1. Which are two best practices used to secure APIs? (Choose two.)

- **use reputable and standard libraries to create the APIs**
- **make internal API documentation mandatory**
- discussing company API development (or any other application development) on public forums
- secure API services to provide HTTP endpoints only
- keep API implementation and API security into one tier allowing the API developer to work on both facets simultaneously

2. Which type of threat actors use cybercrime attacks to promote what they believe in?

- state-sponsored
- **hacktivists**
- organized crime
- insider threats

3. A company conducted a penetration test 6 months ago. However, they have acquired new firewalls and servers to strengthen the network and increase capacity. Why would an administrator request a new penetration test?

- **The attack surface has changed with the new equipment added.**
- The servers require independent performance evaluation.
- The core data has been moved to the cloud infrastructure.
- New cloud-based applications have been implemented.

4. A network administrator performs a penetration test for a company that sells computer parts through an online storefront. The first step is to discover who owns the domain name that the company is using. Which penetration testing tool can be used to do this?

- h8mail
- Maltego
- **WHOIS**
- Exif

5. A penetration tester wants to quickly discover all the live hosts on the 192.168.0.0/24 network. Which command can do the ping sweep using the nmap tool?

- nmap 192.168.1.0/24 -open
- nmap -sP 192.168.0.0/24
- nmap -sV 192.168.0.255
- **nmap -sn 192.168.0.0/24**
- nmap -p 1-65535 localhost

6. A penetration tester runs the command nmap -sF -p 80 192.168.1.1 against a Windows host and receives a response RST packet. What conclusion can be drawn on the status of port 80?

- **undetermined as this is a default response on a Windows system**
- port 80 is open
- port 80 is closed
- port 80 is open/filtered

7. Which common tool is used by penetration testers to craft packets?

- h8mail
- pip3
- nmap
- Recon-ng
- **scapy**

8. Why should a tester use query throttling techniques when running an authorized penetration test on a live network?

- to limit bandwidth on resource heavy applications
- **to reduce the number of attack threads that are being sent to the target at the same time**
- to limit bandwidth on real-time antivirus and malware scanners
- to create a larger attack surface on the target

9. Why would an organization hire a red team?

- to install equipment to protect against physical intrusion
- **to play the role of a threat actor by exposing vulnerabilities regarding technology**
- to defend the organization against cybersecurity threats

- to evaluate the work of the security team of the organization

10. Match the healthcare sector term to the respective description.

Healthcare provider	a person or organization that performs certain functions involving the use of PHI on behalf of, or provides services to, a covered entity
Health plan	a person or an organization that provides patient or medical services
Healthcare clearinghouse	a government program that pays for healthcare
Business associates	an entity that processes nonstandard health information it receives from another entity into a standard format

11. Which two elements are typically on the front of a credit card? (Choose two.)

- date of birth
- **embedded microchip**
- magnetic stripe
- **primary account number**
- card security code

12. What can be used to document the testing timeline in a rules of engagement document?

- OWASP ZAP
- **Gantt charts and work breakdown structures**
- Recon-ng
- Burp Suite

13. A cybersecurity firm has been hired by an organization to perform penetration tests. The tests require a secure method of transferring data over a network. Which two protocols could be used to accomplish this task? (Choose two.)

- **SFTP**
- PGP
- **SCP**
- S/MIME
- HTTPS

14. Match penetration testing methodology and standard with the respective description.

MITRE ATT&CK	this is a compilation of high-level phases of web application security testing and digs deeper into the testing methods used. This is primarily used by penetration testers from the web application security testing perspective.
NIST	this is a document created to provide organizations with guidelines on planning and conducting information security testing. It is considered an industry standard for penetration testing guidance and is called out in many other industry standards and documents.
OWASP WSTG	this is a resource for learning about the tactics of an adversary, techniques, and procedures (TTPs). This framework is a collection of different matrices of tactics, techniques, and sub-techniques used by penetration testers for both offensive and defensive purposes.
OSSTMM	this is a peer-reviewed security testing methodology maintained by the Institute for Security and Open Methodologies (ISECOM). It is an open security research community providing original resources, tools, and certifications in the security field. It uses a document that lays out repeatable and consistent security testing.

15. Which three practices are commonly adopted when setting up a penetration testing lab environment? (Choose three.)

- use a honeypot for all tests run from the physical attack platforms
- **ensure that when something crashes, it can be determined how and why it happened**
- **create the penetration testing environment using virtual machines and virtual switches**
- use an open environment to allow for free passage of attack packets to the target machines
- create the penetration testing environment using physical equipment and switches in order to route the packets freely
- **use a closed environment for all testing purposes**

16. An organization wants to test its vulnerability to an employee with network privileges accessing the network maliciously. Which type of penetration test should be used to test this vulnerability?

