Linux Security:
Intrusion Detection

This material is based on work supported by the National Science Foundation under Grant No. 0802551

National Science Foundation
WHERE DISCOVERIES BEGIN

Lesson Overview

One of the responsibilities of a system administrator is to secure computer systems and keep malicious or unauthorized users out. Unfortunately, computer networks are frequently attacked and probed for vulnerabilities. Depending on the sophistication of the attack and the security precautions guarding the network, some attacks may or may not succeed. In either case, system administrators need to know what attempts were made to infiltrate their systems and must continually monitor computer systems for irregularities.

Administrators have several tools in their arsenal to help them detect, and in some cases, identify potential or ongoing attacks. In this lesson, you will explore intrusion and detection services that may be used to identify, report, and reduce potential attacks against your system.

Understanding this topic is important for any system administrator monitoring critical systems.

Objective

You should know what will be expected of you when you complete this lesson. These expectations are presented as objectives. Objectives are short statements of expectations that tell you what you must be able to do, perform, learn, or adjust after reviewing the lesson.

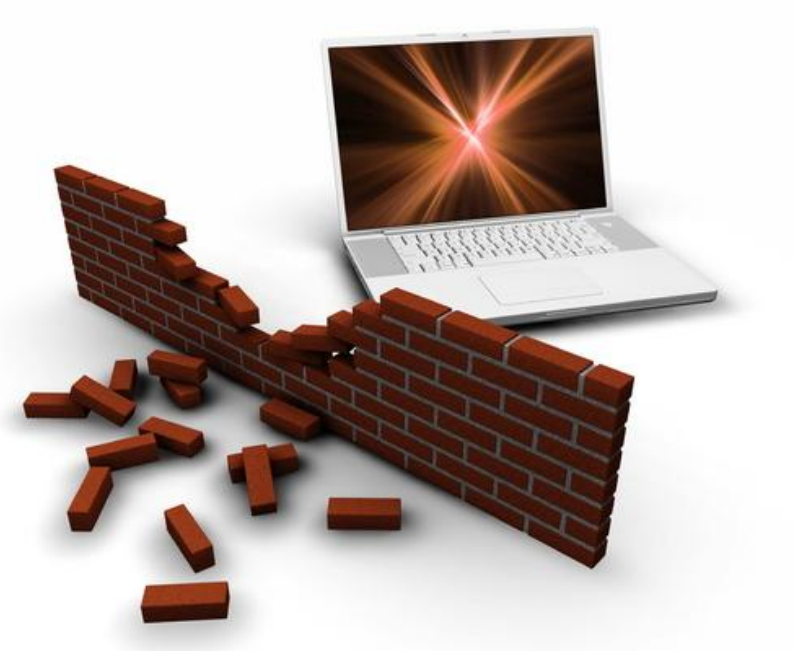
Lesson Objective:

Given the need to monitor the security of a Linux server, the student will design a working intrusion detection and intrusion prevention system using Snort.

Lesson Outline

In this lesson, you will explore:

- Basic Intrusion Prevention
- Intrusion Detection
- Snort



Resources and Notes

This lesson uses Fedora Linux for demonstration. To complete this lesson successfully, you must have access to:

- Fedora Linux on bare metal or as a virtual install
- 10 Gb of hard drive space dedicated to the operating system's use
- A command shell
- Internet for research
- Word processor

Use the resources on the right to configure your system for Fedora.

Resources:

- Download Virtualbox
- Virtualbox for Linux Hosts
- Install Fedora to Virtualbox
- Virtualbox manual
- Using Virtualbox with Ubuntu (process similar to Fedora)

Basic Security Practices

Before we discuss intrusion detection systems, let's review basic security practices.

Intrusion detection will not help if your computer system does not have basic security processes installed and working properly. You need to think of security as a process—not a single product or a group of products. If you do not have an established process for security, a single security product will not be sufficient to protect your computer infrastructure.

Basic security can be categorized into services, passwords, encryption, software updates, and system audits.

Recommended Reading

- How Firewalls Work

Deactivate Unused Services

One of the basic rules of system security is to run only the services you need. Why? Minimal software requires less overall maintenance, less updates, less logs to monitor, less ports to watch, and less opportunities for a security hole to be exposed.

