University of Technology
Department of Computer Sciences
Final Examination 2011-2012

Subject: ***Network Security*** *Year:* ***2011-2012***
Division: ***Computer Security – 3rd Class*** *Time:* ***3 Hours***
Examiner: ***Dr.Mazin S. Ali*** *Date:* ***31 / 5 /2012***

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

Q1: A. Describe in brief the "Kerberos Authentication System".
B. Describe in brief the "Microsoft's Authentication Schemes" *(Windows 2000 Authentication Scheme and Windows NT Authentication Scheme)*.

Q2: Define the "Firewall", and then describe in brief each type of Firewalls *(Packet Filtering Gateways or Screening Routers, Stateful Inspection, Application Proxies, Guards and Personal Firewalls)*.

Q3: Define the "Intrusion Detection System", and then describe in brief each type of Intrusion Detection Systems *(Signature-based and Heuristic Intrusion Detection Systems)*.

Q4: A. How can get the Message Confidentiality and Message Integrity requirements for Secure e-Mail.
B. Define the following:
1. IPsec *(Internet Protocol Security)*.
2. HTTPs *(HTTP Secure)*.

Q5: Compare between the following:-

1- "Automatic Call-Back" and " Silent Modem" Port Protections.
2- "Pad Traffic" and "Routing Control" Traffic Control.
3- "Link Encryption" and "End-to-End Encryption".
4- "Connectivity" and "Flooding" Denial of Service Attack.
5- "Session Hijacking" and "Man-in-the-Middle Attack" Spoofing Attack.

Q6: A. Compare between "Passive" and "Active" Wiretapping, then describe in details the wiretapping on Cable, Microwave and Optical Fiber Cable.
B. Describe in details the security involving programs based "Information Access Problems" *(Trapdoors, Trojan Horse, Salami Attack and Programs that leak Info)*.

Q7: Describe in details (with figures) the "Distributed Denial of Service" Attack.

- Good Luck -

Solutions:

Q1: A. Describe in brief the "Kerberos Authentication System".

Kerberos is ,based on the idea that, a central server provides authenticated tokens, called **tickets**, to requesting applications.

1. A ticket is an unforgeable, nonreplayable, authenticated object.
2. A ticket is an encrypted data structure naming a user and a service that user is allowed to obtain.
3. A ticket also contains a user's authenticated identity, an identification of file, the access rights (for example, to read), a session key for the file server to use this file, and an expiration date for the ticket.

Kerberos is a complete solution, and all applications must use Kerberos authentication and access control. But, currently a few applications use Kerberos authentication, so integration of Kerberos into an existing environment requires modification of existing applications, which is not feasible.

Q1: B. Describe in brief the "Microsoft's Authentication Schemes" *(Windows 2000 Authentication Scheme and Windows NT 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.

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.

Q2: Define the "Firewall", and then describe in brief each type of Firewalls *(Packet Filtering Gateways or Screening Routers, Stateful Inspection, Application Proxies, Guards and Personal Firewalls)*.

A firewall is a code (it runs on a dedicated device) that filters all traffic between a protected (inside) network and a less trustworthy (outside) network. Usually a firewall is implemented on a separate computer, with direct connections only to the outside and inside networks.

A: 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).

B: Stateful Inspection Firewall: Filtering firewalls work on packets one at a time, accepting or rejecting each packet and moving on to the next. They have no concept of "state" or "context" from one packet to the next. A stateful inspection firewall maintains state information from one packet to another in the input stream.

C: 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.

D: Guard: A guard is a sophisticated firewall. Like a proxy firewall, it receives protocol data units, interprets them, and passes through the same or different protocol data units that achieve either the same result or a modified result.

E: Personal Firewalls: A personal firewall is an application program that runs on a workstation to block unwanted traffic, usually from the network. A personal firewall can complement the work of a conventional firewall by screening the kind of data a single host will accept, or it can compensate for the lack of a regular firewall, as in a private DSL or cable modem connection.

Q3: Define the "Intrusion Detection System", and then describe in brief each type of Intrusion Detection Systems *(Signature-based and Heuristic Intrusion Detection Systems)*.

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.

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

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.

Q4: A. 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.

Q4: B. Define the following:

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.

Q5: Compare between the following:-

1- "Automatic Call-Back" and " Silent Modem" Port Protections.

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.

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.

2- "Pad Traffic" and "Routing Control" 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.

Consider a message that is covered in multiple layers, like the layers of an onion. A wants to send a message to B but doesn't want anyone in or intercepting traffic on the network to know A is communicating with B. So A takes the message to B, wraps it in a package for D to send to B. Then, A wraps that package in another package for C to send to D. Finally, A sends this package to C. The internal wrappings are all encrypted under a key appropriate for the intermediate recipient.

3- "Link Encryption" and "End-to-End Encryption".

Link Encryption	End-to-End Encryption
Message exposed in sending host	Message encrypted in sending host
Message exposed in intermediate nodes	Message encrypted in intermediate nodes
Encryption applied by sending host (encryption invisible to user)	Encryption applied by sending process (user applies encryption)
Host maintntains encryption (one facility for all users)	User must use algorithm (user select encryption)
Encryption can be done by H/W	Encryption done by S/W
All or no message encrypted	User chooses to encrypt or not, for each message
Requires one key per host pair	Requires one key per user pair
The number of keys required is n*(n-1)/2 for n nodes	The number of keys required is n*(n-1)/2 for n users
Provides node authentication	Provides user authentication

Q6: A. Compare between "Passive" and "Active" Wiretapping, then describe in details the 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.

Q6: B: Describe in details the security involving programs based "Information Access Problems" *(Trapdoors, Trojan Horse, Salami Attack and Programs that leak Info)*.

a- **Trapdoors**: Trapdoor is a secret and undocumented entry point. The trapdoor is inserted sometime during code development (perhaps to assist test the module, perhaps to assist in the future modifications or enhancements, and perhaps forgets to remove them).

b- **Trojan Horse**: Trojan horse performs a hidden function in addition to its stated, obvious function. In other words, the Trojan horse is a destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

c- **Salami Attack**: Programs that compute amounts of money may be subject to a salami attack, in this attack, a small amount of money is shaved from each computation, the amount shaved is so small that an individual case is unlikely to be noticed. However, accumulated amounts can add up.

d- **Programs that leak Information**: The programs that communicate their information to people who should not receive that information. A general name for these extraordinary paths of communication is 'covert channel'.

Q7: Describe in details (with figures) the "Distributed Denial of Service" 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.