Linux Security:
File Integrity

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 most basic responsibilities of a network administrator or computer technician is preventing information and data corruption or loss. All the physical resources in a computer (hard drive, NIC cards, memory, and power supply) can be replaced if something goes wrong. However, the stored on our computers is priceless and cannot be easily duplicated or replaced if corrupted or destroyed.

In this lesson, students will explore some of the common tools used to detect possible intrusions to a computer system and other malicious methods that can be fatal to our system data. Students will research and discuss common intrusion methods and how they can be detected or prevented.

Understanding this topic is critical to anyone who cares about keeping safe the data for which he or she is responsible. Malicious intrusions to data systems are frequent and sophisticated and threaten the reliability and integrity of stored data.

Select **PLAY** below for a video on the lesson overview:

View Video VideoLesson5Intro(C5L5S2V1).mp4

View Video VideoLesson5Warning(C5L5S2V2).mp4

Warning!

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.

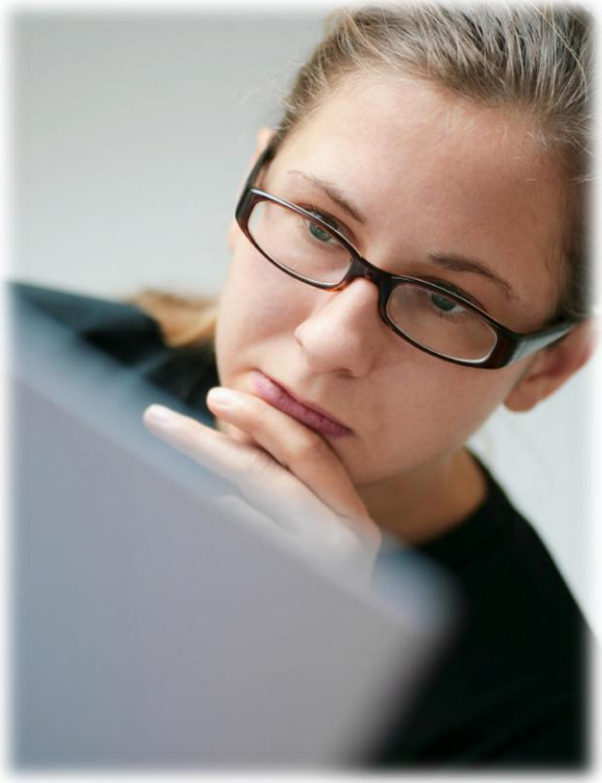
Lesson Objective:

Given a requirement to ensure file integrity, the student will be able to formulate a plan to verify file integrity and configure the use of file integrity checker such as Tripwire or AIDE to investigate tampering on a Linux server.

Lesson Outline

In this lesson, you will explore:

- Important terms
- Intrusion Detection Systems
- Configuring IDS
- Tripwire
- AIDE
- Rootkits
- Chkrootkit
- Rootkit Hunter
- Additional Tools
- Summary



Resources and Notes

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

- Ubuntu 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 Ubuntu.

Resources:

- Download Virtualbox
- Using Virtualbox with Ubuntu
- Virtualbox for Linux Hosts
- Virtualbox manual

Glossary of Terms

- **Tripwire** - An intrusion detection system (IDS) that keeps critical system files and reports under control in the event they are compromised
- **AIDE** - (Advanced Intrusion Detection Environment) is a tool used to check the integrity of a file
- **Chkrootkit** - A tool used to check local systems for signs of a rootkit
- **Metasploit** - Popular open-source tool used for penetration testing
- **Rootkit Hunter** – An open-source tool used to check for rootkits, Trojan horses, backdoors, and exploits
- **Virus** - Malicious code that can duplicate itself and infect computer files
- **Trojan Horse** - Malicious code that hides itself within another application to prevent detection
- **Worm** - Malicious code able to self-replicate and transfer itself over networks
- **File integrity** - The condition of a computer file that indicates a file has not been modified or changed by any means
- **White Hat Hacker** - Penetration testers and system admins who do security testing for the good of computer science
- **Black Hat Hackers** - Crackers and hackers that attempt to gain access to resources through a variety of means without having permission to do so

Required Review:

- Tripwire
- AIDE
- Chkrootkit
- Rootkit Hunter

Maintaining Security with IDS

One of the primary goals of a network administrator is to keep computer systems, networks, and data safe. This goal becomes more difficult as technology improves. As information is exchanged between hackers, and automated tools for hacking are improved, system administrators find it more difficult to protect their systems. Fortunately for administrators, they too have access to a few good tools to protect their systems.