As a Linux administrator, it is very tempting to load every piece of software possible hoping users will need or use them. However, each additional service or product you make available affects the overall security of your system.

Here are some options you may consider. On your test system, review */etc/services* and decide what you absolutely need. Comment out (make inactive) the unnecessary services by placing a pound (#) sign in front of each.

Consider using IPTables (the firewall utility discussed in another lesson of this course) to block all ports of the services you deactivated or made inactive. Make unused services invisible to NMAP and other port scanning utilities.

Recommended Reading

- Securing Linux System
- Secure Redhat System

Use Strong Passwords

Easy-to-guess passwords are one of the biggest problems for administrators who understand system security. Many users choose easy-to-remember passwords because they want to be able to remember them without much difficulty. Even more disturbing is that users sometimes use the same easy password on multiple systems, write passwords on sticky notes, or place them in a "memo" in their email application.

Easy-to-guess passwords are very risky and can give an intruder an easy way to access computer systems and their supporting infrastructure. Additionally, short and easy passwords are more likely to be found using scripts and other utilities hackers use. A password is like a combination lock to the system and should be difficult to guess, longer than eight characters, and not composed of dictionary words or common letter combinations. Good passwords should contain both upper and lower-case letters, contain non-alpha-numeric characters (such as &^%$#@!~*()?), and should not be linked to the user in any way (SSN, D.O.B etc). Additionally, passwords must be changed frequently (every few months or less).

Weak passwords may be short, contain only letters or numbers, upper or lower case letters, and may not contain non-alpha numeric characters. Sometimes, weak passwords are based on words in the dictionary, or linked to the user in some way like children's names, or pets' name. Weak passwords should not be allowed or used on systems with a focus on security.

Required Reading

- Password Security

Force Strong Passwords

One of the best ways to enable strong passwords is through the *pam_cracklib* module.

On a Debian or Ubuntu system, install *libpam-cracklib* using:
apt-get install libpam-cracklib

On a Fedora or Redhat system, install libpam-cracklib using:
yum install libpam-cracklib

Once you have installed *libpam-cracklib*, you will find that users are no longer able to use short passwords, or passwords based on dictionary words. These limitations add layers of security to password systems.

The configuration file is found at: **/etc/pam.d/common-password**

Required Reading
- pam_cracklib

Software Patches & Updates

Running the following commands frequently can prevent or limit the effect of an intrusion into your system:

- **apt-get update**
- **apt-get upgrade**
- **yum upgrade**

When a development team is notified of a bug, or a security problem with a software application is observed, it is standard practice to issue an update through the software management and distribution system before making an announcement of the security hole or bug. This practice prevents hackers from infiltrating systems while fixes are being coded, tested, and distributed.

By updating your systems on a frequent, or daily basis, you are taking advantage of the quick distribution of these patches rather than waiting for an announcement of upcoming changes.

Recommended Reading

- Updating Software

Regular Scans and Audits

A system scan and audit look at file sizes, names, dates, and ownership to make sure nothing has changed. A system audit also reviews users' rights and privileges, password security, SSH keys, and directory structure. What the auditor is looking for is anything out of place, not needed, or questionable.

These scans and audits can be automatic, and in many cases are handled in that way, or scans may be done manually. For example, if an employee of a large company changes positions, he or she may no longer need access to the directories to which he/she had previous access. It is up to the audit to verify that users rights and access have been changed and are appropriate.

One of the most basic rules of system security is that if a user does not need access to a computer resource, he or she should not have it. Another basic rule is that system and file changes (as in file size, file date, or location) should be reviewed to ensure the changes are authorized and the users are legitimate.

Once your system has all the security basics covered, you can safely use an Intrusion Detection System (IDS).

