Midterm-Fall 2024 - Results

Attempt 1 of 1

Written Oct 21, 2024 6:34 PM - Oct 21, 2024 8:24 PM

Attempt Score **98 / 100**

Overall Grade (Highest Attempt) **98 / 100**

Question 1

A symmetric block cipher such as AES provides which security property?

○ Authenticity

✓ ○ Confidentiality

○ Integrity

Question 2

Describe a real-world scenario where all four security principles—**confidentiality**, **integrity**, **authenticity**, and **availability**—must work together. Explain how a failure in each principle could compromise the system.

Alice opens Alice Merchant Store. Bob is their customer. Trudy is a bad guy with tech skills.

Confidentiality: Prevent Unauthorized access to of Bob's credit card info that Bob has saved.
Integrity: Prevent unauthorized creation of orders on Bobs account (with or without Bob paying)/ Prevent Trudy from rewriting Bob's address. Make Bob pay if he is creating an order.
Authenticity: Ensure that it is Bob who is actually making the orders.
Availability: Ensure that the Bob is able to create orders when he feels like.

--

Without Confidentiality, Bob will lose trust in the Alice Merchant Store and will have to go through the hassle of reissuing his card because Trudy has been making unauthorized transactions using it.

Without Integrity, Bob can create orders without paying for them with or Trudy could use Bobs account to order stuff to his address. This could create losses or chargebacks for Alice.

Without Authenticity, Trudy could send false requests from Bob's account. This can cause unnecessary charges for Bob who will again lose trust in Alice Merchant Store.

Without Availability, Bob may have trouble placing orders when he needs to making Alice lose on revenue.

The correct answer is not displayed for Written Response type questions.

Question 3

The security of symmetric encryption algorithms like AES relies on keeping the encryption algorithm secret.

○ True

✓ ○ False

Question 4

Explain two ways in which two-factor authentication enhances the security of an authentication system and two ways in which it reduces usability.

A two factor authentication or MFA can help enhance security. MFA services are normally provided by an independent 3rd party.

1. Adds an additional Layer of security incase the password is compromised.
2. It increases authenticity by ensuring that the person intending to access the system is actually aware of the activities.

It can reduce usability:

1. It increases time required to access the service. People who have a hard time using smartphones may have trouble accessing many on-click MFA apps.
2. Genuine users may not remember answers to security questions which may lock them out of the system causing unnecessary hassle.

The correct answer is not displayed for Written Response type questions.

Question 5

Describe 5 NMAP scan types? Which scan can initiate a connection without completing it, making it harder to detect?

The NMAP scan types are as follows:
Connect scan - It is easily logged and detected because a full 3 way connection is established. Open ports reply with a SYN/ACK, whereas closed ports respond with an RST/ACK.

TCP SYN scan - This type of scan is known as half open because a full TCP three-way connection is not established. Open ports reply with a SYN/ACK, whereas closed ports respond with a RST/ACK.

SYN scan sends a TCP SYN, and then a RST upon receiving an ACK. Thus it can initiate a connection without completing it. This type of scan was originally developed to be stealthy and evade IDS systems although most now detect it. But note that the SYN scan requires root privileges.

TCP FIN scan - This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on UNIX devices.

TCP NULL scan - a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.

TCP ACK scan - This scan attempts to determine access control list (ACL) rule sets or identify if stateless inspection is being used. If an ICMP destination unreachable, communication administrative prohibited message is returned, the port is considered to be filtered.

The correct answer is not displayed for Written Response type questions.

Question 6

Describe the primary issue with ECB mode encryption that renders it vulnerable to a plain-text attacker and how CBC mode encryption mitigates this issue.

In the ECB mode, the plain text attacker may be able to create enough combinations because if k=3 bit inputs. Three bit inputs can be permuted in 40,320 ways. This is not a lot and can be brute forced.
If k is large then the table becomes huge. This is expensive in terms of time and

computational effort.
CBC eliminates the issue of table by implementing rounds for encryption and decryption. We guarantee that the ciphertext is different every time even though the message stays the same by changing the IV (Initialization Vector) for each session. This ensures that there is no easy way to brute force the message.

The correct answer is not displayed for Written Response type questions.

Question 7

Which of the following techniques best ensures confidentiality when transmitting sensitive data over the internet?

○ Packet filtering by firewalls

✓ ○ Symmetric encryption algorithms like AES

○ Hashing algorithms like SHA-256

○ Digital signatures with RSA

Question 8

A VLAN is intended to isolate multiple networks which share the same layer 1 and switching resources.

✓ ○ True

○ False

Question 9

When designing DNS systems for large organization it is typical to employ a technique called split DNS. The purpose of SPLIT DNS is:

○ Provides for redundancy of DNS servers so that they remain highly available. The is an important part of the availability in the CIA triad.

○ Ensures that the DNS servers can be in areas of the network that allow for optimal DNS response times

✓ ○ Uses two DNS systems for internally available host names and externally available host names. This is turn limits the amount of information exposed to an attacker perform recon.

○ Uses two DNS systems so that nmap scans can't be performed on the internal DNS system.

Question 10

Storing md5 hashed passwords is considered best practise.

