Vendor: CompTIA

Exam Code: PT0-002

Exam Name: CompTIA PenTest+ Exam: PT0-002 Exam

Version: DEMO

QUESTION 1

A mail service company has hired a penetration tester to conduct an enumeration of all user accounts on an SMTP server to identify whether previous staff member accounts are still active. Which of the following commands should be used to accomplish the goal?

A. VRFY and EXPN
B. VRFY and TURN
C. EXPN and TURN
D. RCPT TO and VRFY

Answer: A
Explanation:
SMTP servers can also be used for information gathering by connecting to them and using the EXPN and VRFY commands.
https://hackerone.com/reports/193314

QUESTION 2

A penetration tester has obtained shell access to a Windows host and wants to run a specially crafted binary for later execution using the wmic.exe process call create function. Which of the following OS or filesystem mechanisms is MOST likely to support this objective?

A. Alternate data streams
B. PowerShell modules
C. MP4 steganography
D. PsExec

Answer: B
Explanation:
WMI allows scripting languages (such as VBScript or Windows PowerShell) to manage Microsoft Windows personal computers and servers, both locally and remotely.
https://en.m.wikipedia.org/wiki/Windows_Management_Instrumentation

QUESTION 3

A penetration tester wants to scan a target network without being detected by the client's IDS. Which of the following scans is MOST likely to avoid detection?

A. nmap -p0 -T0 -sS 192.168.1.10
B. nmap -sA -sV --host-timeout 60 192.168.1.10
C. nmap -f --badsum 192.168.1.10
D. nmap -A -n 192.168.1.10

Answer: A
Explanation:
If Nmap is run without the -P0 flag when performing third-party scanning, the source IP address of the attacker’s host performs ICMP and TCP pinging of the target hosts before starting to scan; this can appear in firewall and IDS audit logs of security-conscious organizations.

QUESTION 4

A penetration tester runs the following command on a system:

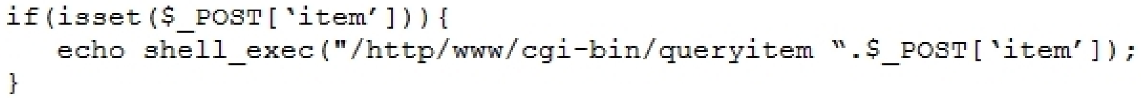
```
find /-user root -perm -4000 -print 2>/dev/null
```

Which of the following is the tester trying to accomplish?

A. Set the SGID on all files in the /directory
B. Find the /root directory on the system
C. Find files with the SUID bit set
D. Find files that were created during exploitation and move them to /dev/null

Answer: C
Explanation:
SUID (Set owner User ID up on execution) is a special type of file permissions given to a file. SUID is defined as giving temporary permissions to a user to run a program/file with the permissions of the file owner rather that the user who runs it.
In simple words users will get file owner's permissions as well as owner UID and GID when executing a file/program/command.
https://www.linux.com/training-tutorials/what-suid-and-how-set-suid-linuxunix/

QUESTION 5
A penetration tester finds a PHP script used by a web application in an unprotected internal source code repository. After reviewing the code, the tester identifies the following:



```
if(isset($_POST['item'])){
    echo shell_exec("/http/www/cgi-bin/queryitem ".$_POST['item']);
}
```

Which of the following tools will help the tester prepare an attack for this scenario?

A. Hydra and crunch
B. Netcat and cURL
C. Burp Suite and DIRB
D. Nmap and OWASP ZAP

Answer: B
Explanation:
It’s shell exec, not all web app host databases. Burp is a great tool for enumeration and intercepting http requests but that line of code (shell exec) is telling us we could place a reverse shell, trigger it with curl and receive the incoming connection via net at.

QUESTION 6
A penetration tester is looking for a vulnerability that enables attackers to open doors via a specialized TCP service that is used for a physical access control system. The service exists on more than 100 different hosts, so the tester would like to automate the assessment. Identification requires the penetration tester to:

```
Have a full TCP connection
Send a "hello" payload
Walt for a response
Send a string of characters longer than 16 bytes
```

Which of the following approaches would BEST support the objective?

A. Run nmap -Pn -sV -script vuln <IP address>.
B. Employ an OpenVAS simple scan against the TCP port of the host.
C. Create a script in the Lua language and use it with NSE.
D. Perform a credentialed scan with Nessus.

