Revision Mock exam
2017/18 exam paper

Question 1

- a. Briefly explain the differences between OSI layers and TCP/IP layers. (6 marks)
- b. In term of cyber security, explain what each of the term below mean:
  - Threat (1 mark)
  - Vulnerability (1 mark)
  - Control (1 mark)
- c. Attacks are usually grouped into four different types: Interception, interruption, modification and fabrication.
  - Explain what each of those types' means in term of the assets for a company. (8 marks)
  - Give an example of each of those attack types. (4 marks)

Question 1 a - a. Briefly explain the differences between OSI layers and TCP/IP layers. (6 marks)

BASIS FOR COMPARISON	TCP/IP MODEL	OSI MODEL
Expands To	TCP/IP- Transmission Control Protocol/ Internet Protocol	OSI- Open system Interconnect
Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
No. Of Layers	4 Layers	7 Layers
Developed by	Department of Defense (DoD)	ISO (International Standard Organization)
Tangible	Yes	No
Usage	Mostly used	Never used

Question 1 b. In term of cyber security, explain what each of the term below mean:

- Threat (1 mark) : circumstances that may lead to loss or harm
- Vulnerability (1 mark) weakness in the security system
- Control (1 mark)something that reduces or removes a vulnerability

Question 1 c- Attacks are usually grouped into four different types: Interception, interruption, modification and fabrication.

- Explain what each of those types means in term of the assets for a company. (8 marks)
  - Interception: unauthorized party gets access to an asset 2 marks
  - Interruption: asset becomes unusable (lost or destroyed)2 marks
  - Modification: existing asset is changes2 marks
  - Fabrication: fake asset is planted in the system2 marks
- Give an example of each of those attack types. (4 marks)
  - Interception: Eavesdropping, Keyloggers, Sniffing 1 marks
  - Interruption: spoofing 1 mark
  - Modification: man in the middle attack 1 mark
  - Fabrication: , Replay Attack 1 mark
- Identify which of those four types is considered a passive attack or an active attack. (4 marks) 1 mark for each
  - Passive attack (Interception)
  - Active attack (Fabrication, Interruption, Modification)

Question 2

- a. Define what elicitation is and explain how it can be used by hackers for information gathering. (6 marks)
- b. Define the different attack stages listed below:
  - Reconnaissance (2 mark)
  - Scanning (2mark)
  - Escalation (2 mark)
  - c. UDP and TCP are the two most used transport layer protocols.
    - State and briefly explain four features of UDP. (4 marks)
    - State and briefly explain four features of TCP. (4 marks)
    - Evaluate TCP and UDP in terms of security and speed of transmission. (5 marks)

Question 2 a- Define what is elicitation and explain how it can be used by hackers for information gathering.(6 marks).

- Elicitation is the extraction of information during an apparently normal and innocent conversation. (2 marks). These conversations can occur anywhere that the target is a restaurant, the gym, a day care, and any where.
- Elicitation works well because it is low risk and often very hard to detect. It is easy to get people to talk about their achievements, or professionals talking about some of their skills and what they do (1 marks).
- All those information are part of the information gathering stage and hackers can use these to escalate an attack (potential passwords, possible hints given for a vulnerability of the system) (3 marks)

Question 2 b. Define the different attack stages listed below: – In each of the attack stages below, any answer that gets the main point across gets the full 2 marks.

- Reconnaissance (2 mark):
  - Attackers leverage information from a variety of factors to understand their target including identifying vulnerable servers, insecure applications, or unpatched systems that can be compromised
- Scanning (2 mark):
  - Once the target is identified, the next step is to identify a weak point that allows the attackers to gain access.
  - This is usually accomplished by scanning an organizations network with tools easily found on the Internet to find entry points.
  - This step of the process usually goes slowly, sometimes lasting months, as the attackers search for vulnerabilities
- Escalation (2 mark)
  - Now that weaknesses in the target network are identified, the next step in the cyber attack is to gain access and then escalate. In almost all such cases, privileged access is needed because it allows the attackers to move freely within the environment. Once the attackers gain elevated privileges, the network is effectively taken over and is now owned by the intruders.

Question 2 b. Define the different attack stages listed below: – In each of the attack stages below, any answer that gets the main point across gets the full 2 marks.

