CERTSHOP

CompTIA® PenTest+ - Quiz Questions with Answers

Domain 1.0: Planning and Scoping

1.

Which of the following topics is NOT typically part of a statement of work (SOW)?

Non-disclosure agreement

Scope of work

Payment schedule

Location of work

Correct answer: Non-disclosure agreement

A statement of work (SOW) is a key document for your penetration testing project. If you are at the stage of executing an SOW, it should mean that you have completed your vetting process and will be locking in your penetration testing vendor.

Key items in a penetration testing SOW:

- *Scope*
- *Deliverables*
- *Price*
- *Completion date*
- *Location of work*
- *Payment schedule*

A non-disclosure agreement (NDA) is typically a separate document and only covers the confidentiality of the information owned by the organization.

2.

A pentester wants to learn about current tactics, techniques, and strategies of adversaries. Which resource can they consult to get a general understanding of how incidents occurred across a wide variety of system types and how those incidents were mitigated?

MITRE ATT&CK framework

OWASP

PTES

OSSTMM

Correct answer: MITRE ATT&CK framework

The ATT&CK framework includes matrices for different tactics and techniques of adversaries. However, it is not a complete penetration testing program.

OWASP focuses on web application attacks. PTES is a penetration standards framework. OSSTMM is a penetration testing methodology.

3.

How should a situation be addressed in which the machines you were targeting for your client's pentest were hosted by another entity?

Approval would usually need to be acquired from the hosting company or the cloud provider

Approval does not need to be granted as long as the assets belong to your client

Approval is required only if the assets were hosted in specific countries

If the client approves it, then there is no additional need for approval

---

Correct answer: Approval would usually need to be acquired from the hosting company or the cloud provider

If the targets are hosted in a third-party environment, such as a cloud service provider (CSP), testing is not only subject to the company's policies, but is also subject to the third party's acceptable use policies. For instance, Amazon Web Services (AWS) requires that tenants submit pentesting request forms to receive authorization prior to penetration testing to or from any AWS resource.

4.

Which term is given to an organization that has received approval from the PCI SSC to conduct external vulnerability scanning services?

ASV

Acquirer

PFI

QSA

Correct answer: ASV

An approved scanning vendor (ASV) is an organization that has been approved by the Payment Card Industry Security Standards Council to carry out vulnerability scanning services.

An acquirer is an institution that maintains relationships with merchants that accept credit cards. A PCI forensic investigator (PFI) is an individual trained in forensic techniques after a breach related to cardholder data. A qualified security assessor (QSA) is an individual certified to carry out PCI DSS compliance assessments.

5.

A client is worried that certain modules in Metasploit could cause serious damage to some systems.

Which aspect of an ethical hacking mindset should the pentester apply to this situation?

Limiting the use of tools

Identifying criminal activity

Maintaining confidentiality of data

Limiting invasiveness based on scope

Correct answer: Limiting the use of tools

A client may not want certain tools used in the test. In these situations, pentesters should limit their toolsets to meet the client's requests.

Identifying criminal activity is important for notifying a client right away if they discover a breach during testing. Maintaining confidentiality of data is important for ensuring that pentest results do not fall into the wrong hands. Limiting invasiveness based on the scope is important for not disrupting business practices.

6.

A pentester is looking for a standard that gives information about the types of questions a pentester should ask their client, as well as how to handle third parties.

Which standard should they consult for this?

PTES

MITRE ATT&CK

ISSAF

OWASP

Correct answer: PTES

The Penetration Testing Execution Standard (PTES) gives information about attack types and methods, as well as tools needed for testing methods. Furthermore, it covers pre-engagement interactions, such as what questions to ask clients and how to work with third parties.

MITRE ATT&CK is a knowledge base for adversarial tactics and techniques. The Information System Security Assessment Framework (ISSAF) provides a general framework for informational security. The Open Web Application Security Project (OWASP) focuses on web application security.

7.

A pentester is conducting a pentest. One of their objectives is to attack the company supply chain. During the OSINT phase, the tester is able to identify third-party resources involved in the supply chain. Those resources are not listed in the scope of testing, but they are part of the supply chain and therefore part of the objectives.

How should they handle the third-party resources?

They should only test in-scope resources and completely exclude any other assets from testing.

They should test the third-party resources as long as the tests are not intrusive.

If the supply chain is in the objectives, then they should test everything related to it.

They should contact the client and ask for permission to test the third-party resources.

Correct answer: They should only test in-scope resources and completely exclude any other assets from testing.

Third-party assets or resources are owned by another company. Unless explicitly approved by that company, they should not attack them. There needs to be a written statement from the third party that such tests are approved.

8.

A pentester is preparing for a pentest, but the client is using NAC, which would prevent most, if not all, of the pentester's packets during testing.

What can be done to enable the testing?

The client can make a security exception in the NAC

The pentester can test outside of office hours

The client can disable the firewall

Devices behind the firewall can be excluded from the testing scope

---

Correct answer: The client can make a security exception in the NAC

Sometimes, a security exception at the network layer is needed to enable a pentester to complete their tests. Network access control (NAC) is a solution for preventing unauthorized devices from connecting to a network.

An exception will be easier and safer to implement than the other answer choices.

9.

When preparing for a pentest, which document defines terms such as the project timeline, the deliverables, the payment schedule, and any miscellaneous items that could become issues?

SoW

RoE

MSA

NDA

Correct answer: SoW

The Statement of Work (SOW) usually contains the following main topics:

- *Purpose*
- *Scope of work*
- *Location of work*
- *Period of performance*
- *Deliverable schedule*
- *Applicable industry standards*
- *Acceptance criteria*
- *Special requirements*
- *Payment schedule*

The rules of engagement (RoE) defines boundaries, conditions, and constraints of a penetration test. A master service agreement (MSA) is used to define terms for future work. A non-disclosure agreement (NDA) is used to ensure that any information learned is kept confidential.

10.

Which document includes a payment schedule for the penetration test?

SOW

RoE

Target list

NDA

Correct answer: SOW

The statement of work (SOW) is a document that defines what deliverables will be created, the timeline for the work to be completed, the price of the work, and any additional terms and conditions.

A rules of engagement (RoE) describes in detail the plan for the test. The target list is the scope of the test. A non-disclosure agreement (NDA) ensures that information that the tester receives is not shared with other parties.

11.

Your client was hacked just one month following a penetration test you conducted. It is a vulnerability newly presented due to a software update.

How can you BEST ensure that you are not held liable for this breach?

Include disclaimers in the agreement and final report

Apologize for not being able to detect the vulnerability earlier

Inform the client that you are not accountable for third-party breaches

Do nothing; once a penetration test is completed, pentesters cannot be held liable for any breaches

---

Correct answer: Include disclaimers in the agreement and final report

Usually, disclaimers are used in the testing agreement and the final report. Such disclaimers state that the list of vulnerabilities and findings is presenting the current security state of the environment and is only valid for the point in time when it was conducted.