- white-box
- black-box
- blue-box
- **gray-box**

17. Refer to the exhibit. A penetration is being prepared to run the EternalBlue exploit using Metasploit against a target with an IP address of 10.0.0.1/8 from the source PC with an IP address of 10.0.0.111/8. What two commands must be entered before the exploit command can be run? (Choose two.)

```
msf > use exploit/windows/smb/ms17_010_eternalblue
msf exploit(windows/smb/ms17_010_eternalblue) > show options
Module options (exploit/windows/smb/ms17_010_eternalblue):
 Name                Current Setting  Required  Description
 ----                ---------------  --------  -----------
 GroomAllocations    12               yes       Initial number of times
                                                 to groom the kernel
                                                 pool.
 GroomDelta          5                yes       The amount to increase
                                                 the groom count per
                                                 try.
 MaxExploitAttempts  3                yes       The number of times to
                                                 retry the exploit.
 ProcessName         spoolsv.exe      yes       Process to inject
                                                 payload into.
 RHOST                                yes       The target address
 RPORT               445              yes       The target port (TCP)
 SMBDomain           .                no        (Optional) The Windows
                                                 domain to use for
                                                 authentication
 SMBPass                              no        (Optional) The password
                                                 for the specified
                                                 username
 SMBUser                              no        (Optional) The username
                                                 to authenticate as
 VerifyArch          true             yes       Check if remote
                                                 architecture matches
                                                 exploit Target.
 VerifyTarget true yes Check if remote OS matches exploit Target.
<output omitted for brevity>
```

- set LHOST 10.0.0.1
- set TARGET 10.0.0.111
- **set LHOST 10.0.0.111**
- **set RHOST 10.0.0.1**
- set RHOST 10.0.0.111
- set TARGET 10.0.0.1

18. A penetration tester runs the Nmap NSE script nmap –script smtp-open-relay.nse 10.0.0.1 command on a Kali Linux PC. What is the purpose of running this script?

- to check whether the smtp authentication is compromised on the target server
- **to check open relay configurations on the target server**
- to compromise any snmp community strings on the target PC

- to compromise any open relays on the target server

19. Refer to the exhibit. What is the penetration tester trying to achieve by running this exploit?

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOSTS 172.16.20.136
RHOSTS => 172.16.20.136
msf auxiliary(scanner/ftp/anonymous) > exploit

[+] 172.16.20.136:21 - 172.16.20.136:21 - Anonymous READ (220 (vsFTPd
3.0.3))
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

- to enumerate FTP login on the target system
- **to check if the target system will allow FTP anonymous login**
- to compromise the target system for a remote session
- to launch 220 packets of fragmented data to the FTP port on the target system

20. A penetration tester deploys a rogue AP in the target wireless infrastructure. What is the first step that has to be taken to force wireless clients to connect to the rogue AP?

- send out false DNS beacons
- spoof the MAC address of the rogue AP
- set the PSK key to match the clients
- **send de-authentication frames to the clients**

21. A cybersecurity student is learning about the Social-Engineer Toolkit (SET), and the student has discovered that this tool can be used to launch various social engineering attacks. Which two social engineering attacks can be launched using SET?

- **Create a payload and listener**
- Google phishing
- Simple hijacker
- Fake flash update
- **Infectious media generator**

22. A threat actor spoofed the phone number of the director of HR and called the IT help desk with a login problem. The threat actor claims to be the director and wants the help desk to change the password. What method of influence is this cybercriminal using?

- scarcity
- social proof
- fear
- **authority**

23. Which statement correctly describes a type of physical social engineering attack?

- Dumpster phishing refers to a threat actor who scavenges for victims' private information in garbage and recycling containers.
- **Social engineering techniques, software, and hardware can perform badge cloning attacks.**
- Tailgating and piggybacking attacks can only be defeated through the use of control vestibules in conjunction with multifactor authentication.
- Shoulder surfing attacks are performed only by a short distance between the threat actor and the victim.

24. What is a characteristic of a pharming attack?

- **a threat actor redirects a victim from a valid website to a malicious legitimate looking site**
- a type of attack in which a social engineer impersonates another person to have physical access to systems in an organization
- a social engineering attack carried out in a phone conversation
- a type of attack where the threat actor obtains confidential data of the victim using binoculars or even a telescope

25. What kind of social engineering attack can be prevented by developing policies such as updating anti-malware applications regularly and using secure virtual browsers with little connectivity to the rest of the system and the rest of the network?

