**The most desirable approach to security is one which is:**

Choose only ONE best answer.

**A**

Perimeter and dynamic

**B**

Layered and dynamic

**C**

Static and perimeter

**D**

Layered and static

CONFIRM

**Which of the following is NOT one of the three major classes of threats?**

Choose only ONE best answer.

**A**

Denial of service attacks

**B**

A computer virus

**C**

Intruding on a system

**D**

Online auction fraud

**This answer is correct.**

**Server Message Block (SMB) protocol runs on which port?**

Choose only ONE best answer.

**A**

443

**B**

8443

**C**

445

**D**

21

**This answer is correct.**

NEXT

QUESTION 4 OF 10

**Blocking attacks seek to accomplish what?**

Choose only ONE best answer.

**A**

Install a virus on a target system

**B**

Shut down security measures

**C**

Prevent legitimate users from accessing a system

**D**

Break into a target system

**This answer is correct.**

NEXT

**Which of the following is the best definition for non-repudiation?**

Choose only ONE best answer.

**A**

Security that does not allow the potential intruder to deny his attack

**B**

Processes that verify which user performs what action

**C**

It is another term for user authentication

**D**

Access Control

**This answer is correct.**

NEXT

**What is the acronym of URL.**

Choose only ONE best answer.

**A**

Uniform Reserved Location

**B**

Unique Resource Locator

**C**

Uniform Resource Locator

**D**

Uniformed Resource Location

**This answer is incorrect.**

NEXT

**Subnetting is used to split a network into smaller portions.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Trivial File Transfer Protocol (TFTP) runs on which port?**

Choose only ONE best answer.

**A**

110

**B**

80

**C**

69

**D**

194

**This answer is correct.**

NEXT

**Class A IPs with range 0-126 are reserved for multicasting.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

QUESTION 10 OF 10

**Malware is NOT a common threat for systems.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

QUESTION 1 OF 9

**Which of the following is the best definition for IP spoofing?**

Choose only ONE best answer.

**A**

Sending a packet that appears to come from a trusted IP address

**B**

Rerouting packets to a different IP address

**C**

Setting up a fake website that appears to be a different site

**D**

Sending packets that are misconfigured

**This answer is correct.**

**The most common session-hijacking is man in the middle attack**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Smurf attack is a popular DoS attack**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**To be protected against Ping of death attacks ensure that all operating systems are patched.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**The point of hijacking a connection is to exploit trust and gain access to a system.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correc**

**Which of the following is the best definition of a virus?**

Choose only ONE best answer.

**A**

Software that causes damage to system files

**B**

Software that self-replicates

**C**

Software that causes damage to any files

**D**

Software that attaches to e-mail

**This answer is correct.**

**What is a Trojan horse? (2 Answers)**

Choose ALL answers that apply.

**A**

Software that self-replicates

**B**

Software that appears to be benign but really has some malicious purpose

**C**

Software that deletes system files then infects other machines

**D**

Software that causes harm to your system

**What is the danger inherent in IP spoofing attacks?**

Choose only ONE best answer.

**A**

They are very damaging to target systems

**B**

Many of these attacks open the door for other attacks

**C**

They can be difficult to stop

**D**

Many firewalls do not examine packets that seem to come from within the network

**This answer is correct.**

**Which of the following best describes session hacking?**

Choose only ONE best answer.

**A**

Taking over a target machine via a Trojan horse

**B**

Taking control of a target machine remotely

**C**

Taking control of the communication link between two machines

**D**

Taking control of the login session

**This answer is correct.**

**What is a Trojan horse? (2 Answers)**

Choose ALL answers that apply.

**A**

Software that self-replicates

**B**

Software that appears to be benign but really has some malicious purpose

**C**

Software that deletes system files then infects other machines

**D**

Software that causes harm to your system

**A device that hides its internal IP addresses is called?**

Choose only ONE best answer.

**A**

Screened host

**B**

Bastion firewall

**C**

Proxy server

**D**

Dual homed host

**This answer is correct.**

**Which of the following are four basic types of Firewalls?**

Choose only ONE best answer.