One of the tools available for system administrators is the Intrusion Detection System (IDS). IDS is an application that runs on a computer and monitors network activity. It is configured to recognize changes in normal system traffic and computer behavior. Once IDS detects an anomaly, it will log the incident and notify the administrative team through email or pager.

One of the downsides of IDS is that it sometimes identifies legitimate traffic as potential hostile code. This mislabeling is called a "false positive" and can tie up system resources and administrators. Administrators may spend valuable time looking for "false positives" while ignoring other important tasks.

Required Reading

- Reducing False Positives
- What is false positive?

Installing & Configuring IDS

Most IDS applications are easy to install. The real skill set is configuring the IDS and setting it up to detect threats while ignoring legitimate traffic and processes.

The five steps to setting up an IDS are:

1. Install the IDS (normally the best time to install an IDS is when you first install the operating system).
2. Add other applications one at a time. Test and configure the IDS after bringing each application online.
3. Create network traffic baseline and configure the IDS once your required applications and services are completely installed and configured.
4. Test the IDS on a regular basis and adjust accordingly to prevent "false positives."
5. Check logs and traffic patterns on a regular basis (daily preferred).

Required Reading

- Checklist for IDS
- Snort on Ubuntu

IDS Apps

Tripwire

Tripwire is a popular IDS application that monitors your file system and alerts the administrator to changes in files. Once initiated, Tripwire scans your file system and creates checksums on each and every file. As time passes, Tripwire continues to check previously scanned files and alerts the administrator if the checksum for a file has changed.

Tripwire is best installed on a fresh Linux installation. You will be asked for two passphrases on the initial configuration. The first one (site passphrase) is used to encrypt and sign the Tripwire system files. The second one (local passphrase) is necessary to launch the Tripwire binaries. Once installed, Tripwire will need to be configured regarding what files and folders to monitor and how to contact the system administrator.

Due to the complexity of the configuration process, students are encouraged to visit the following sites for additional information:

Required Reading

- Using Tripwire
- Tripwire Tutorial
- Tripwire on Linux
- Starting with Tripwire

AIDE

AIDE (Advanced Intrusion Detection Environment) can be used to help track file integrity by comparing a 'snapshot' of the system's files prior to and after a suspected incident.

AIDE uses several message digest algorithms (md5,sha1,rmd160,tiger,haval,etc.) to verify files and additional algorithms can be added with little complications.

AIDE is installed and configured in a similar manner to Tripwire. AIDE should be added to a newly installed Linux platform, and rules will be created based on the services and applications your particular platform requires.

Select **PLAY** below for videos on AIDE:

View Video VideoLesson5AIDEInstall(C5L5S11V1).mp4

Installation

View Video VideoLesson5AIDEConfiguration(C5L5S11V2).mp4

Configuration

Required Reading

- Securing with AIDE
- AIDE File Integrity
- Detection with AIDE

AIDE Contd.

Select **PLAY** below for videos on AIDE:

View Video VideoLesson5Iitialize AIDE(C5L5S12V1).mp4

Initialize AIDE

View Video VideoLesson5FinalizeAIDE(C5L5S12V2).mp4

Finalize AIDE

Rootkits

Rootkits are malicious code hidden deep within the system files that allow privileged access to hackers. Rootkits should be considered extremely dangerous and once installed, are difficult to locate because they are often embedded at the Kernel level.

Rootkits are used by hackers to get access to working systems. After installing the rootkit, the hackers will use them to install additional hostile code such as Trojans, Backdoors, and Bots.