- tailgating
- **watering hole**
- vishing
- SMS phishing

26. An attacker enters the string 'John' or '1=1' on a web form that is connected to a back-end SQL server causing the server to display all records in the database table. Which type of SQL injection attack was used in this scenario?

- error-based SQL injection
- inferential SQL injection
- **boolean SQL injection**
- out-of-band SQL injection

27. What are two examples of immutable queries that should be used as mitigation for SQL injection vulnerabilities? (Choose two.)

- **static queries**
- time-delay queries
- **parameterized queries**
- in-band queries
- stacked queries

28. An attacker enters the string 192.168.78.6;cat /etc/httpd/httpd.conf on a web application hosted on a Linux server. Which type of attack occurred?

- session hijacking
- redirect attack
- SQL injection
- **command injection**

29. Which two misconfigured cloud authentication methods could leverage a cloud asset? (Choose two.)

- **federated authentication**
- biometric authentication
- **identity and access management (IAM) implementations**
- Intelligent Platform Management Interface (IPMI)
- local authentication

30. Match the cloud attack to the description.

Account Takeover	when a threat actor gains access to a user or application account and uses it to then gain access to more accounts and information
Privilege Escalation	act of gathering and stealing valid usernames, passwords, tokens, PINs, and any other types of credentials through infrastructure breaches
Credential Harvesting	act of exploiting a bug or design flaw in a software or firmware application to gain access to resources that normally would have been protected from an application or a user

31. What is the purpose of using the smtp-user-enum -M VRFY -u snp -t 10.0.0.1 command in Kali Linux?

- to initiate an SMTP conversation with an email server 10.0.0.1
- to start a Transport Layer Security (TLS) connection to an email server 10.0.0.1
- **to verify if a certain user exists on the SMTP server 10.0.0.1**
- to compromise SMTP open relay server 10.0.0.1

32. Match the mobile device security testing tool to the description.

ApkX	this tool enables you to decompile Android application package files.
Burp Suite	this open-source framework is used to test the security of iOS applications.
Needle	this can test mobile applications and determine how they communicate with web services and APIs.
Drozer	this Android testing platform and framework provides access to numerous exploits that can be used to attack Android platforms.

33. Match the mobile device attack to the description.

Sandbox analysis	this can enable a threat actor to bypass the access control mechanisms implemented by Android, Apple iOS, and mobile app developers.
Spamming	this presents users with links to redirect them to malicious sites to steal sensitive information or install malware.
Reverse engineering	this is the process of analyzing a mobile app to extract information about the source code to understand the underlying architecture of a mobile application and potentially manipulate the mobile device.

34. Which two Bluetooth Low Energy (BLE) statements are true? (Choose two.)

- All BLE-enabled devices implement cryptographic functions.
- BLE involves a five-phase process to establish a connection.
- **Threat actors can listen to BLE advertisements and leverage misconfigurations.**
- **BLE advertisement can be intercepted using specialized antennas and equipment.**
- BLE pairing is done by mobile apps.

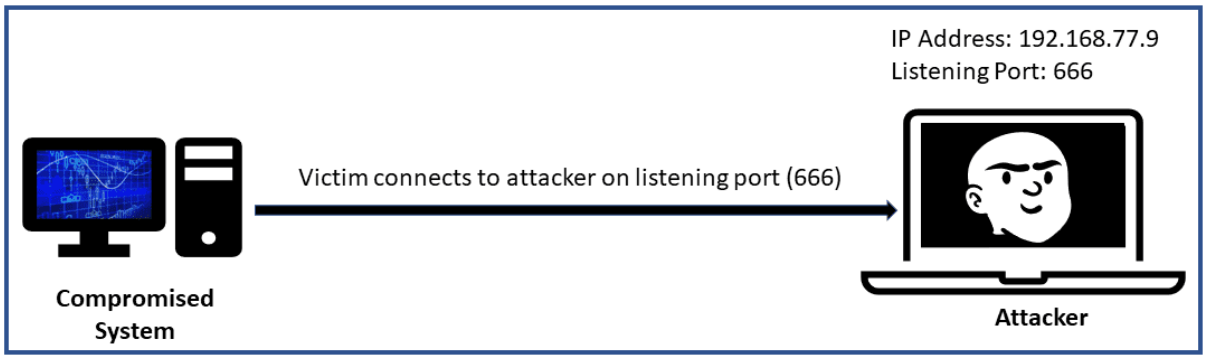
35. Match the insecure code practice to the description.

