Previous Exam and answers

Notes

- Some of the module contents for this year were not given last year.
- **This does not mean that the topics are not part of the exam**
- YOU NEED TO STUDY ALL THE LECTURES FOR THIS TERM
- **This lecture is only to show you the structure of questions and how they can be answered. IT IS NOT A REVISION CLASS**
- **Some questions from previous year were not given in lectures this term.**

DO NOT STUDY ONLY CONTENTS OF THESE SLIDES

IF YOU DO YOU RISK FALING THE EXAM

Question 1- a - Briefly explain the difference between a passive and active attack (6 marks)

- Active attacks is in which a hacker attempt to exploit the network in order to make changes to the targets (victim) data. This is also called Direct Breaches (3 marks)
- Passive attacks is in which an unauthorized party such as a hacker/intruder monitors networks and look for vulnerabilities in a network. This is often called Indirect Breaches (3 Marks)

Question 1b: Explain what IP spoofing is and why it is carried out **(7 marks).**

- IP spoofing is pretending to have the IP address of another machine.
- After the IP is spoofed, hackers wait for legitimate users or other machines to try and message or use the system (maybe entering passwords etc.?) - this is IP Spoofing. (3 marks)
- Intercepting messages passed from server to server, and altering the message in the pro- cess - this is a man-in-the-middle attack.
- Intercepting or saving old messages, then transmitting them later-retransmission (4 marks)

Question 1c: How would you defend your system against known exploit attacks **(2 marks)**

- Ensure all affected programs are replaced with versions not affected by the exploit
- Keep up-to-date with security bulletins and patches

Question 1-d: How would you defend your system against Known man-in-the-middle **(2 marks)**

- Ensure you are speaking to the right host to start with (as with IP Spoofing)
- Establish encrypted sessions, so that an interception cannot happen mid-communication

Question 1-e: How would you defend your system against Trojan horse **(2 marks)**

- Keep a database of signatures of important applications, and regularly check to ensure the programs match the signatures
- On Linux, a program called tripwire will do this automatically

Question 1-f: Define the terms below. **(6 marks)**

1. **Interception**
   - **U**nauthorized party gets access to an asset(1.5 mark)
2. **Fabrication**
   - Fake asset is planted in the system(1.5 mark)
3. **Vulnerability**
   - Weakness in the security system (1.5 mark)
4. **Threat**
   - Circumstances that may lead to loss or harm(1.5 mark)

Question 2-a: Define what “pretexting” is and explain how it can be used by hackers for information gathering **(5 marks)**

- Some people say it is just a story or lie during a social engineering engagement.
- Pretexting is better defined as the background story, dress, grooming, personality, and attitude that make up the character you will be for the social engineering audit.
- Pretexting encompasses everything you would imagine that person to be. The more solid the pretext, the more believable you will be as a social engineer.

Question 2-b: To protect your organization from a cyber-attack, it’s important to understand how an attacker goes about stealing sensitive information. What are the typical stages that an attack goes through? **(8 marks)**

- Reconnaissance
- Incursion and Scanning
- Discovery
- Capture
- Exfiltration

Question 2-c: UDP and TCP are two transport layer protocols mostly used in our Internet communication. Evaluate how suitable TCP and UDP are for the two different services listed below. justify your answers **(4 marks)**

- Online gaming: UDP
- For the most part of the duration. When setting it the online gaming connection you might use TCP. For the rest, a UDP connection will be more reasonable
- Secure shell connection needs a more secure, reliable and a guaranteed end to end connection. TCP should be used.

Question 2-d: TCP is a connection oriented protocol. Explain how TCP ensure reliability of its connection and how it can guarantee delivery of data. **(8 marks)**

- Reliable and connection-based Sequence numbers, timeouts, and retransmissions protect against loss and reordering.
- Sequence numbers: loss, reordering, duplication.
- Timeouts: loss.
- Retransmission: loss
- Should negotiate a connection before packets can be sent (3 way handshake)
- Delivery Ack, packets segments are numbered
- Has congestion control (for busy networks, delays packets delivery)
- Unlike UDP, a TCP packet represents a segment of the input data stream

Question 3-a: A denial of service (DoS) attack is about one thing: making a service unavailable to a user. Answer the following questions on the different types DoS:

- Question 3-a-1: Explain what the meaning of DoS is and how damaging it is for companies? **(4 marks)**
  - A DoS attack attempts to prevent valid users from accessing network resources.
  - A DoS is damaging for companies because they might lose business, it might damage their reputation and disrupt their services. Furthermore, a DoS can lead to several other attacks if hacks decide to escalate the attack.
- Question 3-a-2: What is the difference between DoS and DDoS. **(2 marks)**
  - A distributed denial of service (DDoS) attack has the same goal but amplifies the DoS attack by using multiple hosts.

- Question 3-a-3: Give an example of a recent DDoS attack. **(3 marks)**
  - Mirai bot is one of the recent DDoS attack that damaged thousands of servers and results in a 1.2Tbps attacks
- Question 3-a-4: What was the disruptive technology that made DDoS more damaging than ever before? **(3 marks)**
  - Internet of Things is the disruptive technology that made DDos more damaging as now millions of machines can participate without the awareness of their owners. Simply because IoT devices are difficult to secure and usually not monitored.