Hackers have goals much like those of the system administrator. One of the ultimate goals of the hacker is to gain root privileges on unprotected systems. A "rooted" system can be used for many things including sending SPAM and initiating DDOS attacks for financial gain.

Fortunately for administrators, there are tools that can help detect rootkits.

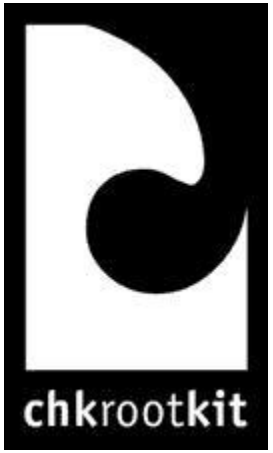
Recommended Reading

- Rootkits
- Rootkit Description
- What is a rootkit?
- Rootkit use

Chkrootkit

Chkrootkit is an open source application that looks for rootkits. Not only does Chkrootkit look for specific files known to be hostile (searches for over 60 known rootkits) but Chkrootkit looks for behaviors that are recognized as hostile as well.

Chkrootkit will detect sniffers and changes in network applications and activities. Its features include detecting binary modification, utmp/wtmp/lastlog modifications, promiscuous interfaces, and malicious kernel modules.



Select **PLAY** below for videos on Chkrootkit:

View Video VideoLesson5Chkrootkit(C5L5S14V1).mp4

View Video VideoLesson5RunChkrootkit(C5L5S14V2).mp4

Run Chkrootkit

Recommended Reading

- Chkrootkit
- Chkrootkit FAQ

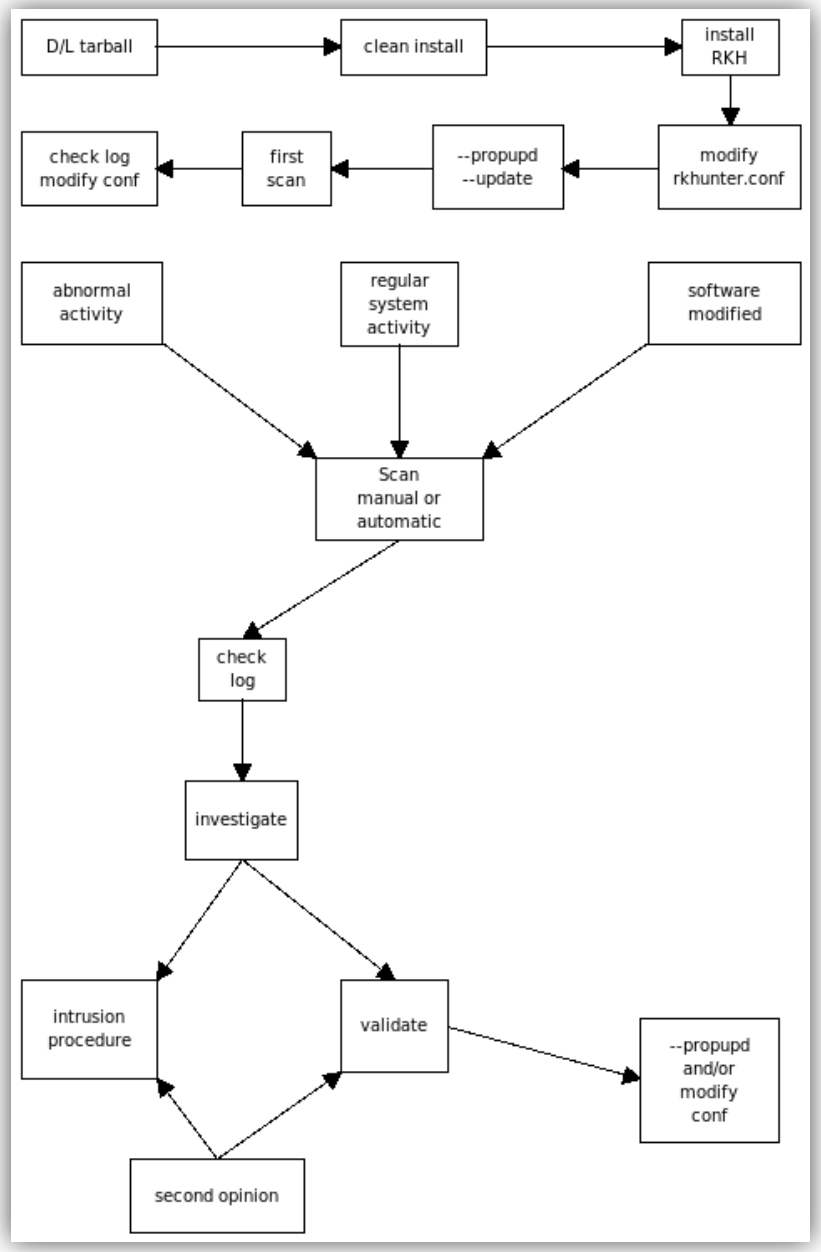
Root Kit Hunter (RKHunter)

