KEAMANAN SISTEM INFORMASI

Cyber Threat Management (CyberTM) Course Final Exam

Disusun untuk Memenuhi Tugas Mata Kuliah Manajemen Jaringan Komputer

Oleh:

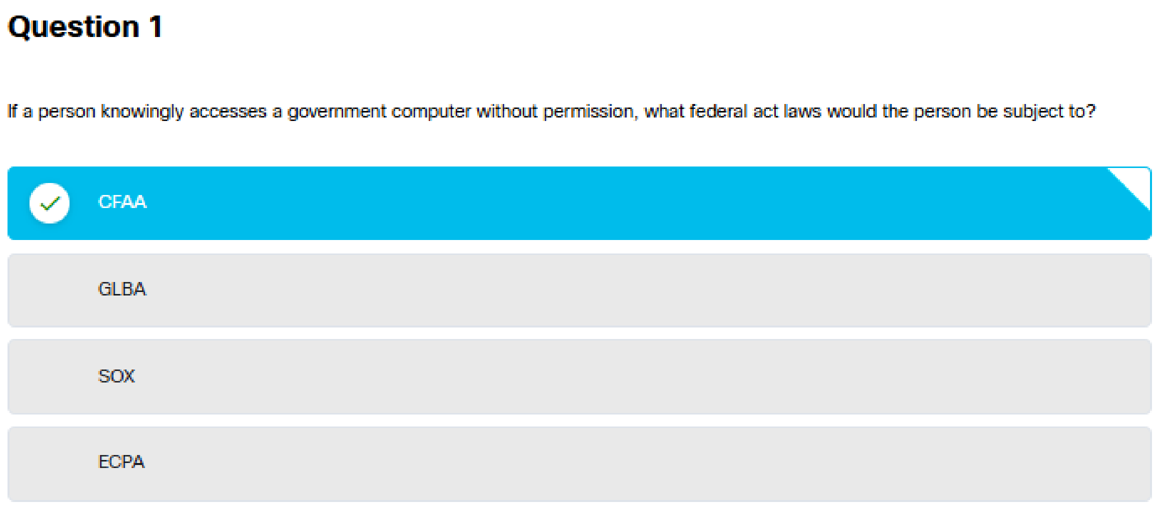
Wiraswanti Rismanda Putri
NIM: 2141762021

PROGRAM STUDI D-IV SISTEM INFORMASI BISNIS

JURUSAN TEKNOLOGI INFORMASI

POLITEKNIK NEGERI MALANG

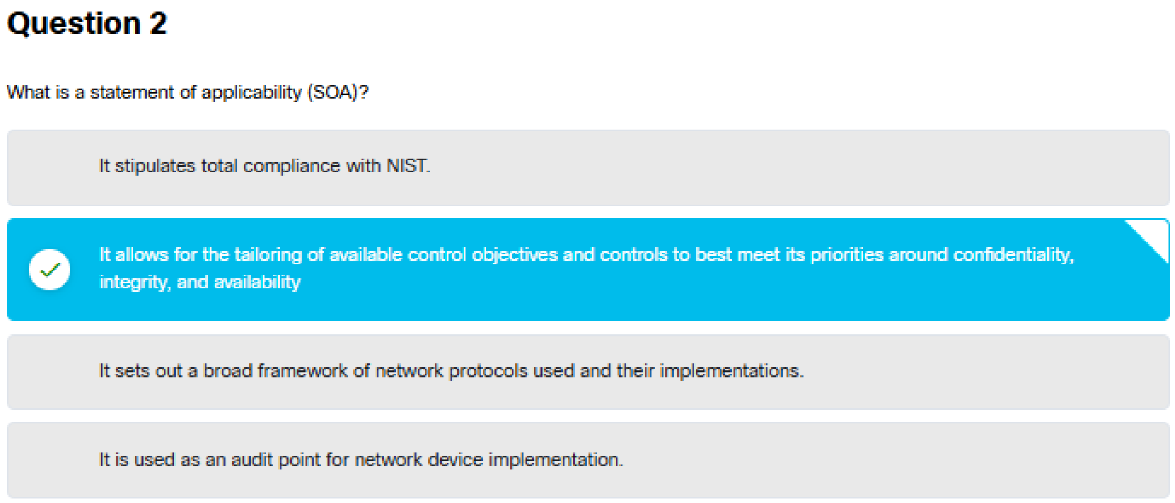
2024



Question 1

If a person knowingly accesses a government computer without permission, what federal act laws would the person be subject to?

