

100% Money Back
Guarantee

Vendor:CompTIA

Exam Code:PT0-003

Exam Name:CompTIA PenTest+

Version:Demo

QUESTION 1

During a security assessment, a penetration tester needs to exploit a vulnerability in a wireless network's authentication mechanism to gain unauthorized access to the network. Which of the following attacks would the tester most likely perform to gain access?

- A. KARMA attack
- B. Beacon flooding
- C. MAC address spoofing
- D. Eavesdropping

Correct Answer: C

MAC address spoofing involves changing the MAC address of a network interface to mimic another device on the network. This technique is often used to bypass network access controls and gain unauthorized access to a network.

Understanding MAC Address Spoofing:

Purpose:

Tools and Techniques:

Step-by-Step Explanation
ifconfig eth0 hw ether 00:11:22:33:44:55
uk.co.certification.simulator.questionpool.PList@2fc317d6 Impact:

Detection and Mitigation:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

Top of Form

Bottom of Form

QUESTION 2

A client wants a security assessment company to perform a penetration test against its hot site. The purpose of the test is to determine the effectiveness of the defenses that protect against disruptions to business continuity. Which of the following is the MOST important action to take before starting this type of assessment?

- A. Ensure the client has signed the SOW.
- B. Verify the client has granted network access to the hot site.
- C. Determine if the failover environment relies on resources not owned by the client.
- D. Establish communication and escalation procedures with the client.

Correct Answer: A

The statement of work (SOW) is a document that defines the scope, objectives, deliverables, and timeline of a penetration testing engagement. It is important to have the client sign the SOW before starting the assessment to avoid any legal or contractual issues.

QUESTION 3

A penetration tester has identified several newly released CVEs on a VoIP call manager. The scanning tool the tester used determined the possible presence of the CVEs based off the version number of the service. Which of the following methods would BEST support validation of the possible findings?

- A. Manually check the version number of the VoIP service against the CVE release
- B. Test with proof-of-concept code from an exploit database
- C. Review SIP traffic from an on-path position to look for indicators of compromise
- D. Utilize an nmap -sV scan against the service

Correct Answer: B

Testing with proof-of-concept code from an exploit database is the best method to support validation of the possible findings, as it will demonstrate whether the CVEs are actually exploitable on the target VoIP call manager. Proof-of-concept code is a piece of software or script that shows how an attacker can exploit a vulnerability in a system or application. An exploit database is a repository of publicly available exploits, such as Exploit Database or Metasploit. Reference: <https://dokumen.pub/hacking-exposed-unified-communications-amp-voip-security-secrets-amp-solutions-2nd-edition-9780071798778-0071798773-9780071798761-0071798765.html>

QUESTION 4

A penetration tester is authorized to perform a DoS attack against a host on a network. Given the following input:

```
ip = IP("192.168.50.2")
```

```
tcp = TCP(sport=RandShort(), dport=80, flags="S")
```

```
raw = RAW(b"X"*1024)
```

```
p = ip/tcp/raw
```

```
send(p, loop=1, verbose=0)
```

Which of the following attack types is most likely being used in the test?

- A. MDK4
- B. Smurf attack
- C. FragAttack
- D. SYN flood

Correct Answer: D

A SYN flood attack exploits the TCP handshake process by sending a large number of SYN packets to a target, consuming resources and causing a denial of service.

Understanding the Script:

Purpose of SYN Flood:

Detection and Mitigation:

References from Pentesting Literature:

Step-by-Step ExplanationReferences:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 5

A penetration tester gains access to a Windows machine and wants to further enumerate users with native operating system credentials. Which of the following should the tester use?

- A. route.exe print
- B. netstat.exe -ntp
- C. net.exe commands
- D. strings.exe -a

Correct Answer: C

The net.exe commands are native to the Windows operating system and are used to manage and enumerate network resources, including user accounts.

