Week #14 – IDS

Overview of the week's objectives

Week #14 will conclude the topic of Intrusion Detection System (IDS) with Modules O3L10 and O5L10.

Linux Computer systems are very reliable and dependable once they are properly configured and regularly maintained. However, network and data systems must be monitored regularly to ensure they are working at peak performance and to address any potential data bottlenecks, data corruption, or system difficulties before small problems lead to system failure or data loss.

In this lesson, you will explore and evaluate various software tools and utilities that administrators use to monitor computer systems. You will also demonstrate use of one tool to perform required monitoring.

It is important that you understand this lesson because the knowledge you will gain will help you become a better administrator equipped with the required tools to monitor critical network systems, improve your company's data throughput, reduce the risk of data loss or reduced performance, and ultimately, keep your clients' data systems healthy and at peak performance.

This lesson is designed to introduce you to general security risks faced by network administrators. In addition to information on protecting public-facing services and exploring techniques to protect valued applications, this lesson also includes additional day-to-day security tips to keep your systems secure.

Moreover, this lesson will explore additional security concepts that have not been covered elsewhere in the Linux curriculum. In our experience, these additional security concerns are often discussed in job interviews. Therefore, you will be well advised to understand and review this material regularly to maintain a competitive advantage within the IT industry.

Please refer to all "PREVIOUS WEEK's OVERVIEWS" for details / advice relating to, or concerning, each of the tasks detailed in the remainder of this overview. You are responsible for recommendations or instructions noted in them!

TODO List

Please refer to all previous "Week's Overview PDFs" for details / advice about each of the tasks detailed in the remainder of this overview. While we focus on instructions specific to this week's material herein, previous instructions still apply.

Learning Activity			**Time in hours**		**Points**
			Expected	**Spent**	
Reading Assignments	O3L10 O5L10	Online Module Guides &Videos	2		
Practice Assignments	O3L10-PQ O5L10-PQ	Taking Practice Quizzes	2		
		Working on PAs & Participating to PA forums	7		
Graded Assignments	W14-GQ	Taking Graded Quiz	1		2
		Participating to Discussion forums			1
			12		**3**

Task #1 – Reading Assignments

You will find one "online module guide" document in this week's folder per module.

Refer to all previous "Week's Overview PDFs" for detailed instructions on how to use online module guides, practice quizzes and our support forum while working on this task.

Task #2 – Practice Assignments

Refer to "ALL PREVIOUS WEEK's Overview PDF" files for detailed instructions applying to all Practice Assignments.

These activities were designed to help you think critically about the topics covered in this lesson and to assess whether your knowledge and application of the content meets the stated objectives. You will need to research each topic and complete the assignment as instructed. Do not rely only on the contents of this lesson or on Wikipedia to complete these assignments.

PA #1 : Assignment – Evaluate System Monitoring Tools (C3L10A1)

Use the Internet to research Nagios, Zenoss, Gnome System Monitor, and one additional system monitoring tool of your choice in order to identify key features of each. Compare and contrast the four and list any features unique to each. Make sure to explain what advantage those features may provide. Features may include ability to monitor a specific function or whether a tool is scalable enough to handle a large enterprise system.

Choose which of the three you would use to monitor a UNIX/Linux system. Explain what factors led you to your choice.

PA #2 : Lab – chrooted DNS Server (C5L10A3)

Download required components and updates for your Ubuntu installation.Make sure you are running Ubuntu 11.04 for this lab. It is a very flavor dependent activity!

To install Chroot:
Enter the following commands from the terminal: **sudo apt-get install dchroot**
sudo apt-get install debootstrap

You will find the following video helpful for this activity: Using Apt Get to install Chroot

Submit a screen shot showing your Chroot install and submit to your instructor via the dropbox.

PA #3 : Lab – Setup chrooted Directory (C5L10A4)

Setup a chrooted directory. Make a directory with URNAMEJAIL in root. Enter the commands below: **sudo mkdir TSTARRJAIL cd TSTARRJAIL sudo mkdir JAIL pwd**

Review the following video to help with this activity: Directory Setup
Submit a screenshot showing the created directory. Upload to your instructor using the dropbox.

PA #4 : Lab – Modify Config File (C5L10A5)

Modify the current configuration file **/etc/schroot/schroot.conf**
Enter the following commands [**in bold**]:

cd /etc
cd schroot
clear
ls
gedit schroot.conf

Add these lines:
[maverick]
description=Ubuntu Maverick Meerkat
location=/TSTARRJAIL/JAIL
priority=3
users=tstarr
groups=sbuild
root-groups=root

Save your configuration and return to root cd /
Review the following video for help on this activity:Edit configuration
Submit a copy of your configuration file to your instructor.

PA #5 : Lab – debootstrap Command (C5L10A6)

Using the debootstrap command

Enter the command in bold below on a command line:
sudo debootstrap -variant=buildd --arch i386 maverick /TSTARRJAIL/JAIL
http://www.gtlib.gatech.edu/pub/ubuntu

View the video below for help on the command above:
Debootstrap
sudo mount –o bind /proc /TSTARRJAIL/JAIL/proc

View the video below for help on the command above:
Video final
Submit a screenshot of your progress to your instructor.

PA #6 : Lab – Setup DNS (C5L10A7)

Setup the DNS! Enter the following commands in [bold]

#cat /etc/resolve.conf
#sudo cp /etc/resolve.conf /tstarr/jail/etc/resolve.conf
#sudo chroot
Note: Install any apps like it were a separate VM
#apt-get install nano
#apt-get install gedit
#Export DISPLAY=:0.0
#apt-get install firefox
#firefox

You are now running Firefox within the chrooted jail using your chroot DNS!
Submit a screenshot showing Firefox with the chrooted jail using your chroot DNS.
.

Task #3 – Use the “Support forum

Refer to all previous “Week’s Overview PDFs” for detailed instructions applying to all discussion forums assignments.

PA #7 : Forum – System Logs (C5L10F3)

System logs are an important tool for security managers. What logs are the most important for your review in a Linux environment and how often should they be reviewed?

Post your responses to the forum and respond to at least two of your classmates' comments.

PA #8 : Services on public facing servers (C5L10F4)

Your group notices that XYZ hosting only provides web hosting, email hosting, and DNS services to the public.

What are the minimum services that XYZ Inc should run in a Linux environment on their public-facing servers?

Add your responses to the forum and comments on two posts from your colleagues.

Task #4 – Graded quizzes

Refer to all previous “Week’s Overview PDFs” and “ALL PREVIOUS WEEK’s Overview PDF” for detailed instructions applying to all graded quizzes.