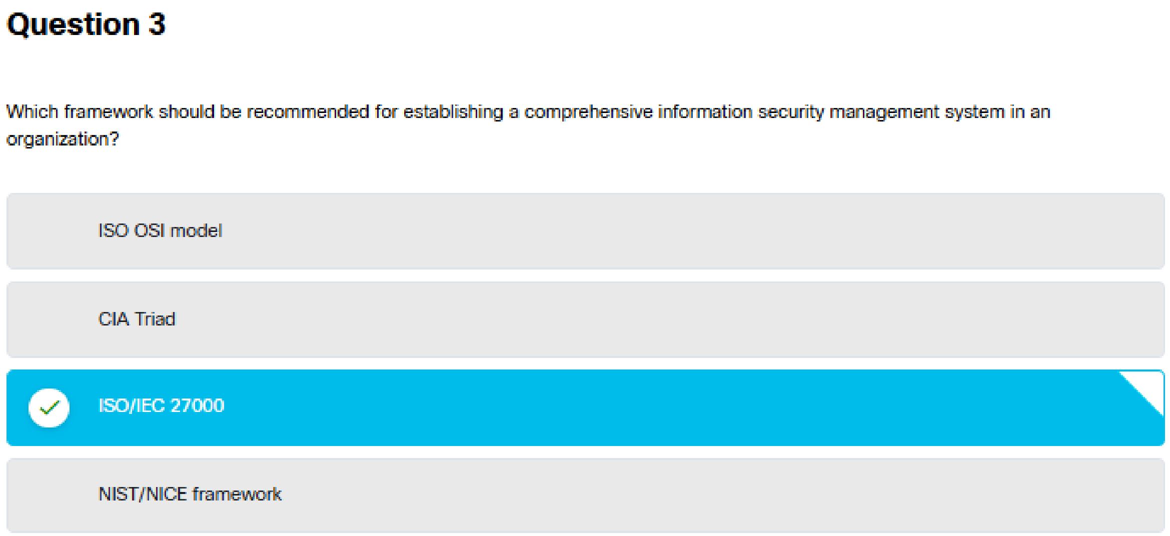
- ✓ CFAA
- GLBA
- SOX
- ECPA



Question 2

What is a statement of applicability (SOA)?

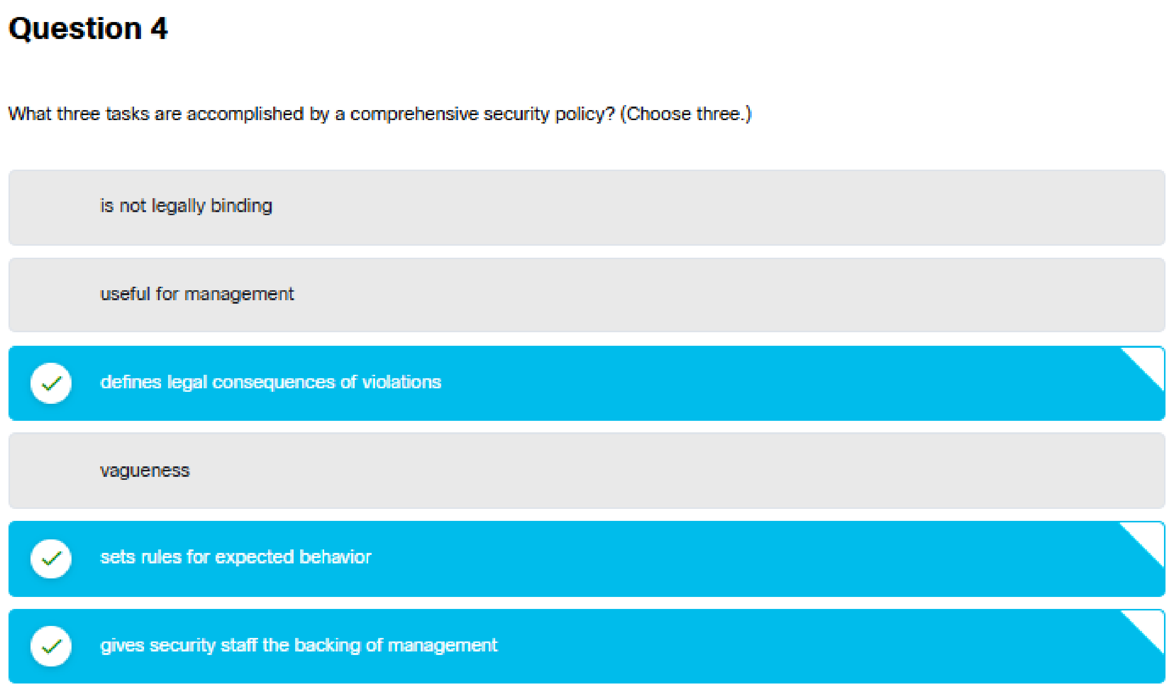
- It stipulates total compliance with NIST.
- ✓ It allows for the tailoring of available control objectives and controls to best meet its priorities around confidentiality, integrity, and availability
- It sets out a broad framework of network protocols used and their implementations.
- It is used as an audit point for network device implementation.