Using net.exe Commands:

Step-by-Step Explanationnet user

uk.co.certification.simulator.questionpool.PList@432e421f net user

Additional net.exe Commands:

net localgroup

net localgroup

uk.co.certification.simulator.questionpool.PList@71e0e60b net session

Advantages:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 6

A tester is performing an external phishing assessment on the top executives at a company. Two-factor authentication is enabled on the executives\\ accounts that are in the scope of work. Which of the following should the tester do to get access to these accounts?

- A. Configure an external domain using a typosquatting technique. Configure Evilginx to bypass two-factor authentication using a phishlet that simulates the mail portal for the company.
- B. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a brute-force attack method.
- C. Configure an external domain using a typosquatting technique. Configure SET to bypass two-factor authentication using a phishlet that mimics the mail portal for the company.
- D. Configure Gophish to use an external domain. Clone the email portal web page from the company and get the two-factor authentication code using a vishing method.

Correct Answer: A

To bypass two-factor authentication (2FA) and gain access to the executives\\ accounts, the tester should use Evilginx with a typosquatting domain. Evilginx is a man-in-the-middle attack framework used to bypass 2FA by capturing session

tokens.

Phishing with Evilginx:

Typosquatting:

Steps:

Pentest References:

Phishing: Social engineering technique to deceive users into providing sensitive information.

Two-Factor Authentication Bypass: Advanced phishing attacks like those using Evilginx can capture and reuse session tokens, bypassing 2FA mechanisms. OSINT and Reconnaissance: Identifying key targets (executives) and crafting

convincing phishing emails based on gathered information. Using Evilginx with a typosquatting domain allows the tester to bypass 2FA and gain access to high-value accounts, demonstrating the effectiveness of advanced phishing

techniques.

QUESTION 7

During a penetration test, a tester attempts to pivot from one Windows 10 system to another Windows system. The penetration tester thinks a local firewall is blocking connections. Which of the following command-line utilities built into Windows is most likely to disable the firewall?

- A. certutil.exe
- B. bitsadmin.exe

C. msconfig.exe

D. netsh.exe

Correct Answer: D

Understanding netsh.exe:

Disabling the Firewall:

```
netsh advfirewall set allprofiles state off
```

Usage in Penetration Testing:

References from Pentesting Literature:

References:

Penetration Testing - A Hands-on Introduction to Hacking HTB Official Writeups

QUESTION 8

A penetration tester obtains password dumps associated with the target and identifies strict lockout policies. The tester does not want to lock out accounts when attempting access. Which of the following techniques should the tester use?

A. Credential stuffing

B. MFA fatigue

C. Dictionary attack

D. Brute-force attack

Correct Answer: A

To avoid locking out accounts while attempting access, the penetration tester should use credential stuffing.

Credential Stuffing:

Other Techniques:

Pentest References:

Password Attacks: Understanding different types of password attacks and their implications on account security.

Account Lockout Policies: Awareness of how lockout mechanisms work and strategies to avoid triggering them during penetration tests. By using credential stuffing, the penetration tester can attempt to gain access using known credentials

without triggering account lockout policies, ensuring a stealthier approach to password attacks.

QUESTION 9

During a penetration test, the tester uses a vulnerability scanner to collect information about any possible vulnerabilities that could be used to compromise the network. The tester receives the results and then executes the following command:

```
snmpwalk -v 2c -c public 192.168.1.23
```

Which of the following is the tester trying to do based on the command they used?

- A. Bypass defensive systems to collect more information.
- B. Use an automation tool to perform the attacks.
- C. Script exploits to gain access to the systems and host.
- D. Validate the results and remove false positives.

Correct Answer: D

The command `snmpwalk -v 2c -c public 192.168.1.23` is used to query SNMP (Simple Network Management Protocol) data from a device. Here's the purpose in the context provided:

SNMP Enumeration:

Purpose of the Command:

Comparison with Other Options:

By using `snmpwalk`, the tester is validating the results from the vulnerability scanner and removing any false positives, ensuring accurate reporting.

