Week #12 – IDS

Overview of the week's objectives

Week #12 will introduce the topic of Intrusion Detection System (IDS), Module O5L5.

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.

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	O5L5	Online Module Guides &Videos	2		
Practice Assignments	O5L5-PQ	Taking Practice Quizzes	1		
		Working on PAs & Participating to PA forums	8		
Graded Assignments	W12-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 – Research Penetration Tools (C5L5A1)

Your group has been contracted to research penetration testing and create a 15 slide PowerPoint presentation outlining various open source penetration tools.

Research and identify 3-5 penetration tools and their popularity.

Include links to tutorials and FAQ pages as well as any other additional information.

Create a two page memo outlining your findings and submit it with your slides to your instructor.

PA #2 : Assignment – Page Essay on Attackers and Administrators (C5L5A2)

Divide your group into two groups—Attackers and Administrators.

Both groups should research tools available on the Internet and how they can be used within their "role". Attackers will seek information on various attack tools and discuss how they could be implemented in a real world environment. The administrators should research popular defensive tools and strategies and how they might be used against the attacker's tools.

Write and submit a one page memo to your instructor on your findings.

PA #3 : Lab – Install AIDE (C5L5A3)

Use a package manager to install AIDE.

As root in terminal: # **aideinit**

This will take some time as the application goes out and checks popular system files and runs the message digests on them to get a baseline.

Send a snap shot to your instructor showing your summary of the AIDEinit process.

PA#4 : Lab – Install chkrootkkit (C5L5A4)

Installation:
Open up the terminal and type the following command to install chkrootkit:
$ sudo apt-get install chkrootkit

Using chkrootkit:
Open up the terminal and type the command: **$ sudo chkrootkit**
This will perform all tests.

Send a snapshot to your instructor showing the final output of the chkrootkit process.

Other Configurations:
If you want an automatic daily run of chkrootkit:
Open /etc/chkrootkit.conf and Replace **RUN_DAILY="false"** with **RUN_DAILY="true"**

If you also want a daily mailed report :
Open /etc/cron.daily/chkrootkit and replace **'$CHKROOTKIT $RUN_DAILY_OPTS'** with
'$CHKROOTKIT $RUN_DAILY_OPTS | mail -s '"\"Daily chkrootkit run from $HOSTNAME \"$YOUR_EMAIL_ADDRESS"'.

.

Task #3 – Use the “Support forum

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

PA #5 : Forum – Attackers and Administrators (C5L5F1)

Divide your group in to two groups—Attacker and Administrators. Both groups should research tools available on the Internet and how they can be used within their "role".

Attackers will seek information on various attack tools and discuss how they could be implemented in a real world environment.

The administrators should research popular defensive tools and strategies and how they might be used against the attacker's tools.

Each group should use the forum to debrief the other group about their findings.

Write and submit a one page memo to your instructor on your findings and upload for Assignment 2 (C5L5A2).

PA #6 : Forum – Benefits of Penetration Tools (C5L5F2)

Briefly review and research penetration tools such as Backtrack, Nessus, NMAP and Netcat.

Discuss the pros and cons of easily available tools used by hackers and administrators.

As a group, decide if these tools are good or bad for the computer industry. Debate your decision with your instructor or other groups.

PA #7 : Forum – Analysis of Training Sites (C5L5F3)

You are on a job interview at XYZ, Inc and the CIO (Chief Information Officer) asks you if you think websites such as Youtube help system administrators more or help hackers more.

What would your response be?

How would you respond if he asked you if these web sites provided good training aid for new technicians and administrators?

Discuss your response in the forum and respond to comments from your classmates.

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.