Question 3

Which framework should be recommended for establishing a comprehensive information security management system in an organization?

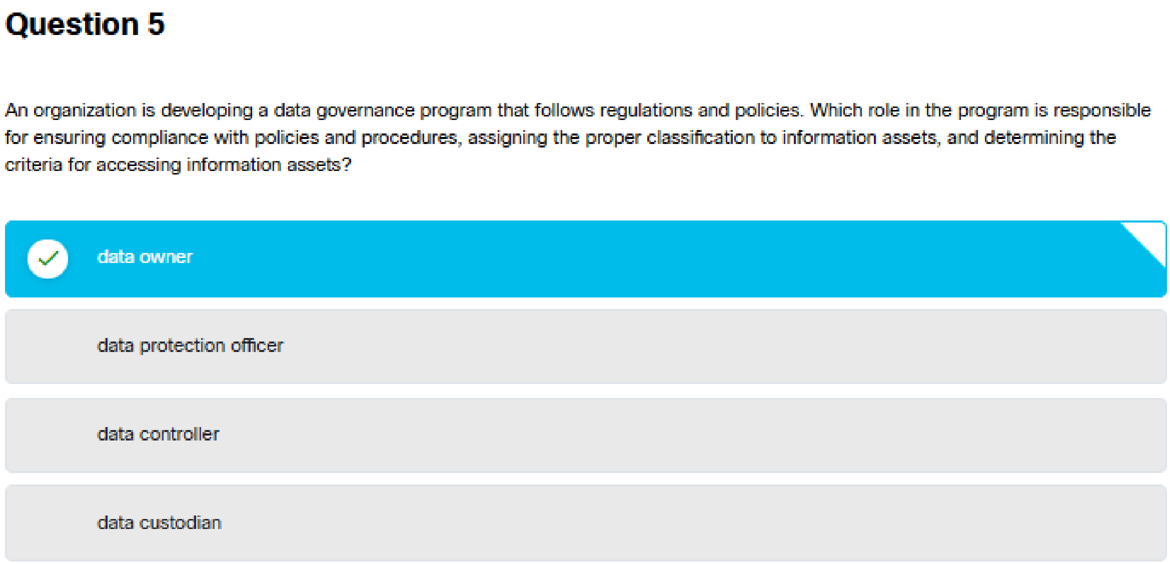
- ISO OSI model
- CIA Triad
- ✓ ISO/IEC 27000
- NIST/NICE framework



Question 4

What three tasks are accomplished by a comprehensive security policy? (Choose three.)

