University of Technology

Department of Computer Sciences

Final Examination 2011-2012

Subject: ***Network Security*** *Year:* ***2011-2012***
Division: ***Computer Security – 4th Class*** *Time:* ***3 Hours***
Examiner: ***Dr.Mazin S. Ali*** *Date:* ***7 / 6 /2012***

Answer 6 Questions Only *(10 marks for each questions)*

Q1: Describe in brief the following Microsoft Network Security Solutions:

A. Microsoft's Windows 2000 Authentication Scheme.
B. Microsoft's Windows NT Authentication Scheme.
C. Windows Firewall (also explains what it does and does not do).

Q2:
A. Define the "Intrusion Detection System", and then describe in brief each type of it *(Signature-based and Heuristic Intrusion Detection Systems)*.
B. Explain in details the Intrusion Detection System's "Stealth Mode" and "False Results".

Q3: Explain in details who the following attack can be done:-

1. Distributed Denial of Service (DDoS) Attack.
2. Wiretapping (on Cable, Microwave and Optical Fiber Cable).

Q4: Draw the overview figure for "Encrypted E-Mail Processing", and then explain how can get the "Message Confidentiality" and "Message Integrity" requirements for Secure e-Mail.

Q5: Compare between the following:-

1. "Packet Filtering Gateways" and "Application Proxies".
2. IPsec *(Internet Protocol Security)* and HTTPs *(HTTP Secure)*.
3. "Missdelivery" and "Exposure" / Message Confidentiality Violations.

Q6: Describe in details the security involving programs based "Service Problems" *(Greedy Programs, Viruses, Bacteria and Worms)*.

Q7: Define the following:

1. "Automatic Call-Back" Port Protection
2. " Silent Modem" Port Protection
3. "Pad Traffic" Traffic Control
4. "Routing Control" Traffic Control
5. "Connectivity" Denial of Service Attack
6. "Flooding" Denial of Service Attack

- Good Luck -

Solutions:

Q1: Describe in brief the following Microsoft Network Security Solutions:

A. Microsoft's Windows 2000 Authentication Scheme.

In *Windows NT 4.0*, the authentication database is distributed among several domain controllers. Each domain controller is designated as a primary or backup controller. All changes to the authentication database must be made to the (single) primary domain controller; then the changes are replicated from the primary to the backup domain controllers.

B. Microsoft's Windows NT Authentication Scheme.

In *Windows 2000*, the network views the controllers as equal trees in a forest, in which any domain controller can update the authentication database. This scheme reflects Microsoft's notion that the system is "multi-master": only one controller can be master at a given time, but any controller can be a master. Once changes are made to a master, they are automatically replicated to the remaining domain controllers in the forest.

C. Windows Firewall (also explains what it does and does not do).

It Does	It Does Not
Help block computer viruses and worms from reaching your computer.	**Detect or disable computer viruses and worms** if they are already on your computer. For that reason, you should also install antivirus software and keep it updated to help prevent viruses, worms, and other security threats from damaging your computer or using your computer to spread viruses to others.
Ask for your permission to block or unblock certain connection requests.	**Stop you from opening e-mail with dangerous attachments**. Don't open e-mail attachments from senders that you don't know. Even if you know and trust the source of the e-mail you should still be cautious.
Create a record (a security log), if you want one, that records successful and unsuccessful attempts to connect to your computer.	**Block spam or unsolicited e-mail** from appearing in your inbox. However, some e-mail programs can help you do this.

C. Q2: Define the "Intrusion Detection System", and then describe in brief each type of it *(Signature-based and Heuristic Intrusion Detection Systems)*.

D. An intrusion detection system (IDS) is a code that run on device, typically on another separate computer, that monitors activity to identify malicious or suspicious events.

E. **Signature-based** intrusion detection systems perform simple pattern-matching and report situations that match a pattern corresponding to a known attack type.

F. **Heuristic** intrusion detection systems, also known as **anomaly based**, build a model of acceptable behavior and flag exceptions to that model; for the future, the administrator can mark a flagged behavior as acceptable so that the heuristic IDS will now treat that previously unclassified behavior as acceptable.

G. Explain in details the Intrusion Detection System's "Stealth Mode" and "False Results".

An IDS is a network device (or, in the case of a host-based IDS, a program running on a network device). Any network device is potentially vulnerable to network attacks. How useful would an IDS be if it itself were deluged with a denial-of-service attack? If an attacker succeeded in logging in to a system within the protected network, wouldn't trying to disable the IDS be the next step?

Intrusion detection systems are not perfect, and mistakes are their biggest problem. Although an IDS might detect an intruder correctly most of the time, it may stumble in two different ways:

- Raising an alarm for something that is not really an attack (called a false positive, or type I error in the statistical community), or
- Not raising an alarm for a real attack (a false negative, or type II error). Too many false positives means the administrator will be less confident of the IDS's warnings, perhaps leading to a real alarm's being ignored.

Q3: Explain in details who the following attack can be done

Distributed Denial of Service (DDoS) Attack

Distributed denial-of-service (DDoS) attack, an attacker does two stages: plant a trojan horse (zombie), and lauch the attack. In the first stage, the attacker uses any convenient attack to plant a Trojan horse on a target machine. That Trojan horse does not necessarily cause any harm to the target machine, so it may not be noticed. The target machine then becomes what is known as a zombie. The attacker repeats this process with many targets, the target systems carry out their normal work, unaware of the resident zombie.

At some point, as a second stage, the attacker chooses a victim and sends a signal to all the zombies to launch the attack. Then, instead of the victim's trying to defend against one denial-of-service attack from one malicious host, the victim must try to counter n attacks from the n zombies all acting at once. Not necessary all of the zombies need to use the same attack.

Wiretapping (on Cable, Microwave and Optical Fiber Cable).