12.

What type of documentation is MOST useful for a penetration test that targets web application servers?

API

DNS

IP ranges

Network diagrams

Correct answer: API

Application requests are usually part of a web application and would be helpful in a web-based pentest. An example of a sample request could be a list of API calls compiled by developers.

DNS, IP ranges, and network diagrams are useful with tests that have a larger scope.

13.

Which of the following elements in a target list for a pentest is MOST important when considering the legal and regulatory compliance of data maintained by the client?

Physical location

IP ranges

SaaS providers

Domains

Correct answer: Physical location

The location of the test can influence the legal and regulatory requirements that the client has to adhere to. For example, if the site is in the European Union, then it must adhere to GDPR.

IP ranges and domains are not bound by geographic jurisdictions. SaaS may reside in various jurisdictions but typically have their own certifications of regulatory compliance and maintain the data.

14.

A client wants to ensure the confidentiality of the organization's internal information during a penetration test. Which document should be signed for this?

NDA

SOW

RoE

MSA

Correct answer: NDA

A Non-Disclosure Agreement (NDA) is protecting the business's competitive advantages from being disclosed to third parties. In the event the organization is compromised, the vendor is obligated to maintain the secrecy of the privileged information it might obtain during the pentest.

An SOW is a statement of the work that will be performed. An RoE is a document that defines the boundaries, scope, and objectives of a penetration test. An MSA is used to define services that can apply to current and future contracts.

15.

An organization needs a penetration test. They want to be sure that the pentesters they hire have an ethical mindset.

What can they request from the pentesting team to ensure this?

Background checks

NDA

Due diligence

Target list

Correct answer: Background checks

Background checks can be used to determine if a penstester has a criminal background and also to verify their credentials. Since pentesters will have access to sensitive information, it is important that they have an ethical mindset.

A non-disclosure agreement (NDA) is used to ensure that data is not shared with other parties. Due diligence is used to assess finances and operations of an organization. A target list is the assets that will be tested.

16.

When performing an on-site pentest, including Wi-Fi access points, what needs to be clearly defined in the pentest's scope?

SSID of the APs being tested

Wi-Fi channels of the APs being tested

Frequencies of the APs being tested

Number of clients for each AP

Correct answer: SSID of the APs being tested

When conducting on-site pentests involving Wi-Fi Access Points (APs), it is important to have a clear understanding of which APs are in the scope of the test. This will help you exclude potential out-of-scope or third-party APs.

Channels, frequencies, and number of clients do not need to be identified in the scope.

17.

A pentester has been given the following specific requirements to test for:

- Password complexity policy
- Encryption algorithm complexity
- Data encryption in transit and at rest

What type of test are they performing?

A compliance-based assessment

A red team assessment

A blue team assessment

A purple team assessment

Correct answer: A compliance-based assessment

Compliance-based assessments audit an organization's ability to implement and follow a given set of security standards within an environment.

A red team assessment tests the overall security posture. A blue team responds to a simulated attack. A purple team coordinates the red and blue teams.

18.

In the planning phase of a pentest, which of the following topics is the MOST important to consider?

Target selection

Pentesting tools

Firewall rules

Number of VLANs in the environment

Correct answer: Target selection

Selecting the targets to include in the engagement is crucial, as the organization may have many assets (people, processes, facilities, and technologies) located throughout the world that need to be considered during the target selection process.

Pentesting tools, firewall rules, and VLANs can be considered after the targets have been determined.

19.

Through threat modeling, the client determines that their main adversary is determined nation-states using complex attacking techniques. Which sort of threat actor is the organization MOST worried about?

APT

Casual hacker

Hacktivist

Insider threat

Correct answer: APT

An advanced persistent threat (APT) is a type of threat actor motivated to steal sensitive information from high-profile targets using sophisticated hacking capabilities.

A casual hacker uses available tools to find weak targets. A hacktivist is motivated by ideology. An insider threat originates from inside the organization.

20.

In the pre-engagement phase of a penetration test, the tester and the client are identifying the systems, applications, and networks that will be tested, as well as any specific requirements that will be needed.

What type of activity are they engaged in?

Scoping

Enumerating

Sniffing

Scraping

Correct answer: Scoping

When determining the list of targets and the limits of the penetration test, this information is structured and detailed as the scope of the test. The test scope could be a separate document or part of some other document related to the pentest. Defining the scope is extremely important and should be done with care.

Enumerating refers to using a tool to get a list of systems on a network. Sniffing involves listening to traffic that crosses a network. Scraping involves systematically gathering information from websites.

21.

What is the ethical course of action to take if a pentester discovers that a real attacker has already breached a client's network?

Notifying the client immediately

Attempting to contact the attacker

Noting the attack to add to the final report later

Covering the tracks of the attacker

Correct answer: Notifying the client immediately

If a pentester discovers an attack, they should immediately notify the client rather than wait until the end of the test.

22.

You are performing a penetration test at a retail store that handles credit cards onsite.

Which of the following do you need to consider when performing this test?

PCI DSS

GDPR

HIPAA

FIPS 140-2

Correct answer: PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) sets the rules for completing assessments for credit card processing environments and systems.

The General Data Protection Regulation (GDPR) is a European Union regulation that protects data and privacy.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law to protect sensitive patient health information.

FIPS 140-2 is a U.S. government computer security standard used to approve cryptographic modules.

23.

A client contacts you three months after the completion of a pentest. They have been hacked through a vulnerability not listed in your report and are asking for an explanation.

What should you do?

Refer the client to the pentest report disclaimers

Accept the responsibility and cover the losses

Refer the client to your legal team

Conduct a security analysis to verify the initial attack vector

---

Correct answer: Refer the client to the pentest report disclaimers

The testing agreement or scope documentation should contain disclaimers explaining that the test is valid only at the point in time when it is conducted and that the scope and methodology that were chosen can impact the comprehensiveness of the test.

24.

Which of the following data types is considered sensitive authentication data by PCI DSS?

CAV2

PAN

Expiration date

Service code

Correct answer: CAV2

Account data is divided into cardholder data and sensitive authentication data. Sensitive authentication data includes the stripe data/microchip, CAV2/CVC2/CVV2/CID, and PINs/PIB blocks.

Primary account number (PAN), expiration date, and service code are considered cardholder data.

25.

As a penetration tester, you are hired by a company to perform a penetration test at their location, which is in a country that is on the US government's list of places where export of encryption technology is restricted. In your bag of tools and software, you have encryption tools that fall under this US export restriction of encryption technology.

What should you do?

Leave behind all restricted tools/software and travel without them

You have legally bought the tools/software; this restriction does not concern you

Transfer the tools to Canada over the internet

Perform the tests remotely to avoid breaching the restrictions

---

Correct answer: Leave behind all restricted tools/software and travel without them

Penetration testers need to be aware of the export restrictions of their country and abide by them.

