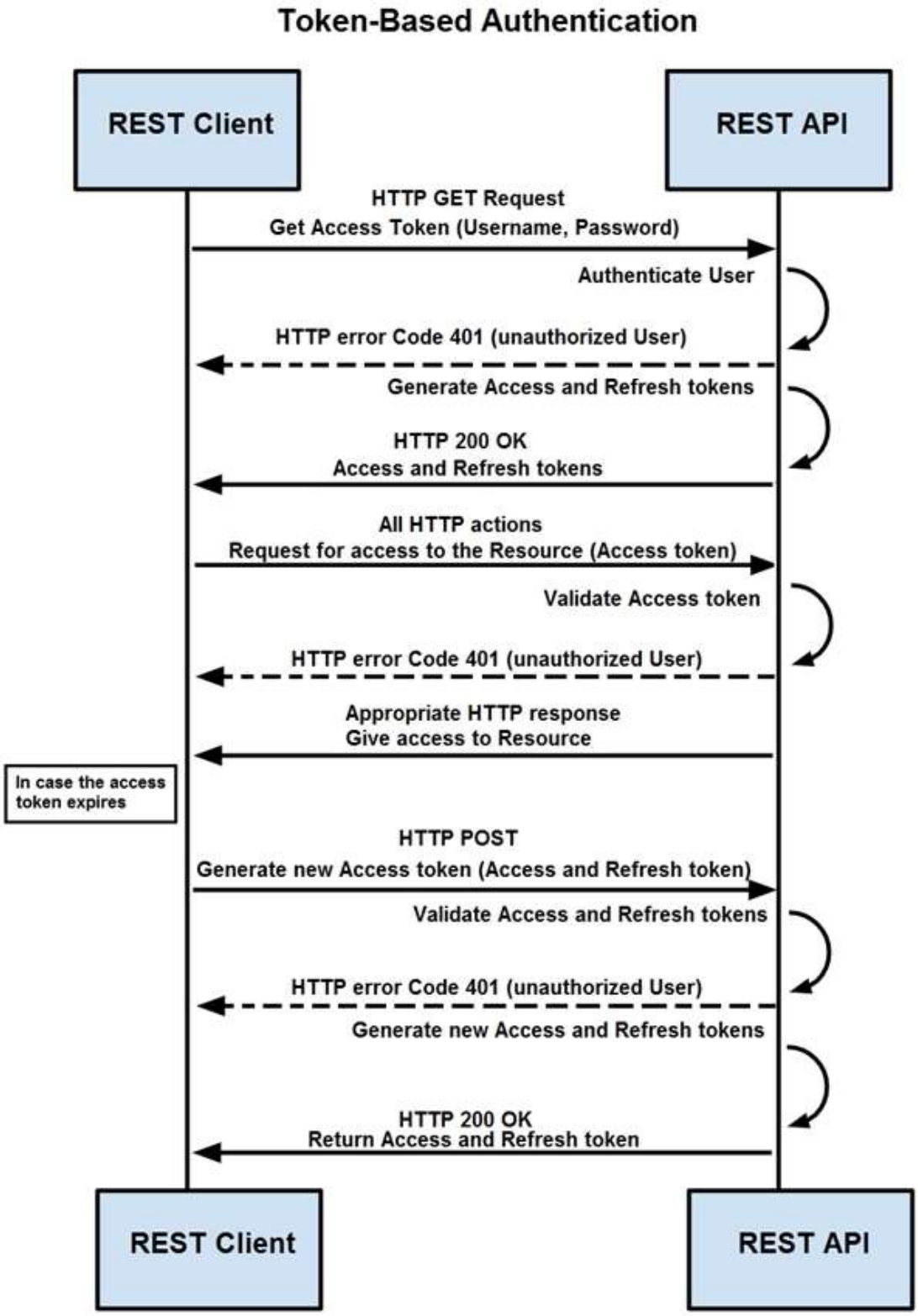
QUESTION 21
An engineer is investigating several cases of increased incoming spam emails and suspicious emails from the HR and service departments. While checking the event sources, the website monitoring tool showed several web scraping alerts overnight. Which type of compromise is indicated?