- Reconnaissance (2 mark):
  - Attackers leverage information from a variety of factors to understand their target including identifying vulnerable servers, insecure applications, or unpatched systems that can be compromised
- Scanning (2 mark):
  - Once the target is identified, the next step is to identify a weak point that allows the attackers to gain access.
  - This is usually accomplished by scanning an organizations network with tools easily found on the Internet to find entry points.
  - This step of the process usually goes slowly, sometimes lasting months, as the attackers search for vulnerabilities
- Escalation (2 mark)
  - Now that weaknesses in the target network are identified, the next step in the cyber attack is to gain access and then escalate. In almost all such cases, privileged access is needed because it allows the attackers to move freely within the environment. Once the attackers gain elevated privileges, the network is effectively taken over and is now owned by the intruders.

Question 2 c. UDP and TCP are the two most used transport layer protocols

- State and briefly explain four features of UDP.(4 marks) – One mark for each feature
  - Lightweight and connectionless
  - Small packet sizes (60% less than TCP), in header size UDP (8 bytes) & TCP (20 bytes)
  - No connection to create and maintain
  - More control over when data is sent
  - Does not compensate for loss of packet
  - Does not deliver or guarantee packet delivery in order
  - Does not check if network is busy
- State and briefly explain four features of TCP.(4 marks)
  - Reliable and connection-based
  - Should negotiate a connection before packets can be sent (3 way handshake)
  - Delivery Ack, packets segments are numbered
  - Retransmission
  - In order delivery
  - Has congestion control (for busy networks, delays packets delivery)
  - Bigger overhead!
  - Not suitable for video streaming or real time voice calls.
- Evaluate TCP and UDP in term of security and speed of transmission. (5 marks)
  - Students need to explain that since TCP is connection oriented, it is more secure than UDP however UDP is faster (2.5 marks for each)

Question 3

- a. A denial of service (DoS) attack is about one thing: making a service unavailable to a user. Answer the following questions the different types of DoS attacks:
  - Explain what the meaning of DoS is and how damaging it is for companies? (4 marks)
  - What is the difference between DoS and DDoS? (2 marks)
    - Give an example of a recent DDoS attack. (2 marks)
    - What is the disruptive technology that led to many DDoS attacks occurring in the last few years? Give an example of a recent attack. (4 marks)
- b. Session hijacking is a method in which attackers are able to intercept and modify communications as well as provide some tricks and techniques attackers use.
  - State the three categories that session hijacking attacks fall in. (3 marks)
  - How is network level session hijacking achieved with TCP? (5 marks)
  - Identify a method that network security undertakes to determine if their network is susceptive to network level session hijacking attacks. (2 marks)
  - Explain what countermeasures can be taken to defeat and stop network level session hijacking attacks. (3 marks)

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 of DoS attacks:

- Explain what is the meaning of DoS and how damaging it is for companies? (4 marks)
  - A denial of service attack is about one thing: making a service unavailable to a user. This could be making it so that customers can't get to a web-based shopping application, which will have an immediate impact to the business that owns the application because users will not be spending money there. If you take a system entirely offline by getting it to fail completely, you have done the same thing as knocking the application offline.
  - What is the difference between DoS and DDoS. (2 marks)
    - DoS originate from one source. DDoS look like it originate from multiple sources. This can be IP addressed that are spoofed.
  - Give an example of a recent DDoS attack. (2 marks)
    - We discussed several in class (Mirai botnet for example or reaver)
  - What is the disruptive technology that led to many DDoS attacks occurring in the last few years? Give an example of a recent attack. (4 marks)
    - Students need to simply mention that Internet of Things devices that are low power, unpatched and insecure make it easy for hackers to use those devices for their botnet of zombies to conduct DDoS (2 marks)
    - An example of a recent attack could be Mirai botnet or Reaver. For example Mirai botnet attack led to an increase from an average of 10 Gbps generated traffic in previous DDoS to over 120 Gbps average in Mirai malware family. Some even reported a 1.2 Tbps in some attacks (2 marks)

Question 3 b- 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 of DoS attacks:

- Explain what is the meaning of DoS and how damaging it is for companies? (4 marks)
  - A denial of service attack is about one thing: making a service unavailable to a user. This could be making it so that customers can't get to a web-based shopping application, which will have an immediate impact to the business that owns the application because users will not be spending money there. If you take a system entirely offline by getting it to fail completely, you have done the same thing as knocking the application offline.
  - What is the difference between DoS and DDoS. (2 marks)
    - DoS originate from one source. DDoS look like it originate from multiple sources. This can be IP addressed that are spoofed.
  - Give an example of a recent DDoS attack. (2 marks)
    - We discussed several in class (Mirai botnet for example or reaver)
  - What is the disruptive technology that led to many DDoS attacks occurring in the last few years? Give an example of a recent attack. (4 marks)
    - Students need to simply mention that Internet of Things devices that are low power, unpatched and insecure make it easy for hackers to use those devices for their botnet of zombies to conduct DDoS (2 marks)
    - An example of a recent attack could be Mirai botnet or Reaver. For example Mirai botnet attack led to an increase from an average of 10 Gbps generated traffic in previous DDoS to over 120 Gbps average in Mirai malware family. Some even reported a 1.2 Tbps in some attacks (2 marks)

Question 3 b- Session hijacking is a method in which attackers are able to intercept and modify communications as well as provide some tricks and techniques attackers use.