Answer: C
Explanation:
The Nmap Scripting Engine (NSE) is one of Nmap's most powerful and flexible features. It allows users to write (and share) simple scripts (using the Lua programming language) to automate a wide variety of networking tasks.
https://nmap.org

QUESTION 7
A penetration tester needs to perform a test on a finance system that is PCI DSS v3.2.1 compliant. Which of the following is the MINIMUM frequency to complete the scan of the system?

A. Weekly
B. Monthly
C. Quarterly
D. Annually

Answer: C
Explanation:
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Address vulnerabilities and perform rescans as needed, until passing scans are achieved. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, complete four consecutive quarters of passing scans. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes and internal scans may be performed by internal staff.
https://www.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

QUESTION 8
A penetration tester has been hired to configure and conduct authenticated scans of all the servers on a software company's network.
Which of the following accounts should the tester use to return the MOST results?

A. Root user
B. Local administrator
C. Service
D. Network administrator

Answer: C
Explanation:
Service accounts are a special type of non-human privileged account used to execute applications and run automated services, virtual machine instances, and other processes. Service accounts can be privileged local or domain accounts, and in some cases, they may have domain administrative privileges.
https://www.beyondtrust.com/blog/entry/how-to-manage-and-secure-service-accounts-best-practices

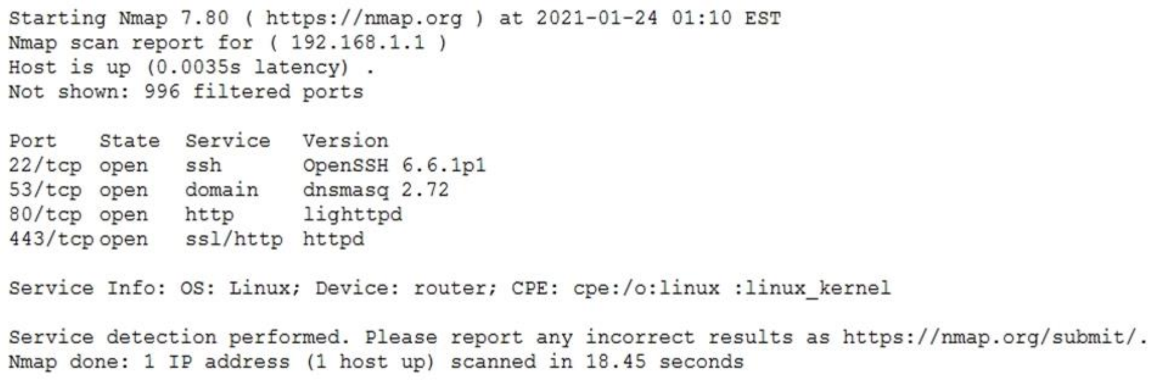
QUESTION 9

A penetration tester who is conducting a vulnerability assessment discovers that ICMP is disabled on a network segment. Which of the following could be used for a denial-of-service attack on the network segment?

A. Smurf
B. Ping flood
C. Fraggle
D. Ping of death

Answer: C
Explanation:
A Fraggle Attack is a denial-of-service (DoS) attack that involves sending a large amount of spoofed UDP traffic to a router's broadcast address within a network. It is very similar to a Smurf Attack, which uses spoofed ICMP traffic rather than UDP traffic to achieve the same goal. Given those routers (as of 1999) no longer forward packets directed at their broadcast addresses, most networks are now immune to Fraggle (and Smurf) attacks.

QUESTION 10
The results of an Nmap scan are as follows:



```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-24 01:10 EST
Nmap scan report for ( 192.168.1.1 )
Host is up (0.0035s latency) .
Not shown: 996 filtered ports

Port    State  Service   Version
22/tcp  open   ssh       OpenSSH 6.6.1p1
53/tcp  open   domain    dnsmasq 2.72
80/tcp  open   http      lighttpd
443/tcp open   ssl/http  httpd

Service Info: OS: Linux; Device: router; CPE: cpe:/o:linux :linux_kernel

Service detection performed. Please report any incorrect results as https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 18.45 seconds
```

Which of the following would be the BEST conclusion about this device?

A. This device may be vulnerable to the Heartbleed bug due to the way transactions over TCP/22 handle heartbeat extension packets, allowing attackers to obtain sensitive information from process memory.
B. This device is most likely a gateway with in-band management services.
C. This device is most likely a proxy server forwarding requests over TCP/443.
D. This device may be vulnerable to remote code execution because of a butter overflow vulnerability in the method used to extract DNS names from packets prior to DNSSEC validation.

