Week #13 – IDS

Overview of the week's objectives

Week #13 will continue with the topic of Intrusion Detection System, Module O5L9.

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.

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	O5L9	Online Module Guides &Videos	2		
Practice Assignments	O5L9-PQ	Taking Practice Quizzes	1		
		Working on PAs & Participating to PA forums	8		
Graded Assignments	W13-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 – Comprehensive IDS (C5L9A1)

You are a Linux Administrator for an attorney's office. The lawyers are working on several high profile cases but are worried that hackers may attempt to access their computer systems and gather sensitive information.

Using your knowledge gained from this, and prior lessons, develop an in-depth security and intrusion detection and prevention policy for this office. Make use of Internet resources, flow-charts, and any other resources available as you develop your intrusion detection and prevention system.

Upload using standard naming conventions for credit.

PA #2 : Lab – Install Snort (C5L9A2)

Configure and install snort on your Fedora system. Make the required changes in the /etc/snort/snort.conf file and get the system running. Capture the output of ps -ax and ls -l /var/log/snort/

Archive the capture output into a tar.bz2 file.

Upload the tar.bz2 file to the dropbox using standard naming convention of: firstname_lastname_course5_lesson9_lab1.tar.bz2 to receive credit.

PA #3 : Lab – Dump File to MySQL (C5L9A3)

Allow the computer on which you installed Snort to run for a few days if possible, or at least a few hours. Once you have some traffic that has been analyzed, run a port scan on your test machine from another machine. Use mysqldump -a -add-drop-table -u root -p snort > snort-yourname_lesson9_lab2.sql to dump the MySQL databases into a file.

Upload this MySQL file using standard naming convention of: firstname_lastname_course5_lesson9_lab2.sql to receive credit.

.

Task #3 – Use the "Support forum

Refer to all previous "Week's Overview PDFs" for detailed instructions applying to all discussion forums assignments.

PA #4 : Forum – IDS as Package (C5L9F1)

Why is Intrusion Detection and Prevention a system rather than a single package?

Think about the company for which you work and or the school you attend and identify the job functions of those involved in Intrusion Detection and Prevention.

Once you respond to the question, comment constructively on two responses from your classmates.

PA #5 : Forum – Response to Encrypted Packets (C5L9F2)

You are monitoring the Snort logs and you notice an alert of unauthorized traffic coming through the firewall from the internal network to the external network. The traffic is unusual because it occurs on a port that is not often used and the traffic is a constant stream of encrypted data packets.

Will you ignore the alert or take an action? If you ignore, why? If you take action, what action will you take? Support your answers.

Once you respond to the questions, comment on two responses 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.