CS-GY 6823 NETWORK SECURITY, CF01 > Tests & Quizzes

Tests & Quizzes

Midterm Exam Spring - 2020 USE THIS VERSION PLEASE

Return to Assessment List

Part 1 of 1 - 85.0/ 100.0 Points

Question 1 of 18

5.0/ 5.0 Points

Why would an attacker use a proxy sever?

- ✓ ○ **A. To create a stronger connection with the target.**
- ✓ ○ **B. To create a ghost server on the network.**
- ✓ ○ **C. To obtain a remote access connection.**
- ✓ ○ **D. To hide the source of their malicious activity.**

Answer Key: D

Question 2 of 18

5.0/ 5.0 Points

Which of the below is a symmetric key algorithm and a streaming cipher used to encrypt information?

- ✓ ○ **A. RC4**
- ✓ ○ **B. SHA2**

- ✓ ○ **C. AES**
- ✓ ○ **D. MD5**

Answer Key: A

Question 3 of 18

5.0/ 5.0 Points

To hide information inside a picture, what technology is used?

- ✓ ○ **A. Rootkits**
- ✓ ○ **B. Bitmapping**
- ✓ ○ **C. Steganography**
- ✓ ○ **D. Image Rendering**

Answer Key: C

Question 4 of 18

0.0/ 5.0 Points

A digital signature is one of the most important methods to ensure the authenticity of digital information. How is a digital signature created and used from the digital fingerprint (hash) of the message?

- ✓ ○ **A. The hash is encrypted with the session key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with a corresponding session key.**
- ✓ ○ **B. The hash is encrypted with the public key of the sender. Verification is done by the receiver of the information by decrypting the digital fingerprint with the corresponding private key.**
- ✓ ○ **C. The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the hash with the corresponding public key.**

- ✖ ○ **D. The hash is encrypted with the private key of the sender. Verification is done by the receiver of the information by decrypting the message with the corresponding public key.**

Answer Key: C

Feedback: Signature verification is performed by taking the hash of the message and decrypting with the public key of the sender. This hash is then compared to the result of the hash of the message done locally by the received. If the two are equal then the message is authentic.

Question 5 of 18

5.0/ 5.0 Points

The IPSec security specification provides several methods of implementation. For what purpose and how is the IPSec tunnel mode used?

- ✔ ○ **A. For end-to-end protection. Only the IP payload is protected.**
- ✔ ○ **B. For link protection. Only the IP payload is protected.**
- ✔ ○ **C. For link protection. Both the IP payload and IP header are protected.**
- ✔ ○ **D. For overall protection only the ip header is protected.**

Answer Key: C

Question 6 of 18

5.0/ 5.0 Points

Hackers and cyber criminals usually perform their activities according to a wellstructured plan. What is the best order in which these activities are performed within a well-structured plan?

- ✔ ○ **A. Vulnerability Identification, Recon, Scanning(Enumeration), Keeping Access, Covering Tracks**
- ✔ ○ **B. Recon, Scanning(Enumeration), Vulnerability Identification, Keeping Access, Covering Tracks**
- ✔ ○ **C. Enumeration, footprinting, getting access, privilege escalation, erasing tracks**

- ✓ ○ **D. Scanning, enumeration, getting access, privilege escalation, maintaining access**

Answer Key: B

Question 7 of 18

5.0/ 5.0 Points. Point(s) deducted for incorrect answer: 5.0

Jack is conducting a risk assessment for his firm and is evaluating the risks associated with a flood inundating the firm's data center. Consulting FEMA maps, he determines that the data center is located in a 100-year flood plain. Therefore the Annualized Rate of Occurrence is 1%. He estimates that a flood would cause $5M of damage to his $40M facility. What is the annualized loss expectancy?

- ✓ ○ **A. $500,000**
- ✓ ○ **B. $50,000**
- ✓ ○ **C. $500,000,000**
- ✓ ○ **D. $5,000**

Answer Key: B

Question 8 of 18

5.0/ 5.0 Points

What IPsec protocol provides confidentiality for the payload of data packets?