A. phishing
B. dumpster diving
C. social engineering
D. privilege escalation

Answer: C

QUESTION 22
Refer to the exhibit. How are tokens authenticated when the REST API on a device is accessed from a REST API client?



A. The token is obtained by providing a password. The REST client requests access to a resource using the access token. The REST API validates the access token and gives access to the resource.
B. The token is obtained by providing a password. The REST API requests access to a resource

using the access token, validates the access token, and gives access to the resource.

C. The token is obtained before providing a password. The REST API provides resource access, refreshes tokens, and returns them to the REST client. The REST client requests access to a resource using the access token.

D. The token is obtained before providing a password. The REST client provides access to a resource using the access token. The REST API encrypts the access token and gives access to the resource.

Answer: D

QUESTION 23
Refer to the exhibit. Where are the browser page rendering permissions displayed?

```
pragma: no-cache
server: Apache
status: 200
strict-transport-security: max-age=31536000
vary: Accept-Encoding
x-content-type-options: nosniff
x-frame-options: SAMEORIGIN
x-test-debug: nURL=www.cisco.com,realm=0,isRealm=0,realDomain=0,shortrealm=0
x-xss-protection: 1; mode=block
```

A. x-frame-options
B. x-xss-protection
C. x-content-type-options
D. x-test-debug

Answer: C
Explanation:
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options

QUESTION 24
An engineer is utilizing interactive behavior analysis to test malware in a sandbox environment to see how the malware performs when it is successfully executed. A location is secured to perform reverse engineering on a piece of malware. What is the next step the engineer should take to analyze this malware?

A. Run the program through a debugger to see the sequential actions
B. Unpack the file in a sandbox to see how it reacts
C. Research the malware online to see if there are noted findings
D. Disassemble the malware to understand how it was constructed

Answer: C

QUESTION 25
What is a limitation of cyber security risk insurance?

A. It does not cover the costs to restore stolen identities as a result of a cyber attack
B. It does not cover the costs to hire forensics experts to analyze the cyber attack
C. It does not cover the costs of damage done by third parties as a result of a cyber attack
D. It does not cover the costs to hire a public relations company to help deal with a cyber attack

Answer: A
Explanation:
https://tplinsurance.com/products/cyber-risk-insurance/

QUESTION 26
An engineer returned to work and realized that payments that were received over the weekend were sent to the wrong recipient. The engineer discovered that the SaaS tool that processes these payments was down over the weekend. Which step should the engineer take first?

A. Utilize the SaaS tool team to gather more information on the potential breach
B. Contact the incident response team to inform them of a potential breach
C. Organize a meeting to discuss the services that may be affected
D. Request that the purchasing department creates and sends the payments manually

Answer: A

QUESTION 27
An analyst is alerted for a malicious file hash. After analysis, the analyst determined that an internal workstation is communicating over port 80 with an external server and that the file hash is associated with Duqu malware. Which tactics, techniques, and procedures align with this analysis?

A. Command and Control, Application Layer Protocol, Duqu
B. Discovery, Remote Services: SMB/Windows Admin Shares, Duqu
C. Lateral Movement, Remote Services: SMB/Windows Admin Shares, Duqu
D. Discovery, System Network Configuration Discovery, Duqu

Answer: A

QUESTION 28
A Mac laptop user notices that several files have disappeared from their laptop documents folder. While looking for the files, the user notices that the browser history was recently cleared. The user raises a case, and an analyst reviews the network usage and discovers that it is abnormally high. Which step should be taken to continue the investigation?

A. Run the sudo sysdiagnose command
B. Run the sh command
C. Run the w command
D. Run the who command

Answer: A
Explanation:
https://eclecticlight.co/2016/02/06/the-ultimate-diagnostic-tool-sysdiagnose/

QUESTION 29
A SOC analyst is investigating a recent email delivered to a high-value user for a customer whose network their organization monitors. The email includes a suspicious attachment titled "Invoice RE: 0004489". The hash of the file is gathered from the Cisco Email Security Appliance. After searching Open Source Intelligence, no available history of this hash is found anywhere on the web. What is the next step in analyzing this attachment to allow the analyst to gather indicators of compromise?