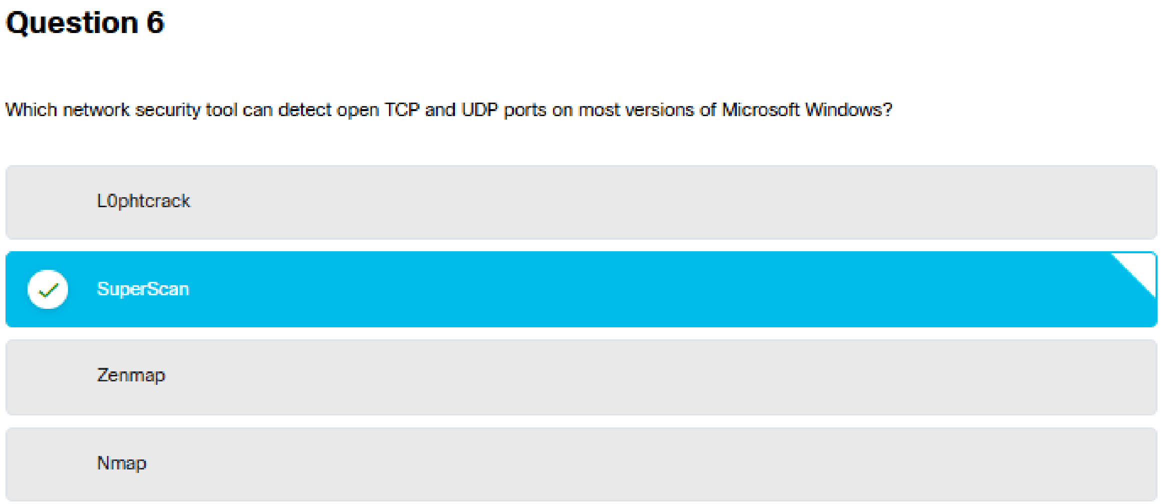
- is not legally binding
- useful for management
- ✓ defines legal consequences of violations
- vagueness
- ✓ sets rules for expected behavior
- ✓ gives security staff the backing of management



Question 5

An organization is developing a data governance program that follows regulations and policies. Which role in the program is responsible for ensuring compliance with policies and procedures, assigning the proper classification to information assets, and determining the criteria for accessing information assets?

- ✓ data owner
- data protection officer
- data controller
- data custodian



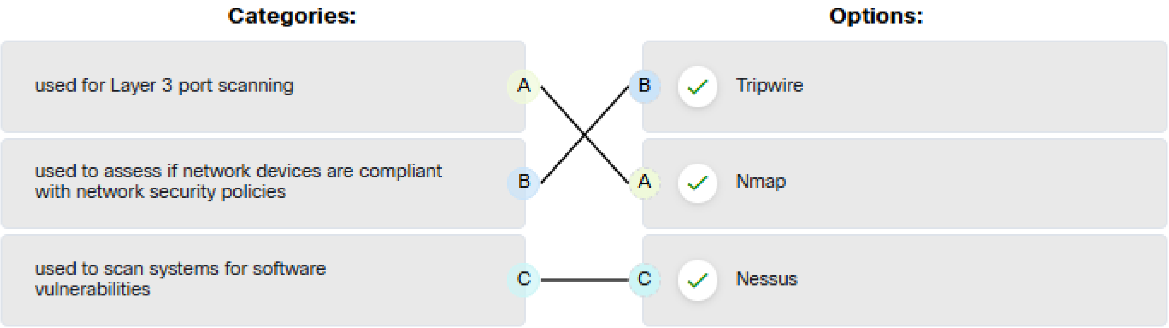
Question 6

Which network security tool can detect open TCP and UDP ports on most versions of Microsoft Windows?

- L0phtcrack
- ✓ SuperScan
- Zenmap
- Nmap

Question 7

Match the network security testing tool with the correct function. (Not all options are used.)



Categories:			Options:
used for Layer 3 port scanning	A	B	✓ Tripwire
used to assess if network devices are compliant with network security policies	B	A	✓ Nmap
used to scan systems for software vulnerabilities	C	C	✓ Nessus