**A**

Screening, bastion, dual-home, circuit level

**B**

Application gateway, bastion, dual-homed, screening

**C**

Packet filtering, application gateway, circuit level, stateful packet inspection

**D**

Stateful packet inspection, gateway, bastion, scre

**What type of IDS is Snort?**

Choose only ONE best answer.

**A**

Router based

**B**

Operating system based

**C**

Host based

**D**

Client based

**This answer is correct.**

**Which of the following is an advantage of the network host based configuration?**

Choose only ONE best answer.

**A**

It is resistant to IP spoofing

**B**

It is inexpensive or free

**C**

It is more secure

**D**

It has user authentication

**This answer is correct.**

**Why  a stateful packet inspection firewall is less susceptible to spoofing attacks?**

Choose only ONE best answer.

**A**

It examines the source IP of all packets

**B**

It automatically blocks spoofed packets

**C**

It requires user authentication

**D**

It requires client application authentication

**This answer is correct.**

**What type of firewall requires client applications to be authorised to connect?**

Choose only ONE best answer.

**A**

Screened gateway

**B**

Stateful packet inspection

**C**

Dual homed

**D**

Application gateway

**This answer is correct.**

**.**

QUESTION 9 OF 10

**Which of the following is a combination of firewalls?**

Choose only ONE best answer.

**A**

Screened firewalls

**B**

Router based firewalls

**C**

Dual homed firewalls

**D**

Bastion host firewalls

**This answer is correct.**

**Which of the following can be shipped preconfigured?**

Choose only ONE best answer.

**A**

Stateful packet inspection firewalls

**B**

Network host-based firewalls

**C**

Router-based firewalls

**D**

Dual-homed firewalls

**This answer is correct.**

**Which type of firewall is considered the most secure?**

Choose only ONE best answer.

**A**

Dual-homed

**B**

Stateful packet inspection

**C**

Circuit level gateway

**D**

Packet screening

**This answer is correct.**

**What is the most important security advantage to NAT**

Choose only ONE best answer.

**A**

It blocks incoming ICMP packets

**B**

It hides internal network addresses

**C**

It blocks all ICMP packets

**D**

By default allows only outbound connections

**This answer is correct.**

**.**

**Why might a proxy gateway be susceptible to a flood attack?**

Choose only ONE best answer.

**A**

It does not properly filter packets

**B**

It does not require user authentication

**C**

It allows multiple simultaneous connections

**D**

Its authentication method takes time and resources

**This answer is correct.**

**A system that is setup for attracting and monitoring intruders is called?**

Choose only ONE best answer.

**A**

Fly paper

**B**

Trap door

**C**

Honeypot

**D**

Hacker cage

**This answer is correct.**

**Specter aggressive mode tries to trace the attacker and gain its identity**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**IDS is an acronym for:**

Choose only ONE best answer.

**A**

Intrusion-detection system

**B**

Intrusion-deterrence system

**C**

Intrusion-deterrence service

**D**

Intrusion detection service

**This answer is correct.**

**A profiling technique that monitors how applications use resources is called?**

Choose only ONE best answer.

**A**

System monitoring

**B**

Resource profiling

**C**

Application monitoring

**D**

Executable profiling

**This answer is correct.**

**Attempting to attract intruders to a system setup for monitoring them is called?**

Choose only ONE best answer.

**A**

Intrusion deterrence

**B**

Intrusion detection

**C**

Intrusion banishment

**D**

Intrusion routing

**This answer is correct.**

NEXT

**Which of the following is NOT a profiling strategy used in anomaly detection?**

Choose only ONE best answer.

**A**

Threshold monitoring

**B**

Resource profiling

**C**

Executable profiling

**D**

System monitoring

**This answer is correct.**

**Specter is an advanced IDS system**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**A system that is setup for attracting and monitoring intruders is called?**

Choose only ONE best answer.

**A**

Intrusion detection

**B**

Banishment vigilance

**C**

User deflection

**D**

Intruder blocking

**This answer is incorrect.**

**A series of ICMP packets sent to your ports in sequence might indicate what?**

Choose only ONE best answer.

**A**

A DoS attack

**B**

A ping flood

**C**

A packet sniffer

**D**

A port scan

**This answer is correct.**

**What is another term for preemptive blocking?**

Choose only ONE best answer.