Answer: B
Explanation:
The heartbleed bug is an openssl bug which does not affect SSH.
https://www.sos-berlin.com/en/news-heartbleed-bug-does-not-affect-jobscheduler-or-ssh

QUESTION 11
A company is concerned that its cloud service provider is not adequately protecting the VMs housing its software development. The VMs are housed in a datacenter with other companies sharing physical resources. Which of the following attack types is MOST concerning to the

company?

A. Data flooding
B. Session riding
C. Cybersquatting
D. Side channel

Answer: D
Explanation:
Cross-VM Cache Side Channel Attacks make it Vulnerable:
One of the most sophisticated forms of attack is the cross-VM cache side channel attack that exploits shared cache memory between VMs. A cache side channel attack results in side channel data leakage, such as cryptographic keys. In cases where there exist shared hardware resources, the side channel attack exploits information obtained from the usage of, for example, Central Processing Unit (CPU) core and high level cache memory as opposed to exploiting theoretical weaknesses like the brute force attack.
Ref: https://arxiv.org/pdf/1606.01356.pdf

QUESTION 12
A penetration tester who is doing a company-requested assessment would like to send traffic to another system using double tagging. Which of the following techniques would BEST accomplish this goal?

A. RFID cloning
B. RFID tagging
C. Meta tagging
D. Tag nesting

Answer: D
Explanation:
Since vlan hopping requires 2 vlans to be nested in a single packet.
Double tagging occurs when an attacker adds and modifies tags on an Ethernet frame to allow the sending of packets through any VLAN. This attack takes advantage of how many switches process tags.
Most switches will only remove the outer tag and forward the frame to all native VLAN ports. With that said, this exploit is only successful if the attacker belongs to the native VLAN of the trunk link.
https://cybersecurity.att.com/blogs/security-essentials/vlan-hopping-and-mitigation

QUESTION 13
SIMULATION

You are a penetration tester running port scans on a server.

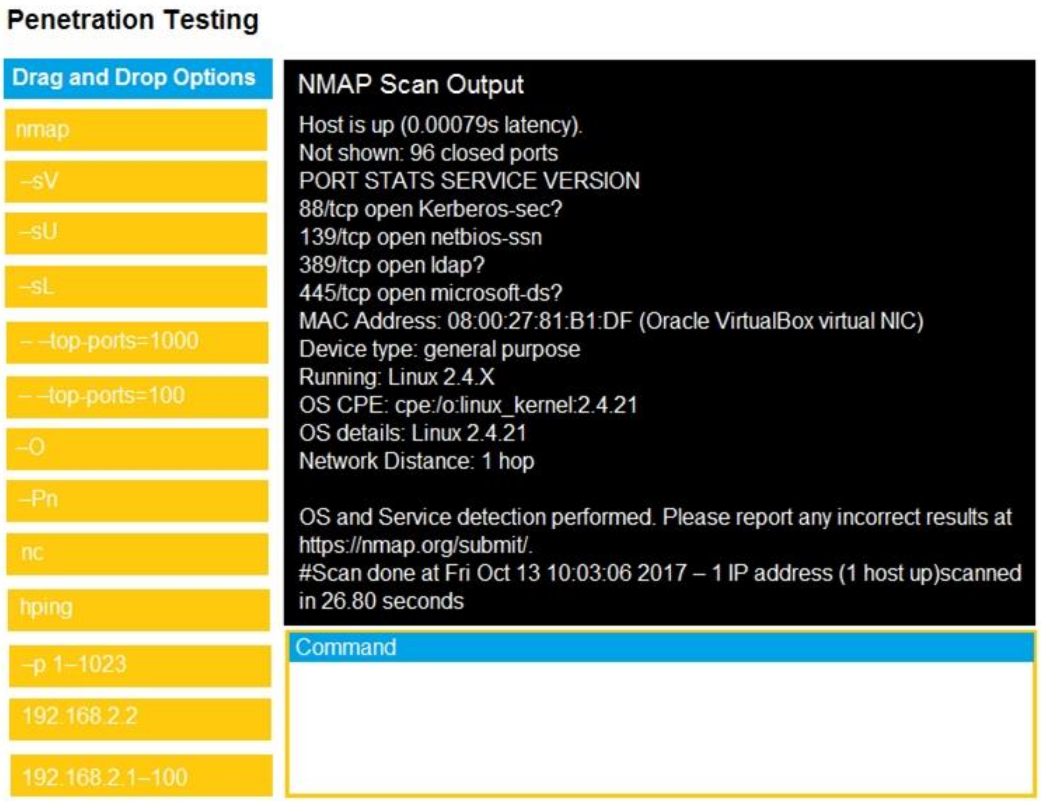
INSTRUCTIONS

Part1: Given the output, construct the command that was used to generate this output from the available options.

