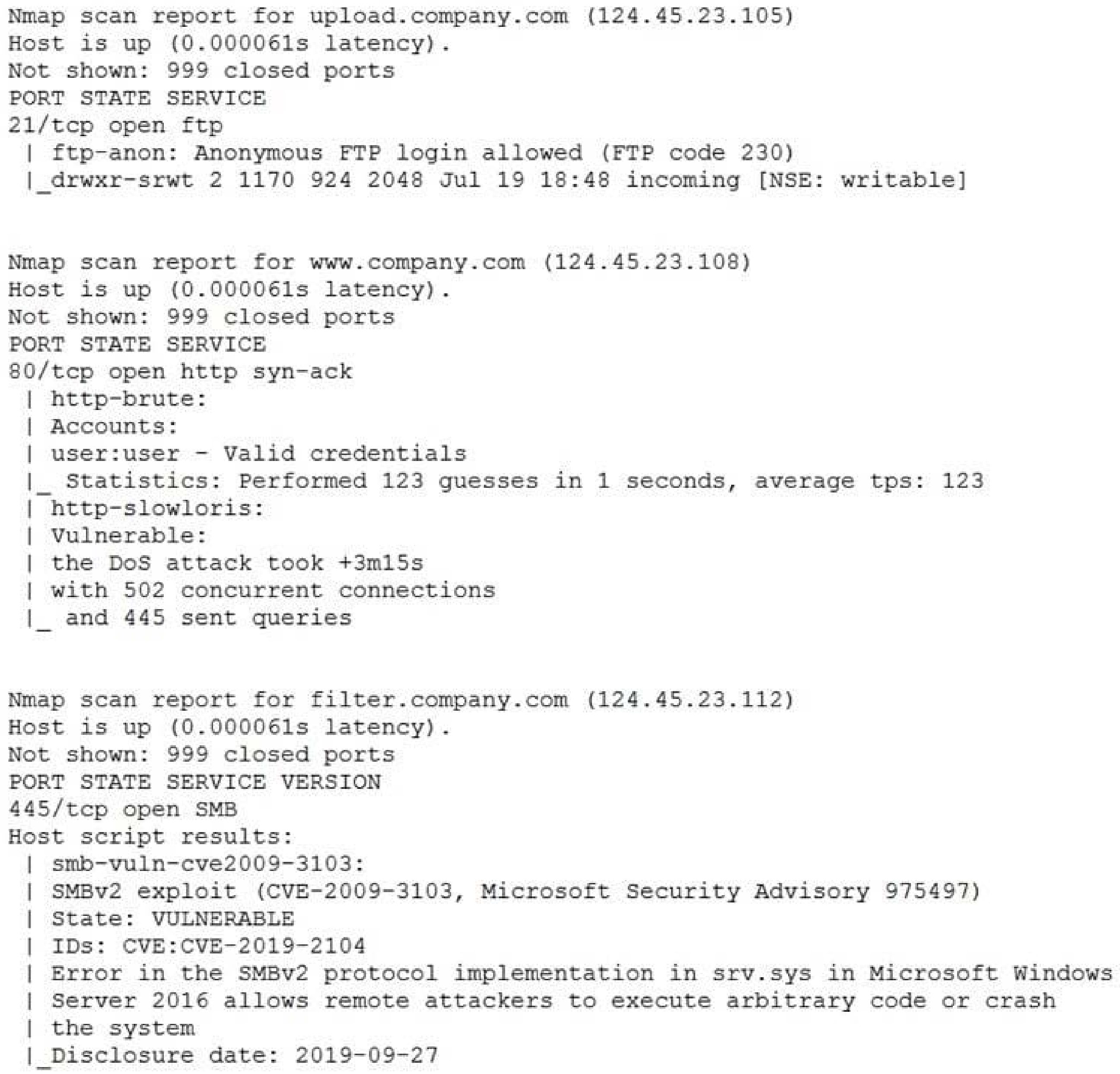
CS0-002$^{Q\&As}$

CompTIA Cybersecurity Analyst (CySA+)

QUESTION 1

A security analyst is probing a company\\'s public-facing servers for vulnerabilities and obtains the following output:



```
Nmap scan report for upload.company.com (124.45.23.105)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
21/tcp open ftp
 | ftp-anon: Anonymous FTP login allowed (FTP code 230)
 |_drwxr-srwt 2 1170 924 2048 Jul 19 18:48 incoming [NSE: writable]


Nmap scan report for www.company.com (124.45.23.108)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE
80/tcp open http syn-ack
 | http-brute:
 | Accounts:
 | user:user - Valid credentials
 |_ Statistics: Performed 123 guesses in 1 seconds, average tps: 123
 | http-slowloris:
 | Vulnerable:
 | the DoS attack took +3m15s
 | with 502 concurrent connections
 |_ and 445 sent queries


Nmap scan report for filter.company.com (124.45.23.112)
Host is up (0.000061s latency).
Not shown: 999 closed ports
PORT STATE SERVICE VERSION
445/tcp open SMB
Host script results:
 | smb-vuln-cve2009-3103:
 | SMBv2 exploit (CVE-2009-3103, Microsoft Security Advisory 975497)
 | State: VULNERABLE
 | IDs: CVE:CVE-2019-2104
 | Error in the SMBv2 protocol implementation in srv.sys in Microsoft Windows
 | Server 2016 allows remote attackers to execute arbitrary code or crash
 | the system
 |_Disclosure date: 2019-09-27
```

Which of the following changes should the analyst recommend FIRST?

A. Implement File Transfer Protocol Secure on the upload server

B. Disable anonymous login on the web server

C. Configure firewall changes to close port 445 on 124.45.23.112

D. Apply a firewall rule to filter the number of requests per second on port 80 on 124.45.23.108

Correct Answer: C

SMB exploitation and remote code execution can do a lot more damage to files/network compared to a DoS causing a site to be down.

QUESTION 2

Which of the following weaknesses associated with common SCADA systems are the MOST critical for organizations to address architecturally within their networks? (Choose two.)

A. Boot processes that are neither measured nor attested

B. Legacy and unpatchable systems software

C. Unnecessary open ports and protocols

D. No OS kernel mandatory access controls

E. Unauthenticated commands

F. Insecure filesystem permissions

Correct Answer: BF

QUESTION 3

An incident response team detected malicious software that could have gained access to credit card data. The incident response team was able to mitigate significant damage and implement corrective actions. By having incident response mechanisms in place. Which of the following should be notified for lessons learned?

A. The human resources department

B. Customers

C. Company leadership

D. The legal team

Correct Answer: C

QUESTION 4

An organization is requesting the development of a disaster recovery plan. The organization has grown and so has its infrastructure. Documentation, policies, and procedures do not exist. Which of the following steps should be taken to assist in the development of the disaster recovery plan?

A. Conduct a risk assessment.

B. Develop a data retention policy.

C. Execute vulnerability scanning.

D. Identify assets.

Correct Answer: D

QUESTION 5

During a quarterly review of user accounts and activity, a security analyst noticed that after a password reset the head of human resources has been logging in from multiple external locations, including several overseas. Further review of the account showed access rights to a number of corporate applications, including a sensitive accounting application used for employee bonuses. Which of the following security methods could be used to mitigate this risk?

A. RADIUS identity management

B. Context-based authentication

C. Privilege escalation restrictions

D. Elimination of self-service password resets

Correct Answer: B