CLARUSWAY

WAY TO REINVENT YOURSELF

CompTIA (13A-13B-13C)

AGENDA

- 13A - Malware Attack Indicators
- 13B - Physical and Network Attack Indicators
- 13C - Application Attack Indicators

AGENDA

- 13A - Malware Attack Indicators (3)
- 13B - Physical and Network Attack Indicators (10)
- 13C - Application Attack Indicators (1)
- TOTAL: 14

CompTIA (13A)

13A - Malware Attack Indicators

13A - Malware Attack Indicators

NO.1 A systems administrator receives the following alert from a file integrity monitoring tool: *The hash of the cmd.exe file has changed.*
The systems administrator checks the OS logs and notices that no patches were applied in the last two months.

Which of the following most likely occurred?

A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.

13A - Malware Attack Indicators

NO.1 A systems administrator receives the following alert from a file integrity monitoring tool: *The hash of the cmd.exe file has changed.*
The systems administrator checks the OS logs and notices that **no patches were applied** in the last two months.

Which of the following most likely occurred?

A. The end user changed the file permissions.
B. A cryptographic collision was detected.
C. A snapshot of the file system was taken.
D. A rootkit was deployed.

13A - Malware Attack Indicators

NO.2 An administrator finds that all user workstations and servers are displaying a message that is associated with files containing an extension of .ryk.

Which of the following types of infections is present on the systems?

A. Virus
B. Trojan
C. Spyware
D. Ransomware

13A - Malware Attack Indicators

NO.2 An administrator finds that all user workstations and servers are displaying a **message** that is associated with files containing an extension of **.ryk.**

Which of the following types of infections is present on the systems?

A. Virus
B. Trojan
C. Spyware
D. Ransomware

13A - Malware Attack Indicators

NO.3 An administrator is investigating an incident and discovers several users' computers were infected with malware after viewing files malware shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins.

Which of the following attacks Is most likely the cause of the malware?
A. Malicious flash drive
B. Remote access Trojan
C. Brute-force password
D. Cryptojacking

13A - Malware Attack Indicators

NO.3 An administrator is investigating an incident and discovers several users' **computers were infected with malware** after viewing files malware shared with them. The administrator discovers no degraded performance in the infected machines and an examination of the log files does not show excessive failed logins.

Which of the following attacks Is most likely the cause of the malware?

A. Malicious flash drive

B. Remote access Trojan

C. Brute-force password

D. Cryptojacking

CompTIA (13B)

13B - Physical and Network Attack Indicators

13B - Physical and Network Attack Indicators

NO.1 A company's end users are reporting that they are unable to reach external websites. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the network interface is flooded with inbound traffic. Network logs show only a small number of DNS queries sent to this server.

Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage
B. Secure DNS cryptographic downgrade
C. On-path resource consumption
D. Reflected denial of service

13B - Physical and Network Attack Indicators

NO.1 A company's end users are reporting that they are **unable to reach external websites**. After reviewing the performance data for the DNS servers, the analyst discovers that the CPU, disk, and memory usage are minimal, but the **network interface is flooded with inbound traffic.** Network logs show only a small number of DNS queries sent to this server.

Which of the following best describes what the security analyst is seeing?

A. Concurrent session usage

B. Secure DNS cryptographic downgrade

C. On-path resource consumption

D. Reflected denial of service

13B - Physical and Network Attack Indicators

NO.2 An employee fell for a phishing scam, which allowed an attacker to gain access to a company PC. The attacker scraped the PC's memory to find other credentials. Without cracking these credentials, the attacker used them to move laterally through the corporate network.

Which of the following describes this type of attack?

