CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (2A-2B-2C)

AGENDA

- **2A - Threat Actors (13)**
- **2B - Attack Surfaces (2)**
- **2C - Social Engineering (12)**
- **TOTAL: 27**

2A - Threat Actors

2A - Threat Actors

NO.1 Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?

A. Hacktivists
B. Script kiddies
C. Competitors
D. Shadow IT

2A - Threat Actors

NO.1 Which of the following is most likely associated with introducing vulnerabilities on a corporate network by the deployment of unapproved software?

A. Hacktivists
B. Script kiddies
C. Competitors
D. Shadow IT

2A - Threat Actors

NO.2 Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist

2A - Threat Actors

NO.2 Which of the following threat actors is the most likely to use large financial resources to attack critical systems located in other countries?

A. Insider
B. Unskilled attacker
C. Nation-state
D. Hacktivist

2A - Threat Actors

NO.3 Which of the following is a hardware-specific vulnerability?

A. Firmware version
B. Buffer overflow
C. SQL injection
D. Cross-site scripting

2A - Threat Actors

NO.3 Which of the following is a hardware-specific vulnerability?

A. Firmware version
B. Buffer overflow
C. SQL injection
D. Cross-site scripting

2A - Threat Actors

NO.4 Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist
B. Whistleblower
C. Organized crime
D. Unskilled attacker

2A - Threat Actors

NO.4 Which of the following threat actors is the most likely to be hired by a foreign government to attack critical systems located in other countries?

A. Hacktivist
B. Whistleblower
C. Organized crime
D. Unskilled attacker

2A - Threat Actors

NO.5 An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device. Which of the following best describes the user's activity?

A. Penetration testing
B. Phishing campaign
C. External audit
D. Insider threat

2A - Threat Actors

NO.5 An administrator was notified that a user logged in remotely after hours and copied large amounts of data to a personal device. Which of the following best describes the user's activity?

A. Penetration testing
B. Phishing campaign
C. External audit
D. Insider threat

2A - Threat Actors

NO.6 The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

2A - Threat Actors

NO.6 The marketing department set up its own project management software without telling the appropriate departments. Which of the following describes this scenario?

A. Shadow IT
B. Insider threat
C. Data exfiltration
D. Service disruption

2A - Threat Actors

NO.7 A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

2A - Threat Actors

NO.7 A Chief Information Security Officer (CISO) wants to explicitly raise awareness about the increase of ransomware-as-a-service in a report to the management team. Which of the following best describes the threat actor in the CISO's report?

A. Insider threat
B. Hacktivist
C. Nation-state
D. Organized crime

2A - Threat Actors

NO.8 A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.

2A - Threat Actors

NO.8 A security analyst receives alerts about an internal system sending a large amount of unusual DNS queries to systems on the internet over short periods of time during non-business hours. Which of the following is most likely occurring?

A. A worm is propagating across the network.
B. Data is being exfiltrated.
C. A logic bomb is deleting data.
D. Ransomware is encrypting files.

2A - Threat Actors

NO.9 An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker

2A - Threat Actors

NO.9 An administrator discovers that some files on a database server were recently encrypted. The administrator sees from the security logs that the data was last accessed by a domain user. Which of the following best describes the type of attack that occurred?

A. Insider threat
B. Social engineering
C. Watering-hole
D. Unauthorized attacker

2A - Threat Actors

NO.10 A department is not using the company VPN when accessing various company-related services and systems.

Which of the following scenarios describes this activity?

A. Espionage
B. Data exfiltration
C. Nation-state attack
D. Shadow IT

2A - Threat Actors

NO.10 A department is **not using the company VPN** when accessing various company-related services and systems.

Which of the following scenarios describes this activity?

A. Espionage
B. Data exfiltration
C. Nation-state attack
D. Shadow IT

2A - Threat Actors

NO.11 An organization maintains intellectual property that it wants to protect.

Which of the following concepts would be most beneficial to add to the company's security awareness training program?

A. Insider threat detection
B. Simulated threats
C. Phishing awareness
D. Business continuity planning

2A - Threat Actors

NO.11 An organization **maintains intellectual property** that it wants to protect.

