COMP 5370/6370 Test #2 – This is the take-home part Instructor: A. Skjellum; TA. A. Ravipati November 4, 2015

YOUR NAME: **John Carroll**

CLASS (5370 or 6370): 5370 TIME SPENT ON EXAM: 2 hours

YOUR ID: jcc0044

MAXIMUM TIME: 5 hours. Expected time: 2-3 hours.

**Test conditions:** It has to be done on your own, on your honor. No sharing materials, talking, or use of electronic devices other than to look up data of your own, without sharing it with others, during the exam. Academic Honestly rules of Auburn University apply as does the class syllabus. COMP5370 students: complete problems A and B. COMP6370 students: complete problem C as well. Undergrads, you can do problem “C” for extra credit, but still within the total time available.

This is due by class time on Monday, November 9, 2015. You will submit that by bringing hardcopy to class on Monday. It will be an additional 50 points for both sections.

Turn in this cover sheet, with your answers (written or printed, or both) attached with a staple, and please make sure the entire package has your name on every page.

High quality responses include: Concepts enumerated; comparisons and contrasts, cited sources, explanations; diagrams if appropriate.

**PROBLEM A**. (25 points for COM5350, 20 for COMP6350). You are on a desert island with “Computer Security: Art and Science,” by Matt Bishop. You’re well fed and warm and safe, and have time to read and write about computer security. You also have a working tablet that can surf the web (but only purposive sites about computers, security, and assurance).

Learn about ways to attack the integrity of virtual machines – in the cloud, and standalone. Write about what you learn. Describe known attacks, how they work, what they do. Cite your sources.

Please note that attacks that steal secret keys are of interest here.

Ans:  
The VMM subjects are users and virtual machines. VMM has a basic, flat file system for its own use and partitions the remaining disk space among the virtual machines. Those machines may use any file structure they desire, and each virtual machine has its own set of file systems. Each subject and object has a multilevel security and integrity label, and the security and integrity levels form an access class. Two entities have the same access class if and only if their security and integrity labels are the same, and one entity dominates another if and only if both the security and integrity classes dominate. (“Computer Security: Art and Science,” by Matt Bishop)

The simplest attack that malicious code can perform on avirtual machine emulator is to detect it. As more security researchers rely on virtual machine emulators, malicious code samples have appeared that are intentionally sensitive to the presence of virtual machine emulators. Those samples alter their behavior (including refusing to run) if a virtual machine emulator is detected. This behaviour makes analysis more complicated, and possibly highly misleading.

A harsher attack that malicious code can perform against a virtual machine emulator is the denial-of-service; specifically, this type of attack causes the virtual machine emulator to exit.

Finally, the most interesting attack that malicious code can perform against a virtual machine emulator is to escape from its protected environment. (https://www.symantec.com/avcenter/reference/Virtual\_Machine\_Threats.pdf)

**PROBLEM B**. (25 points for COM5350, 20 for COMP6350). Explain “HIDS” and “NIDS” and how they work and what they do. Compare and contrast. Use your book and web resources. Differentiate anomaly from intrusion. Explain false positives and false negatives. Which is worse in either case?

Ans:  
Intrusion detection systems are of two main types, network based (NIDS) and host based (HIDS) intrusion detection systems.

**Network Intrusion Detection Systems**Network Intrusion Detection Systems (NIDS) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. It performs an analysis of passing traffic on the entire subnet, and matches the traffic that is passed on the subnets to the library of known attacks. Once an attack is identified, or abnormal behavior is sensed, the alert can be sent to the administrator. An example of an NIDS would be installing it on the subnet where firewalls are located in order to see if someone is trying to break into the firewall. Ideally one would scan all inbound and outbound traffic, however doing so might create a bottleneck that would impair the overall speed of the network. OPNET and NetSim are commonly used tools for simulation network intrusion detection systems. NID Systems are also capable of comparing signatures for similar packets to link and drop harmful detected packets which have a signature matching the records in the NIDS. When we classify the designing of the NIDS according to the system interactivity property, there are two types: on-line and off-line NIDS. On-line NIDS deals with the network in real time and it analyses the Ethernet packet and applies it on the some rules to decide if it is an attack or not. Off-line NIDS deals with a stored data and pass it on a some process to decide if it is an attack or not.[4]

**Host Intrusion Detection Systems**  
Host Intrusion Detection Systems (HIDS) run on individual hosts or devices on the network. A HIDS monitors the inbound and outbound packets from the device only and will alert the user or administrator if suspicious activity is detected. It takes a snapshot of existing system files and matches it to the previous snapshot. If the critical system files were modified or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission critical machines, which are not expected to change their configurations.

An **Anomaly-Based** Intrusion Detection System, is a system for detecting computer intrusions and misuse by monitoring system activity and classifying it as either normal or anomalous. The classification is based on heuristics or rules, rather than patterns or signatures, and attempts to detect any type of misuse that falls out of normal system operation. This is as opposed to signature-based systems, which can only detect attacks for which a signature has previously been created. There are other equally obvious advantages to using anomaly-based IDS. For example, because it detects any traffic that is new or unusual, the anomaly method is particularly good at identifying sweeps and probes towards network hardware. It can, therefore, give early warnings of potential intrusions, because probes and scans are the predecessors of all attacks.

A false positive occurs when an intrusion detection system reports an attack, but no attack is underway. False positives reduce confidence in the correctness of the results as well as increase the amount of work involved. However, false negatives (occurring when an intrusion detection system fails to report an onging attack) are worse, because the purpose of an intrusion detection system is to report attacks. The goal of an intrusion detection system is to minimize both types of errors.