A. Privilege escalation
B. Buffer overflow
C. SQL injection
D. Pass-the-hash

13B - Physical and Network Attack Indicators

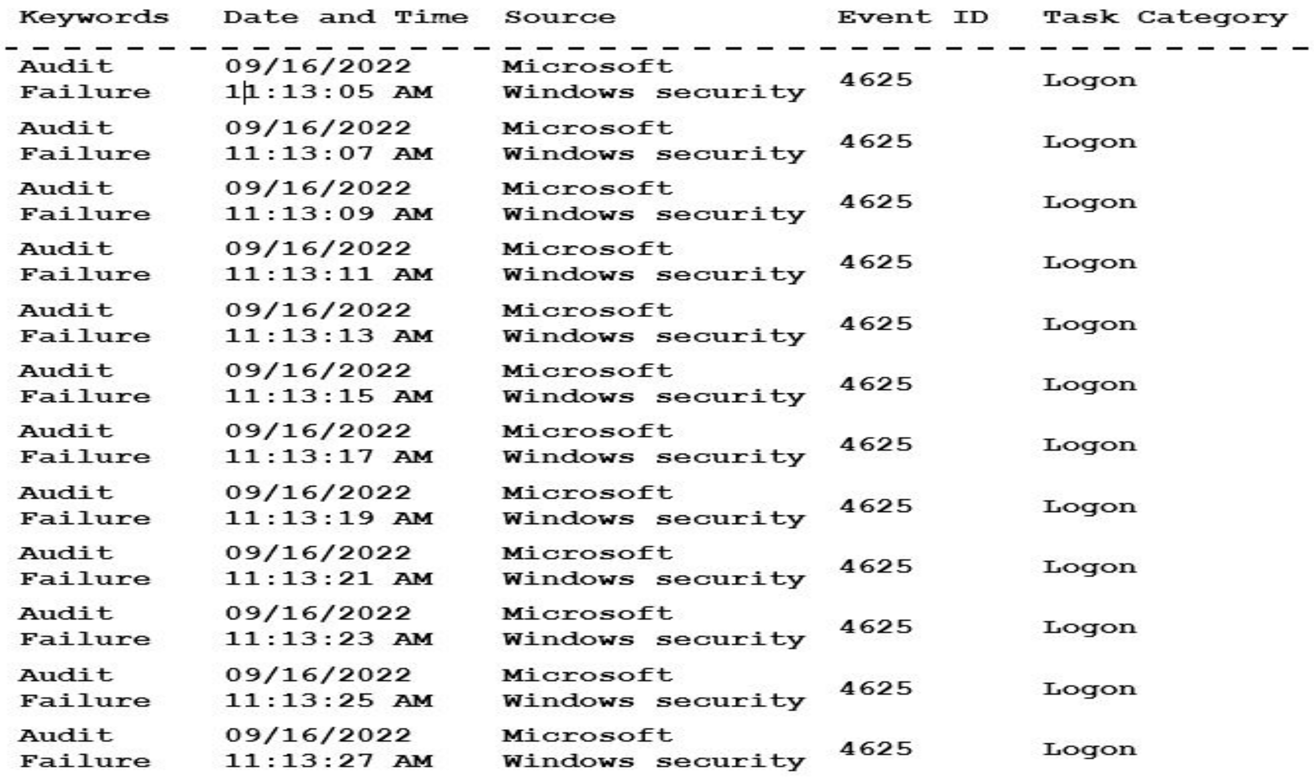
NO.2 An employee fell for a **phishing scam**, which allowed an attacker to gain access to a company PC. The attacker scraped the PC's memory to find other credentials. Without cracking these credentials, the attacker used them **to move laterally through the corporate network.**

Which of the following describes this type of attack?

A. Privilege escalation
B. Buffer overflow
C. SQL injection
D. Pass-the-hash

13B - Physical and Network Attack Indicators

NO.3 An administrator is reviewing a single server's security logs and discovers the following;



```
Keywords   Date and Time   Source              Event ID   Task Category
------------------------------------------------------------------------
Audit      09/16/2022      Microsoft
Failure    11:13:05 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:07 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:09 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:11 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:13 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:15 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:17 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:19 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:21 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:23 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:25 AM     Windows security    4625       Logon
Audit      09/16/2022      Microsoft
Failure    11:13:27 AM     Windows security    4625       Logon
```

Which of the following best describes the action captured in this log file?