"RKHunter is scanning tool that checks for signs of various pieces of nasty software on your system like rootkits, backdoors and local exploits. It runs many tests, including MD5 hash comparisons, default filenames used by rootkits, wrong file permissions for binaries, and suspicious strings in LKM and KLD modules."

Source: http://sectools.org/rootkit-detectors.html

Recommended Reading

- Tutorial RKHunter
- RKHunter Site
- RKHunter FAQ



Flowchart of RKHunter process.

Source:
http://sourceforge.net/apps/trac/rkhunter/wiki/SPRKH

Additional Tools

One of the best security tools websites is located at http://sectools.org/index.html and consists of tools for both network administrators and hackers alike. As a system administrator, you will become familiar with both the tools that hackers use and how to circumvent potential attacks. Good administrators will probably spend a minimum of five hours a week just reviewing new technologies and tools used by hackers and script kiddies.

Popular Hacking tools include:

Metasploit - The Metasploit Framework is the de-facto standard for penetration testing with more than one million unique downloads per year and the world's largest, public database of quality assured exploits. (From the website: www.metasploit.org)

Wireshark – Open source protocol analyzer that can be used to actively monitor network services. www.wireshark.org

NMAP – Popular port scanning tool used by hackers for reconnaissance or system administrators to identify open ports and services. www.nmap.org

Select **PLAY** below for videos on IDS tools.

View Video VideoLesson5Wireshark (C5L5S17V1).mp4

Wireshark

View Video VideoLesson5NMAP(C5L5S17V2).mp4

Nmap

Additional Tools (Contd.)

Popular hacking tools include:

Angry IP Scanner – Popular tool used to test for open ports on a target system http://www.angryip.org/w/Home

Nessus – Excellent and top rated vulnerability assessment tool used by hackers and system administrators alike http://www.nessus.org/products/nessus

Snort – Recognized as one of the most popular Intrusion Detection Systems. Snort is able to assess a variety of malicious attacks and behaviors. Snort offers both an open source application as well as a commercial version for enterprise applications. http://www.snort.org/

Netcat – Also referred to as the Network Swiss Army Knife. Netcat provides a variety of back-end services for network administrators. One of Netcat's distinguishing marks is the ability to use it with custom scripts for specific requirements. Netcat is easily integrated with other tools and applications or through the use of numerous scripting options.

Backtrack – Popular Live CD Linux toolbox used for penetration testing. http://www.backtrack-linux.org/

Hardening Tips Website - http://www.cyberciti.biz/tips/linux-security.html

Lesson Summary

In today's ever changing computer industry, applications for both hackers and administrators are constantly changing. Good administrators will need to know what is being used by attackers and how to protect their data and file systems at the same time.

Administrators in the real world will need to be proactive and know how to find and use the tools that their enemies will use so that they can create the necessary defense to protect their data.

In this lesson, you were introduced to intrusion detection systems (IDS), rootkit tools, and other popular attack mechanisms. In the assessments, you will discuss various attack methods and countermeasures used to protect system resources and data. Additionally, you will install and configure Tripwire to detect attacks.

Select **PLAY** below for a summary video on IDS.

View Video VideoLesson5Summary(C5L5S19).mp4