Recommended Reading

- Ten Linux Tools
- Linux Security Tools

Intrusion & Detection

IDS

Intrusion Detection Systems

An intrusion detection system is very much like a burglar alarm system for your computer. Intrusion and detection detects and logs the following:

- Port scans and network reconnaissance
- Hacking attempts
- Intrusion attempts
- Any other malicious activity

A good system intrusion detection system (IDS) also provides additional functions including:

- Monitoring and analyzing user and system activity
- Auditing system configuration
- Checking for system vulnerabilities
- Checking for integrity of system and data files
- Providing a statistical analysis of activity patterns and match them to known attack patterns
- Analyzing abnormal activity
- Providing an operating system audit

Recommended Reading

- Understanding IDS

Types of IDS

There are three basic types of IDSs (Intrusion Detection Systems) which are frequently wrapped together in a full intrusion detection process. These types are:

- **NIDS** – Network intrusion detection system – these are network-based tools that analyze traffic passing through the machine or on the subnet. The traffic is compared against a library of known attacks. Once an attack is identified, or if new abnormal behavior is noticed, an alert is sent to the security administrator or security team.
- **HIDS** – Host Intrusion Detection System – these are host-based intrusion detection systems that take a snap shot of your system and match it to a prior snap shot. If any critical system files are found to be modified or deleted, an alert is sent to the administrator to investigate. HIDS are recommended for mission-critical machines that are not expected to change their configuration frequently.
- **NNIDS** – Network Node Intrusion Detection System – these are tools that watch the network traffic passing through a specific host on the network. The difference between the NIDS and the NNIDS is that NNIDS watch for traffic on a specific host only and not the entire subnet.

An intrusion detection system can help provide real-time security for your machine and network.

Recommended Reading

- Intrusion Detection
- Intro to IDS
- Advanced Security

Types of IDS

Intrusion Detection Systems (IDS) can:

- Add a greater degree of integrity to the network infrastructure
- Trace user activity from point of entry to point of impact
- Recognize and report alterations to data
- Automate monitoring of the Internet for the latest attacks
- Detect when the system or network is under attack
- Detect errors in your system configuration
- Guide an administrator in establishing a policy for computing assets
- Make security management possible by non-expert staff

While IDS tools provide excellent security benefits, you should know their limitations. These will be presented next.

Recommended Reading

- Role of IDS

Limits of IDS

An IDS cannot:

- Compensate for weak identification and authentication (bad passwords)
- Conduct investigation of attacks without human intervention
- Compensate for weaknesses in established network protocols
- Compensate for problems in the quality or integrity of the information the system provides
- Analyze all the traffic on a busy network
- Always deal with problems involving packet-level attacks
- Handle some modern network hardware and features

For Review

- Intrusion & Detection

Why Deploy IDS?

There are several reasons for deploying an IDS in addition to the basic fact that doing so helps with security needs.

- If you are connected to the Internet, you will be subject to regular hacking attacks whether you realize it or not
- 80-90% of attacks against computers come from internal sources such as infected machines, disgruntled employees, or employees experimenting with new technology
- If you do not log and analyze these attacks, and if you are not made aware of them, you will not know and will not be able to respond to serious attacks until it is too late
- For industries such as health care, education, and government contractors, you may be required to install an IDS for legal and compliance reasons
- Your commitment to security will be taken more seriously if you deploy an IDS

On the next few screens, we will discuss installing an IDS on a Linux system.

For Review

- Justification for IDS

Intrusion & Detection

SNORT

What is Snort NIDS?

We are going to install Snort—an NIDS that serves as a full-featured, open-source network security application that is very mature (been around long enough for most problems to be worked out). Snort is extendable, which means it can accommodate additional modules and functionality.

Snort detects, scans, probes, and looks for attacks. It is flexible, and has a rules-based configuration that can be updated to the most recent attack patterns easily. It performs stateful, real-time traffic analysis and packet logging.

Additionally, it is easy to setup and can be deployed in as little as 30 minutes.

Snort has three modes of operation.

Resources

- Snort Documents
- Snort Manual

Snort Modes

Snort can be operated in one of three modes:

1. **Packet sniffer** - In this mode, Snort will read packets and display them on a console.
2. **Packet Logger** - In this mode, Snort will read packets and log them to the disk.
3. **Network Intrusion Detection** - In this mode, Snort will analyze network traffic, log and alert an administrator if any attacks or unusual activity is detected.