**A**

Intrusion detection

**B**

Banishment vigilance

**C**

User deflection

**D**

Intruder blocking

**This answer is correct.**

**Which of the following encryption algorithms is a block cipher and uses the Rijndael algorithm?**

Choose only ONE best answer.

**A**

DES

**B**

RSA

**C**

AES

**D**

NSA

**This answer is correct.**

**Which hashing algorithm do modern Windows systems use?**

Choose only ONE best answer.

**A**

SHA1

**B**

SHA2

**C**

LM

**D**

NTLM

**This answer is correct.**

**Blowfish is an asymmetric stream cipher**

Choose only ONE best answer.

**A**

True

**B**

Flase

**This answer is correct.**

**Which of the following is an encryption method developed by three mathematicians?**

Choose only ONE best answer.

**A**

PGP

**B**

DES

**C**

DSA

**D**

RSA

**This answer is correct.**

**What is the purpose of a certificate?**

Choose only ONE best answer.

**A**

To verify that software is virus free

**B**

To guarantee that a signature is valid

**C**

To validate the sender of a digital signature or software

**D**

To validate the recipient of a software.

**This answer is correct.**

**Which of the following uses key sizes equal to 128, 192 and 256 bits?**

Choose only ONE best answer.

**A**

DES

**B**

RSA

**C**

3DES

**D**

AES

**This answer is correct.**

**Secure Multipurpose Internet Mail Extensions (S/MIME) use X.509 certificates to secure e-mail communication**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**What is a digital signature?**

Choose only ONE best answer.

**A**

A piece of encrypted data added to other data to verify the sender

**B**

A scanned version of your signature, often in .jpg format

**C**

A signature that is entered via a digital pad or other device

**D**

A method for verifying the recipient of a document

**This answer is correct.**

**Which encryption algorithm uses a variable length symmetric key?**

Choose only ONE best answer.

**A**

RSA

**B**

Blowfish

**C**

DES

**D**

PGP

**This answer is correct.**

**Which of the following is a symmetric key system using blocks?**

Choose only ONE best answer.

**A**

RSA

**B**

DES

**C**

PGP

**D**

Diffie-Hellman

**This answer is correct.**

**PPTP is an acronym for which of the following?**

Choose only ONE best answer.

**A**

Point-to-Point Transmission Protocol

**B**

Point-to-Point Tunneling Protocol

**C**

Point-to-Point Transmission Procedure

**D**

Point-to-Point Tunneling Procedure

**This answer is correct.**

**What does L2TP stand for?**

Choose only ONE best answer.

**A**

Level 2 Transfer Protocol

**B**

Layer 2 Tunnelling Protocol

**C**

Level 2 Tunnelling Protocol

**D**

Level 2 Transfer Protocol

**This answer is correct.**

**Which authentication protocols are available under PPTP?**

Choose only ONE best answer.

**A**

MS-CHAP, PAP, SPAP

**B**

EAP, CHAP

**C**

PAP, EAM, MS-CHAP

**D**

SPAP, MS-CHAP

**This answer is correct.**

**The ESP Protocol provides data confidentiality and authentication.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is an important security feature in CHAP**

Choose only ONE best answer.

**A**

It periodically re-authenticates

**B**

It used 3DES encryption

**C**

It is immune to spoofing

**D**

It uses AES encryption

**This answer is correct.**

**Openswan is a VPN solution provided by CISCO.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is generally considered the least secure?**

Choose only ONE best answer.

**A**

PAP

**B**

SPAP

**C**

MS-CHAP

**D**

X-PAP

**This answer is correct.**

NEXT

**What is the purpose of IKE?**

Choose only ONE best answer.

**A**

Key exchange

**B**

Packet encryption

**C**

Header protection

**D**

Authentication

**This answer is correct.**

**PPTP is based on which protocol?**

Choose only ONE best answer.

**A**

SLIP

**B**

L2TP

**C**

IPSec

**D**

PPP

**This answer is correct.**

**Which of the following is a weakness in PPTP?**

Choose only ONE best answer.

**A**

Clear text passwords

**B**

No encryption

**C**

Used only with IP networks

**D**

Not supported on most platforms

**This answer is correct.**

**What is the purpose of IKE?**

Choose only ONE best answer.

