Chapter 2

Planning and Scoping Penetration Tests

OUTLINES

- Scoping and Planning Engagements
- Assessment Types
  - Goals-based or objectives-based assessments
  - Compliance-based assessments
  - Red-team assessments
- White Box, Black Box, Gray Box
- Rules of Engagement
- Documentation
- Access and Accounts
- Certificate Pinning
- Budget
- Contracts
- Data Ownership & Retention
- Authorization
- Third-Party Authorization
- Environmental Differences

Scoping and Planning Engagements

The first step in most penetration testing engagements is determining what should be tested, or the scope of the assessment.
The scope of the assessment determines what penetration testers will do and how their time will be spent. Determining the scope requires working with the person or organization for whom the penetration test will be performed.
Testers need to understand all of the following:

- Why the test is being performed; whether specific requirements such as compliance or business needs are driving the test
- What systems, networks, or services should be tested and when
- What information can and cannot be accessed during testing
- What the rules of engagement for the test are
- What techniques are permitted or forbidden and to whom the final report will be presented.

Assessment Types

Goals-based or objectives-based assessments

Conducted for specific reasons.

Examples:

- **Validation of a new security design**
- **Testing an application or service infrastructure before it enters production**
- **Assessing the security of an organization that has recently been acquired**

Compliance-based assessments

Designed around the compliance objectives of a law, standard, or other guidance and may require engaging a specific provider or assessor that is certified to perform the assessment

Red-team assessments

Typically more targeted than normal penetration tests. Red teams attempt to act like an attacker, targeting sensitive data or systems with the goal of acquiring data and access. Unlike other types of penetration tests, red-team assessments are not intended to provide details of all of the security flaws a target has. This means that red-team assessments are unlikely to provide as complete a view of flaws in the environment, but they can be very useful as a security exercise to train incident responders or to help validate security designs and practices.

White Box, Black Box, Gray Box

White Box

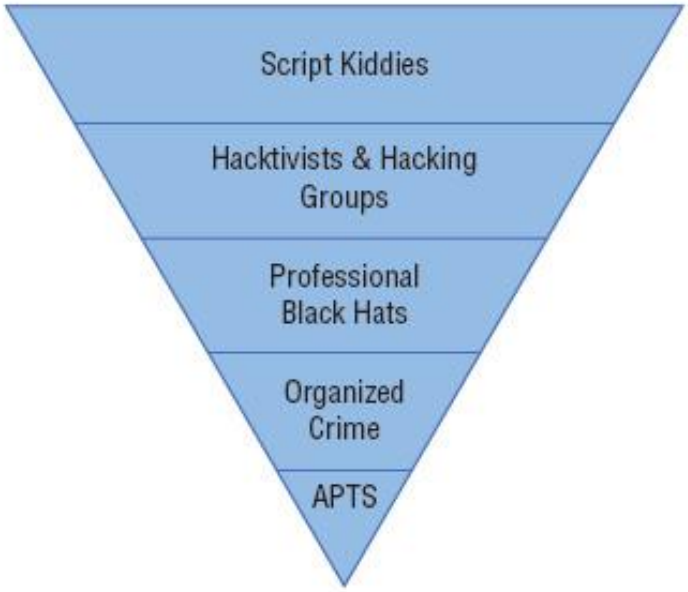
Sometimes called "crystal box" or "full knowledge" tests, as in you see everything inside, are performed with full knowledge of the underlying technology, configurations, and settings that make up the target.
Testers will typically have information including network diagrams, lists of systems and IP network ranges, and even credentials to the systems they are testing. White box tests allow effective testing of systems without requiring testers to spend time identifying targets and determining which of them may allow a way in.

Black box

Sometimes called "zero knowledge" tests, are intended to replicate what an attacker would encounter. Testers are not provided with access to or information about an environment, and instead, they must gather information, discover vulnerabilities, and make their way through an infrastructure or systems as an attacker would. This can be time-consuming for the penetration tester, but it can better reveal what vulnerabilities might be exploited by someone starting with nothing. It can also help provide a reasonably accurate assessment of how secure the target is against an attacker of similar or lesser skill. It is important to note that the quality and skill set of your penetration tester or team is very important when conducting a black box penetration test—if the threat actor you expect to target your organization is more capable, a black box tester can't provide you with a realistic view of what they could do.

Gray box

Blend of black box and white box testing. A gray box test may provide some information about the environment to the penetration testers without giving full access, credentials, or configuration details. A gray box test can help focus penetration testers' time and effort while also providing a more accurate view of what an attacker would actually encounter.