Snort can also be enhanced with some additional plugins to expand its default feature-set. Additional features include:

- Logging to mysql, postgres, oracle, and ODBC databases
- Winpopup, SNMP, and other custom alerts
- Works with tcpdump format logs for inbound and outbound traffic
- Can generate graphical reports
- Has support in Webmin for the Snort plugin
- Supports interfaces with other intrusion detection systems

For the remainder of this lesson, we will show the steps to install Snort on a Fedora test server.

Fedora is a good distro for this demonstration because it is a RedHat-based operating system commonly used as servers in the corporate environment. The same process will also work on your Ubuntu machine, though some of your commands may be slightly different.

Snort Warning!

Snort is a network packet sniffing software. Please heed the following important warnings:

If you are doing this lesson on a network other than your own, you should STOP now! If you are doing this lesson at work, or at school, or similar environment, and you install and run Snort, you risk getting in trouble or getting fired for network and computer use violations.

ONLY complete this lesson by following the examples on your own personal network, or one that is NOT tied to your income or education, and to which you have express permission to use for this purpose. Network traffic sniffers and packet sniffers are not looked upon kindly by network administrators on any production network. So tread carefully. Now, let's move forward with our installation.

As you go through the following slides you will notice some slides refer to Fedora and some to Ubuntu. The second slide of each step provides directions for Ubuntu. If there is only one slide shown, the steps are the same for both Fedora and Ubuntu.

Step 1 – Update System (Fedora)

The first step in any software installation is to update the system to the latest version of software and patches.

On your Fedora machine, follow these directions:

1. Type: **su**
2. Enter your root password when requested
3. Type: **yum update**
4. When asked to accept updates type: **y**
5. Type: **yum install pam_passwdqc**
6. Accept any dependencies if asked

At this point, your machine is updated to the latest versions of software, and all security patches have been installed. Use PAM's password quality control to secure all your passwords.

Select **PLAY** below for a video on updating your system.

View Video VideoLesson9UpdateSystem(C5L9S22).mp4

Required Reading

- Pam_passwdqc ManPage

Step 1 – Update System (Ubuntu)

The first step in any software install is to update the system to the latest version of software and patches.

On your Ubuntu machine, follow these directions:

1. Type: **sudo apt-get update**
2. Enter your root password when requested
3. Type: **sudo apt-get upgrade**
4. When asked to accept updates type: **y**
5. Type: **sudo apt-get install libpam_passwdqc**
6. Accept any dependencies if asked

At this point, your machine is updated to the latest versions of software, and all security patches have been installed. Use PAM's password quality control to secure all your passwords.

Suggested Review

- Snort & Ubuntu
- Snort Installation

Step 2– Install Prerequisites (Fedora)

Normally, we would want to install the Snort software packages through package manager. However, in this case, the rules and configurations are not distributed with the package manager and the ones you need to download from the Snort web site do not match the version of software in the package manager. So, we are going to build Snort from source.

The first thing we need to do is install the build-prerequisites. These are the libraries, packages, and utilities that are needed to build the Snort packages. We are also going to add your user ID to the wheel group, so we can use *sudo* properly for some commands. To install these packages:

1. Open a terminal window and log into root.
2. Type: **yum install libnet-devel bison pcre-devel libpcap-devel libdnet-devel gcc flex pcre wget mysql-devel**
3. When asked, accept all dependencies
4. Type: **groupmems –a [your user id] –g wheel**
5. Type: **visudo**
6. Scroll down to find the commented line that begins with *%wheel* and uncomment by removing the # (pound) sign in front of it. Do not uncomment the line that includes *NOPASSWORD*. Choose the other one.
7. Save and exit vi.
8. Reboot your system.

Select **PLAY** below for a video on installing prerequisites.

View Video VideoLesson9InstallDepend(C5L9S24).mp4

Step 2– Install Prerequisites (Ubuntu)

To install prerequisites for Ubuntu, follow these directions:

1. Open a terminal window.
2. Type: **sudo apt-get install libnet-dev bison libpcre3-dev libpcap-dev libdnet-dev gcc flex wget libmysqld-dev**
3. When asked, accept all dependencies.