Part2: Once the command is appropriately constructed, use the given output to identify the potential attack vectors that should be investigated further.

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

Part1



Penetration Testing

Drag and Drop Options

nmap

–sV

–sU

–sL

– –top-ports=1000

– –top-ports=100

–O

–Pn

nc

hping

–p 1–1023

192.168.2.2

192.168.2.1–100

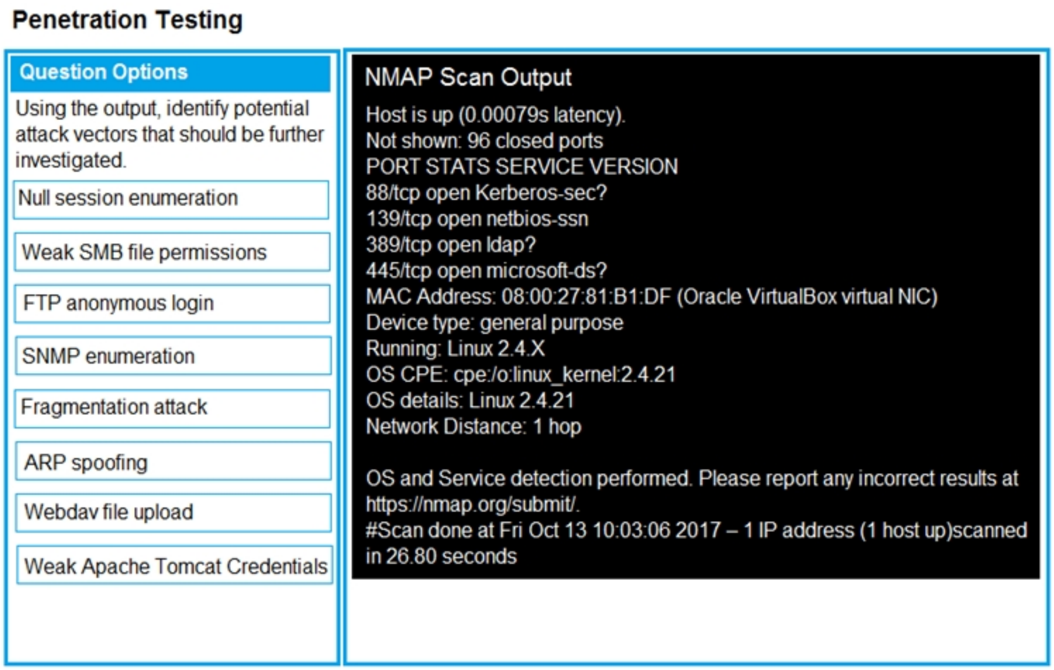
NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open Kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
#Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)scanned
in 26.80 seconds
```

Command

Part2



Penetration Testing

Question Options

Using the output, identify potential attack vectors that should be further investigated.

Null session enumeration

Weak SMB file permissions

FTP anonymous login

SNMP enumeration

Fragmentation attack

ARP spoofing

Webdav file upload

Weak Apache Tomcat Credentials

NMAP Scan Output