Question 3-b:Session hijacking is a serious threats for end devices and servers likewise.

- **Question 3-b-1:** Explain what blind hijack attack is **(4 marks)**
  - An attacker can inject data such as malicious commands into those communications
  - This type of attack is called blind hijacking because the attacker can only inject data into the communications stream;
  - He cannot see the response to that data, such as the command completed successfully.
  - This method of hijacking is still very effective.
- Question 3-b-2: How you can identify how vulnerable your network is to session hijacking (**4 marks)**
  - Try to hijack actual network sessions using common attacker tools such as Juggernaut or Hunt.
  - Using live attacker tools against your organizations production networks, however, is not recommended.
  - A safer litmus test would be to simply determine whether your organization uses transport protocols that do not use cryptographic protection such as encryption for transport security or digital signatures for authentication verification.
  - Common example protocols include Telnet, File Transfer Protocol (FTP), and Domain Name System (DNS). If such network protocols exist in your organizations networks, sessions traveling over those unencrypted protocols have strong potential to be hijacked.

Question 3-c: HTTP and HTTPS are two of the most used application layer protocols.

- **Question 3-c-1:** Explain what the difference between them is. **(2 marks)**
  - HTTP Collect user credentials through a simple form and submit to server for validation as a plain text. HTTPS uses other application layer protocol to encrypt the messages. HTTPS stands for secure HTTP.
- Question 3-c-2: Show the process that HTTPS uses with SSL and TLS to encrypt messages. **(3 marks)**
  - Negotiate the cipher suite
  - Authenticate sever and/or client
  - Exchange information for building cryptographic secrets
  - All encrypted except the header!

Question 4-a: When it comes to network forensics, forensic analysts need to look within the sources of Network-Based Evidence. There are many sources of network-based evidence in any environment

- **Question 4-a-1:** Discuss “Central log servers” evidence and how much forensics value they hold. **(5 marks)**
  - Central log servers are designed to help security professionals identify and respond to network security incidents.
  - Even if an individual server is compromised, logs originating from it may remain intact on the central log server
- Question 4-a-2: Discuss ‘routers” evidence and how much forensics value they hold. **(4 marks)**
  - Routers connect different subnets or networks together and facilitate transmission of packets between different network segments, even when they have different addressing schemes routers have routing tables. Routing tables map ports on the router to the networks that they connect
  - This allows a forensic investigator to trace the path that network traffic takes to traverse multiple networks. (Note that this path can vary dynamically based on network traffic levels and other factors.).

Question 4-b: Network-based evidence poses special challenges in several areas including acquisition, content, storage, privacy, seizure, and admissibility.

- **Question 4-b-1:** Explain why acquisition is a challenge in network based evidence **(4 marks)**
  - It can be difficult to locate specific evidence in a network environment.
  - Networks contain so many possible sources of evidence from wireless access points to web proxies to central log servers that sometimes pinpointing the correct location of the evidence is tricky.
  - Even when you do know where a specific piece of evidence resides, you may have difficulty gaining access to it for political or technical reasons.
- Question 4-b-2: Explain why privacy is a challenge in network based evidence **(4 marks)**
  - Depending on jurisdiction, there may be legal issues involving personal privacy that are unique to network-based acquisition techniques

Question 4-c: For a successful investigation, it is extremely important to know how to handle the evidence. A set of fundamental rules should be followed

- **Question 4-c-1:** List those rules and explain them briefly **(3 marks)**
  - Rule 1: never mishandle the evidence: evidence has to be handled with extreme care.
  - The objective is to minimize any disruptive contact with the evidence
  - Rule 2: never work on the original evidence or system: Any interaction with the original evidence in digital form causes the evidence to be compromised. Metadata such as dates and time stamps on files change almost instantly.
  - Rule 3: document everything: Documentation for all the exhibits and authenticated images of the exhibits is a must. A comprehensive chain of custody, or CoC as it is known

- Question 4-c-2: What are the characteristics for getting to satisfactory completion of a digital forensics case **(5 marks)**
  - Preparation: Trained personnel with the necessary tools and processes should be available to tackle any contingency. Just as organizations carry out fire drills on a regular basis, incident response drills should be institutionalized as part of the organization policy.
  - Information gathering/evidence gathering: A comprehensive system to monitor network events & activity, store logs, and back them up is essential. Different inputs are generated by different event logging tools, firewalls, intrusion prevention & detection systems, and so on.
  - Understanding of human nature: An understanding of human nature is critical. This helps the investigator to identify the modus operandi, attribute a motive to the attack, and anticipate and pre-empt the enemy's next move.
  - Instant action: Based on the preparations done and the incident response planned, immediate action must be taken when a network compromise is suspected
  - Deductive reasoning: A logical thought process, the ability to reason through all the steps involved, and the desire to see the case to its rightful conclusion are the skills that need to be a part of a network 007's arsenal