Suggested Review

- Snort & Ubuntu
- Snort Installation

Step 3– Create Users & Directories

Despite setting up this package as root, we do not want to execute Snort as the root user. We also need to create some required directories. We will do both these steps at this time. From your terminal, follow these directions (as a root user):

1. Type: **sudo groupadd snort**
2. Type: **sudo useradd –g snort snort –s /sbin/nologin**
3. Type: **sudo mkdir /usr/local/lib/snort-dynamicrules**
4. Type: **sudo mkdir /etc/snort**
5. Type: **sudo mkdir /etc/snort/rules**
6. Type: **sudo mkdir /etc/snort/preproc_rules**
7. Type: **sudo mkdir /var/log/snort**
8. Type: **sudo mkdir /etc/snort/so_rules**
9. Type: **cd**

We have now created all the required users and have returned to our non-privileged user account (your default login) to continue compiling and installing the software packages.

Select **PLAY** below for a video on installing prerequisites.

View Video VideoLesson9MakeDirs (C5L9S26).mp4

Step 4– Retrieve and Install Snort (Fedora)

In this step, we are going to download and install the most recent Snort source packages. It is important that we retrieve the Snort source code from the authors' web site as we need to have the most recent code. Please follow these directions:

1. Open FireFox
2. Go to: http://www.snort.org
3. You must first create a userID and login on the Snort website to Download Snort.
4. Click on **Download Snort**
5. Download: *snort-2.9.05.tar.gz*
6. Click on **Save file** if prompted. Do not open with archive utility.
7. Download: *daq-0.5.tar.gz*
8. Click on **Save file** if prompted. Do not open with archive utility.
9. Click on **Download Rules**
10. Scroll down to find the **Registered User Rules**
11. Download *snortrules-snapshot-2905.tar.gz*
12. Click on **Save file** if prompted. Do not open with archive utility.
13. Open a terminal window, but do not log in as root.

Continued on next slide . . .

Select **PLAY** below for a video on installing Snort from source code.

View Video VideoLesson9InstallSource(C5L9S27).mp4

Step 4– Retrieve and Install Snort (Contd)

Directions continued from previous . . .

14. Type: **cd**
15. Type: **mkdir code**
16. Type: **cd code**
17. Type: **tar xvzf ~/Downloads/snort-2.9.0.5.tar.gz**
18. Type: **tar xvzf ~/Downloads/daq-0.5.tar.gz**
19. Type: **mkdir rulespackage**
20. Type: **cd rulespackage**
21. Type: **tar xvzf ~/Downloads/snortrules-snapshot-2905.tar.gz**

We have now downloaded the source code for *daq* and *snort*. We have also downloaded the rules for the 2.9.0.5 version of Snort.

We then created our build directories under our user account/code. Next we unarchived our two build files into the code directory. We are now ready to build and configure daq.

Required Reading

- Snort on Fedora

Step 4– Retrieve & Install Snort (Ubuntu)

From the terminal window of your Ubuntu server, follow these instructions to install Snort:

1. Type: **sudo apt-get install snort-mysql snort-rules-default**
2. Accept any dependencies when asked.
3. Follow any directions that are given to you during the automatic configuration.

Once you have completed these steps, jump ahead to **Step 7: Snort Configuration file** (C5L9S33) to continue your installation.

Required Reading

- Snort setup guides

Step 5– Configure and Install Daq

The first step of our build process is to configure, build, and install daq. Daq is the Data Acquisition Library for Snort.

Follow these directions from your terminal session:

1. Type: **cd ~/code/daq-0.5**
2. Type: **./configure**
3. Type: **make**
4. Type: **sudo make install**

Once this process completes without errors, we are ready to configure and install Snort.

Select **PLAY** below for a video on building Daq for Snort.

View Video VideoLesson9BuildDaq Snort(C5L9S30).mp4

Required Reading

- Snort Essentials

Step 5– Configure and Install Libdnet (Ubuntu)

If you are on Ubuntu, you must download and install libdnet because the version in the Ubuntu package is broken.