Which of the following concepts would be most beneficial to add to the company's security awareness training program?

A. Insider threat detection
B. Simulated threats
C. Phishing awareness
D. Business continuity planning

2A - Threat Actors

NO.12 After performing an assessment, an analyst wants to provide a risk rating for the findings.

Which of the following concepts should most likely be considered when calculating the ratings?

A. Owners and thresholds
B. Impact and likelihood
C. Appetite and tolerance
D. Probability and exposure factor

2A - Threat Actors

NO.12 After performing an assessment, an analyst wants to **provide a risk rating for the findings.**

Which of the following concepts should most likely be considered when calculating the ratings?

A. Owners and thresholds
B. Impact and likelihood
C. Appetite and tolerance
D. Probability and exposure factor

2A - Threat Actors

NO.13 Which of the following threat vectors is most commonly utilized by insider threat actors attempting data exfiltration?

A. Unidentified removable devices
B. Default network device credentials
C. Spear phishing emails
D. Impersonation of business units through typosquatting

2A - Threat Actors

NO.13 Which of the following threat vectors is most commonly utilized by **insider threat actors** attempting data exfiltration?

A. Unidentified removable devices

B. Default network device credentials

C. Spear phishing emails

D. Impersonation of business units through typosquatting

2B - Attack Surfaces

2B - Attack Surfaces

NO.1 After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access
B. Routing protocols
C. VLANs
D. Web-based administration

2B - Attack Surfaces

NO.1 After a recent vulnerability scan, a security engineer needs to harden the routers within the corporate network. Which of the following is the most appropriate to disable?

A. Console access
B. Routing protocols
C. VLANs
D. Web-based administration

2B - Attack Surfaces

NO.2 Which of the following is the most common data loss path for an air-gapped network?

A. Bastion host
B. Unsecured Bluetooth
C. Unpatched OS
D. Removable devices

2B - Attack Surfaces

NO.2 Which of the following is the most common data loss path for an air-gapped network?

A. Bastion host
B. Unsecured Bluetooth
C. Unpatched OS
D. Removable devices

2C - Social Engineering

2C - Social Engineering

NO.1 After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling

2C - Social Engineering

NO.1 After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

A. Insider threat
B. Email phishing
C. Social engineering
D. Executive whaling

2C - Social Engineering

NO.2 83 An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting
B. Phishing
C. Impersonation
D. Vishing
E. Smishing
F. Misinformation

2C - Social Engineering

NO.2 83 An employee receives a text message that appears to have been sent by the payroll department and is asking for credential verification. Which of the following social engineering techniques are being attempted? (Choose two.)

A. Typosquatting
B. Phishing
C. Impersonation
D. Vishing
E. Smishing
F. Misinformation

2C - Social Engineering

NO.3 Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address." Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

2C - Social Engineering

NO.3 Several employees received a fraudulent text message from someone claiming to be the Chief Executive Officer (CEO). The message stated: "I'm in an airport right now with no access to email. I need you to buy gift cards for employee recognition awards. Please send the gift cards to following email address." Which of the following are the best responses to this situation? (Choose two).

A. Cancel current employee recognition gift cards.
B. Add a smishing exercise to the annual company training.
C. Issue a general email warning to the company.
D. Have the CEO change phone numbers.
E. Conduct a forensic investigation on the CEO's phone.
F. Implement mobile device management.

2C - Social Engineering

NO.4 An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

2C - Social Engineering

NO.4 An employee clicked a link in an email from a payment website that asked the employee to update contact information. The employee entered the log-in information but received a "page not found" error message. Which of the following types of social engineering attacks occurred?

A. Brand impersonation
B. Pretexting
C. Typosquatting
D. Phishing

2C - Social Engineering

NO.5 An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

A. Vishing
B. Smishing
C. Pretexting
D. Phishing

2C - Social Engineering

NO.5 An employee receives a text message from an unknown number claiming to be the company's Chief Executive Officer and asking the employee to purchase several gift cards. Which of the following types of attacks does this describe?