26.

In what document might you find the expectations for the penetration tester such as availability, reliability, and quality of service?

SLA

NDA

SOW

MSA

Correct answer: SLA

A service level agreement (SLA) sets expectations for services, including things such as availability, reliability, and quality of service. Although SLAs are most often associated with service providers, SLAs may also be used for pentesters as part of their contract.

An NDA is used to ensure confidentiality. An SOW is a statement of work that needs to be completed. An MSA is a re-usable contract.

27.

A company is hiring an external pentesting company to conduct a penetration test. The company is concerned that in case of successful exploitation, the pentester will gain access to internal information that should be considered confidential.

What can be used to make a one-way agreement of confidentiality to ensure that the penetration testing company does NOT disclose this information?

Unilateral NDA

Bilateral NDA

Multilateral NDA

RoE

Correct answer: Unilateral NDA

A non-disclosure agreement (NDA) is an agreement that legally obliges the parties involved to not disclose any information obtained during the penetration test. A unilateral agreement only ensures that one party in the agreement maintains confidentiality.

In a bilateral NDA, both companies must keep confidentiality. In a multilateral NDA, all parties involved must keep confidentiality. A rules of engagement (RoE) is used to define such information as the scope and boundaries of a pentest.

28.

When planning a penetration test, the client informs the testing company of a specific type of data that falls under national export restrictions. What does that mean for the penetration testers?

It means the testing company cannot export this data to restricted countries.

It means this data is outside of the pentest's scope.

It means that an NDA should be signed.

It means the pentester will need to specify the data in the RoE in order to export it.

Correct answer: It means the testing company cannot export this data to restricted countries.

Export restrictions apply to services, technology, or data. National export restrictions would mean that the given services, data, or technology should not leave the country.

The data may still be included in the scope. NDAs are used to ensure confidentiality. Specifying the data in an RoE will not circumvent the export restriction.

29.

Which aspect of an ethical mindset is needed to ensure that a client's rival organization does not discover the results of a penetration test?

Maintaining confidentiality of data

Limiting invasiveness of the scope

Adhering to the scope of the engagement

Immediately reporting breaches

Correct answer: Maintaining confidentiality of data

A penetration test will result in sensitive data that should not be shared with anyone outside of the client's organization. This information must be kept protected at all times.

Limiting invasiveness of the scope can help from disrupting client activities. Adhering to the scope of the engagement can help from testing systems outside of the initial scope. Immediately reporting breaches helps the client know of a situation right away.

30.

What does a pentester have that a nonethical hacker does not?

Permission to attack

Access to network diagrams

Ability to perform OSINT

Expertise in social engineering tools

Correct answer: Permission to attack

It is important that pentesters receive formal authorization to conduct security tests. Pentesters need to be sure that the individual granting permission to attack is also authorized to approve a penetration test as well.

Pentesters may not have access to network diagrams if the test is in an unknown environment. Both pentesters and nonethical hackers have access to OSINT and social engineering tools.

31.

Which of the following standards gives a general framework for penetration testing, although it has not been updated since 2005?

ISSAF

PTES

OWASP

MITRE ATT&CK

Correct answer: ISSAF

The Information System Security Assessment Framework (ISSAF) gives general guidance on penetration testing but is outdated. It still has use as a reference for understanding best practices in pentesting.

The Penetration Testing Execution Standard (PTES) is an actively maintained framework for planning and executing pentests. The Open Web Application Security Project (OWASP) focuses on web application security. MITRE ATT&CK focuses on threat actors' tactics, techniques, and knowledge.

32.

A penetration test in which the tester is provided with a network topology schema prior to the test, but no other insider information, is considered a:

Partially known environment test

Known environment test

Unknown environment test

Red team assessment

Correct answer: Partially known environment test

Partially known environment testing is a combination of known environment testing and unknown environment testing. The aim of this testing is to search for the defects, if any, due to improper structure or improper usage of applications. The attacker would have limited knowledge of the targeted environment. Being provided with network topology could help the attacker, but at the same time, it does not reveal too much of the infrastructure. Partially known environment testing gives the ability to test both sides of an application, presentation layer as well as the code part.

Unknown environment testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings. This method of test can be applied virtually to every level of software testing: unit, integration, system and acceptance.

Known environment testing is a method of software testing that tests internal structures or workings of an application, as opposed to its functionality. In known environment testing, an internal perspective of the system, as well as programming skills, are used to design test cases. Known environment tests allow the pentester to have insider information that could aid the test process. Such information could include network firewall policies, security patches, etc.

A red team assessment is similar to a penetration test in many ways but is more targeted. The goal of the red team assessment is not to find as many vulnerabilities as possible. The goal is to test the organization's detection and response capabilities. The red team will try to get in and access sensitive information in any way possible, as quietly as possible. The red team assessment emulates a malicious actor targeting attacks and looking to avoid detection, similar to an advanced persistent threat (APT).

33.

A client wants a detailed penetration test that would simulate how an attack could be performed by an insider with credentials and access to documentation about the organization's networks, systems, and architecture.

What strategy should be used for their penetration test?

Known environment assessment

Unknown environment assessment

Partially known environment

Compliance-based assessment

Correct answer: Known environment assessment

Known environment testing allows the pentest team to have insider knowledge of organizational network assets, policies, and procedures.

An unknown environment simulates an outside attack with little insider knowledge. A partially known environment is a hybrid strategy that may include credentials but not full documentation. A compliance-based assessment has specific objectives related to the type of compliance the organization needs.

34.

While conducting a penetration test, a tester notices that their scans reveal new hosts on the targeted network. Those hosts are not listed in the initial scope document and were only revealed through extensive testing.

What sort of scenario has developed?

Scope creep

Stakeholder influence

Project drift

Feature creep

Correct answer: Scope creep

Scope creep occurs during a pentest when additional tasks or testing activities are added to the project and exceed the original expectations documented in the statement of work. This can negatively affect the overall schedule or delivery of the final pentest report.

Stakeholder influence refers to changes or additional requests coming from stakeholders. Project drift refers to a project losing its direction over time. Feature creep refers to adding features to a project beyond its original scope.

35.

You are devising a penetration test plan. The client has informed you that their mission-critical VLAN is only running on a 10 Mbit network and is usually using 90% of the bandwidth just for normal working operations between 9 a.m. and 5 p.m.

Taking this into account, what would you suggest to the client?

Perform network testing outside of working hours and use less aggressive scanning techniques

Do not scan this VLAN, as it might interfere with normal business operations

Scan the VLAN as planned and notify the client in case of congestion

Postpone the test until they upgrade the network to 1 Gbps

Correct answer: Perform network testing outside of working hours and use less aggressive scanning techniques

Obviously, there are some client considerations to take into account. Many tools, like Nessus, OpenVAS, and others, do have options for scheduling tasks. You could configure less aggressive scans and schedule them to be run outside the client's working hours.