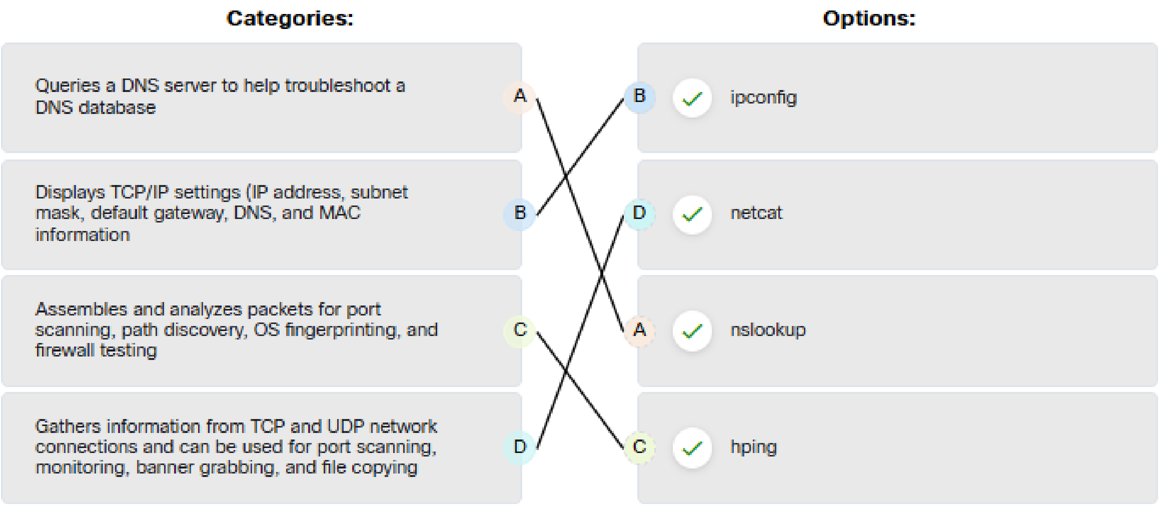
Question 8

What are two tasks that can be accomplished with the Nmap and Zenmap network tools? (Choose two.)

- ✓ Identification of Layer 3 protocol support on hosts
- ✓ TCP and UDP port scanning
- Password auditing
- Password recovery
- Validation of IT system configuratio

Question 9

Match the command line tool with its description.



Categories:			Options:
Queries a DNS server to help troubleshoot a DNS database	A	B	✓ ipconfig
Displays TCP/IP settings (IP address, subnet mask, default gateway, DNS, and MAC information	B	D	✓ netcat
Assembles and analyzes packets for port scanning, path discovery, OS fingerprinting, and firewall testing	C	A	✓ nslookup
Gathers information from TCP and UDP network connections and can be used for port scanning, monitoring, banner grabbing, and file copying	D	C	✓ hping

Question 10

What type of security test uses simulated attacks to determine possible consequences of a real threat?

- vulnerability scanning
- network scanning
- ✓ penetration testing
- integrity checking

Question 11

Which type of controls help uncover new potential threats?

- Preventive controls
- ✓ Detective controls
- Corrective controls

Question 12

As a Cybersecurity Analyst, it is very important to keep current. It was suggested by some colleagues that NewsBites contains many good current articles to read. What network security organization maintains this weekly digest?

- MITRE
- ✓ SANDS
- CIS
- (ISC)^2

Question 13

What is a characteristic of CybOX?

- ✓ It is a set of standardized schemata for specifying, capturing, characterizing, and communicating events and properties of network operations.
- It enables the real-time exchange of cyberthreat indicators between the U.S. Federal Government and the private sector.
- It is the specification for an application layer protocol that allows the communication of CTI over HTTPS.
- It is a set of specifications for exchanging cyberthreat information between organizations.

Question 14

What three services are offered by FireEye? (Choose three.)

- creates firewall rules dynamically
- subjects all traffic to deep packet inspection analysis
- ✓ blocks attacks across the web
- ✓ identifies and stops email threat vectors
- ✓ identifies and stops latent malware on files
- deploys incident detection rule sets to network security tools

Question 15

Which security organization maintains a list of common vulnerabilities and exposures (CVE) and is used by prominent security organizations?

- ✓ MITRE
- SecurityNewsWire
- CIS
- SANDS

Question 16

Which class of metric in the CVSS Base Metric Group defines the features of the exploit such as the vector, complexity, and user interaction required by the exploit?

- Exploit Code Maturity
- ✓ Exploitability
- Impact
- Modified Base

Question 17

When a server profile for an organization is being established, which element describes the TCP and UDP daemons and ports that are allowed to be open on the server?

- software environment
- service accounts
- critical asset address space
- ✓ listening ports

Question 18

Which two classes of metrics are included in the CVSS Base Metric Group? (Choose two.)

- Exploit Code Maturity
- ✓ Impact metrics
- Modified Base
- ✓ Exploitability
- Confidentiality Requirement

Question 19

Which step in the Vulnerability Management Life Cycle performs inventory of all assets across the network and identifies host details, including operating system and open services?

