# Week 1

# Lab 1 (a): Configure a firewall to protect a perimeter network

The vCloud environment is accessible from within the University network or at home through your web browser. For access instructions, consult the vCloud Student Connection Instructions document, available on Canvas.

Read all instructions in this lab thoroughly and complete the lab as prescribed. Email the professor with any questions. Be sure to submit questions as early as possible to ensure time for answers so that you have the opportunity to complete and submit the lab on time.

# Preparation

## Using VMware

Some important points to know about VMware:

* To release the keyboard and mouse cursor a VMware session, press CTRL and ALT at the same time.
* The VMware image you are using can take a snapshot of the current state of the machine. There is a button labeled “snapshot” in the browser window to do this.
	+ The “revert” window will restore the snapshot, destroying any changes since then.
	+ Taking a snapshot will destroy any prior snapshots
* To perform “CTRL-ALT-DEL” in the VM, use the button, so labeled, inside of the browser window.

## Taking Screenshots

* "How to use the Snipping Tool on Windows 10" video at <https://www.youtube.com/watch?v=ayi5-7QPNcA>
* "How to Take a Screenshot on a Mac" video at <https://www.youtube.com/watch?v=h3RkDPfphSQ>

**COMMENTS**: Care should be used so that only that window is captured. Devote as much of the screen capture’s real-estate as possible to the display of the VM itself, minimizing superfluous content. **DO NOT** take a screenshot of your entire desktop.

Screenshots that are difficult to read due to sizing or other issues may be rejected and points taken off.



## Completing the Lab

To complete the lab, fill out the questions in the section below in this document, pasting in screenshots for each question. Save the updated document and upload to Canvas. Be sure to use Microsoft Word when editing and saving this document.

DO NOT change any formatting in the document. Simply type in your answers and paste in your screenshots.

**Alternate submission formats** **will not be accepted!!!**

## Lab Overview

In this lab, students will configure a Linux firewall to restrict access to a server on one side of it from a host on the outside. Students will implement packet filter rules and stateful rules for a variety of services, as well as a web proxy. Students will also use various tools to troubleshoot firewall issues.

Each student will be given their own firewall in VCloud to use for the duration of the course. Due to limitations in VMware, the firewalls will be grouped into clusters of four. Student credential for the Firewall VMs, User ID: student Password: password



The firewall rules in this lab will be implemented on the command line, using the **iptables** command. Be sure to read the man page of iptables for details on how to use the command, specifically lines 1-230. You may also consult any Internet resource. Students are allowed to work together, but each student must submit their own lab with all of the screenshots from their own firewall.

## Exercises

Complete the following exercises. For each question, paste in a screenshot of the completed activity. Be sure to show all relevant details.

|  |
| --- |
| 1. When you first login to your firewall, it is allowing all traffic. What type of a firewall is your system at this point?

Answer the question here.Lock down the firewall so that its default policy for all tables is deny. What type of a firewall is your system after this change?Answer the question here.What change was needed to accomplish this? Type out your answer below, as well as the commands you used in this question.Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here a print screen of the output from TCP dump that shows traffic from the South host, and the lack of replies from both the firewall and the North host. |
| 1. Configure the firewall to explicitly allow ping to the firewall, and nothing else. What change was needed to make this work? Type out your answer below, as well as the commands you used in this question.

Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here a print screen of the output from TCP dump that captures the ping from the remote host, and the reply from the firewall. |
| 1. In addition to the rules from the last question, configure the firewall to allow ping from the firewall, and nothing else. What change was required to make this work? Type out the commands in this question.

Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here the output from ping command, executed on the firewall, and the reply from the remote host. |
| 1. In addition to the rules from the questions 2 and 3, configure the firewall with stateless rules to allow HTTP from only the South host as web client, below the firewall to only the North host as web server above firewall, and nothing else. What change was needed to make this work? Type out the commands in this question.

Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here a print screen of the output from TCP dump that captures the HTTP request from the remote host, and the reply from the web server. |
| 1. Remove the HTTP rules from the firewall and replace them with statefull rules to allow HTTP from only the South host as web client below the firewall to only the North host as web server above firewall, and nothing else. What change was needed to make this work? Type out the commands in this question.

Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here a print screen of the output from TCP dump that captures the HTTP request from the remote host, and the reply from the web server. |
| 1. Configure the firewall to behave as a proxy for HTTP from the South to the North client. What changes were needed to make this work? Type out the commands in this question.

Answer the question here.Paste here a print screen of all of the rules on your firewall, including those just implemented. Paste here a print screen of the output from TCP dump that captures the HTTP request from the South host to the firewall, and the reply from the firewall.Paste here a print screen of the output from TCPdump that captures the HTTP request from the firewall to the North host, and the reply from the North host.What type of proxy have you created?Answer the question here. |

# Lab 1 (b): Intrusion Detection

##

In this lab, students will install and configure Snort on their Linux firewall in vCloud. This software will be used to detect hostile activity occurring in the network.

The vCloud environment is accessible from within the University network or at home through your web browser. For access instructions, consult the vCloud Student Connection Instructions document, available on Canvas.

Read all instructions in this lab thoroughly and complete the lab as prescribed. Email the professor with any questions. Be sure to submit questions as early as possible to ensure time for answers so that you have the opportunity to complete and submit the lab on time.

# Preparation

## Using VMware

Some important points to know about VMware:

* To release the keyboard and mouse cursor a VMware session, press CTRL and ALT at the same time.
* The VMware image you are using can take a snapshot of the current state of the machine. There is a button labeled “snapshot” in the browser window to do this.
	+ The “revert” window will restore the snapshot, destroying any changes since then.
	+ Taking a snapshot will destroy any prior snapshots
* To perform “CTRL-ALT-DEL” in the VM, use the button, so labeled, inside of the browser window.