A. Brute-force attack

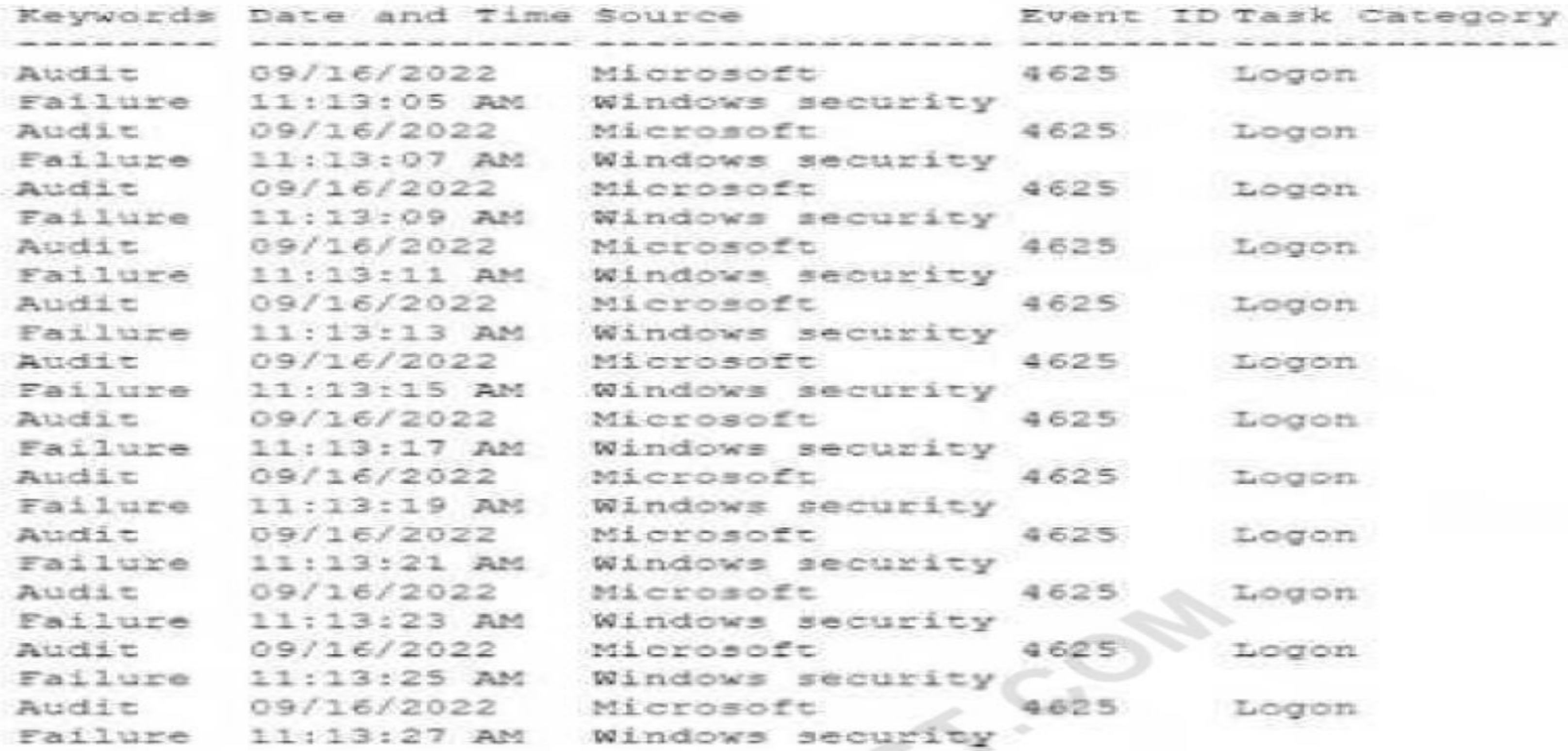
B. Privilege escalation

C. Failed password audit

D. Forgotten password by the user

13B - Physical and Network Attack Indicators

NO.3 An administrator is reviewing a single server's security logs and discovers the following;



```
Keywords  Date and Time Source             Event  ID Task Category
--------  ------------- ------------------ --------- -------------
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:05 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:07 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:09 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:11 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:13 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:15 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:17 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:19 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:21 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:23 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:25 AM   Windows security
Audit     09/16/2022    Microsoft          4625      Logon
Failure   11:13:27 AM   Windows security
```

Which of the following best describes the action captured in this log file?