- [✓ discover]
- prioritize assets
- assess
- remediate

Question 20

The IT security personnel of an organization notice that the web server deployed in the DMZ is frequently targeted by threat actors. The decision is made to implement a patch management system to manage the server. Which risk management strategy method is being used to respond to the identified risk?

- risk avoidance
- [✓ risk reduction]
- risk sharing
- risk retention

Question 21

Your risk manager just distributed a chart that uses three colors to identify the level of threat to key assets in the information security systems. Red represents high level of risk, yellow represents average level of threat and green represents low level of threat. What type of risk analysis does this chart represent?

- loss analysis
- quantitative analysis
- [✓ qualitative analysis]
- exposure factor analysis

Question 22

What is the first step taken in risk assessment?

- Establish a baseline to indicate risk before security controls are implemented.
- Perform audits to verify threats are eliminated.
- Compare to any ongoing risk assessment as a means of evaluating risk management effectiveness.
- ✓ Identify threats and vulnerabilities and the matching of threats with vulnerabilities.

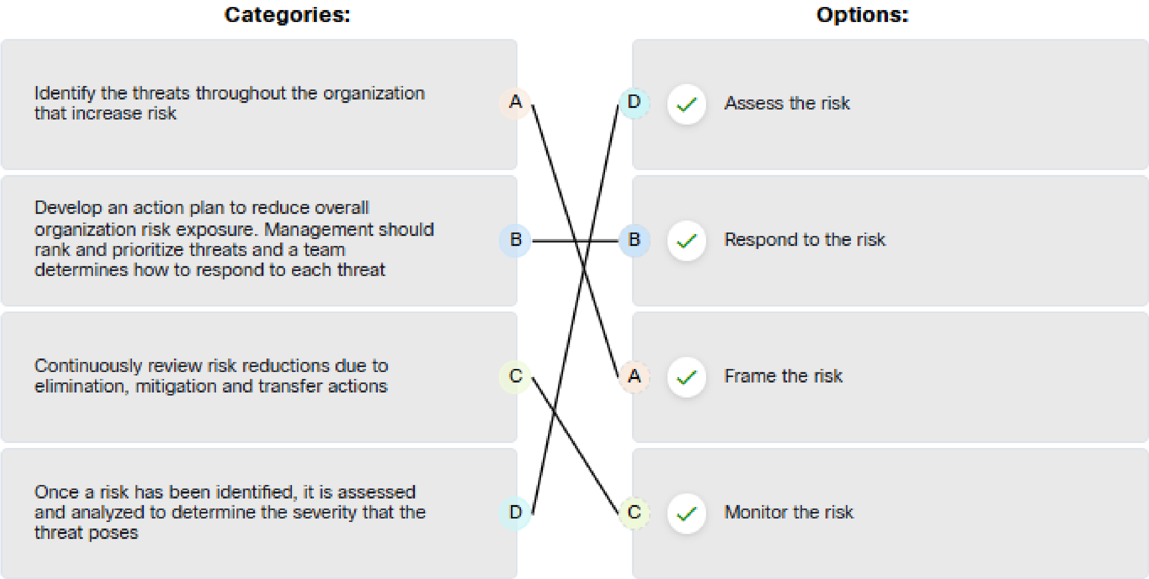
Question 23

A company manages sensitive customer data for multiple clients. The current authentication mechanism to access the database is username and passphrase. The company is reviewing the risk of employee credential compromise that may lead to a data breach and decides to take action to mitigate the risk before further actions can be taken to eliminate the risk. Which action should the company take for now?

- ✓ Implement multi-factor authentication.
- Install fingerprint or retinal scanners.
- Purchase an insurance policy.
- Enhance data encryption with an advanced algorithm.

Question 24

Match the stages in the risk management process to the description.



Categories:

Identify the threats throughout the organization that increase risk A

Develop an action plan to reduce overall organization risk exposure. Management should rank and prioritize threats and a team determines how to respond to each threat B

Continuously review risk reductions due to elimination, mitigation and transfer actions C

Once a risk has been identified, it is assessed and analyzed to determine the severity that the threat poses D

Options:

D ✓ Assess the risk

B ✓ Respond to the risk

A ✓ Frame the risk

C ✓ Monitor the risk

Question 25

The manager of a new data center requisitions magnetic door locks. The locks will require employees to swipe an ID card to open. Which type of security control is being implemented?