○ True

✓ ○ False

Question 11

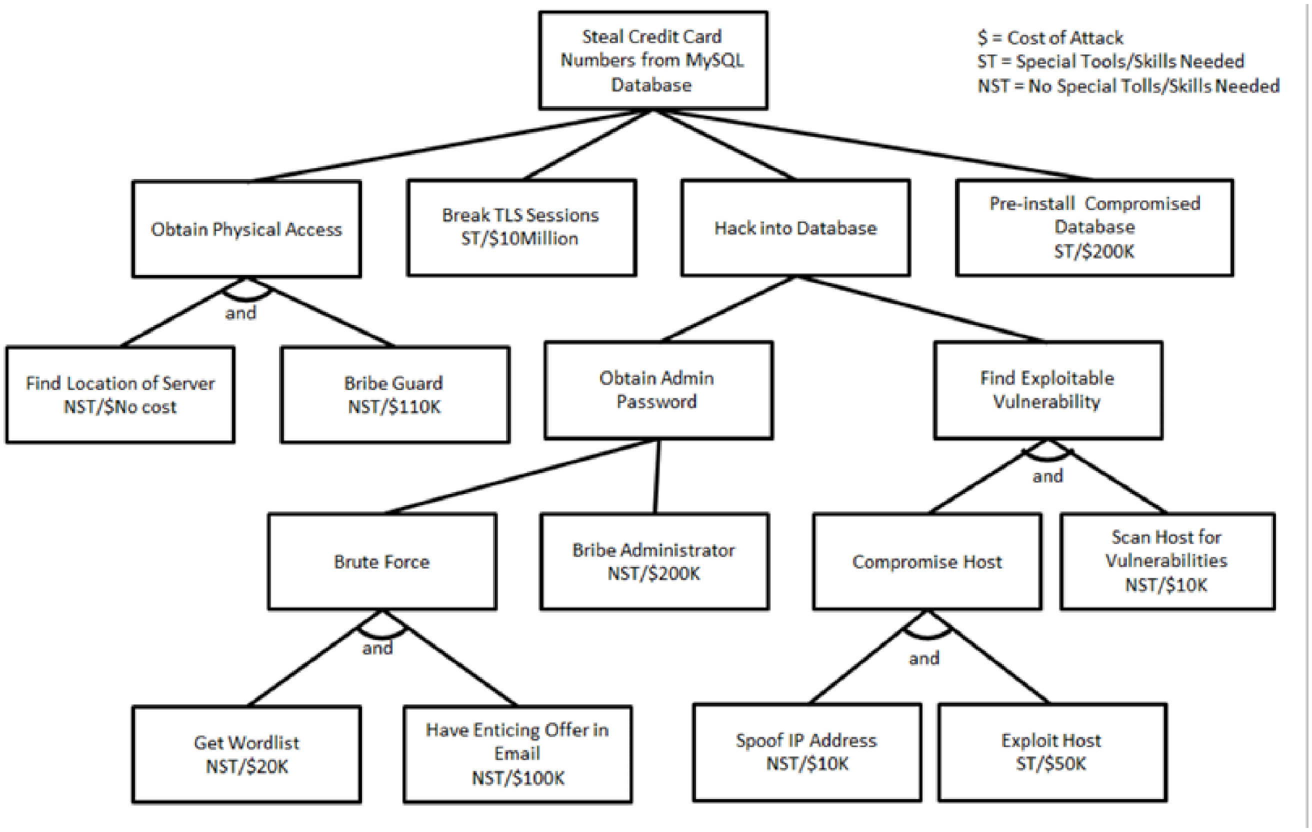
Any IP addresses is normally authenticated so that is not easily spoofed.

○ True

✓ ○ False

Question 12

Referring to the attack tree shown in the image, what is the cheapest attack that requires no special tools or skills?


Steal Credit Card Numbers from MySQL Database
$ = Cost of Attack
ST = Special Tools/Skills Needed
NST = No Special Tolls/Skills Needed
Obtain Physical Access
Break TLS Sessions ST/$10Million
Hack into Database
Pre-install Compromised Database ST/$200K
and
Find Location of Server NST/$No cost
Bribe Guard NST/$110K
Obtain Admin Password
Find Exploitable Vulnerability
and
Brute Force
Bribe Administrator NST/$200K
Compromise Host
Scan Host for Vulnerabilities NST/$10K
and
and
Get Wordlist NST/$20K
Have Enticing Offer in Email NST/$100K
Spoof IP Address NST/$10K
Exploit Host ST/$50K

○ Spoof IP Address, 10K

○ Obtain Physical Access, $90K

○ Obtain Admin Password $5K

✓ ○ Obtain Physical Access, $110K

Question 13

Many DDoS attacks use misconfigured UDP services to amplify traffic, but require a network without egress filtering to launch the attack. Explain why we do not know which networks are the source of these DDoS amplification attacks.

Attack traffic can be made similar to legitimate traffic in order to hinder detection. So sources are not readily detectable.
If UDP is the underlying protocol can becomes connectionless (bots) and without egress filtering it can easily spread.
UDP is required for any amplification attack since the incoming packet is spoofed with the "source" being changed to the target.

The correct answer is not displayed for Written Response type questions.

Done