A. Brute-force attack

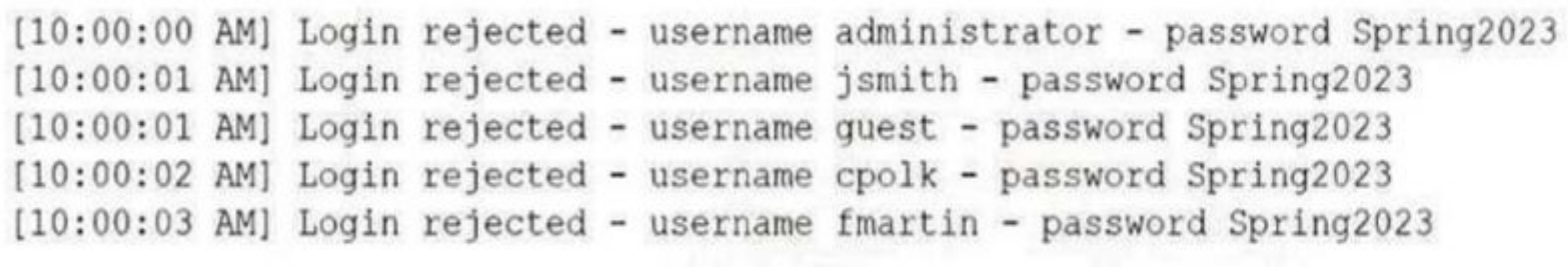
B. Privilege escalation

C. Failed password audit

D. Forgotten password by the user

13B - Physical and Network Attack Indicators

NO.4 A security analyst is reviewing the following logs:



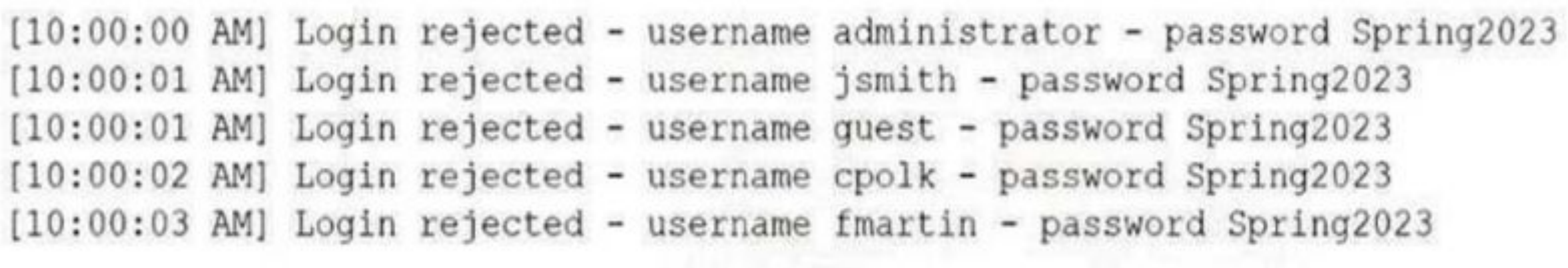
```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying
B. Account forgery
C. Pass-the-hash
D. Brute-force

13B - Physical and Network Attack Indicators

NO.4 A security analyst is reviewing the following logs:



```
[10:00:00 AM] Login rejected - username administrator - password Spring2023
[10:00:01 AM] Login rejected - username jsmith - password Spring2023
[10:00:01 AM] Login rejected - username guest - password Spring2023
[10:00:02 AM] Login rejected - username cpolk - password Spring2023
[10:00:03 AM] Login rejected - username fmartin - password Spring2023
```

Which of the following attacks is most likely occurring?

A. Password spraying

B. Account forgery

C. Pass-the-hash

D. Brute-force

13B - Physical and Network Attack Indicators

NO.5 Which of the following security concepts is being followed when implementing a product that offers protection against DDoS attacks?

A. Availability
B. Non-repudiation
C. Integrity
D. Confidentiality

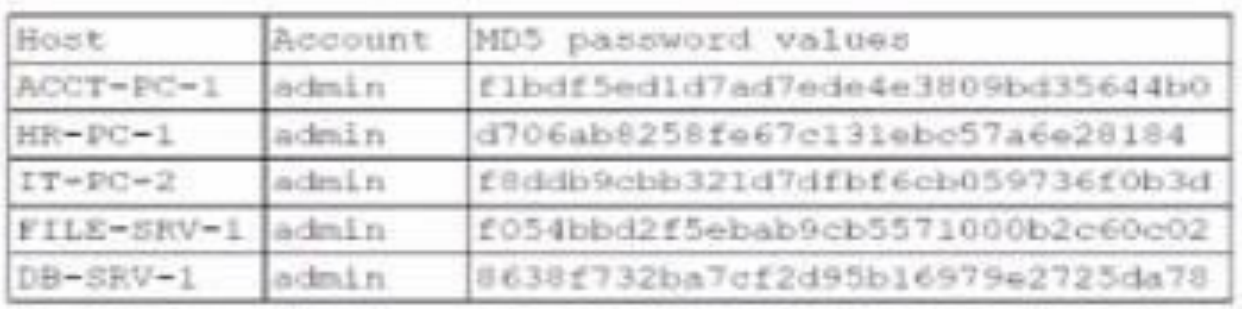
13B - Physical and Network Attack Indicators

NO.5 Which of the following security concepts is being followed when implementing a product that offers **protection against DDoS attacks?**

A. Availability
B. Non-repudiation
C. Integrity
D. Confidentiality

13B - Physical and Network Attack Indicators

NO.6 A security administrator recently reset local passwords and the following values were recorded in the system:



Host	Account	MD5 password values
ACCT-PC-1	admin	f1bdf5ed1d7ad7ede4e3809bd35644b0
HR-PC-1	admin	d706ab8258fe67c131ebc57a6e28184
IT-PC-2	admin	f8ddb9cbb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following is the security administrator most likely protecting against?

A. Account sharing

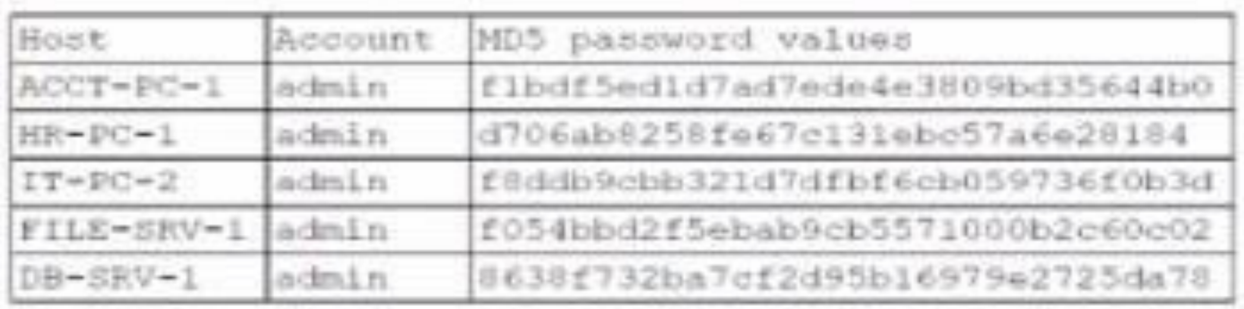
B. Weak password complexity

C. Pass-the-hash attacks

D. Password compromise

13B - Physical and Network Attack Indicators

NO.6 A security administrator recently **reset local passwords** and the following values were recorded in the system:



Host	Account	MD5 password values
ACCT-PC-1	admin	f1bdf5ed1d7ad7ede4e3809bd35644b0
HR-PC-1	admin	d706ab8258fe67c131ebc57a6e28184
IT-PC-2	admin	f8ddb9cbb321d7dfbf6cb059736f0b3d
FILE-SRV-1	admin	f054bbd2f5ebab9cb5571000b2c60c02
DB-SRV-1	admin	8638f732ba7cf2d95b16979e2725da78

Which of the following is the security administrator most likely protecting against?

A. Account sharing

B. Weak password complexity

C. Pass-the-hash attacks

D. Password compromise

13B - Physical and Network Attack Indicators

NO.7 A security analyst discovers that a large number of employee credentials had been stolen and were being sold on the dark web. The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.

Most employees clocked in and out while they were inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.

Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet.

Which of the following is the most likely reason for this compromise?

A. A brute-force attack was used against the timekeeping website to scan for common passwords.

B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.

C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site

D. ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.

13B - Physical and Network Attack Indicators