36.

You are in the middle of a pentest engagement when one of the hosts you are testing suddenly goes offline. What can you do to remediate the issue?

Contact the appropriate support based on the predefined escalation path

Call the client CEO to inform them of the issue

Note the issue in the report and keep testing other targets

Look for support contacts on the official client website

Correct answer: Contact the appropriate support based on the predefined escalation path

The escalation path is a pre-engagement document to be used in case an issue arises during the engagement. This escalation path usually contains contact details for appropriate support teams.

37.

A pentester is about to conduct a test. The client has informed them that a large percentage of their services are hosted by a third party. What requirement would have to be fulfilled before they can proceed with the test?

A third-party provider authorization

An NDA with the third-party provider

A new pentest agreement with the third-party provider

The pentest should be declined due to the third party

Correct answer: A third-party provider authorization

In cases where a third-party provider is involved, additional authorization would be required by that particular provider.

38.

Which of the following standards covers pentesting methodologies?

NIST 800-115

NIST 800-37

NIST 800-63

NIST 800-88

Correct answer: NIST 800-115

The National Institute of Standards and Technology (NIST) produced document 800-115 to provide organizations with information on planning and conducting security assessments.

NIST 800-37 covers risk management frameworks. NIST 800-63 covers digital identity guidelines. NIST 800-88 covers media sanitization.

39.

You are tasked with helping an organization with threat modeling before a pentest. Your client shares that their most valuable asset is the information they have and the extensive R&D they have invested in. It worries them that data could easily be exfiltrated by almost anyone employed by the organization.

What sort of threat actor are they MOSTLY concerned about?

- **Insider threat**
- Social engineering attacker
- Red team attack
- APT

Correct answer: Insider threat

Insider threat is usually related to information exfiltration. It is fairly easy to copy sensitive internal information to a thumb drive and take it off the premises.

Social engineering and APTs are external threats. A red team attack is part of a penetration test.

40.

Which type of assessment involves stealth and blended methodologies to mimic a real threat actor when exposing vulnerabilities?

Red team

Black box

Vulnerability scanning

Compliance

Correct answer: Red team

Red team assessment involves stealth and blended methodologies (i.e., network penetration testing and social engineering) to conduct scenarios of real-world attacks and determine how well an organization would fare with the use of the customer's existing counter-defense and detection capabilities (i.e., what an attacker could do with a certain level of access).

Black box testing involves the attacking team having no prior knowledge of the target. Vulnerability scanning does not attempt to exploit weaknesses. Compliance testing centers on whether certain laws or regulations are being followed.

41.

A pentester has successfully completed a pentest. The client would like to retain the pentester for subsequent pentests twice a year. Which document should be used to specify the terms so that they do not have to be renegotiated each time?

MSA

NDA

RoE

SLA

Correct answer: MSA

The master service agreement (MSA) is used so that the same terms do not have to be renegotiated each time. They document such topics as:

- *Payment terms*
- *Product warranties*
- *Intellectual property ownership*
- *Dispute resolution*
- *Allocation of risk*
- *Indemnification*

An NDA is for maintaining confidentiality. An RoE defines such items as targets and boundaries. An SLA defines the levels of service that a provider offers to a client.

42.

Allowed and disallowed testing types are usually detailed in which of the following?

RoE

MSA

SOW

NDA

Correct answer: RoE

The rules of engagement (RoE) usually includes the following:

- *Method of communication*
- *Target selection*
- *Time windows*
- *Allowed and disallowed testing types*

An MSA is used to cover multiple contracts over time. A Statement of Work describes the tasks to be performed along with the payment. An NDA ensures confidentiality.

43.

How can companies that conduct penetration testing help protect themselves from risks such as fees, fines, and criminal charges?

Limited liability insurance

NDA

Background checks

Limiting invasiveness of the scope

Correct answer: Limited liability insurance

Many types of professionals use limited liability insurance to protect against malpractice. This can protect against legal claims due to error or negligence.

An NDA is used to keep information private between parties. Background checks are used to ensure that pentesters are ethical and have proper credentials. Limiting the invasiveness of the scope is used to limit disruptions to a business.

44.

An attacker whose arsenal consists mainly of open-source tools and scripts found online. What kind of attacker is Larry considered?

Script kiddie

Hacktivist

APT

Unauthorized hacker

Correct answer: Script kiddie

In programming and hacking cultures, a script kiddie, skiddie, or skid is an unskilled individual who uses scripts or programs developed by others to attack computer systems, networks, and websites. They rely heavily on open-source tools and scripts.

Hacktivism (the individual is known as a hacktivist) is the use of computer-based techniques, such as hacking, as a form of civil disobedience to promote a political agenda or social change.

An Advanced Persistent Threat (APT) is a stealthy computer network threat actor that gains unauthorized access to a computer network and remains undetected for an extended period.

An unauthorized hacker is a hacker who violates computer security for personal gain or maliciousness.

45.

Which are the three main goals of information security?

Confidentiality, Integrity, Availability

Controls, Identity, Awareness

Cryptography, Internet, Authentication

Credentials, Infrastructure, Authorization

Correct answer: Confidentiality, Integrity, Availability

The CIA triad is a model that shows the three main goals needed to achieve information security. While a wide variety of factors determine the security situation of information systems and networks, some factors stand out as the most significant. The assumption is that there are some factors that will always be important in information security. These factors are the goals of the CIA triad, as follows:

1. *Confidentiality — preventing unauthorized access to information or systems*
2. *Integrity — preventing unauthorized changes and modifications of information or systems*
3. *Availability — ensure that use or access to systems and information remains possible*

Confidentiality, integrity, and availability are the most basic concepts to information security. These concepts in the CIA triad must always be part of the core objectives of information security efforts.

46.

What role does the OSSTSMM play in penetration testing?

Providing a comprehensive framework for security testing

Providing a list of current adversarial tactics and techniques

Providing a database of publicly-known vulnerabilities and exposures

Providing a rating system for the severity of vulnerabilities

---

Correct answer: Providing a comprehensive framework for security testing

The Open Source Security Testing Methodology Manual (OSSTMM) is a comprehensive framework and methodology for security testing. It is broadly based, with information about such topics as analysis, client interactions, and compliance.

MITRE ATT&CK has information about current adversarial tactics and techniques. The CVE is a database of publicly known vulnerabilities and exposures. The CVSS is a rating system for the severity of vulnerabilities.

47.

A tester is creating a target list in the planning stages of a test. The client has asked that certain wireless networks be added to the list. What information should the tester get from the client to know which wireless devices to include?

SSIDs

Broadcast address

GHz band

SDKs

Correct answer: SSIDs

The target list should include the service set identifiers (SSIDs) of the wireless devices that need to be tested. The SSID is the name of the wireless network.

The broadcast address is the last address in a subnet which all devices listen to. The GHz band refers to the frequencies used by the wireless network. Software development kits are used to help test applications or services.