```
Host is up (0.00079s latency).
Not shown: 96 closed ports
PORT STATS SERVICE VERSION
88/tcp open Kerberos-sec?
139/tcp open netbios-ssn
389/tcp open ldap?
445/tcp open microsoft-ds?
MAC Address: 08:00:27:81:B1:DF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.4.X
OS CPE: cpe:/o:linux_kernel:2.4.21
OS details: Linux 2.4.21
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/.
#Scan done at Fri Oct 13 10:03:06 2017 – 1 IP address (1 host up)scanned
in 26.80 seconds
```

Answer:

Part 1 – nmap -sV -O --top-ports=100 192.168.2.2
Tried scanning 1 host on my machine. Without -sV you will not get question marks in your port services. We can also clearly see only 100 ports are being scanned. Commander123 is correct.

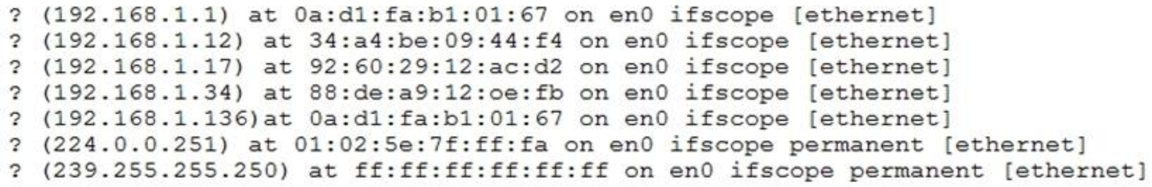
Part 2 – Null session enumeration
Looking at the output you can see ports 139 and 445 are opened. This is wide open for a Null session attack.

QUESTION 13
During a penetration-testing engagement, a consultant performs reconnaissance of a client to identify potential targets for a phishing campaign.
Which of the following would allow the consultant to retrieve email addresses for technical and billing contacts quickly, without triggering any of the client's cybersecurity tools? (Choose two.)

A. Scraping social media sites
B. Using the WHOIS lookup tool
C. Crawling the client's website
D. Phishing company employees
E. Utilizing DNS lookup tools
F. Conducting wardriving near the client facility

Answer: AC
Explanation:
Technical and billing addresses are usually posted on company websites and company social media sites for the their clients to access.
The WHOIS lookup will only avail info for the company registrant, an abuse email contact, etc but it may not contain details for billing addresses.

QUESTION 14
A consultant is reviewing the following output after reports of intermittent connectivity issues:



```
? (192.168.1.1) at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (192.168.1.12) at 34:a4:be:09:44:f4 on en0 ifscope [ethernet]
? (192.168.1.17) at 92:60:29:12:ac:d2 on en0 ifscope [ethernet]
? (192.168.1.34) at 88:de:a9:12:oe:fb on en0 ifscope [ethernet]
? (192.168.1.136)at 0a:d1:fa:b1:01:67 on en0 ifscope [ethernet]
? (224.0.0.251) at 01:02:5e:7f:ff:fa on en0 ifscope permanent [ethernet]
? (239.255.255.250) at ff:ff:ff:ff:ff:ff on en0 ifscope permanent [ethernet]
```

Which of the following is MOST likely to be reported by the consultant?

A. A device on the network has an IP address in the wrong subnet.
B. A multicast session was initiated using the wrong multicast group.
C. An ARP flooding attack is using the broadcast address to perform DDoS.
D. A device on the network has poisoned the ARP cache.

Answer: D
Explanation:
The gateway for the network (192.168.1.1) is at 0a:d1:fa:b1:01:67, and then, another machine (192.168.1.136) also claims to be on the same MAC address.

With this on the same network, intermittent connectivity will be inevitable as along as the gateway remains unreachable on the IP known by the others machines on the network, and given that the new machine claiming to be the gateway has not been configured to route traffic.

QUESTION 15
Which of the following web-application security risks are part of the OWASP Top 10 v2017? (Choose two.)

A. Buffer overflows
B. Cross-site scripting
C. Race-condition attacks
D. Zero-day attacks
E. Injection flaws
F. Ransomware attacks

Answer: BE
Explanation:
The 2017 owasp top 10 list has these items:
A01-Injection
A02-Broken Authentication
A03-Sensitive Data Exposure
A04-XXE
A05-Broken Access Control
A06-Security Misconfiguration
A07-XSS
A08-Insecure Deserialization
A09-Using Components with Known Vulnerabilities
A10-Insufficient Logging & Monitoring

QUESTION 16
An attacker uses SET to make a copy of a company's cloud-hosted web mail portal and sends an email in hopes the Chief Executive Officer (CEO) logs in to obtain the CEO's login credentials. Which of the following types of attacks is this an example of?

A. Elicitation attack
B. Impersonation attack
C. Spear phishing attack
D. Drive-by download attack

Answer: C
Explanation:
The Social Engineer Toolkit (SET) provides a framework for automating the social engineering process, including sending spear phishing messages, hosting fake websites, and collecting credentials. Social engineering plays an important role in many attacks. SET is a menu-driven social engineering attack system. In this scenario, the penetration tester is attempting a spear phishing attack.

QUESTION 17
A tester has determined that null sessions are enabled on a domain controller.
Which of the following attacks can be performed to leverage this vulnerability?

A. RID cycling to enumerate users and groups
B. Pass the hash to relay credentials
C. Password brute forcing to log into the host
D. Session hijacking to impersonate a system account

Answer: A
Explanation:
One of the first steps when looking to gain access to a host, system, or application is to enumerate usernames. Once usernames are guessed, targeted password-based attacks can then be attempted. A RID cycling attack attempts to enumerate user accounts through null sessions. If a tester specifies a password file, it will automatically attempt to brute force the user accounts when it’s finished enumerating. So, in this scenario, attempting RID cycling will be the next step the tester should try.

QUESTION 18
A company planned for and secured the budget to hire a consultant to perform a web application penetration test.
Upon discovered vulnerabilities, the company asked the consultant to perform the following tasks:

```
- Code review
- Updates to firewall setting
```

A. Scope creep
B. Post-mortem review
C. Risk acceptance
D. Threat prevention

Answer: A
Explanation:
A scope creep, or the addition of more items and targets to the scope of the assessment, is a constant menace for penetration testing. During the scoping phase, a tester is unlikely to know all of the details of what may be uncovered, and during the assessment itself, a tester may encounter unexpected new targets. Scope creep refers to how a project’s requirements tend to increase over a project life cycle.

QUESTION 19
A penetration tester is preparing to conduct API testing.
Which of the following would be MOST helpful in preparing for this engagement?

A. Nikto
B. WAR
C. W3AF
D. Swagger

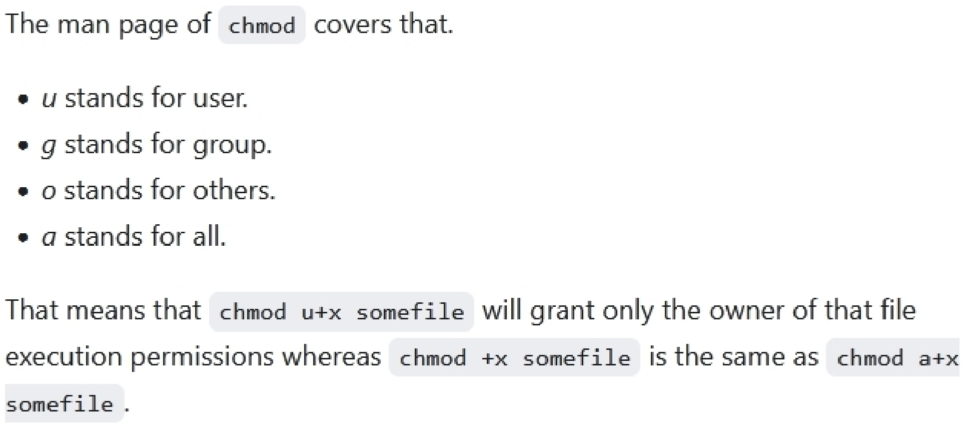
Answer: D
Explanation:
Swagger is an open specification for defining REST APIs. A Swagger document is the REST API equivalent of a WSDL document for a SOAP-based web service. The Swagger document specifies the list of resources that are available in the REST API and the operations that can be called on those resources. It also specifies the list of parameters to an operation, including the name and type of the parameters, whether the parameters are required or optional, and

information about acceptable values for those parameters. So, access to a Swagger document provides testers with a good view of how the API works and thus how they can test it.

QUESTION 20
Which of the following commands will allow a penetration tester to permit a shell script to be executed by the file owner?

A. `chmod u+x script.sh`
B. `chmod u+e script.sh`
C. `chmod o+e script.sh`
D. `chmod o+x script.sh`

Answer: A
Explanation:



The man page of `chmod` covers that.

- *u* stands for user.
- *g* stands for group.
- *o* stands for others.
- *a* stands for all.

That means that `chmod u+x somefile` will grant only the owner of that file execution permissions whereas `chmod +x somefile` is the same as `chmod a+x somefile`.

https://newbedev.com/chmod-u-x-versus-chmod-x

QUESTION 21
A consulting company is completing the ROE during scoping.

Which of the following should be included in the ROE?

A. Cost of the assessment
B. Report distribution
C. Testing restrictions
D. Liability

Answer: C
Explanation:
The Rules of Engagement, or ROE, are meant to list out the specifics of your penetration testing project to ensure that both the client and the engineers working on a project know exactly what is being testing, when its being tested, and how its being tested.