A. Vishing
B. Smishing
C. Pretexting
D. Phishing

2C - Social Engineering

NO.6 Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing

2C - Social Engineering

NO.6 Malware spread across a company's network after an employee visited a compromised industry blog. Which of the following best describes this type of attack?

A. Impersonation
B. Disinformation
C. Watering-hole
D. Smishing

2C - Social Engineering

NO.7 Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
B. Employees who open an email attachment receive messages demanding payment in order to access files.
C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

2C - Social Engineering

NO.7 Which of the following scenarios describes a possible business email compromise attack?

A. An employee receives a gift card request in an email that has an executive's name in the display field of the email.
B. Employees who open an email attachment receive messages demanding payment in order to access files.
C. A service desk employee receives an email from the HR director asking for log-in credentials to a cloud administrator account.
D. An employee receives an email with a link to a phishing site that is designed to look like the company's email portal.

2C - Social Engineering

NO.8 An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

2C - Social Engineering

NO.8 An attacker posing as the Chief Executive Officer calls an employee and instructs the employee to buy gift cards. Which of the following techniques is the attacker using?

A. Smishing
B. Disinformation
C. Impersonating
D. Whaling

2C - Social Engineering

NO.9 Which of the following are common VoIP-associated vulnerabilities? (Choose two).

A. SPIM
B. Vishing
C. VLAN hopping
D. Phishing
E. DHCP snooping
F. Tailgating

2C - Social Engineering

NO.9 Which of the following are common VoIP-associated vulnerabilities? (Choose two).

A. SPIM
B. Vishing
C. VLAN hopping
D. Phishing
E. DHCP snooping
F. Tailgating

2C - Social Engineering

NO.10 An accounting clerk sent money to an attacker's bank account after receiving fraudulent instructions to use a new account.

Which of the following would most likely prevent this activity in the future?

A. Standardizing security incident reporting
B. Executing regular phishing campaigns
C. Implementing insider threat detection measures
D. Updating processes for sending wire transfers

2C - Social Engineering

NO.10 An accounting clerk **sent money to an attacker's bank account** after receiving fraudulent instructions to use a new account.

Which of the following would most likely prevent this activity in the future?

A. Standardizing security incident reporting
B. Executing regular phishing campaigns
C. Implementing insider threat detection measures
D. Updating processes for sending wire transfers

2C - Social Engineering

NO.11 An employee in the accounting department receives an email containing a demand for payment for services performed by a vendor. However, the vendor is not in the vendor management database.

Which of the following is this scenario an example of?

A. Pretexting

B. Impersonation

C. Ransomware

D. Invoice scam

2C - Social Engineering

NO.11 An employee in the accounting department **receives an email** containing a demand for payment for services performed by a vendor. However, the vendor is not in the vendor management database.

Which of the following is this scenario an example of?

A. Pretexting

B. Impersonation

C. Ransomware

D. Invoice scam

2C - Social Engineering

NO.12 A new employee logs into the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the links do not correspond to links associated with the company.

Which of the following attack vectors is most likely being used?

A. Business email

B. Social engineering

C. Unsecured network

D. Default credentials

2C - Social Engineering

NO.12 A new employee logs into the email system for the first time and notices a message from human resources about onboarding. The employee hovers over a few of the links within the email and discovers that the **links do not correspond to links associated with the company.**

Which of the following attack vectors is most likely being used?

A. Business email

B. Social engineering

C. Unsecured network

D. Default credentials

THANKS!

Any questions?

Our Graduates are Hired By

DEPARTMENT OF EDUCATION
UNITED STATES OF AMERICA

Google

Deloitte.

AT&T

ally
do it right.

DEN NORSKE KIRKE
Kirkepartner

Robinhood

VIZNET

COMCAST

INSPARK

ING BANK

proValus™

SOCRadar®
Extension to Your SOC Team!

AGILIS
TECHNOLOGIES

Humana
Wellness

EQUANS

BBS

BGA
SECURITY

gravITy
IT RESOURCES

GetMoneyGlobal

northramp

ease
LEARNING

proximus