the Snorby Dashboard, click the High Severity report to view a list of potential high severity vulnerabilities.

Make a screen capture showing the list of high severity vulnerabilities and paste it into your Lab Report file.

Graphical user interface

Description automatically generated

From the Snorby navigation bar, click the Dashboard tab to return to the Snorby dashboard.

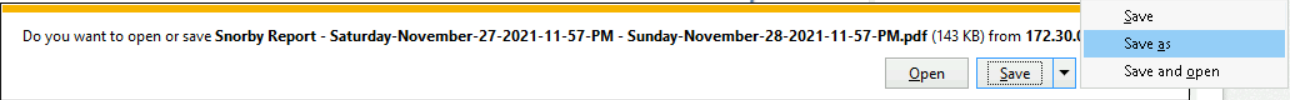


In the upper-left corner of the Snorby dashboard, click the More Options link and select Export to PDF to save the Snorby results as a PDF.

Graphical user interface, text, application

Description automatically generated

When prompted, click the Save arrow to expand the Save menu, then select Save as to open the Save As dialog box.



In the Save As dialog box, type yourname\_S1\_ScanIDS, replacing yourname with your own name, and click Save to save the report to the Desktop.

Graphical user interface, text, application, email

Description automatically generated

Close the Snorby window.

Close the Nessus window.

Close the remote TargetWindows02 connection.

On the vWorkstation desktop, double-click the yourname\_S1\_ScanIDS.pdf file to open the Snorby report.

In the Snorby report, locate the Top 15 Signatures section.

Make a screen capture showing the Top 15 Signatures and paste it into the Lab Report file. If necessary, take multiple screen captures.

Graphical user interface

Description automatically generated

Note: It is possible to identify the digital signatures of common reconnaissance and probing scans, such as Ping, Nmap, and Nessus. It is best practice to configure any IDS and IPS devices to specifically alert and block reconnaissance and probing IP packets that are commonly used by these attack tools. All of the normal hacking applications and tools that generate ICMP, IP, UDP, and TCP should also be identified and blocked on your external IDS/IPS device, including denial of service (DoS) and distributed denial of services (DDoS) digital signatures.

Close the Snorby report.

**Section 2: Applied Learning**

Part 1: Configure an Intrusion Detection System (IDS)

In the Connections folder, open the SnortSSH shortcut to open a remote terminal session with the TargetIDS virtual machine.

At the command prompt, execute the command to enable sudo privileges for the student user.

When prompted for the password, enter toor to continue with root-level access.

When prompted for the password, execute nsm\_sensor\_ps-start to verify that Snort is running and check the configuration files, database rules, sensors, and other configuration options.

At the command prompt, execute the command to change the working directory to /etc/nsm/SCO-eth0, the location of the Snort configuration files.

Note: The location /etc/nsm is the main directory for Snort and its configuration files; in this instance, the SCO-eth0 directory will contain a copy of the snort.conf file for the student profile. In the next steps, you will make some configuration changes to better tune Snort for this environment.

At the command prompt, execute the command to open the snort.conf file in the vi Editor.

Text

Description automatically generated

In the vi Editor, type i to open edit (insert) mode, then locate the ipvar HOME\_NET line.

In the vi Editor, remove the 10.0.0.0/8 address and replace the 172.16.0.0/12 address with 172.30.0.0/24.

Text

Description automatically generated

In the vi Editor, press Esc to exit edit mode.

In the vi Editor, locate the var RULE\_PATH /etc/nsm/rules line.

This is the location of all Snort rules files for all profiles. You will need this location later in the lab.

In the vi Editor, type :wq! and press Enter to save your changes, close the vi Editor, and return to the command prompt.

At the command prompt, execute the command to change the working directory to /etc/nsm/rules.

Text

Description automatically generated

At the command prompt, execute the command to display the contents of the reference.config file.

Text

Description automatically generated

The reference.config file includes links to web sites with information for all the alerts.

At the command prompt, execute the command to open the local.rules file in the vi Editor.

Note: The local.rules file in Snort can be customized with rules that perform a specific task on recognizing a specific action. A sample of these tasks can be found in the following list.

ALERT - Generate an alert using the selected alert method, and then log the packet:

alert <protocol> <any Source IP> <any Source Port> - Direction > <$HOME\_NET destination IP> <port>

LOG - Log the packet:

log udp any any -> $HOME\_NET 1:1024

PASS - Ignore the packet:

pass icmp any any -> $HOME\_NET any

ACTIVATE - Alert and then turn on another dynamic rule:

activate tcp any any -> any any (msg:”HFS Exploit Attempt”; content:”%TEMP%”; flowbits:set,payload; sid:1000014; rev:1; activates:1;)

DYNAMIC - Remain idle until activated by an activate rule, then act as a log rule:

dynamic tcp $HOME\_NET any -> any any (activated\_by:1; count:100; sid:1000018;)

DROP - Block and then log the packet:

drop tcp any 21 -> $HOME\_NET any

In the next steps, you will create a custom alert rule using the format in this list.