A. Run and analyze the DLP Incident Summary Report from the Email Security Appliance
B. Ask the company to execute the payload for real time analysis
C. Investigate further in open source repositories using YARA to find matches
D. Obtain a copy of the file for detonation in a sandbox

Answer: D

QUESTION 30
A SOC analyst is notified by the network monitoring tool that there are unusual types of internal traffic on IP subnet 103.921.2239.0/24. The analyst discovers unexplained encrypted data files on a computer system that belongs on that specific subnet. What is the cause of the issue?

A. DDoS attack
B. phishing attack
C. virus outbreak
D. malware outbreak

Answer: D

QUESTION 31
Refer to the exhibit. An employee is a victim of a social engineering phone call and installs remote access software to allow an "MS Support" technician to check his machine for malware. The employee becomes suspicious after the remote technician requests payment in the form of gift cards. The employee has copies of multiple, unencrypted database files, over 400 MB each, on his system and is worried that the scammer copied the files off but has no proof of it. The remote technician was connected sometime between 2:00 pm and 3:00 pm over https.
What should be determined regarding data loss between the employee's laptop and the remote technician's system?

Max (K)	Retain	OverflowAction	Entries	Log
15,168	0	OverwriteAsNeeded	20,792	Application
15,168	0	OverwriteAsNeeded	12,559	System
15,360	0	OverwriteAsNeeded	11,173	Windows PowerShell

A. No database files were disclosed
B. The database files were disclosed
C. The database files integrity was violated
D. The database files were intentionally corrupted, and encryption is possible

Answer: C

QUESTION 32
Refer to the exhibit. Which asset has the highest risk value?

Asset	Threat	Vulnerability	Likelihood (1-10)	Impact (1-10)
Servers	Natural Disasters – Flooding	Server Room is on the zero floor	3	10
Secretary Workstation	Usage of illegitimate software	Inadequate control of software	7	6
Payment Process	Eavesdropping, Misrouting/re-routing of messages	Unencrypted communications	5	10
Website	Website Intrusion	No IDS/IPS usage	6	8

A. servers
B. website
C. payment process
D. secretary workstation

Answer: C

QUESTION 33
What is the purpose of hardening systems?

A. to securely configure machines to limit the attack surface
B. to create the logic that triggers alerts when anomalies occur
C. to identify vulnerabilities within an operating system
D. to analyze attacks to identify threat actors and points of entry

Answer: A

QUESTION 34
A company launched an e-commerce website with multiple points of sale through internal and external e- stores. Customers access the stores from the public website, and employees access the stores from the intranet with an SSO. Which action is needed to comply with PCI standards for hardening the systems?

A. Mask PAN numbers
B. Encrypt personal data
C. Encrypt access
D. Mask sales details

Answer: B

QUESTION 35
An organization installed a new application server for IP phones. An automated process fetched user credentials from the Active Directory server, and the application will have access to on-premises and cloud services. Which security threat should be mitigated first?

A. aligning access control policies
B. exfiltration during data transfer
C. attack using default accounts
D. data exposure from backups

Answer: B

QUESTION 36
A threat actor has crafted and sent a spear-phishing email with what appears to be a trustworthy link to the site of a conference that an employee recently attended. The employee clicked the link and was redirected to a malicious site through which the employee downloaded a PDF attachment infected with ransomware. The employee opened the attachment, which exploited vulnerabilities on the desktop. The ransomware is now installed and is calling back to its command and control server. Which security solution is needed at this stage to mitigate the attack?