**PROBLEM C** (10pts for COMP 6350 only). Explain how to perform denial of service attacks against TCP/IP using one of several approaches. Look them up, cite them, explain how they work. How do you mitigate them?

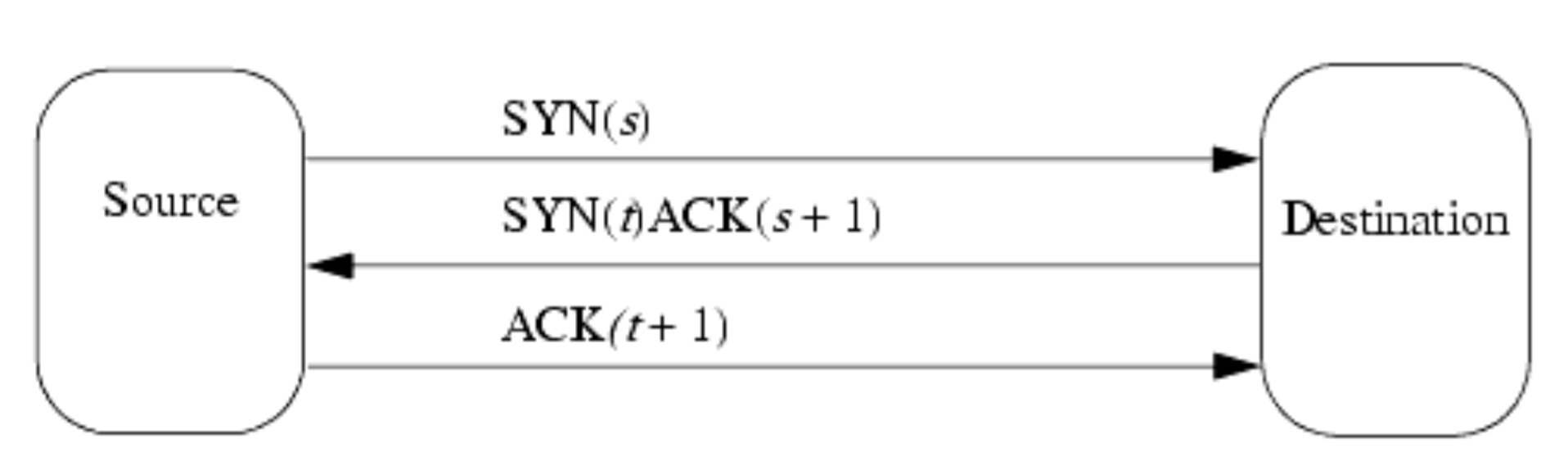
Ans:  
Attempts to block availability, called denial of service attacks, can be the most difficult to detect, because the analyst must determine if the unusual access patterns are attributable to deliberate manipulation of resources or of environment.

Daniels and Spafford [255] present an analysis of the Land attack [222], which causes a denial of service by causing the target of the attack to hang or to respond very slowly. This attack is built on an exchange that begins a TCP connection.

When a TCP connection begins, the source sends a SYN packet to the destination. This packet contains a sequence number s. The destination receives the packet and returns a SYN/ACK packet containing the acknowledgment number s + 1 and a second sequence number t. The source receives this packet and replies with the acknowledgment number t + 1. Figure 24-2 illustrates this exchange, called a three-way handshake.

(T. Daniels and E. Spafford, "Identification of Host Audit Data to Detect Attacks on Low-Level IP Vulnerabilities," Journal of Computer Security 7 (1), pp. 3–35 (1999))

Figure 24-2. The TCP three-way handshake. The SYN packet is a TCP packet with sequence number s (or t) and the SYN flag set. Likewise, the ACK packet is a TCP packet with acknowledgment number s + 1 (or t + 1) and the ACK flag set. The middle message is a single TCP packet with both SYN and ACK flags set.



The Land attack arises from an ambiguity of the TCP specification [511]. When the source and destination differ, or the TCP port numbers of the source and destination differ, the two sequence numbers s and t are from different processes. But what happens if the source and destination addresses and ports are the same? The TCP specification is ambiguous.

Consider what happens in the three-way handshake in this case. The target host receives a SYN packet with sequence number s. It responds with a SYN/ACK packet containing sequence number t and acknowledgment number s + 1. At this point, the internal state of the connection in that host is that the next acknowledgment number will be t + 1. Because the source and destination addresses and ports are the same, the packet returns to the host. The host checks the packet and finds that the acknowledgment number (s + 1) is incorrect. At this point, the TCP specification suggests two different ways to handle the situation.

According to one part of the specification,[1] the connection should send a reset (RST). If this is done, it terminates the connection and the attack fails.

According to a different part of the specification,[2] the host should reply with an empty packet with the current sequence number and the expected acknowledgment number. Hence, the host sends a packet with sequence number t + 1 and acknowledgment number s + 1. Naturally, it receives that packet. It checks that the acknowledgment number is correct, and—again—it is not. Repeating the sequence causes the same packet to be generated, resulting in an infinite loop. If the host has disabled interrupts during this part, the system hangs. Otherwise, it runs very slowly, servicing interrupts but doing little else. The denial of service attack is now successful.

Detecting this attack requires that the initial Land packet be detected. The characteristic of this packet is that the source and destination addresses and port numbers are the same. So, the logging requirement is to record that information. The audit requirement is to report any packets for which the following condition holds.

*source address = destination address and   
source port number = destination port number*