- ✓ ○ **A. AH**
- ✓ ○ **B. ESP**
- ✓ ○ **C. IKE**
- ✓ ○ **D. OAKLEY**

Answer Key: B

Question 9 of 18

5.0/ 5.0 Points

Your organization recently purchased a cybersecurity insurance policy that will cover his organization’s expenses in the event of a data breach. What risk management strategy is your organization pursuing?

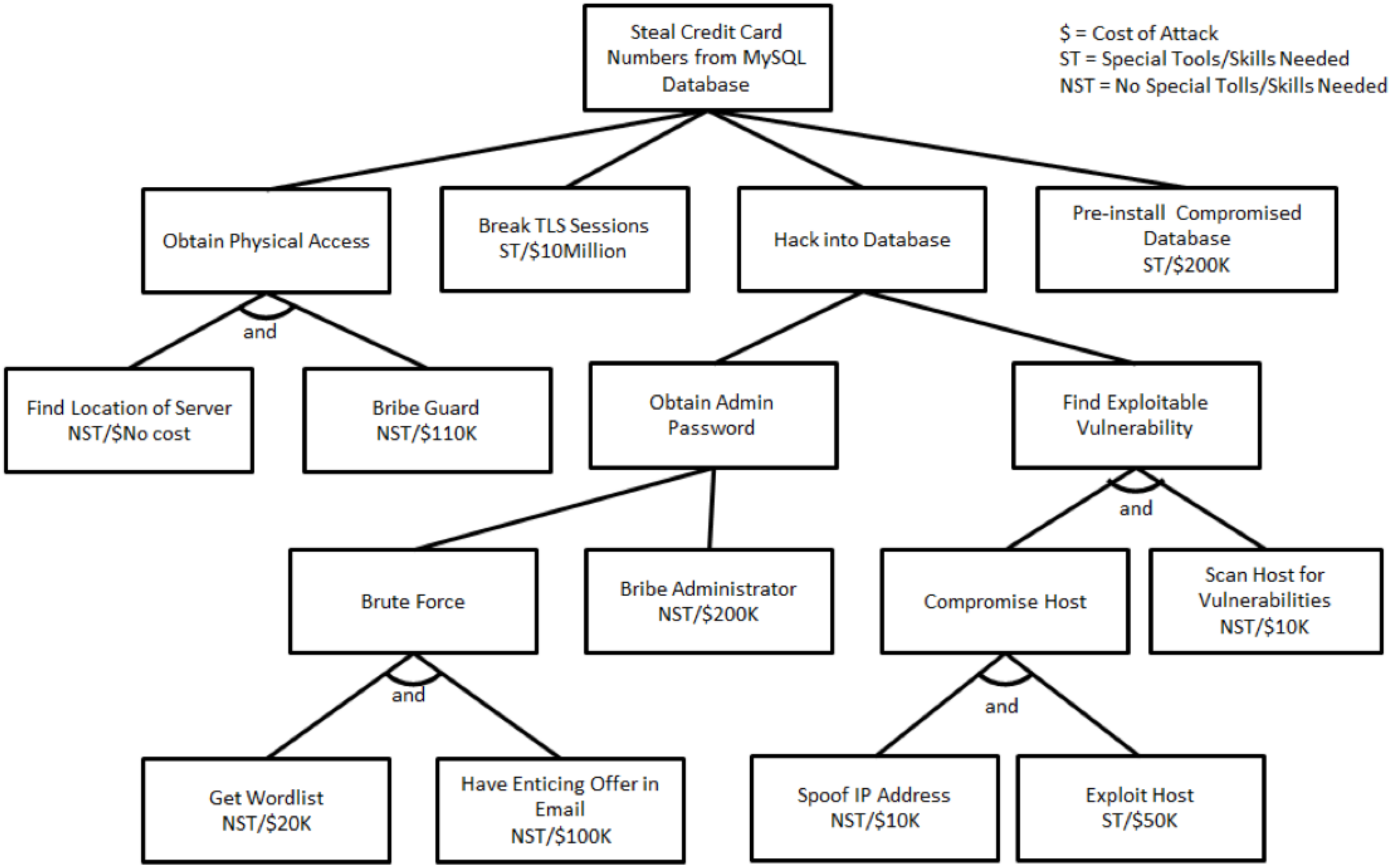
- ✓ ○ **A. Risk avoidance**
- ✓ ○ **B. Risk acceptance**
- ✓ ○ **C. Risk transference**
- ✓ ○ **D. Risk mitigation**