48.

You are assessing an organization's key management system and policies. The organization has delegated this responsibility to a cloud provider. In this case, how should you proceed with the assessment?

Examine the cloud provider and its key management policies and procedures

The cloud provider is out of your scope, and the client's interactions with it should not be reviewed

There is no need to review the client's key management system if it's delegated or outsourced

Research the cloud provider, but do not contact it directly

Correct answer: Examine the cloud provider and its key management policies and procedures

In some cases, cloud providers are already certified with the necessary compliance for key management services. They could easily provide documentation to support it. If the cloud provider is not compliant with the specific requirements, the assessment should be extended to the cloud provider's key management policies and procedures.

49.

During a pentest discussion, it becomes clear that the client wants to specifically test if the penetration tester could gain access to one particular domain controller.

What type of assessment does this client want?

Goal-based assessment

Compliance-based assessment

Red team assessment

The client wants to perform all of these assessments

Correct answer: Goal-based assessment

Goal-based or objective-based assessments usually provide general instruction for a given scenario. For example, obtain administrative access from a specific server.

Compliance-based assessments audit an organization's ability to follow and implement a given set of security standards within an environment. Red team assessment, or red teaming, will evaluate how well an organization would fare given a scenario of a real-world attack.

50.

The group of stakeholders usually involved in the penetration test discussions includes executive management, security personnel, the IT department, pentesters, and:

The legal department

A local law enforcement representative

A Microsoft representative

A company sales representative

Correct answer: The legal department

Legal representation may be necessary to ensure that legal and contractual commitments are upheld by all parties involved in the engagement. The group of stakeholders usually involved in the penetration test discussions includes executive management, security personnel, the IT department, pentesters, and the legal department.

51.

Which of the following is mandatory for a compliance scan?

Test the environment against the security standards

Scan all registered ports of all systems of the organization

Sign a non-disclosure agreement

Involve a compliance officer

Correct answer: Test the environment against the security standards

Compliance-based assessments audit an organization's ability to follow and implement a given set of security standards in an environment. Many industry standards affect and regulate the way sensitive data may be protected, stored, and processed within an information system.

52.

A penetration has started performing a pentest. During the test, they are unsure if brute-force tests are allowed. In which document would they find information regarding pentest constraints?

RoE

NDA

SOW

SLA

Correct answer: RoE

Rules of Engagement (RoE) is a document that deals with the manner in which the penetration test is to be conducted. Some of the directives that should be clearly spelled out in RoE before you start the penetration test are as follows:

- *The type and scope of testing*
- *Client contact details*
- *Client IT team notifications*
- *Sensitive data handling*
- *Status meetings and reports*

Any constraints regarding the execution of a pentest are usually listed in the Rules of Engagement (RoE) document under the type and scope of testing.

The NDA binds the tester to not divulge sensitive information. The SOW includes details of the work but does not focus on boundaries. An SLA describes the services a provider offers to a client.

53.

Which of the following statements is TRUE?

A penetration test is limited to the devices and services listed in the scope.

A penetration test is never intrusive and only lists the vulnerabilities found.

Penetration tests must actively test third-party cloud services a client uses.

Only external entities can conduct a penetration test.

Correct answer: A penetration test is limited to the devices and services listed in the scope.

The scope of the test defines all machines that should be tested, services running on those machines, and any other details that should be included. Unless a target is specifically listed in the documented scope, it should not be tested.

54.

Prior to a penetration test, the tester and the client create a document that outlines such items as the testing time, location, preferred methods of communication, allowed/disallowed tests, and scope of the test.

What type of document are they preparing?

ROE

Target list

OSSTMM

TTPs

Correct answer: ROE

A rules of engagement (ROE) is a detailed document describing what will occur during the test that has been agreed upon by the client. It includes such elements as time information, the scope, types of tests allowed, and data handling procedures.

A target list is just the scope of the project. The Open-source Security Testing Methodology Manual (OSSTMM) is an approach for performing tests. Tactics, techniques, and procedures (TTPs) are common behaviors of threat actors.

55.

Which of the following threats is the MOST skilled, determined, and well-prepared?

APTs

Professional unauthorized hackers

Script kiddies

Hacktivists

Correct answer: APTs

APTs (advanced persistent threats) are the most motivated and well-prepared threat actors.

Professional unauthorized hackers are in the middle of the adversary tier. Script kiddies are less prepared and skilled. Hacktivists have determination but are not the most skilled.

56.

A company has customers living in the European Union. They need to store identifiable data about those users. Which regulation do they need to comply with?

GDPR

PCI DSS

GLBA

SOX

Correct answer: GDPR

The General Data Protection Regulation (GDPR) is a European Union regulation that protects data and privacy. GDPR was introduced in 2016.

PCI DSS, the Payment Card Industry Data Security Standard, is used for environments that process payment card information. The Gramm-Leach-Bliley Act (GLBA) regulates how financial institutions handle the personal information of individuals. SOX, the Sarbanes-Oxley Act, is a U.S. federal law that sets standards for U.S. public company boards, management, and accounting firms.

57.

What sort of compliance-based assessment would come into play for systems that are covered in the compliance assessment but are maintained separately from the other elements of the organizational infrastructure?

Data isolation compliance assessment

Key management compliance assessment

Password policy compliance assessment

User access compliance assessment

Correct answer: Data isolation compliance assessment

Understanding how the data isolation design fits in the context of the organization's infrastructure is crucial. Data isolation is also an important concept to understand when dealing with third-party service providers.

58.

Before a penetration test, which type of document needs to be signed by a proper authority from the organization that includes indemnification language in case something goes wrong?

Permission to Attack

NDA

SoW

SLA

Correct answer: Permission to Attack

A permission to attack document, or letter of authorization, needs to be signed by the appropriate person at the organization. It requires indemnification language in case something goes wrong to protect the tester from liability.

An NDA is used to ensure privacy. A SoW describes a work order. An SLA describes the services that a provider offers.

Domain 2.0: Information Gathering and Vulnerability Scanning

59.

A pentester is performing a network scan against a subnet of Windows servers. One of the machines reported port 445 to be open.

What service is listening on port 445?

Windows SMB share

Windows mail server

Windows Remote Desktop Service

Microsoft SQL Server

Correct answer: Windows SMB share

The Windows Server Message Block (SMB) protocol is a network file sharing protocol that allows applications on a computer to read and write to files and to request services from server programs in a computer network. The SMB protocol can be used on top of its TCP/IP protocol or other network protocols. Windows SMB shares are usually using port 445. There are many exploits and attacking methods against port 445.

Mail servers relay mail on port 25. Windows Remote Desktop Service is port 3389. Windows Database Server is 1433.

60.

Which command is used for a stealth scan?

Nmap -sS

Nmap -sT

Nmap -sA

Nmap -0

Correct answer: Nmap -sS

The Nmap -sS command will initiate a "syn scan," which is also called a "stealth scan" due to not completing the TCP handshake.