- State the three categories that session hijacking attacks fall in. (3 marks)
  - Man-in-the-middle (MITM) attack, Blind hijack attacks and Session theft attacks
- How is network level session hijacking achieved with TCP? (5 marks)
  - Session hijacking at the network level is especially attractive for attackers.
  - They dont need to have access on a host as they do with host-level session hijacking.
  - If the attacker wanted to inject data into the TCP session as the client, he would need to be able to do the following:
    - 1- Spoof the clients IP address.
    - 2- Determine the correct sequence number the server is expecting from the client
    - 3- Inject data into the session before the client sends its next packet.(3 marks)
  - The attacker sends a single Z character to the server with sequence number X+2; the server accepts it and sends the real client an ACK packet with acknowledgement number X+3 to confirm that it has received the Z character.
  - When the client receives the ACK packet, it will be confused either because it didn't send any data or because the next expected sequence is incorrect. (2 marks)
- Identify a method that network security undertakes to determine if their network is suspecting to network level session hijacking attacks. (2 marks)
  - One obvious way to determine whether your organizations networks are susceptible to network-level session hijacking attacks is to try to hijack actual network sessions using common attacker tools such as Juggernaut or Hunt.
- Explain what countermeasures can be taken to defeat and stop network level session hijacking attacks. (3 marks)
  - Defeating network-level session hijacking threats can be done by implementing encrypted transport protocols such as Secure Shell (SSH), Secure Socket Layers (SSL), and Internet Protocol Security (IPSec).

Question 4

- a. For any successful digital forensics investigation, it is extremely important to successfully collect, collate, preserve, and analyse the evidence. To begin with, we need to identify the sources of evidence for any investigation.
  - Briefly discuss evidence obtainable from within the network (8 marks)
- b. 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.
  - Discuss “On the Wire” evidence and how much forensics value they hold. (6 marks)
  - Discuss “Authentication Servers” evidence and how much forensics value they hold. (6 marks)
- c. There are many methods to investigate network forensics. One of those methodologies is TAARA investigation methodology
  - Explain TAARA methodology and all its stages (5 marks)

Question 4 a- For any successful digital forensics investigation, it is extremely important to successfully collect, collate, preserve, and analyze the evidence. To begin with, we need to identify the sources of evidence for any investigation

- Briefly discuss evidence obtainable from within the network (8 marks)
  - Students will need to state and discuss briefly
    1. Evidence from network & device logs,
    2. Network traffic
    3. Memory of the individual computers under investigation
    4. Evidence residing on the hard drives of individual computers under investigation

Question 4 b- 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.

- Discuss “On the Wire” evidence and how much forensics value they hold. (6 marks) 3 for explaining the evidence, 3 for identifying forensics value
  - On the wire, Physical cabling is used to provide connectivity between stations on a LAN and the local switches, as well as between switches and routers
  - Network forensic investigators can tap into physical cabling to copy and preserve network traffic as it is transmitted across the line
- Discuss “Authentication servers ” evidence and how much forensics value they hold. (6 marks)
  - Authentication servers are designed to provide centralized authentication services to users throughout an organization so that user accounts can be managed in one place, rather than on hundreds or thousands of individual computers.
  - Authentication servers typically log successful and/or failed login attempts and other related events. Investigators can analyze authentication logs to identify brute-force password-guessing attacks, account logins at suspicious hours or unusual locations, or unexpected privileged logins

Question 4 c- There are many methods to investigate network forensics. One of those methodologies is TAARA investigation methodology

- Explain TAARA methodology and all its stages (5 marks)
  - Trigger: This is the event that leads to an investigation.
  - Acquire: This is the process that is set in motion by the trigger; this is predefined as part of the incident response plan and involves identifying, acquiring, and collecting information and evidence relating to the incident.
  - Analysis: All the evidence that is collected is now collated, correlated, and analysed. The sequence of events is identified.
  - Report: Based on the preceding analysis, a report is produced before the stakeholders to determine the next course of action
  - Action: The action recommended in the report is usually implemented during this stage