Answer Key: C

Question 10 of 18

5.0/ 5.0 Points

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

- ✓ ○ A. Obtain Physical Access, $90K
- ✓ ○ B. Obtain Physical Access, $110K
- ✓ ○ C. Spoof IP Address, 10K
- ✓ ○ D. Obtain Admin Password $5K

Answer Key: B

Question 11 of 18

5.0/ 5.0 Points

The purpose of a SYN Cookie is to:

- ✓ ○ **A. Store the state of a request to a website in the client browser so that the session can be resumed at a later time.**
- ✓ ○ **B. Prevent SYN Flooding attacks by not allocating resources to half open connections.**
- ✓ ○ **C. Prevent DDOS attacks by overflowing the attacks command and control SYN queue**
- ✓ ○ **D. Prevents SYN Flooding attacks by immediately sending a RST if the cookie from the client matches on the server side.**

Answer Key: B

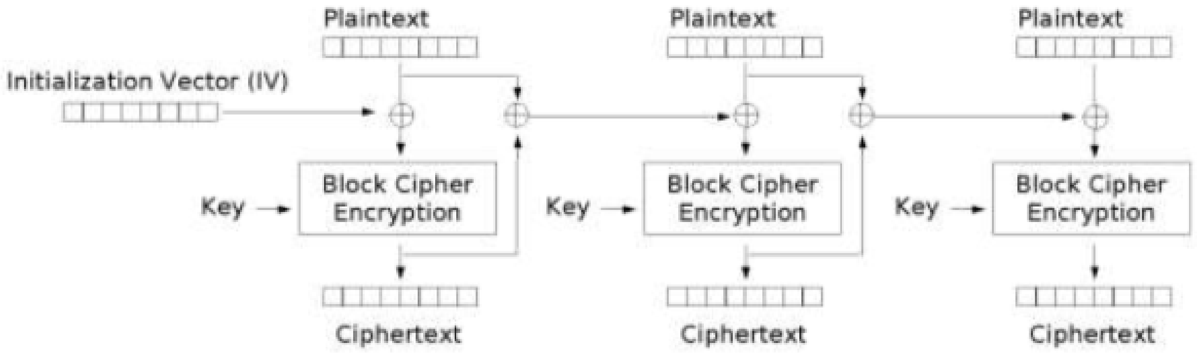
Question 12 of 18

5.0/ 5.0 Points

Block Cipher mappings

IN	OUT
1100	0000
1010	1101
1000	1111
1100	1011
1001	1110

Refer to the diagram shown. Using an IV of 1011 the encryption of 110001100011 results in a ciphertext of:



Propagating Cipher Block Chaining (PCBC) mode encryption

- ✗ ○ **A. 1011 1011 1110**
- ✓ ○ **B. 1010 1101 1101**
- ✓ ○ **C. 1101 1111 1111**
- ✓ ○ **D. 0000 1101 1111**

Answer Key: D

Question 13 of 18

5.0/ 5.0 Points

A rainbow table is a precomputed table for reversing cryptographic hash functions, usually for cracking password hashes. An effective method of defeating the use of a rainbow table is:

- ✓ ○ **A. Using a SALT with the password HASHs**
- ✓ ○ **B. Enforcing good password selection from your users**
- ✓ ○ **C. Selecting a secure HASHing function**

- ✓ ○ **D. Using an NONCE**

Answer Key: A

Question 14 of 18

5.0/ 5.0 Points

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

- ✓ ○ **A. Provides for redundancy of DNS servers so that they remain highly available. The is an important part of the availability in the CIA triad.**
- ✓ ○ **B. Insures that the DNS servers can be in areas of the network that allow for optimal DNS response times.**
- ✓ ○ **C. 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.**
- ✓ ○ **D. Uses two DNS systems so that nmap scans can't be performed on the internal DNS system.**

Answer Key: C

Question 15 of 18

0.0/ 5.0 Points

DNS and NTP amplification attacks are similar in the following ways:

- ✓ ○ **A. Both leverage the fact that UDP is the underlying protocol and connectionless.**
- ✓ ○ **B. Both DNS and NTP take a large request size inbound and directs this large request to the target.**
- ✗ ○ **C. Both incorporate timing of the arrival packets with the amplification on the outbound.**
- ✓ ○ **D. Both rely on a bounce scan directed at a vulnerable server.**

Answer Key: A

Feedback: Both leverage the fact that UDP is the underlying protocol and connectionless. UDP is required for any amplification attack since the incoming packet is spoofed with the "source" being changed to the target.