- corrective
- compensative
- [✓ preventive]
- recovery

Question 26

To ensure that the chain of custody is maintained, what three items should be logged about evidence that is collected and analyzed after a security incident has occurred? (Choose three.)

- ✓ location of all evidence
- ✓ serial numbers and hostnames of devices used as evidence
- measures used to prevent an incident
- ✓ time and date the evidence was collected
- extent of the damage to resources and assets
- vulnerabilities that were exploited in an attack

Question 27

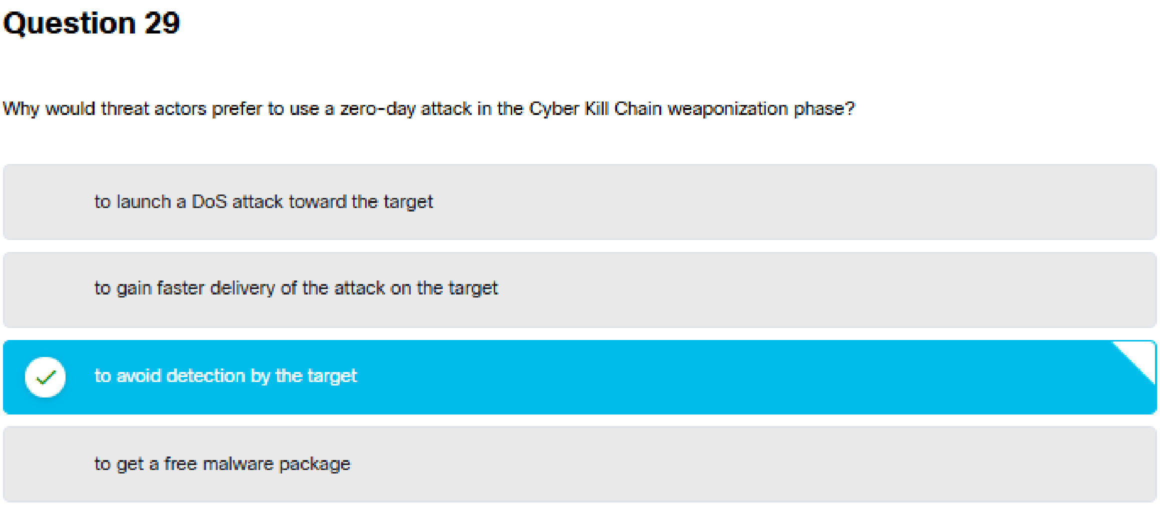
Which meta-feature element in the Diamond Model classifies the general type of intrusion event?

- ✓ methodology
- results
- phase
- direction

Question 28

A threat actor has identified the potential vulnerability of the web server of an organization and is building an attack. What will the threat actor possibly do to build an attack weapon?

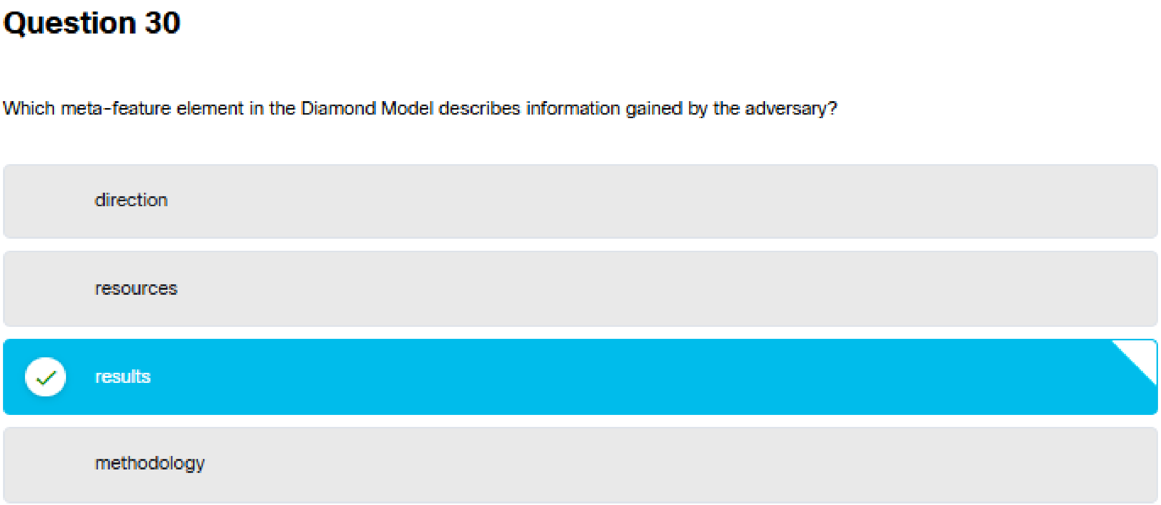
- Install a webshell on the web server for persistent access.
- Create a point of persistence by adding services.
- Collect credentials of the web server developers and administrators.
- ✓ Obtain an automated tool in order to deliver the malware payload through the vulnerability.