**A**

Key exchange

**B**

Packet encryption

**C**

Header protection

**D**

Authentication

**This answer is correct.**

**What account lockout threshold does the NSA reccomends?**

Choose only ONE best answer.

**A**

5 tries

**B**

3 tries

**C**

4 tries

**D**

2 tries

**This answer is correct.**

**A Linux system has a repository of packages available to be installed on the system**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**What type of ecnryption does EFS utilize?**

Choose only ONE best answer.

**A**

Single key

**B**

Multi-alphabet

**C**

Public key encryption

**D**

 Secret algorithm proprietary to Microsoft

**This answer is correct.**

**What is the rule for unused services on any computer?**

Choose only ONE best answer.

**A**

Turn them off only if they are critical

**B**

Turn them off

**C**

Monitor them carefully

**D**

Configure them for minimal privileges

**This answer is correct.**

**Which of the following best describes the registry**

Choose only ONE best answer.

**A**

A relational database containing system settings

**B**

A database containing system settings

**C**

A database where software is registered

**D**

A relational database where software is registered

**This answer is correct.**

**What operating system require periodic patches?**

Choose only ONE best answer.

**A**

Linux

**B**

Windows

**C**

Mac OS X

**D**

All

**This answer is correct.**

**The command sudo find / -perm -4000 checks for the location of suid binaries**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**1.   What minimum password length does the NSA recommends?**

Choose only ONE best answer.

**A**

6

**B**

8

**C**

10

**D**

12

**This answer is correct.**

**1.   What level of privileges all users must have?**

Choose only ONE best answer.

**A**

Administrator

**B**

Guest

**C**

Most possible privileges

**D**

Least possible

**This answer is correct.**

**What maximum password age does Microsoft reccomends?**

Choose only ONE best answer.

**A**

20 days

**B**

3 months

**C**

1 year

**D**

42 days

**This answer is correct.**

**1.   What level of privileges all users must have?**

Choose only ONE best answer.

**A**

Administrator

**B**

Guest

**C**

Most possible privileges

**D**

Least possible

**This answer is incorrect.**

**What is heuristic scanning?**

Choose only ONE best answer.

**A**

Scanning using a rules-based approach

**B**

Scanning based on a virus definition file

**C**

Scanning only system management areas (registry, boot sector, etc.)

**D**

Scheduled scanning

**This answer is correct.**

**What is the most common method of virus propagation?**

Choose only ONE best answer.

**A**

On infected floppy disks

**B**

On infected CDs

**C**

Through instant messaging attachments

**D**

Through e-mail attachments

**This answer is correct.**

**What is active code scanning?**

Choose only ONE best answer.

**A**

Scanning that is occurring all the time (i.e., actively)

**B**

Scanning for active web elements (scripts, ActiveX, and so on)

**C**

Actively scanning for malicious code

**D**

Actively scanning for worms

**This answer is correct.**

**The first known ransomware was the 1995 PC Trojan**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**In the event of a virus infection, the first priority is to contact the IT department.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**The unfortunate side effect of heuristic scanning is that it can easily lead to false positives**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**In the context of viruses what is a .dat file?**

Choose only ONE best answer.

**A**

A file containing system information

**B**

A file that is infected

**C**

A file with corrupt data

**D**

A file with virus definitions

**This answer is correct.**

**What malicious activity did the Rombertik virus attempt?**

Choose only ONE best answer.

**A**

It overwrote the master boot record

**B**

It tried to overwrite parts of virus scanners

**C**

It tried to overwrite key system files

**D**

It sent out information about the infected computer

**This answer is correct.**

### QUESTION 9 OF 10

**Which of the following should be the least important consideration when purchasing antivirus software?**

Choose only ONE best answer.

**A**

The type of scanning the software uses

**B**

How quickly the software updates in response to new viruses

**C**

How easy it is to configure and use

**D**

Cost of the software

**This answer is correct.**

**Which of the below are famous Trojan Horses? (Choose two)**

Choose ALL answers that apply.

**A**

Netbus

**B**

Shodan

**C**

Censys

**D**

FinFisher

**This answer is correct.**

### QUESTION 9 OF 10

**Which of the following should be the least important consideration when purchasing antivirus software?**

Choose only ONE best answer.