Question 16 of 18

What is the objective of Diffie-Hellman key exchange?

5.0/ 5.0 Points

- ✓ ○ **A. To protect encrypted data from man-in-the-middle attack**
- ✓ ○ **B. To establish a shared secret key between the sender and receiver**
- ✓ ○ **C. To prove to another party that one holds a secret key without revealing it**
- ✓ ○ **D. none of the above**

Answer Key: B

Question 17 of 18

Suppose an external attacker is performing reconnaissance on ACME Corporation using only the DNS protocol.

10.0/ 10.0 Points

2a. [6pts] Describe a method using only the DNS protocol that an external attacker can use to perform reconnaissance on ACME Corporation and identify internal names of servers and resources?
2b. [4pts] Describe a mitigation strategy to minimize what an attacker can obtain using this DNS recon technique.

The attacker can use the Dig command and see information of the company such as location, phone number and the public IP, and other IP addresses that link to ACME DNS server which attackers can use that as there advantage to get more data by finding IP or credentials in dumpster diving or even social engineering by contacting administrator phone number and war dialing the extension of the company to find other users the can leak out information. attackers can find vulnerabilities of other DNS that are in the result using the DIG command on ACME DNS.

For mitigation we can use 2 DNS one for internal and external (split dns), which can separate the information from the internal side and external side whenever users or attackers request and query. Also physical security and Security training staff are important when attackers find contact number on DNS information using dig to social engineers ACME staffs.

Feedback: Either using brute force DNS on different DNS names to determine if there is an entry in the DNS database. A zone transfer can also be performed. Using split DNS and/or turning off zone transfer for an external DNS are possible mitigation strategies.

Question 18 of 18

5.0/ 10.0 Points

Trudy is an employee of ACME Corporation and wants to exfiltrate data out of the ACME to her server. Trudy has found that ACME is not properly monitoring DNS requests and responses so has decided to use DNS as the basis for exfiltration. Trudy has set up a DNS server ns.evil.com.
(5pts)
Explain how Trudy would be able to send information out of ACME to her DNS server using only the DNS protocol.
(5pts)
Explain how ACME corp could prevent this type of exfiltration.

1) Since the person set up a ns.evil.com , Trudy would take any incoming query request from the end user and redirect to the ns.evil DNS and give it a fake public IP that would route to the an attacker server and do malicious activity such as phishing or malicious Trojan .

2) To prevent that attack we can enable DNS sec which one feature would double the bit of the transaction id. for an attacker to perform a successful attacker that person need to guess the transaction id of the end user question query and spoof the answer to the attacker side. although by doubling the bit, it would be much harder for an attacker to guess the transaction ID.

Comment: What you described doesn't allow for the exfiltration of data
An attacker may covertly embed ASCII characters in mandatory tcp packet headers for extraction by an attacker-controlled server or an attacker may embed data in DNS requests that traverse the DNS hierarchy to a name server set up by the attacker (ns.evil.com) for a domain zone setup by the attacker. The unmonitored DNS request would land on the attacker-controlled name server where data extraction can occur as part of different DNS record type requests.

Timezone: America/New_York

- Terms of Use
- Send feedback to the NYU Classes Team

- Powered by Sakai
-

Change Profile Picture

Error removing image

Error uploading image

Upload Choose File No file chosen

Save Cancel Connections ✖ Remove

Search for people ...

View More

My Connections Pending Connections

You don't have any connections yet. Search for people above to get started.

You have no pending connections.

⟵Back to My Connections

Search for people ...

${cmLoader.getString("connection_manager_no_results")}

Done