Nmap -sT is used to perform a TCP connect. Nmap -sA is used to conduct a TCP ACK scan. Nmap -0 is used for OS detection.

61.

Which type of reconnaissance activity is MOST likely to be detected by an organization?

Nmap scan from internal network

Wardriving

Port scan from external network

Recon-ng reconnaissance campaign

Correct answer: Nmap scan from internal network

An Nmap scan from inside an organization's network is a highly suspicious activity that will likely be detected.

Wardriving involves finding Wi-Fi networks. Port scans from external networks are common occurrences. Recon-ng is a form of passive reconnaissance.

62.

During reconnaissance, a pentester decides to use the following plugin/module to collect emails from a host:

"auxiliary/gather/search_email_collector"

Which tool are they using?

- **Metasploit**
- Burp
- ZAP
- Nmap

Correct answer: Metasploit

Metasploit is a powerful framework and consists of multiple modules. Auxiliary modules are usually scanners or other reconnaissance tools. This module is useful for automated information gathering during a penetration test.

Burp and ZAP are for web application scanning. Nmap is a network scanner.

63.

What type of information can be found in a captured ARP packet?

Sender hardware address

TCP port

Payload data

Error checking fields

Correct answer: Sender hardware address

The Address Resolution Protocol (ARP) is used to determine which hosts have which IP addresses. ARP packets include a header with hardware type, protocol type, hardware address length, protocol address length and operation, and a data portion with the sender hardware address, sender protocol address, target hardware address, and target protocol address.

ARP packets do not have information on TCP ports, a payload, or error checking fields.

64.

A penetration tester is gathering information about a client and wants to fingerprint their network. One aspect they want to see is if their web applications are located on-premises or hosted in the cloud.

Which tool can they use to track the path that data packets take until they reach the web applications?

- **traceroute**
- nslookup
- nmap
- ping

Correct answer: traceroute

The traceroute tool shows the path packets take to a remote host. This can give insights into the routers that an organization uses and where they are located based on the routers' IP addresses and hostnames.

The nslookup tool is used to translate between IP addresses and domain names. Nmap is used for enumerating networks. Ping is used to test network connectivity.

65.

Before doing a penetration test, a pentester wants to gather information about the company's employees. Which of the following methods would be BEST for retrieving such information?

Social media scraping

Nmap scanning

Metasploit scanning modules

DNS zone transfers

Correct answer: Social media scraping

The majority of people use social media, which is publicly available. Social engineering techniques can trick people into giving away personal information.

Nmap is a port scanner tool. Metasploit is an attacking framework. There is enough information online so that you do not need to get access to the database. DNS zone transfers give information about hostnames and mail servers.

66.

A pentester is using a tool to follow all the links on a website to see which directories are accessible. What activity BEST describes what they are engaged in?

Crawling

Scraping

Scanning

Scoping

Correct answer: Crawling

Crawling involves using a tool to follow all the links in a website. By crawling the site, a tester can learn about the structure and organization of information stored on the servers.

Scraping captures useful information off of web pages, such as email addresses and files. Scanning is used for enumerating systems, ports, or vulnerabilities. Scoping can refer to defining the targets of a pentest, or it can refer to finding the limitations of a token.

67.

You are preparing an Nmap scan. You need the results to be both in XML (so you can import them in another tool) and in a grepable format (so you can quickly walk through the results using grep and focus on specific services).

Which flag in Nmap could produce the final results in both XML and grepable formats?

- **-oA**
- -oX
- -oG
- -oN

Correct answer: -oA

Nmap can produce reports in a few different outputs, but sometimes you need more than one at the same time. Instead of conducting the same scan twice to get the desired output, you could use -oA to output the results into all available formats.

The -oX flag outputs to XML. The -oG flag outputs to a greppable format. The -oN flag is for normal output.

68.

When scanning a scope of IP addresses, you want to visualize the results so you can better understand where you can pivot in order to avoid security controls.

What can you do to accomplish this task?

Generate a network topology

Divide the network into subnets and try to identify where the security controls are

There is no need to pivot when you have scope

Use brute force to identify security controls

Correct answer: Generate a network topology

A network topology would help you to visualize the hosts and give you a good understanding of the infrastructure.

Simply dividing the network cannot identify security controls. There is a need to pivot when trying to escalate privileges. If you use brute force, security controls are most likely to block the source of the attack.

69.

You are preparing to use Recon-ng for reconnaissance. You have installed the module you need with the 'marketplace install' command.

Which command do you need to run before you can run a query in the module?

modules load

info

options set

marketplace refresh

Correct answer: modules load

After installing a Recon-ng module, it needs to be loaded with the 'modules load' command. After being loaded, a tester can set options and run queries.

The 'info' command displays module options. The 'options set' command changes options. The 'marketplace refresh' command refreshes data in the marketplace.

70.

You need to scan all ports from 512 to 2000 on a targeted host. Using Nmap, which flag do you need to use to specify the port range?

-p 512-2000

-p 512:2000

-Pn 512-2000

-Pn 512:2000

Correct answer: -p 512-2000

The -p flag in Nmap is used to specify ports for scanning. If you need to scan all ports from 512 to 2000, you can use "-" between the starting and the ending numbers. Ports can also be listed using commas. For example, "Nmap -p 21,22,25,80 <host>" will scan only ports 21, 22, 25, and 80 and will skip everything else.

The -Pn flag is used to disable ping.

71.

What is the CVSS used for?

To determine the severity of a vulnerability

To describe how attackers exploit a vulnerability

To catalog instances of data breaches

To enumerate common software vulnerabilities

Correct answer: To determine the severity of a vulnerability

CVSS stands for Common Vulnerability Scoring System. This system is used to provide metrics that can be used to determine the impact and severity of a vulnerability to the environment of the organization. Things that are considered when assigning a CVSS score are exploitation difficulty, impact on data integrity, etc.

The CAPAC describes how attackers exploit a vulnerability. Several third-party websites keep track of data breaches. The CWE is used to enumerate common software vulnerabilities.

72.

What can be used to passively search by domain name or IP for exposed systems belonging to an organization?

Shodan

Nmap

WHOIS

DuckDuckGo

Correct answer: Shodan

Shodan is a security search engine for misconfigured or exposed systems.

Nmap is a tool for active scanning. WHOIS does not provide exposed device information. DuckDuckGo is simply a normal search engine, like Google.

73.

Why would an Nmap syn scan (-sS) produce more results than an Nmap full connect scan (-sT)?

A syn scan can work through most firewalls

A syn scan uses ICMP echo requests to find hosts

A full connect scan takes longer, and some hosts drop the requests

A syn scan is compatible with all operating systems, unlike a full connect scan

---

Correct answer: A syn scan can work through most firewalls

Firewalls tend to allow "syn" packets to pass through, assuming they are part of a live connection, while a full connect scan attempts to initiate a new connection and is recognized by firewalls.