Comments in source code	many APIs lack adequate controls and are difficult to monitor. The breadth and complexity of APIs also make it difficult to automate effective security testing.
Lack of error handling and overly verbose error handling	developers include information in source code that could provide too much information and might be leveraged by an attacker.
Hard-coded credentials	a type of weakness and security malpractice that can provide information to help an attacker perform additional attacks on the targeted system.
Unprotected APIs	a catastrophic flaw that an attacker can leverage to completely compromise an application or the underlying system.

36. Which C2 utility can be used to create multiple reverse shells?

- WMImplant
- TrevorC2
- **Socat**
- Wsc2

37. Refer to the exhibit. The attacking system has a listener (port open), and the victim initiates a connection back to the attacking system. Which two resources can create this type of malicious activity? (Choose two.)



- **Empire**
- Sysinternals
- BloodHound
- Steghide
- **Netcat**

38. Match the PowerSploit module/script to the respective description.

PowerView	does a simple TCP port scan using regular sockets, based rather loosely on Nmap
PowerUp	causes the machine to blue screen upon exiting PowerShell
Invoke-Portscan	displays Windows vault credential objects, including plaintext web credentials
Set-CriticalProcess	performs network and Windows domain enumeration and exploitation
Get-VaultCredential	acts as clearinghouse of common privilege escalation checks, along with some weaponization vectors

39. Which two tools can create a remote connection with a compromised system? (Choose two.)

- Nmap
- Mimikatz
- **Metasploit**
- BloodHound
- **Sysinternals**

40. Which two options are PowerSploit modules/scripts? (Choose two.)

- Get-ChildItem
- **Get-Keystrokes**
- Get-HotFix
- Get-Process
- **Get-SecurityPackages**

41. Why is it important to use Common Vulnerability Scoring System (CVSS) to reference the ratings of vulnerabilities identified when preparing the final penetration testing report?

- It is authorized by governments around the world.
- It is an international standard for listing publicly known vulnerabilities.
- It is easy to use.
- **It has been adopted by many tools, vendors, and organizations.**

42. A company hires a professional to perform penetration testing. The tester has identified and verified that one web application is vulnerable to SQL injection and cross-site scripting attacks. Which technical control measure should the tester recommend to the company?

- process-level remediation
- role-based access control (RBAC)
- multifactor authentication
- **user input sanitization**

43. The IT security department of a company has developed an access policy for the datacenter. The policy specifies that the datacenter is locked between 5:30 pm through 7:45 am daily except for emergency access approved by the IT manager. What is the operational control implemented?

- mandatory vacations
- job rotation
- **time-of-day restrictions**
- user training

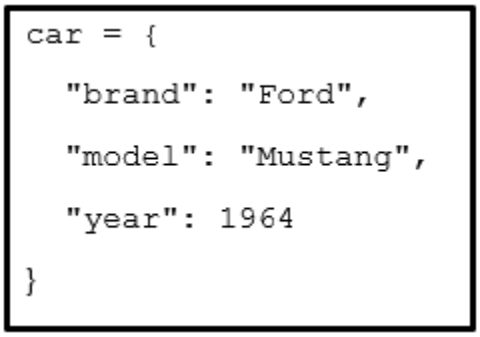
44. A security audit for a company recommends that the company implement multifactor authentication for the datacenter access. Which solution would achieve the goal?

- access control vestibule
- **biometric controls**
- video surveillance
- minimum password requirements

45. What are three examples of the items a penetration tester must clean from systems as part of the post-engagement cleanup process? (Choose three.)

- given passwords
- network diagrams
- **shells**
- **tools**
- system patches
- **tester-created credentials**

46. Refer to the exhibit. Which Python data structure is used?



```
car = {
  "brand": "Ford",
  "model": "Mustang",
  "year": 1964
}
```

- **dictionary**
- array
- list
- tree

47. Which statement describes the concept of Bash shell in operating systems?

- Bash shell is a command shell that supports interactive command execution only.
- Bash shell is a Linux GUI.
- Bash shell is a GUI that can be used in operating systems.
- **Bash shell is a command shell and language interpreter for an operating system.**

48. Which three tools can be used to perform passive reconnaissance? (Choose three.)

- Nmap
- **Dig**
- Enum4linux
- Zenmap
- **Host**

- **Nslookup**

49. An attacker uses John the Ripper to crack a password file. The attacker issued the ~$ john –list=formats command in Kali Linux. Which information is the attacker trying to find?

- the command line format to crack a password file
- the password file format
- **the ciphertext formats supported by the current version**
- the output format supported by the current version

50. What are two exploitation frameworks? (Choose two.)

- **BeEF**
- Proxychains
- Tor
- **Metasploit**
- Encryption