Wiretap means to intercept communications. Although the term has physical connection, no actual contact is necessary. The passive wiretapping is just listening that is intercepting communication, while the active wiretapping means injecting something into the communication.

All signals sent through the cable are available for anyone to intercept. For example, each LAN connector called a 'packet sniffer' can retrieve all packets on the net, and the process called 'inductance an intruder' can pick up signals from the wire.

All signals sent through the air are available to anyone who wants to pick them up, the microwave and satellite communication are a very insecure medium.

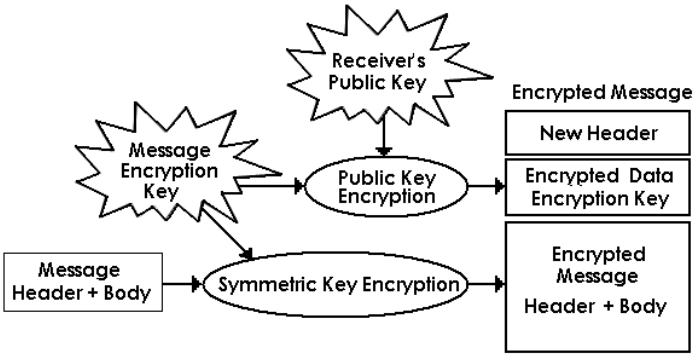
No one can tap an optical fiber cable without detection, because, firstly the entire optical network must be tuned carefully each time a new connection is made, secondly, optical fiber carries light energy, not electricity, light does not emanate a magnetic field as electricity does. While the repeaters, splices, and taps along a optical cable are places where data may be available more easily than in the fiber cable itself. The connections from computing equipment to the fiber may also be points for penetration. By itself, fiber is much more secure than cable, but it has vulnerabilities also.

Q4: Draw the overview figure for "Encrypted E-Mail Processing", and then explain how can get the "Message Confidentiality" and "Message Integrity" requirements for Secure e-Mail.

If we were to make a list of the requirements for secure e-mail, our wish list would include the following protections.

- *Message confidentiality* (the message is not exposed en route to the receiver)
- *Message integrity* (what the receiver sees is what was sent)
- *Sender authenticity* (the receiver is confident who the sender was)
- *Nonrepudiation* (the sender cannot deny having sent the message)

Not all of these qualities are needed for every message, but an ideal secure e-mail package would allow these capabilities to be invoked selectively.



Q5: Compare between the following:

1. **"Packet Filtering Gateways" and "Application Proxies".**

   Packet Filtering Gateway: A packet filtering gateway or screening router is the simplest, and in some situations, the most effective type of firewall. A packet filtering gateway controls access to packets based on packet address (source or destination) or specific transport protocol type (such as HTTP web traffic).

Application Proxy: Packet filters look only at the headers of packets, not at the data inside the packets. Therefore, a packet filter would pass anything to port 25, assuming its screening rules allow inbound connections to that port. But applications are complex and sometimes contain errors. Worse, applications often act on behalf of all users, so they require privileges of all users. A flawed application, running with all users' privileges, can cause much damage.

2. IPsec *(Internet Protocol Security)* and HTTPs *(HTTP Secure)*.

IPsec *(Internet Protocol Security)*: Providing the Authenticating and Encrypting for each IP packet of a communication session.

HTTPs *(HTTP Secure)*: It provides encrypted communication and secure identification of a network web server. It is a combination of HTTP with the SSL/TLS protocol.

Q6: Describe in details the security involving programs based "Service Problems" *(Greedy Programs, Viruses, Bacteria and Worms)*.

a- **Greedy Programs**: Programs that can block a computing system (infinite cycle or loop) so that no other computation can go on.

b- **Viruses**: A virus is a program that can infect other programs by modifying them (by include a copy of the virus program itself), so that the infected program then begins to act as a virus, infecting other programs.

c- **Bacteria**: Bacteria are programs that do not explicitly damage any files. Their sole purpose is to replicate themselves. Bacteria may do nothing more than execute two copies of itself simultaneously, or perhaps create two new files, both of those programs then may copy themselves twice, and so on. Bacteria reproduce exponentially, eventually taking up all the processor capacity, memory, or disk space, denying users to those resources.

d- **Worms**: Network worms programs use network connections to spared from system to system. The worms can behave as a virus or bacteria or it could implant trojan horse programs or perform any number of disruptive actions. As with viruses, worms can be embedded in almost any other meaningful programs.

Q7: Define the following:

"Automatic Call-Back" Port Protection:

With an automatic call-back system, an authorized user dials a computer system. After the user identifies him, the computer breaks the communication line. The computer then consults an internal table of telephone numbers and calls the user back at a predetermined number. Clearly, the table of telephone numbers must be well-protected against modification.

"Pad Traffic" Traffic Control

The countermeasure to traffic flow threats is to disguise the traffic flow. If traffic between A and B is encrypted so that the attacker can detect only the number of packets flowing, A and B can agree to pass recognizable (to them) but meaningless encrypted traffic. When A has much to communicate to B, there will be few meaningless packets; when communication is light, A will pad the traffic stream with many spurious packets.

"Silent Modem" Port Protection

Typically, a computer receiving an incoming call establishes the connection by sending a modem signal. However, it can also wait silently until the caller's modem sends the first tone. In this way, the computer does not reveal itself as a computer until the caller has revealed that it is a computer.

"Connectivity" Denial of Service Attack

Every point in the network must be reachable from every other points. So, most nodes are connected by multiple paths, so that when one path is unavailable, communication can be maintained using another path, but if the failure occur on a critical path or node will block the communication.

"Flooding" Denial of Service Attack

An intruder can damage network communications by generating spurious messages. Their essential purpose is to increase the traffic on the network, thereby degrading service to the users.