A. web security solution
B. email security solution
C. endpoint security solution
D. network security solution

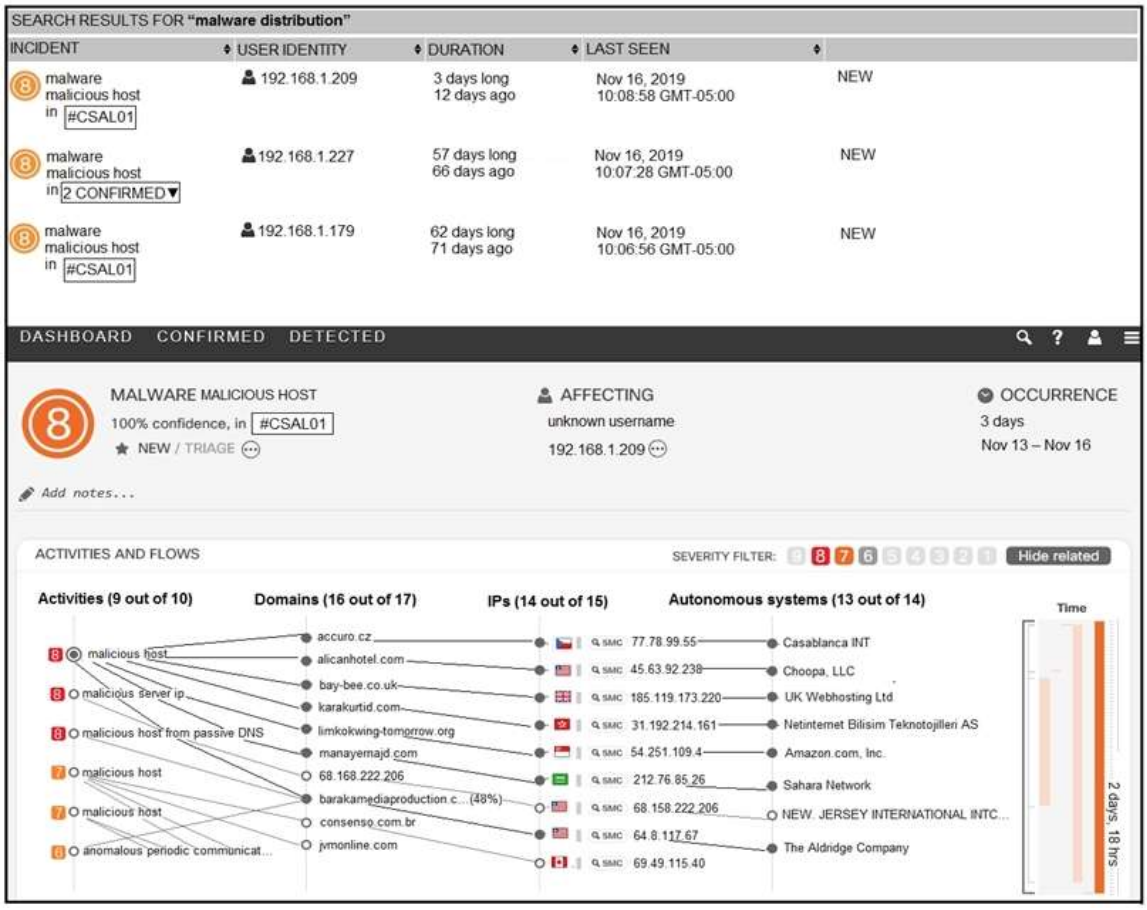
Answer: D

QUESTION 37
Refer to the exhibit. An engineer is investigating a case with suspicious usernames within the active directory. After the engineer investigates and cross-correlates events from other sources, it appears that the 2 users are privileged, and their creation date matches suspicious network traffic that was initiated from the internal network 2 days prior. Which type of compromise is occurring?

A. compromised insider
B. compromised root access
C. compromised database tables
D. compromised network

Answer: D

QUESTION 38
Refer to the exhibit. For IP 192.168.1.209, what are the risk level, activity, and next step?



A. high risk level, anomalous periodic communication, quarantine with antivirus
B. critical risk level, malicious server IP, run in a sandboxed environment
C. critical risk level, data exfiltration, isolate the device
D. high risk level, malicious host, investigate further

Answer: A

QUESTION 39
Refer to the exhibit. What is the connection status of the ICMP event?