1. Open Firefox and go to: http://code.google.com/p/libdnet/downloads/list
2. Download the *libdnet-1.12.tgz* file and save to your Downloads packages.
3. Type: **cd ~/code/**
4. Type: **tar xvzf libdnet-1.12.tgz**
5. Type: **cd ~/code/libdnet-1.12**
6. Type: **./configure**
7. Type: **make**
8. Type: **sudo make install**

Once this process completes without errors, we are ready to configure and install daq.

Required Reading

- Snort setup guides

Step 6– Configure & Install Snort (Fedora)

To configure, build, and install the Snort application, follow these directions:

1. Type: **cd ~/code/snort-2.9.05**
2. Type: **./configure --with-mysql --enable-dynamicplugin**
3. Type: **make**
4. Type: **sudo make install**
5. Type: **cd etc**
6. Type: **sudo cp * /etc/snort/**
7. Type: **sudo vi /etc/snort/snort.conf**
8. Find all lines with **ipvar** and change to **var**
9. Find all instances of **compress_depth** and delete them (around line 212 in the file).
10. Type: **cd ~/code/rulespackage**

Continued on next slide . . .

Select **PLAY** below for a video on Snort.

View Video
VideoLesson9
Missing File
.mp4

Step 6– Configure & Install Snort (Fedora)

Continued from previous . . .

11. Type: **cd rules**
12. Type: **sudo cp * /etc/snort/rules/**
13. Type: **cd ../so_rules**
14. Type: **sudo cp -a * /etc/snort/so_rules/**
15. Type: **cd ../preproc_rules**
16. Type: **sudo cp –a * /etc/snort/proproc_rules/**
17. Type: **cd /etc/init.d**
18. Type: **sudo wget** http://internetsecurityguru.com/snortinit/snort
19. Type: **chmod 755 snort**
20. Type: **chkconfig snort on**
21. Type: **sudo mkdir /usr/local/lib/snort_dynamicrules**

NOTE: If for some reason the snort startup file from Internet security does not work on your system, you can use the one linked from this lesson.

Next, we need to fix a few things in the snort configuration file.

Resource

- Snort setup guides

Step 7– Update Snort Configuration File

The Snort configuration file needs some corrections to account for the differences between builds and versions of Snort. Follow these directions from your terminal window:

1. Type: **sudo vi /etc/snort/snort.conf**
2. Search for the line with *HOME_NET* and change the *All* to ***192.168.2.0/24***
3. Search for the line with *EXTERNAL_NET* and change the All to ***!$HOME_NET***
4. Search for the line with *RULE_PATH* and change *../rules*" to ***/etc/snort/rules***
5. Search for the line with SO_RULE_PATH and change to **/etc/snort/so_rules**
6. Search for the line with PREPROC_RULE_PATH and change to **/etc/snort/preproc_rules**
7. Your Snort configuration file is complete. Now we are going to setup our MySQL environment for Snort.

If you have configuration problems or wish to look at a sample *snort.conf* configuration file, use the one linked to this lesson.

Select **PLAY** below for a video on configuring Snort and MySQL.

View Video VideoLesson9ConfigSnort MySQL(C5L9S34).mp4

Suggested Reading

- Snort.conf file

Step 8– MySQL for Snort

We compiled this version of Snort to use the MySQL database for part of the storage and reporting operations. In this step, we are going to configure this MySQL environment. Before you begin this process on your own machine, make sure you have an operational MySQL server and can access it using a root password that you know. Once you have met those requirements, follow these directions:

1. Type: **mysql –u root –p**
2. Enter your root MySQL user password when prompted
3. Type: **create database snort;**
4. Type: **grant INSERT,SELECT on root.* to snort@localhost;**
5. Type: **set password for snort@localhost=PASSWORD('yourpassword');**
6. Substitute a password of your choice for [**yourpassword**]
7. Type: **grant CREATE,INSERT,DELETE,UPDATE on snort.* to snort@localhost;**
8. Type: **grant CREATE,INSERT,DELETE,UPDATE on snort.* to snort;**
9. Type: **exit**
10. Type: **cd ~/code/snort-2.9.0.5**
11. Type: **mysql –u root –p < schemas/create_mysql snort**

You have now created your MySQL environment for Snort. Next, we need to install Barnyard to communicate with Snort and MySQL.