Rules of Engagement

- The timeline for the engagement and when testing can be conducted. Some assessments will intentionally be scheduled for noncritical time frames to minimize the impact of potential service outages, while others may be scheduled during normal business hours to help test the organization's reaction to attacks.

- What locations, systems, applications, or other potential targets are included or excluded. This also often includes discussions about third-party service providers that may be impacted by the test, such as Internet service providers, Software as a Service or other cloud service providers, or outsourced security monitoring services. Any special technical constraints should also be discussed in the RoE.

- Data handling requirements for information gathered during the penetration test. This is particularly important when engagements cover sensitive organizational data or systems. Penetration tests cannot, for example, legally expose protected health information (PHI), even under an NDA. Requirements for handling often include confidentiality requirements for the findings, such as encrypting data during and after the test, and contractual requirements for disposing of the penetration test data and results after the engagement is over.

- What behaviors to expect from the target. Defensive behaviors like shunning, blacklisting, or other active defenses may limit the value of a penetration test. If the test is meant to evaluate defenses, this may be useful.

- What resources are committed to the test? In white and gray box testing scenarios, time commitments from the administrators, developers, and other experts on the targets of the test are not only useful, they can be necessary for an effective test.

- Legal concerns should also be addressed, including a synopsis of any regulatory concerns affecting the target organization, pentest team, any remote locations, and any service providers who will be in-scope.

- When and how communications will occur. Should the engagement Include daily or weekly updates regardless of progress, or will the penetration testers simply report out when they are done with their work?
- Whom to contact in case of particular events, such as evidence of ongoing compromise, accidental breach of RoE, a critical vulnerability discovered, and other events that warrant immediate attention.

- Who is permitted to engage the pentest team; for example, can the CFO request an update? Including this in RoE helps avoid potentially awkward denials.

Documentation

The documentation that an organization creates and maintains to support its infrastructure and services can be incredibly useful to a penetration tester.

- XML documentation like Web Services Description Language (WSDL) Web Application Description Language (WADL), SOAP, or other XML-based schema definitions
  XML code is usually reasonably human-readable, and you should be able to get a general idea of what the definition or documentation describes by reading through

- Application programming interface (API) documentation describes how software components communicate. While APIs can be described in many ways, including via the Web Services Description Language (WSDL) Tools such as Swagger, Apiary, and RAML are some of the most popular ways of developing and documenting the REST-ful APIs that are part of many modern service stacks

- Software development kits (SDKs) also provide documentation and organizations may either create their own SDKs or use commercial or open-source SDKs

- Internal documentation may also include examples like sample application requests, API examples, or other useful code that testers can use to validate or improve their own testing.

- Architectural diagrams, dataflow diagrams, and other system and design documentation can provide penetration testers with an understanding of potential targets, how they communicate, and other configuration and design details.

- Configuration files can be treasure troves of information and may contain details including accounts; IP addresses, and even passwords or API keys.

The W3C and XML -Based Standards

The World Wide Web Consortium (W3C) is an international community organization that defines web standards, including HTML, CSS, XML, web services, and many others. The W3C website at www.w3.org contains information about each of these standards.
(https://www.w3schools.com/xml/default.asp)

Access and Accounts

White box assessments will provide direct access to the systems that are being tested. This may include permitting penetration testers past defenses that are normally in place. A black box assessment team won't have that luxury and will have to make their way past those

- Whitelisting testers in Intrusion Prevention Systems (IPSs), Web Application Firewalls (WAFs), and other security devices will allow them to perform their tests without being blocked. For a white box test, this means that testers won't spend time waiting to be unblocked when security measures detect their efforts. Black box and red-team tests are more likely to result in testers being blacklisted or blocked by security measures.

- Security exceptions at the network layer, such as allowing testers to bypass network access controls (NACs) that would normally prevent unauthorized devices from connecting to the network.

- Bypassing or disabling certificate pinning.

Certificate Pinning

Certificate pinning associates a host with an X.509 certificate (or a public key) and then uses that association to make a trust decision. That means that if the certificate changes, the remote system will no longer be recognized and the client shouldn't be able to visit it. Pinning can cause issues, particularly if an organization uses data loss prevention (DLP) proxies that intercept traffic. Pinning can work with this if the interception proxy is also added to the pinning list, called a pinset.

- Access to user accounts and privileged accounts can play a significant role in the success of a penetration test. White box assessments should be conducted using appropriate accounts to enable testers to meet the complete scope of the assessment. Black box tests will require testers to acquire credentials and access.

- Physical access to a facility or system is one of the most powerful tools a penetration tester can have. In white box assessments, testers often have full access to anything they need to test. Black box testers may have to use social engineering techniques or other methods we will discuss later in this book to gain access.