74.

What port range includes ports known as "registered ports" that are assigned by IANA when requested?

1024–49151

0–1023

0–1024

5000–50000

Correct answer: 1024–49151

Ports ranging from 1024 to 49151 are registered ports and are assigned by IANA when requested. Many are also used arbitrarily for services.

Ports 0-1023 are known as well-known ports or system ports.

75.

Which OSINT is a good place to check for configuration settings, IP addresses, and even passwords or private keys?

Source code repositories

WHOIS

Job postings

SSL certificates

Correct answer: Source code repositories

Source code repositories such as GitHub can sometimes hold valuable information for a pentester. Organizations may even hard-code passwords into code which gets uploaded publicly onto code repositories.

WHOIS is used to learn about the entity that registered a domain. Job postings can be used to learn about an organization's technology stack. SSL certificates include public keys but not private keys.

76.

Preparing for a pentest, you have obtained the social media profiles of the targeted organization's employees. What sort of attack could you develop using this information?

Social engineering attack

Directory traversal attack

Remote code execution

Fuzzing attack

Correct answer: Social engineering attack

Having a lot of information about a person can make your manipulation strategy easier. Gaining information about the person's habits, regular online shopping behavior, and so on, could potentially aid in a social engineering attack.

Directory traversal attacks and remote code execution are based on web app vulnerability. Fuzzing is an application attack.

77.

What are tools such as h8mail and the haveibeenpwned.com website used for?

Password dumps

File metadata

Website archiving

Social media scraping

Correct answer: Password dumps

Usernames and passwords from previous breaches can be easily accessed through various tools, including h8mail, Pastebin, and online databases. It is important to monitor these services, even for your own personal information.

An example of a file metadata application is Exif. An example of a website archiving tool is The Wayback Machine. An example of a social media scraping tool is Scrapy.

78.

Which method can be used to try to detect if a website is using a load balancer?

Using ping to look for different TTLs

Reviewing cookie names for common patterns

Examining header information for specific signatures

Searching for FIN/RST packets to end connections

Correct answer: Using ping to look for different TTLs

A few different methods can be employed to try to detect if a website is using a DNS- or HTTP-based load balancer. By using ping, a pentester can examine TTLs, check for varying response times, or see if different IP addresses respond to different requests.

Reviewing cookie names, examining header information, and searching for FIN/RST packets are methods of detecting web application firewalls.

79.

Which Nmap scan method is the MOST popular and is known as half-open scanning?

TCP SYN (-sS)

UDP scan (-sU)

No Ping (-Pn)

TCP FIN (-sF)

Correct answer: TCP SYN (-sS)

TCP SYN (Stealth) Scan (-sS) SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. It requires raw-packet privileges and is the default TCP scan when they are available. Because the three-way handshake is never completed, SYN scan is sometimes called half-open scanning.

UDP scans identify UDP services. No ping scans skip the host discovery part of a scan. TCP FIN scans send FIN packets to ports.

80.

During a penetration test, you are discovering hosts using Nmap. You would like to have the host OS identified and the list of results outputted into an XML file.

Which Nmap command would cover both conditions?

nmap -O 10.15.0.0/24 -oX results

nmap -oP -sS 10.15.0.0/24 -x results

nmap -P0 -O 10.15.0.0/24 -oS results

nmap -sS -O 10.15.0.0/24 -oS results

Correct answer: nmap -O 10.15.0.0/24 -oX results

The "-O" option stands for OS detection. 10.15.0.0/24 is the IP range for scanning. The-oX flag stands for outputting to an XML file.

81.

What does scraping a website entail?

Capturing specific information from a website

Scanning a website for vulnerabilities

Indexing the pages of a website

Performing a DOS against a website.

Correct answer: Capturing specific information from a website

Scraping a website involves gathering information from it for reconnaissance. Useful information such as contacts, email addresses, filenames, and directories can be learned.

Vulnerability scanning looks for weaknesses in a web application server. Crawling involves indexing the pages and content of a website. A DOS is an attack against a website.

82.

A penetration tester is operating a test that is being conducted without the knowledge of the company's cybersecurity staff. The tester wants to remain stealthy so as not to alert IPSs or firewalls.

When using Nmap, which flag should they use to be stealthy?

- **-sS**
- -sT
- -sU
- -sN

Correct answer: -sS

A TCP SYN scan (-sS) is a half-open scan. It is stealthy because it does not complete the TCP handshake and can often bypass firewalls and IPSs.

A TCP Connect scan (-sT) scan completes the TCP handshake. A UDP scan(-sU) sends UDP packets, which is noisy because no handshake is involved. A TCP Null scan (-sN) is noisy because it can be considered abnormal.

83.

Which open data source can an attacker leverage to learn about an organization's potential cryptographic flaws, weak implementations, and OCSP information?

SSL certificates

Google Dorks

Scapy

CWE

Correct answer: SSL certificates

SSL certificates reveal a lot of information about the organization that uses them. This includes the validity period, algorithm, and key size.

Google Dorks is useful for finding misconfigurations and exposed data. Scapy is an interactive packet manipulation tool. The CWE is a list of common hardware and software security flaws.

84.

Each CWE record should include:

A weakness ID

Exploitation methods

A tool to exploit it

The group that exploited it

Correct answer: A weakness ID

The Common Weakness Enumeration (CWE) contains broad baselines of software weaknesses that can be used to describe specific vulnerabilities. Each CWE record should include a weakness ID. The name of each CWE is also its ID. For example, CWE-36 stands for "Absolute Path Traversal."

85.

During information gathering, you want to enumerate the operating systems of live hosts. What is this process called?

Fingerprinting

Service and version identification

Eavesdropping

Packet crafting and inspection

Correct answer: Fingerprinting

Fingerprinting refers to identifying a system's operating system by analyzing its network traffic. Differences such as the services a system runs and the order it sends packets can give clues about its operating system and version.

Service and version identification refers to identifying a service on a system based on its responses. Eavesdropping refers to passively sniffing packets that cross a network. Packet crafting and inspection refers to creating custom packets and analyzing the response to gain the information needed from a target.

86.

Which of the following is NOT a vulnerability scanner?

Maltego

Nessus

Nikto

Acunetix

Correct answer: Maltego

Maltego is a commercial product used to visualize the results of OSINT. It is a popular tool for passive reconnaissance.

Nessus is a proprietary vulnerability scanner. Nikto is a free software command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software, and other problems. It performs generic and server type specific checks. It also captures and prints any cookies received. Acunetix is an end-to-end web security scanner that offers a 360 view of an organization's security.

87.

A software developer is interested in creating an application that handles network print jobs. What can they consult to see a broad range in weaknesses associated with similar types of software?