Suggested Reading

- Adding User Accounts

Step 9 – Download and Install Barnyard

Barnyard is a program that decouples the output overhead from the Snort network intrusion detection system and allows Snort to run at full speed. In our install, we are going to install Barnyard from the source code. Follow these directions to install Barnyard:

1. Go to http://www.sourceforge.net/projects/barnyard
2. Download the *barnyard-0.2.0.tar.gz* file and save to your *Downloads* directory.
3. Open up your terminal session.
4. Type: **cd ~/code**
5. Type: **tar xvzf ~/Downloads/barnyard-0.2.0.tar.gz**
6. Type: **cd barnyard-0.2.0**
7. Type: **./configure --enable-mysql**
8. Type: **make**
9. Type: **sudo make install**
10. Type: cd **etc/**
11. Type: **sudo cp barnyard.conf /etc/snort**
12. Type: **cd /etc/snort**
13. Type: **sudo vi /etc/snort/barnyard.conf**

Continued on next slide . . .

Select **PLAY** below for a video on configuring Barnyard.

View Video VideoLesson9Barnyard(C5L9S36).mp4

Required Reading

- Snort Requirements

Step 9 – Download and Install Barnyard

Continued from previous . . .

14. Find the **config interface** line
15. Change the "fxp0" to **eth0** or **eth1** depending on your network interface.
16. Locate the line for "*output alert_acid*" and the "*output log_acid*" and uncomment the lines.
17. Add the password keyword to the end of the line using the Password keyword. The format is right above it in the file.
18. Save and exit vi.
19. Type: **sudo /usr/local/bin/snort –c /etc/snort/snort.conf**
20. Because of various distribution issues, you will need to adjust the snort.conf file to resolve any errors. Most often, you will just have to remove the keywords. Once everything is running properly, let it run for a few minutes and then press **CTL-C** to return to the Bash prompt.
21. Type: **cd /etc/init.d/**
22. Type: **sudo wget http://www.internetsecurityguru.com/barnyard**
23. Type: **sudo chmod 755 barnyard**
24. Type: **sudo chkconfig barnyard on**
25. Type: **sudo service barnyard start**
26. Type: **sudo /etc/init.d/barnyard start**

Resources

- Barnyard startup script
- barnyard.conf

Start Snort

Once our configuration is complete we can now start Snort and begin monitoring. From your terminal program:

1. Type: **sudo service snort start**
2. Enter your password when requested.
3. Type: **ps ax | grep snort**
4. Verify that the snort service is running.
5. Type: **cd /var/log/snort**
6. Type: **ls –l**
7. Look at the number that follows the *snort.log* file.
8. Type: **sudo touch /var/log/snort/barnyard.waldo**
9. Type: **sudo vi /var/log/snort/barnyard.wald**
10. Enter the insert mode by typing **I**
11. Type: **/var/log/snort snort.log** [number from step 7 without brackets]
12. Exit insert mode by pressing **ESC**
13. Save and exit vi
14. Type: **sudo /etc/init.d/barnyard restart**

Snort is now up and running, and we can begin to monitor our network.

Resources

- Snort Setup Guides

Snort Alerts

The primary purpose of Snort is to provide alerts for irregular network activity or actions that violate established security rules.

One of the primary methods of locating these alerts is to look in the */var/log/snort/alert*. You can access this log.

From your terminal window, type:

more /var/log/snort/alert

Scroll through the log to find alerts.

You will want to add this log file to logrotate and maintain prior copies based on your security protocol. I would recommend maintaining 52 weeks of logs.

Snort is now up and running and monitoring your traffic.

Required Reading

- Evaluating Snort Alerts
- Snort on Ubuntu

Lesson Summary

In this lesson, we discussed the various types of intrusion detections systems. We also discussed port monitoring and downloaded, compiled, and installed Snort and its dependent programs.

We also learned that intrusion detection and prevention is not just a piece of software, it is a system. This system includes software, hardware, policy, people, and procedures.

Recommended Reading

- Snort Troubleshooting
- Snort on Debian

Additional Resources

- Snort on Fedora
- Snort Manual
- Understanding IDS