# CIS-481: Introduction to Information Security

## Module 9 - Security Technology - IDPS and Other Security Tools

## Exercise #7

**Team:**

**Participants: Charles Degboe, Nicholas Zhang, Abril Beascoechea, Ricardo Portillo**

**Logistics**

A. Get together with other students on your assigned **Team** in person and/or virtually.

B. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning and may impact your performance on assessments, especially with respect to the essay questions.

C. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

**Problem 1** *(5 points)*

How does a *false positive* alarm differ from a *false negative* alarm? From a security perspective, which is less desirable?

False negative: When an intrusion detection system fails to respond to a real attack event, it is a false negative. Since an IDS is meant to detect attacks, this is the most serious. It may be applied to tell the difference between actual attacks and these stimuli

False positive: An alert or alarm that, in reality, does not imply that an attack has taken place, is ongoing, or has been successful. an attack-related false positive operation or activity. By gradually reducing users to alarms and events, false positives have the tendency to make users more sensitive to alerts and decrease their speed and intensity of response to real intrusion events. This may alert a person who is less likely to respond quickly when an actual intrusion occurs.

**Problem 2** *(8 points)*

How does a *network-based IDPS* differ from a *host-based IDPS*? Which has the ability to analyze encrypted packets?

Network-based IDPS is connected to a segment of an organization's network and focuses on protecting network information assets. While host-based IDPS resides on a particular computer

and protects the server's or host's information. The type of IDPS that has the ability to analyze encrypted packets is Host-based IDPS.

**Problem 3** *(5 points)*
Explain the difference between network *footprinting* and network *fingerprinting*.
Network footprinting is the process of collecting publicly available data on a subject/target. This can involve researching internet addresses controlled by the target, and then using specific browser tools such as the "view source" option to gather more specific information about the target such as internal network configuration, server names & addresses, and locations for CGI script bins. Furthermore, attackers may use targeted search queries in an attempt to find the weakest link in an organization's security. Common tools such as web scanners can conduct many different types of scans and probes on a target in search of information. One example is a web scanner called "Sam Spade" which can perform network analysis queries, send ICMP requests.

While footprinting is considered an early step in the process of conducting an attack on a target, fingerprinting is the next step in the attack. After data or web addresses have been collected in the footprinting phase, attackers will now scan these addresses for any potential vulnerabilities. Targets that attackers look for while fingerprinting are the target's operating system, what the target network/firewall accepts or rejects, and open ports. Attackers can use tools such as packet sniffers, active or passive vulnerability scanners, and firewall analysis tools.

**Problem 4** *(7 points)*
What is a *vulnerability scanner*? What is the difference between *active* and *passive* vulnerability scanners?

A vulnerability scanner is a software program or network appliance that scans a range of network addresses and port numbers for open services.

Active scanning works by starting traffic on the network to find data with great detail. Active scanning is a vulnerability scanner that performs network initiation of traffic to find and assess ports of service. This scanner type identifies exposed usernames and groups, shows open network shares, and exposes configuration problems and other server vulnerabilities, too. Active scanners try to penetrate the systems in much the same way that a real hacker would. They can occasionally cause network services to hang or bring down servers and thus should be run when network usage is low, such as at night or on the weekend. Active scanners perform a far more aggressive, extensive scan.

The passive scanner listens in on the network and determines vulnerable versions of both server and client software. A passive scanner evaluates the service ports available from hosts utilizing the traffic in the target network segment. The advantage of using passive scanners: the

services available to each host are indexed; therefore, they are serviceable without prior approval to test the target. They are more dipped in regarding being tools designed to simply monitor what is going on in the network, where the connections are going and coming from a server, to eventually develop a list of applications that are found vulnerable. Secondly, the passive vulnerability scanners can point out client-side vulnerabilities that often go unscanned in their active counterparts. For instance, it could not establish the version of Internet Explorer running on a desktop machine because a live scanner was being run without DOMAIN Admin rights. In contrast, a passive scanner could establish that simply by catching the traffic to and from the client. Products also exist for passive scanning that should not interfere regular network activity. They can run in the background and scan the devices continuously without affecting network performance and, basically, not crashing the systems. Where appropriate, organizations may want to deploy a passive scanner "continuously" and then launch regular active scans for a more thorough examination.