CWE

CVE

CAPEC

FOCA

Correct answer: CWE

The Common Weakness Enumeration (CWE) is a community-developed list of common software and hardware security weaknesses. It is published and maintained by The MITRE Corporation.

The CVE identifies specific vulnerabilities that have occurred. CAPEC catalogs attack patterns in the wild. FOCA is a tool that extracts metadata.

88.

How could a pentester use The Wayback Machine?

To see an archive of the client's website that may include previously posted sensitive information

To view the source code of the client's back-end web application code along with previous code versions

To filter web pages based on advanced queries that can reveal sensitive information

To extract information from the metadata of files

Correct answer: To see an archive of the client's website that may include previously posted sensitive information

The Wayback Machine is run by the Internet Archive, and it keeps archives of websites. A pentester can see any sensitive information that may been posted but later deleted.

The client's back-end web application code is not likely to be made public. Google dorks are used to filter web pages based on advanced queries that can reveal sensitive information. Tools such as Exif are used to extract information from the metadata of files.

89.

Which of the following types of reconnaissance can be gathered passively?

Infrastructure, domains, IP ranges and routes for the organization

Open ports

Running services

Vulnerabilities

Correct answer: Infrastructure, domains, IP ranges and routes for the organization

Infrastructural recon is a part of the passive information-gathering process.

Opened ports and running services are discovered by active scanning. Vulnerabilities are discovered by active scanning or manual validation (which is also active).

90.

Why would an attacker be happy if Telnet traffic was captured during sniffing?

Telnet does not enforce encryption, and communication is plain text

Telnet uses weak cryptography and could be easily decrypted

Telnet is a vulnerable application, and any host with a Telnet server is vulnerable

Telnet supports pass the hash and could be exploited

Correct answer: Telnet does not enforce encryption, and communication is plain text

Telnet is a communication application similar to SSH, but, as it is quite old and hasn't been updated for a long time, it is lacking in cryptographic security, and all the communication passing through it is in plain text.

91.

You are being tasked to perform a scan against the subnet 10.0.10.0/24 and find all running services on ports between 100 and 2000. You need to determine the software version and OS of each host. You know that there is no firewall, but this task is time-sensitive.

Which Nmap command would you choose?

Nmap -sS -A -Pn -p 100-2000 10.0.10.0/24

Nmap -sA -Pn -P 100-2000 10.0.10.0-254

Nmap -Pn -S -p 2000 10.0.10.0

Nmap -sS -Pn -p 100-2000 10.0.10.0/24

Correct answer: Nmap -sS -A -Pn -p 100-2000 10.0.10.0/24

Using -sS will tell Nmap to perform SYN scan (a fast method), -A will make it an aggressive scan that attempts OS and software version detection. -Pn will tell Nmap to skip pinging and treat all hosts as live, and -p 100-2000 will define the port range. Finally, you provide the subnet using /24 as a mask identifier.

92.

During the enumeration phase of a partially known environment penetration test, a tester is using port scanners like Nmap to identify hosts on the targeted network.

What other methods could they use to improve their results?

Search through inventory management systems

Use firewall detection techniques

Scanning through code repositories

Gather information from the Google Hacking Database

Correct answer: Search through inventory management systems

In some tests (usually known environment or partially known environment), an SCCM (System Center Configuration Manager) or other inventory system is available to the penetration testers. A simple search in those systems might reveal hosts that are not detectable by regular port scanning.

Firewall detection focuses on identifying the presence and types of firewalls. Scanning through code repositories is a technique to find data leaks. Gathering information from the Google Hacking Database is for finding sensitive information exposed on the internet.

93.

Which tool can a pentester use to detect antivirus software on a system once they have gained access?

BeEF

SET

Patator

Scout Suite

Correct answer: BeEF

The Browser Exploitation Framework (BeEF) is used for exploiting web browsers. It has modules that can aid in detecting antivirus software.

The Social Engineering Toolkit (SET) is used to aid in social engineering attacks. Patator is a vulnerability assessment tool. The Scout Suite is a web application security scanner.

94.

What information could be found with a WHOIS query against a domain?

Information about the domain owner

Open ports on the server hosting the domain

All domains owned by the same owner

All servers hosting this domain

Correct answer: Information about the domain owner

Even though there are many online services that provide WHOIS anonymity, some useful information could be extracted from the WHOIS database. It could contain information about the domain owner, contact details and addresses, as well as DNS servers.

95.

What is an attacker attempting with the following command?

nmap -n -sn 10.0.0.1/24 -oX file

The attacker is doing a ping scan and outputting the results in XML format

The attacker is doing a running services scan and outputting the results in grepable format

The attacker is scanning for vulnerable hosts from a file list

The attacker is testing exploits from the file against the network segment 10.0.0.1/24

Correct answer: An attacker is doing a ping scan and outputting the results in XML format

An Nmap ping scan (-sn or -sP flag) is a simple method of determining if a host is alive on the network. The ping scan uses the layer 3 Internet Control Message Protocol (ICMP) for sending ping probes to hosts over the network. Hosts communicate over the network using ICMP messages, which are defined as specific types and codes that determine the state of the communication.

96.

You are doing DNS enumeration and would like to obtain the IP address behind the company domain: example.com.

Which command would resolve the IP?

- **nslookup example.com**
- ifconfig example.com
- ipconfig example.com
- whois example.com

Correct answer: nslookup example.com

nslookup is an integrated tool on both Linux and Windows machines. It can be used to interrogate DNS servers.

Ipconfig and ifconfig are used to manage a network interface. WHOIS is used to learn about the entity that registered a domain.

97.

Which of the following conditions will let a pentester issue tokens?

Access to private keys

Access to currently valid tokens

Access to a revoked token

Access to captured API responses

Correct answer: Access to private keys

A pentester will need access to the private keys that sign a token in order to issue legitimate tokens. A popular token format used with web applications is the JSON Web Tokens (JWTs) format.

Access to valid tokens, revoked tokens, or API responses will not lead to the ability to issue tokens.

98.

If a host is configured not to reply to ICMP echo requests or such requests are not routed in a network you are currently scanning, which Nmap flag should be used to make sure that the host is considered alive, even though it does not respond to ping requests?

-Pn

-sT

-sS

-p

Correct answer: -Pn

Nmap flags are the parameters we use after calling the program; for example, -Pn (no ping) is the flag or parameter to prevent Nmap from pinging targets. The Nmap flag used to treat all hosts as online is -Pn.

The "-sT" flag performs a TCP connect scan. The "-sS" flag does a stealth scan. The "-p" flag specifies a port range.

99.

When is the BEST time to run a vulnerability scan on a production network?

In the early hours, when the fewest number of people are using it

During the middle of the day, when employees are at lunch

During peak times, to make the scan more realistic

When employees first come to the office in the morning

Correct answer: In the early hours, when the fewest number of people are using it

Vulnerability scans will cause a lot of disruptions when they are being performed. Additionally, they could cause systems to crash when testing for specific vulnerabilities.