## Taking Screenshots

* "How to use the Snipping Tool on Windows 10" video at <https://www.youtube.com/watch?v=ayi5-7QPNcA>
* "How to Take a Screenshot on a Mac" video at <https://www.youtube.com/watch?v=h3RkDPfphSQ>

**COMMENTS**: Care should be used so that only that window is captured. Devote as much of the screen capture’s real-estate as possible to the display of the VM itself, minimizing superfluous content. **DO NOT** take a screenshot of your entire desktop.

Screenshots that are difficult to read due to sizing or other issues may be rejected and points taken off.



## Completing the Lab

To complete the lab, fill out the questions in the section below in this document, pasting in screenshots for each question. Save the updated document and upload to Canvas. Be sure to use Microsoft Word when editing and saving this document.

DO NOT change any formatting in the document. Simply type in your answers and paste in your screenshots.

**Alternate submission formats** **will not be accepted!!!**

## Lab Overview

In this lab, students will install configure Snort on their Linux firewalls. Snort is an open-source Intrusion Detection software package that can alert on hostile activity. In this lab, captures of hostile activity will be replayed. It is the students’ job to detect this activity.

To complete this lab, you will need to use the ALT Function Key combinations to change console windows in your Linux firewalls. Normally, any Linux system starts on the first console window: **NOTE: Do not use ALT-F4, it will close your browser.**



To change to another console window, hold down ALT F2. Your display should now show that you are in the second console window.


To switch back, press ALT-F1.

Each student will use the same firewall in vCloud that they had been assigned for Lab #1 and will also need to install and configure Snort. All commands in this lab should be executed as root.

## Exercises

Complete the following exercises. For each question, paste in a screenshot of the completed activity. Be sure to show all relevant details.

|  |
| --- |
| 1. Install Snort on your Firewall

sudo apt install snortWhen asked for the Interface should listen on, use ens32. This question may come up twice during the install.When asked for the Address range for the local Network, use 192.168.0.0/16. |
| 1. Verify your installation

sudo apt list –installed | grep -i snortList the contents of the /etc/snort directory. Paste in a screenshot showing the results of both here. |
| 1. View snort.conf and verify local.rules is not commented out.

Paste your screen shot here. |
| 1. Execute the following commands:

Start snort with the following command:# snort –c /etc/snort/snort.conf -l /var/log/snort -A fullSwitch to another tty and run the following command: # tail –f /var/log/snort/alertWait for a couple of minutes until you see alerts. End the tail with CTRL-C and paste screenshots of the output here. |
| 1. Paste in the screenshot each unique alert type (SID) from the last question.

Explain each element of it in detail:Answer the question here. |
| 1. What does the alert indicate? Explain the vulnerability and the attack being conducted.

Answer the question here. |
| 1. Switch back to the first tty and kill snort with CTRL-C. Re-run Snort with the following command:

snort –c /etc/snort/snort.conf -l /var/log/snort -A fullSwitch to another tty and run the following command: # tail –f /var/log/snort/alert | grep -I -B1 -A4 attackSwitch to another tty and run the following command: # ping -b 192.168.100.255 -p “7569643d3028726f6f74290a” -c3Wait for a couple minutes. Switch to the tty running t tail and issue a CTRL-C. Hint: You are looking for three “Attacks”.  |
| 1. Paste in screenshots of each unique alert (SID).

Explain each element of it in detail:Answer the question here. |
| 1. What do the alerts indicate? Explain the vulnerability and the attack being conducted.

Answer the question here. |

Four snort rules are presented for analysis. For each rule, answer the questions that follow.

Jun 9 18:38:36 ubuntusvr-t1v2 snort: [1:17322:1] SHELLCODE x86 OS agnostic fnstenv geteip dword xor decoder [Classification: Executable Code was Detected] [Priority: 1] {TCP} 192.168.202.50:60322 -> 192.168.22.252:445

|  |
| --- |
| 1. What does the alert indicate? Explain the technical details of what the signature is looking for and the ramifications of a true positive.

Answer the question here. |
| 1. Which host is the attacker and which host is the victim?

Answer the question here. |

Jun 9 18:38:36 ubuntusvr-t1v2 snort: [129:2:1] Data on SYN packet [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 192.168.199.58:63000 -> 192.168.28.100:60000

|  |
| --- |
| 1. What does the alert indicate? Explain the technical details of what the signature is looking for and the ramifications of a true positive.

Answer the question here. |
| 1. What part of the Snort architecture does this alert come from?

Answer the question here. |

Jun 9 18:39:41 ubuntusvr-t1v2 snort: [1:5897:5] SPYWARE-PUT Hacker-Tool timbuktu pro runtime detection - udp port 407 [Classification: Misc activity] [Priority: 3] {UDP} 192.168.199.58:59173 -> 192.168.22.201:407

|  |
| --- |
| 1. What does the alert indicate? Explain the technical details of what the signature is looking for and the ramifications of a true positive.

Answer the question here. |
| 1. Which host is the attacker and which host is the victim?

Answer the question here. |

Jun 9 18:39:46 ubuntusvr-t1v2 snort: [1:3815:6] SMTP eXchange POP3 mail server overflow attempt [Classification: Misc Attack] [Priority: 2] {TCP} 192.168.199.58:60327 -> 192.168.21.151:25

|  |
| --- |
| 1. What does the alert indicate? Explain the technical details of what the signature is looking for and the ramifications of a true positive.

Answer the question here. |
| 1. Which host is the attacker and which host is the victim?

Answer the question here. |