**A**

The type of scanning the software uses

**B**

How quickly the software updates in response to new viruses

**C**

How easy it is to configure and use

**D**

Cost of the software

**This answer is incorrect.**

### QUESTION 1 OF 10

**Always open email attachments coming from unknown sources.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following should be recommended as acceptable e-mail attachments?**

Choose only ONE best answer.

**A**

Flash animations

**B**

Excel spreadsheets from a colleague

**C**

Attachments the user expected

**D**

Plain text attachments from known sources

**This answer is correct.**

**Instant messaging can be used not only for business communication but also for personall communication.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is NOT an example of a user password policy?**

Choose only ONE best answer.

**A**

Users may not keep copies of passwords in their office

**B**

Passwords must be eight characters long

**C**

Users may share passwords only with their assistants

**D**

Passwords may not be shared with any employee

**This answer is correct.**

**What is the best rule of thumb in access control?**

Choose only ONE best answer.

**A**

Allow the most access you can securely give

**B**

Allow the least access job requirements allow

**C**

Standardise access for all users

**D**

Strictly limit access for most users

**This answer is correct.**

**Which of the following is the best reason users should be prohibited from installing software?**

Choose only ONE best answer.

**A**

They may not install it correctly, which could cause security problems for the workstation

**B**

They may install software that disables existing security programs on your machine

**C**

Software installation is often complex and should be done by professionals

**D**

If a user’s account does not have privileges to install, then it is likely that a Trojan horse will not be inadvertently installed under her account

**This answer is correct.**

**What should an employee do if she believes her password has been revealed to another party?**

Choose only ONE best answer.

**A**

If it is a trusted employee or friend just ignore it

**B**

Change her password immediately

**C**

Notify the IT department

**D**

Ignore it

**This answer is correct.**

**1.   Logon accounts, VPN, network and any other resources should NOT be disabled for leaving employees.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Passwords must always be shared with any person for any reason.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is NOT an area user policies need to cover.**

Choose only ONE best answer.

**A**

Minimum length of passwords

**B**

A description of websites user may or may not visit

**C**

If and when to share passwords

**D**

What to do when the user believes the password has been compromised

**This answer is correct.**

**Virus attacks utilize uncommon ports to gain access to a system.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is the most fundamental aspect of security?**

Choose only ONE best answer.

**A**

Shutting down unused services

**B**

Implementing an IDS

**C**

Patching the operating system

**D**

Conducting periodic security audits

**This answer is correct.**

**Which of the following best describes risk assessment.**

Choose only ONE best answer.

**A**

Scanning a single server to find vulnerabilities.

**B**

Scanning the network to find open ports

**C**

Evaluating the security of a network

**D**

Patching an operating system

**This answer is correct.**

**All employees within a company must have access to the server room.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Open Web Application Security Project is the standard for risk assessment.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**What is NOT a primary reason for documenting your security activity and audits?**

Choose only ONE best answer.

**A**

To prove due diligence in case of litigation

**B**

To provide information in case of any external or internal audit

**C**

To get new personnel up to speed on the current state of security

**D**

To demonstrate how much work the network administrators usually do

**This answer is correct.**

**You should have a document that lists physical security is in place**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which of the following is the least necessary security device/software**

Choose only ONE best answer.

**A**

Firewall at the perimeter

**B**

Anti-spyware on all machines

**C**

Antivirus on all machines

**D**

Encryption for all internal transmissions

**This answer is correct.**

### QUESTION 9 OF 10

**All visitors to the building must be logged in and escorted by an employee at all times.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Ports 1 through 1024 are NOT assigned and used for well-known protocols**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which U.S. standard should you consult to guide you in developing security policies?**

Choose only ONE best answer.

**A**

NIST SP 800-35

**B**

NIST SP 800-14

**C**

ISO 27004

**D**

ISO 27008

**This answer is correct.**

**What is the acronym of GDPR?**

Choose only ONE best answer.