Question 29

Why would threat actors prefer to use a zero-day attack in the Cyber Kill Chain weaponization phase?

- to launch a DoS attack toward the target
- to gain faster delivery of the attack on the target
- ✓ to avoid detection by the target
- to get a free malware package

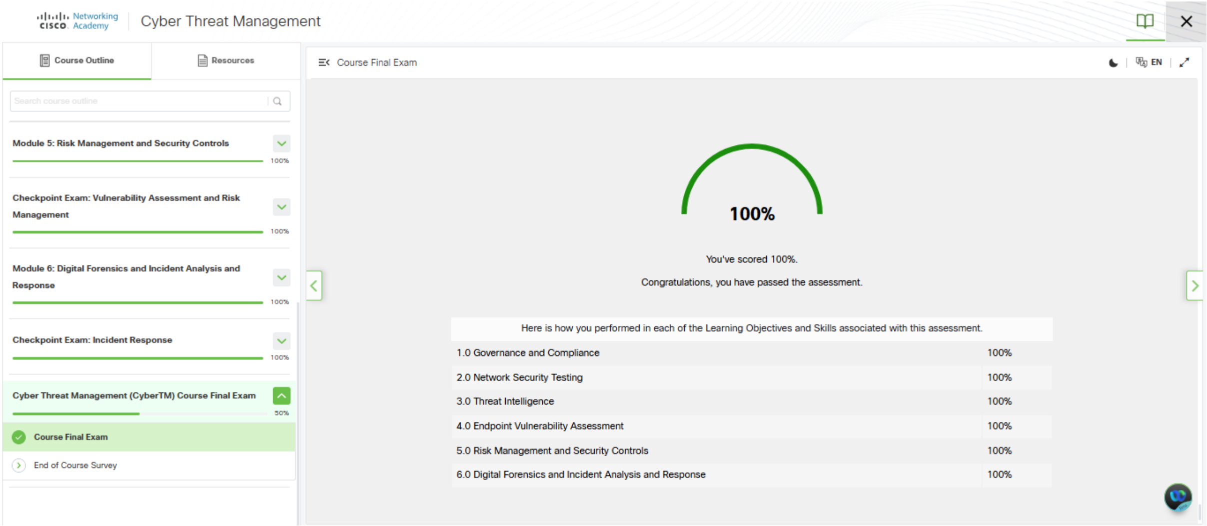


Question 30

Which meta-feature element in the Diamond Model describes information gained by the adversary?

- direction
- resources
- ✓ results
- methodology

Hasil Akhir



Cyber Threat Management

Course Outline | Resources

Search course outline

Module 5: Risk Management and Security Controls 100%

Checkpoint Exam: Vulnerability Assessment and Risk Management 100%

Module 6: Digital Forensics and Incident Analysis and Response 100%

Checkpoint Exam: Incident Response 100%

Cyber Threat Management (CyberTM) Course Final Exam 50%

Course Final Exam

End of Course Survey

Course Final Exam

EN

100%

You've scored 100%.

Congratulations, you have passed the assessment.

Here is how you performed in each of the Learning Objectives and Skills associated with this assessment.	
1.0 Governance and Compliance	100%
2.0 Network Security Testing	100%
3.0 Threat Intelligence	100%
4.0 Endpoint Vulnerability Assessment	100%
5.0 Risk Management and Security Controls	100%
6.0 Digital Forensics and Incident Analysis and Response	100%