Distribution Port/ICMP Code	Message	Classification	Application Protocol	Client	Application Risk	Business Relevance	Access Control Rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	ICMP	ICMP client	Medium	Medium	rule
80 (http) / tcp	STREAMS_DATA_ON_SYN (129:2:2)	Generic Protocol Command Decode	DNS	DNS client	Very Low	Very High	Default Action
0 (No Code) / icmp	PROTOCOL-ICMP Echo Reply (1:408:8)	Misc Activity	DNS	DNS client	Very Low	Very High	Allow ICMP
54107 / udp	PROTOCOL-DNS TMG Firewall Client long host entry exploit attempt (3:19187:7)	Attempted User Privilege Gain	DNS	DNS client	Very Low	Very High	
49367 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57477 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54879 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60999 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52240 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
54359 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52489 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
60169 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52250 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52485 / up	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
49940 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
57214 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
51608 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
52652 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55528 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
61222 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55640 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected(1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	
55991 / udp	PROTOCOL-DNS dns response for rtc 1918 192.168/16 address detected (1:15935:7)	Potential Corporate Policy Violation	DNS	DNS client	Very Low	Very High	

A. blocked by a configured access policy rule
B. allowed by a configured access policy rule
C. blocked by an intrusion policy rule
D. allowed in the default action

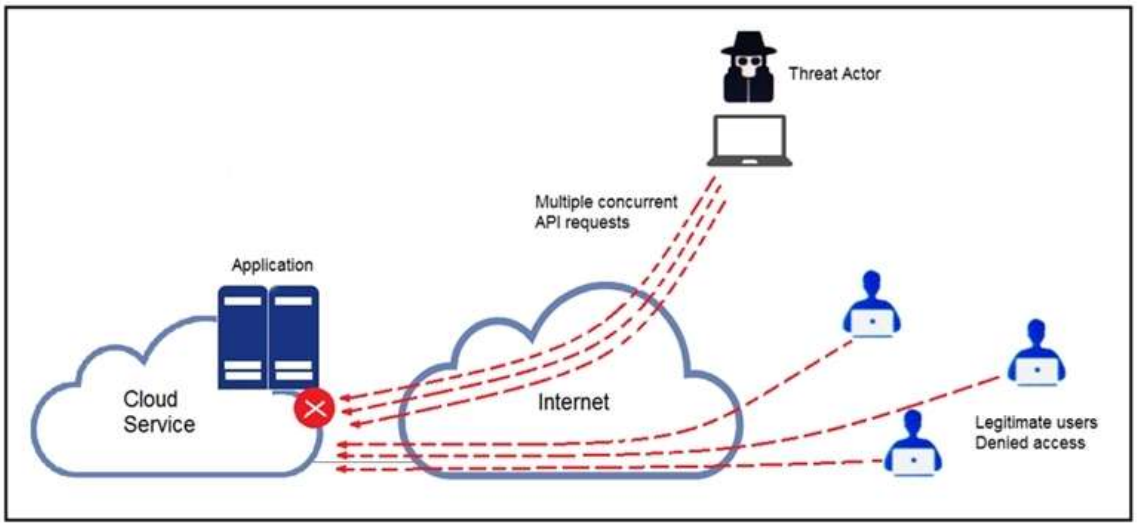
Answer: B

QUESTION 40
An intruder attempted malicious activity and exchanged emails with a user and received corporate information, including email distribution lists. The intruder asked the user to engage with a link in an email. When the fink launched, it infected machines and the intruder was able to access the corporate network.
Which testing method did the intruder use?

A. social engineering
B. eavesdropping
C. piggybacking
D. tailgating

Answer: A

QUESTION 41
Refer to the exhibit. A threat actor behind a single computer exploited a cloud-based application by sending multiple concurrent API requests. These requests made the application unresponsive. Which solution protects the application from being overloaded and ensures more equitable application access across the end-user community?



A. Limit the number of API calls that a single client is allowed to make
B. Add restrictions on the edge router on how often a single client can access the API
C. Reduce the amount of data that can be fetched from the total pool of active clients that call the API
D. Increase the application cache of the total pool of active clients that call the API

Answer: A

QUESTION 42
A threat actor attacked an organization's Active Directory server from a remote location, and in a thirty- minute timeframe, stole the password for the administrator account and attempted to access 3 company servers. The threat actor successfully accessed the first server that contained sales data, but no files were downloaded. A second server was also accessed that contained marketing information and 11 files were downloaded. When the threat actor accessed the third server that contained corporate financial data, the session was disconnected, and the administrator's account was disabled. Which activity triggered the behavior analytics tool?

A. accessing the Active Directory server
B. accessing the server with financial data
C. accessing multiple servers
D. downloading more than 10 files

Answer: C