**A**

Generic Description Protection Regulatory

**B**

General Data Protection Regulation

**C**

General Description Protection Regulation

**D**

General Data Protective Regulation

**This answer is correct.**

**PCI DSS is a proprietary information security standard for organisations that handle cardholder data.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**What does the Step 3 in NIST 800-30 Rev.1 clarifies?**

Choose only ONE best answer.

**A**

Impact Analysis

**B**

Control Analysis

**C**

Threat Identification

**D**

Vulnerability Identification

**This answer is correct.**

**Which of the following describes ISO 27003?**

Choose only ONE best answer.

**A**

Network Security

**B**

Digital Forensics

**C**

ISMS Implementation

**D**

Risk Management

**This answer is correct.**

**Which U.S. standard covers risk assessment?**

Choose only ONE best answer.

**A**

ISO 27037

**B**

NIST SP 800-30

**C**

ISO 27005

**D**

NIST SP 800-14

**This answer is correct.**

**NIST SP 800-30 Rev.1 is a standard for conducting risk assessments.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**ISO 27035 describes incident management.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which standard defines Management System Auditing?**

Choose only ONE best answer.

**A**

ISO 27007

**B**

NIST SP 800-30

**C**

NIST SP 800-35

**D**

ISO 27004

**This answer is correct.**

**What standard should you consult for managing incident response?**

Choose only ONE best answer.

**A**

ISO 27035

**B**

NIST SP 800-35

**C**

NIST SP 800-14

**D**

ISO 27004

**This answer is correct.**

**How should a company test the integrity of its backup data**

Choose only ONE best answer.

**A**

Using testing software

**B**

Using software to recover deleted files

**C**

Restoring the backup

**D**

By conducting another backup

**This answer is correct.**

**The disaster recovery plan has as a major goal to get the organisation back to full functionality.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which RAID level uses mirroring?**

Choose only ONE best answer.

**A**

1

**B**

2

**C**

4

**D**

5

**This answer is correct.**

**RAID 0 does not offer fault tolerance**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**Which RAID level offers dual parity**

Choose only ONE best answer.

**A**

3

**B**

4

**C**

5

**D**

6

**This answer is correct.**

**Which of the following is NOT considered a disaster?**

Choose only ONE best answer.

**A**

Hard drive crash

**B**

Server maintenance

**C**

Fire

**D**

Hacker deleted critical files

**This answer is correct.**

**Cameras must be placed so that they have an unobstructed view of the areas you want to monitor.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**The plan for recovering from an IT disaster and having the IT infrastructure back in operation is called?**

Choose only ONE best answer.

**A**

BIA

**B**

DRP

**C**

RTO

**D**

RPO

**This answer is correct.**

NEXT

**have a locked door or barrier requiring employee ID.**

Choose only ONE best answer.

**A**

True

**B**

False

**This answer is correct.**

**What is a mantrap?**

Choose only ONE best answer.

**A**

Fire suppression device

**B**

A logical access control mechanism

**C**

A trusted security domain

**D**

A double door facility used for physical access control

**This answer is correct.**

**If you send a SYN to an open port what is the correct response?**

Choose only ONE best answer.

**A**

SYN

**B**

ACK

**C**

FIN

**D**

SYN/ACK

**This answer is correct.**

### QUESTION 2 OF 5

**Julie has been hired to perform a penetration test on xyz.com. She begins by looking at IP address ranges owned by the company and details of domain name registration. She then goes to news groups and financial websites to see whether any of the company’s sensitive information or technical details are online. What is Julie doing?**

Choose only ONE best answer.

**A**

Passive Information Gathering

**B**

Active Information Gathering

**C**

Attack Phase

**D**

Vulnerability Mapping

**This answer is correct.**

NEXT

**From a port scanning you identified that port 88 is open. What does this tell you?**

Choose only ONE best answer.

**A**

The target system uses Telnet

**B**

The target system uses Kerberos authentication

**C**

The target system uses SMB

**D**

The target system uses SNMP

**This answer is correct.**

**Trying to identify machines on a target network is called?**

Choose only ONE best answer.

**A**

Enumeration

**B**

Scanning

**C**

Checking

**D**

Assessing

**This answer is correct.**

**Which of the following is the most reliable type of scan?**

Choose only ONE best answer.

**A**

SYN

**B**

Passive

**C**

FIN

**D**

Connect