QUESTION 10

During an assessment, a penetration tester obtains an NTLM hash from a legacy Windows machine. Which of the following tools should the penetration tester use to continue the attack?

- A. Responder
- B. Hydra
- C. BloodHound
- D. CrackMapExec

Correct Answer: D

When a penetration tester obtains an NTLM hash from a legacy Windows machine, they need to use a tool that can leverage this hash for further attacks, such as pass-the-hash attacks, or for cracking the hash. Here's a breakdown of the

options:

Option A: Responder

Option B: Hydra

Option C: BloodHound

Option D: CrackMapExec

References from Pentest:

Forge HTB: Demonstrates the use of CrackMapExec for leveraging NTLM hashes to gain further access within a network.

Horizontall HTB: Shows how CrackMapExec can be used for various post- exploitation activities, including using NTLM hashes to authenticate and execute commands.

Conclusion:

Option D, CrackMapExec, is the most suitable tool for continuing the attack using an NTLM hash. It supports pass-the-hash techniques and other operations that can leverage NTLM hashes effectively.

QUESTION 11

A penetration tester wants to use multiple TTPs to assess the reactions (alerted, blocked, and others) by the client's current security tools. The threat-modeling team indicates the TTPs in the list might affect their internal systems and servers. Which of the following actions would the tester most likely take?

- A. Use a BAS tool to test multiple TTPs based on the input from the threat-modeling team.
- B. Perform an internal vulnerability assessment with credentials to review the internal attack surface.
- C. Use a generic vulnerability scanner to test the TTPs and review the results with the threat-modeling team.
- D. Perform a full internal penetration test to review all the possible exploits that could affect the systems.

Correct Answer: A

BAS (Breach and Attack Simulation) tools are specifically designed to emulate multiple TTPs (Tactics, Techniques, and Procedures) used by adversaries. These tools can simulate various attack vectors in a controlled manner to test the

effectiveness of an organization's security defenses and response mechanisms. Here's why option A is the best choice:

Controlled Testing Environment: BAS tools provide a controlled environment where multiple TTPs can be tested without causing unintended damage to the internal systems and servers. This is critical when the threat-modeling team indicates

potential impacts on internal systems.

Comprehensive Coverage: BAS tools are designed to cover a wide range of TTPs, allowing the penetration tester to simulate various attack scenarios. This helps in assessing the reactions (alerted, blocked, and others) by the client's security

tools comprehensively.

Feedback and Reporting: These tools provide detailed feedback and reporting on the effectiveness of the security measures in place, including which TTPs were detected, blocked, or went unnoticed. This information is invaluable for the

threat- modeling team to understand the current security posture and areas for improvement.

References from Pentest:

Anubis HTB: This write-up highlights the importance of using controlled tools and methods for testing security mechanisms. BAS tools align with this approach by providing a controlled and systematic way to assess security defenses. Forge

HTB: Emphasizes the use of various testing tools and techniques to simulate real-world attacks and measure the effectiveness of security controls. BAS tools are mentioned as a method to ensure comprehensive coverage and minimal risk to

internal systems.

Conclusion:

Using a BAS tool to test multiple TTPs allows for a thorough and controlled assessment of the client's security tools' effectiveness. This approach ensures that the testing is systematic, comprehensive, and minimally disruptive, making it the

best choice.

QUESTION 12

A penetration tester attempts to run an automated web application scanner against a target URL. The tester validates that the web page is accessible from a different device. The tester analyzes the following HTTP request header logging output:

```
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
```

```
200; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
```

```
No response; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: curl 200; POST /login.aspx HTTP/1.1 Host: foo.com; User-Agent: Mozilla/5.0
```

No response; GET /login.aspx HTTP/1.1 Host: foo.com; User-Agent: python Which of the following actions should the tester take to get the scans to work properly?

- A. Modify the scanner to slow down the scan.
- B. Change the source IP with a VPN.
- C. Modify the scanner to only use HTTP GET requests.
- D. Modify the scanner user agent.

Correct Answer: D