In the vi Editor, insert the following new line, replacing yourname with your own name:

alert tcp any any -> $HOME\_NET 22 (msg:”yourname SSH connection attempt”; sid:1000002; rev:1;)

In the vi Editor, save the changes to the local.rules file to return to the command prompt.

At the command prompt, execute the command to display the contents of the local.rules file.

Make a screen capture showing the contents of the local.rules file and paste it into your Lab Report file.

Text

Description automatically generated

At the command prompt, execute the command to restart the Snort system, then close the terminal window.

After any reboot, the terminal window will be deactivated. The reboot process takes about 5 minutes to completely reset. Wait at least 5 minutes before continuing with the next step.

From the Connections folder, open a new terminal session to TargetIDS, then execute the command to enable sudo privileges for the student user, enter the password, and minimize the terminal window.

From the Connections folder, open the SnorbyWWW shortcut to open the Snorby tool in a new browser window.

If prompted with a security certificate warning, click Continue to this website (not recommended) to continue. This warning appears when visiting a website that either has an expired certificate, a mismatched certificate, or a self-signed certificate.

Note: Snorby is a web-based front-end to other applications, such as Snort. When Snort captures and examines IP packets, it does not save every IP packet. Rather, it is looking for specific IP packet traffic patterns and abnormal traffic attempting to enter a network. The IDS maintains logs and alerts and alarms when certain IP packet traffic patterns are identified inbound to the organization’s network. Alerts or alarms can be automated to send information to a network or security operations help desk. Should you receive an IDS alert about a port scan detected from the same IP on a subnet it is one of the first signs of a possibly compromised machine. An attacker may have remote access to a workstation and has enabled a vulnerability assessment scan from within your organization. The results of his scan will be sent back to the attacker unnoticed by your organization.

At the Snorby log-in screen, log in using the following credentials.

Username: student@securelabsondemand.com

Password: student

Note: Your organization’s security policies should define what are acceptable and unacceptable protocols, applications, and services running on your network. Performing a network traffic baseline definition analysis will provide you with information about what protocols and traffic behavior patterns are normal. Using this as a baseline, the IDS can be configured to recognize abnormal digital signatures or IP traffic patterns, which helps harden the LAN-to-WAN domain at the Internet ingress/egress point.

On the Snorby dashboard, click the Events tab to view all of the events captured by Snorby.

On the Events page, click the event you just generated by opening the new terminal session.

If you do not see an event for your most recent terminal session, wait five minutes, then reload the browser.

In the Signature Information section, click the View Rule button to open the Rule Information window.

Make a screen capture showing rule information for the alert you created and paste it into your Lab Report file.

A screenshot of a computer

Description automatically generated

Close the Rule Information window, then navigate back to the Snorby dashboard.

Minimize the Snorby window.

Part 2: Conduct a Vulnerability Scan

Open a remote connection to the TargetWindows02 machine.

Open the Nessus web client.

Login to Nessus using the following credentials:

Username: administrator

Password: P@ssw0rd!

Graphical user interface

Description automatically generated

Create a new Basic Network Scan using the following parameters:

Name: yourname\_S2\_ScanIDS

Description: Scan the IDS system

Folder: My Scans

Targets: 172.30.0.8

Graphical user interface

Description automatically generated

Launch the yourname\_S2\_ScanIDS scan, then restore down the remote TargetWindows02 connection.

Graphical user interface, text, application, Teams

Description automatically generated

On the vWorkstation, restore the Snorby browser window, then click TODAY in the dashboard pane, and arrange the windows so you can see both the Nessus scan and the Snorby dashboard.

Graphical user interface, website

Description automatically generated

The Nessus scan will take 20-25 minutes to complete. As the Nessus scan continues to run in the TargetWindows02 window, you should periodically refresh your browser window on the vWorkstation. You will notice that the Snorby Dashboard recognizes the Nessus scan, and catalogs the network traffic according to threat severity. Scan results will vary, so your results may not reflect what you see in the following figure.

Part 3: View the Scan Results

When the Nessus scan is complete, maximize the Snorby window.

From the Snorby dashboard, navigate to the High Severity report and review the high severity events.

Graphical user interface, website

Description automatically generated

Return to the Snorby Dashboard and export the report to the TargetWindows02 desktop as a PDF titled yourname\_S2\_ScanIDS, replacing yourname with your own name, then close the Snorby window.

Graphical user interface, text, application

Description automatically generated

Close the remote TargetWindows02 connection.

On the vWorkstation desktop, open the Snorby report.

In the Snorby report, locate the Top 15 Signatures section.

Make a screen capture showing the Top 15 Signatures and paste it into the Lab Report file.

Table

Description automatically generated with medium confidence

Note: It is possible to identify the digital signatures of common reconnaissance and probing scans, such as Ping, Nmap, and Nessus. Program your IDS and IPS devices to specifically alert and block reconnaissance and probing IP packets that are commonly used by these attack tools. All of the normal hacking applications and tools that generate ICMP, IP, UDP, and TCP should also be identified and blocked on your external IDS/IPS device, including denial of service (DoS) and distributed denial of services (DDoS) digital signatures.

In the Lab Report file, research and describe three of the signatures alerts captured in the Snorby report.

Close the Snorby report.