NO.7 A security analyst discovers that a l**arge number of employee credentials had been stolen and were being sold on the dark web.** The analyst investigates and discovers that some hourly employee credentials were compromised, but salaried employee credentials were not affected.

Most employees clocked in and out while they were inside the building using one of the kiosks connected to the network. However, some clocked out and recorded their time after leaving to go home. Only those who clocked in and out while inside the building had credentials stolen. Each of the kiosks are on different floors, and there are multiple routers, since the business segments environments for certain business functions.

Hourly employees are required to use a website called acmetimekeeping.com to clock in and out. This website is accessible from the internet.

Which of the following is the most likely reason for this compromise?

A. A brute-force attack was used against the timekeeping website to scan for common passwords.

B. A malicious actor compromised the time-keeping website with malicious code using an unpatched vulnerability on the site, stealing the credentials.

C. The internal DNS servers were poisoned and were redirecting acmetimkeeping.com to malicious domain that intercepted the credentials and then passed them through to the real site

D. ARP poisoning affected the machines in the building and caused the kiosks lo send a copy of all the submitted credentials to a machine.

13B - Physical and Network Attack Indicators

NO.8 A business uses Wi-Fi with content filleting enabled. An employee noticed a coworker accessed a blocked sue from a work computer and repotted the issue. While Investigating the issue, a security administrator found another device providing internet access to certain employees.

Which of the following best describes the security risk?
A. The host-based security agent Is not running on all computers.
B. A rogue access point Is allowing users to bypass controls.
C. Employees who have certain credentials are using a hidden SSID.
D. A valid access point is being jammed to limit availability.

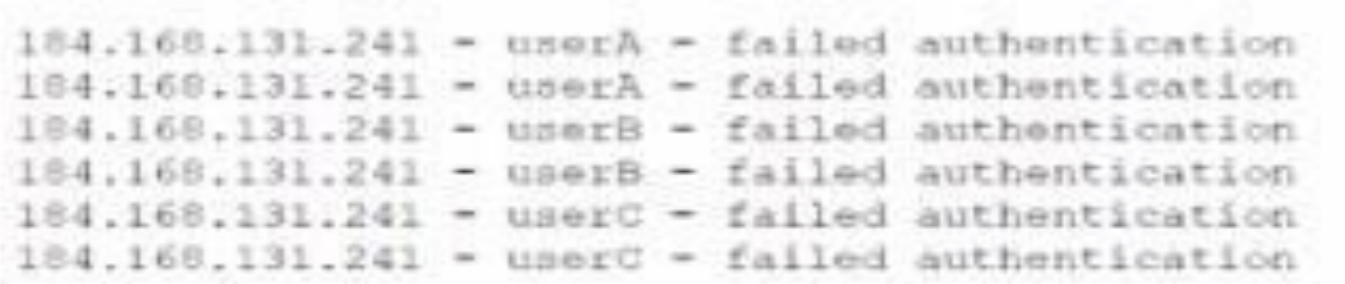
13B - Physical and Network Attack Indicators

NO.8 A business uses Wi-Fi with content filleting enabled. An employee noticed a coworker accessed a blocked sue from a work computer and repotted the issue. While Investigating the issue, a security administrator found **another device providing internet access to certain employees.**

Which of the following best describes the security risk?
A. The host-based security agent Is not running on all computers.
B. A rogue access point Is allowing users to bypass controls.
C. Employees who have certain credentials are using a hidden SSID.
D. A valid access point is being jammed to limit availability.

13B - Physical and Network Attack Indicators

NO.9 The security operations center is researching an event concerning a suspicious IP address A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced failed log-in attempts when authenticating from the same IP address:



```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

Which of the following most likely describes attack that took place?

A. Spraying

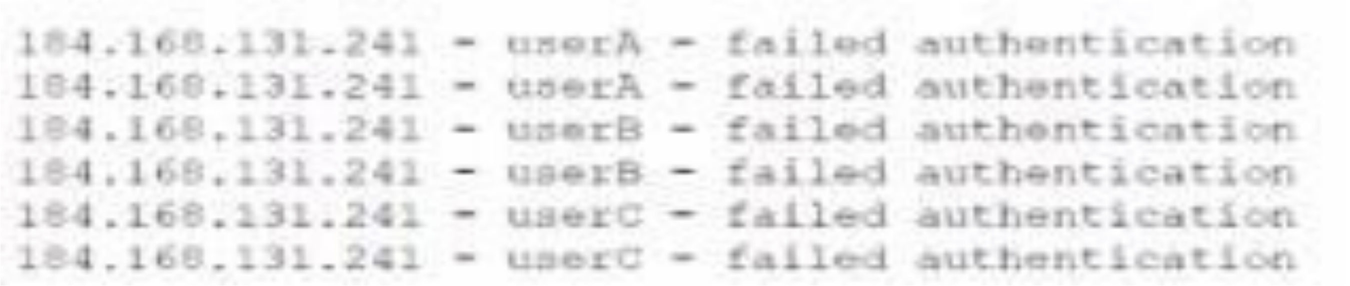
B. Brute-force

C. Dictionary

D. Rainbow table

13B - Physical and Network Attack Indicators

NO.9 The security operations center is researching an event concerning a suspicious IP address. A security analyst looks at the following event logs and discovers that a significant portion of the user accounts have experienced **failed log-in attempts when authenticating from the same IP address:**



```
184.168.131.241 - userA - failed authentication
184.168.131.241 - userA - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userB - failed authentication
184.168.131.241 - userC - failed authentication
184.168.131.241 - userC - failed authentication
```

Which of the following most likely describes attack that took place?

A. Spraying

B. Brute-force

C. Dictionary

D. Rainbow table

13B - Physical and Network Attack Indicators

NO.10 An organization experiences a cybersecurity incident involving a command-and-control server.

Which of the following logs should be analyzed to identify the impacted host? (Select two).

A. Application

B. Authentication

C. DHCP

D. Network

E. Firewall

F. Database

13B - Physical and Network Attack Indicators

NO.10 An organization experiences a cybersecurity incident involving a command-and-control server.

Which of the following logs should be analyzed **to identify the impacted host?** (Select two).

A. Application

B. Authentication

C. DHCP

D. Network

E. Firewall

F. Database

CompTIA (13C)

13C - Application Attack Indicators

13C - Application Attack Indicators

NO.1 A website user is locked out of an account after clicking an email link and visiting a different website Web server logs show the user's password was changed, even though the user did not change the password.

Which of the following is the most likely cause?
A. Cross-site request forgery
B. Directory traversal
C. ARP poisoning
D. SQL injection

13C - Application Attack Indicators

NO.1 A website **user is locked out of an account after clicking an email link** and visiting a different website. Web server logs show the user's password was changed, even though the user did not change the password.

Which of the following is the most likely cause?

A. Cross-site request forgery

B. Directory traversal

C. ARP poisoning

D. SQL injection

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

BGA
SECURITY

BBS

gravity
IT RESOURCES

GetMoneyGlobal

proximus

northramp

ease
LEARNING