- Network access, either on site, via a VPN, or through some other method, is also important, and testers need access to each network segment or protected zone that should be assessed. That means that a good view of the network in the form of a network diagram and a means to cross network boundaries are often crucial to success.

Budget

Technical considerations are often the first things that penetration testers think about, but budgeting is also a major part of the business process of penetration testing. Determining a budget and staying within it can make the difference between a viable business and a failed effort.
The budget required to complete a penetration test is determined by the scope and rules of engagement (or, at times, vice versa if the budget is a limiting factor, thus determining what can reasonably be done as part of the assessment!). For internal penetration testers, a budget may simply involve the allocation of time for the team to conduct the test. For Key Legal Concepts for external or commercial testers, a budget normally starts from an estimated number of hours based on the complexity of the test, the size of the team, and any costs associated with the test such as materials, insurance, or other expenditures that aren't related to personnel time.

Contracts

statement of work (SOW)
statements of objectives (SOOs)
performance work statements (PWSs)
master services agreement (MSA)
sign nondisclosure agreements (NDAs)
confidentiality agreements (CAs)

Many penetration tests start with a contract, which documents the agreement between the penetration tester and the client or customer who engaged them for the test. Some penetration tests are done with a single contract, while others are done with a statement of work, or SOW

document that defines the purpose of the work, what work will be done, what deliverables will be created, the timeline for the work to be completed, the price for the work, and any additional terms and conditions that cover the work

Alternatives to statements of work include statements of objectives (SOOs) and performance work statements (PWSs), both of which are used by the US government.

Many organizations also create a master services agreement, or (MSA), which defines the terms that the organizations will use for future work.

This makes ongoing engagements and SOWs much easier to work through, as the overall MSA is referred to in the SOW, preventing the need to renegotiate terms. MSAs are common when organizations anticipate working together over a period of time or when a support contract is created.

Penetration testers are often asked to sign nondisclosure agreements (NDAs) or confidentiality agreements (CAs), which are legal documents that help to enforce confidential relationships between two parties. NDAs protect one or more parties in the relationship and typically outline the parties, what information should be considered confidential, how long the agreement lasts, when and how disclosure is acceptable, and how confidential information should be handled.

Data Ownership & Retention

When a penetration test ends, the penetration tester will typically have a significant amount of data about the target of the test. That data may include sensitive information, internal documentation, usernames, passwords, and of course the report itself with a list of findings. The ownership of this data after the test is an important consideration and should be covered in the contract, MSA, or SOW for each engagement with clear expectations of who owns the data, how it will be stored and secured, and what will be done with it after the engagement is done.

Authorization

Penetration tests also require appropriate authorization. Regardless of whether they are conducted by an internal team or as part of a contract between two parties, penetration tests need signatures from proper signing authorities. If you are conducting an internal penetration test, make sure the person who is approving the test is authorized to do so.

Third-Party Authorization

Additional authorization may be needed for many penetration tests, particularly those that involve complex IT infrastructure. Third parties are often used to host systems, as Software as a Service, Platform as a Service, or Infrastructure as a Service cloud providers, or for other purposes, and a complete test could impact those providers. Thus, it is important to determine what third-party providers or partners may be in scope and to obtain authorization. At the same time, you should make sure you make both your customer and the third party aware of potential impacts from the penetration test.

Environmental Differences

The United Kingdom's Computer Misuse Act (CMA) of 1990 serves as an excellent example of the type of international law that a penetration tester needs to be aware of prior to conducting a test. The CMA includes criminal penalties for unauthorized individuals who access programs or data on computers or who impair the operation of systems. It also addresses the creation of tools that can be used as part of these violations. While the CMA primarily targets creators of malware and other malicious tools, exploit tools like the AutoSploit automated exploit tool released in 2018 could potentially be covered by laws like this that target "dangerous" software.

Compliance-Based Assessments

- The rules to complete assessments that are set by the compliance standard. The PCI DSS standard provides examples of this, including its definition of what a cardholder data environment (CDE) penetration test should include: the entire external, public-facing perimeter as well as the LAN-to-LAN attack surfaces.
- Password policies, which are important for both the scope of the engagement and the rules of engagement. Again, the PCI DSS penetration testing guidance provides a useful example by noting that whether or not the tester must disclose all passwords they discover during their assessment is an important part of the rules of engagement and the scoping of the assessment.
- Data isolation may come into play when systems that are covered by a compliance agreement or requirement are maintained separately from other elements of an organization's infrastructure. Scoping the penetration test to only validate the compliance environment can be important, but understanding how the data isolation design fits in the context of the organization's infrastructure is crucial too.
- Key management testing may be required to meet a standard like the US federal government's Federal Information Processing Standard (FIPS)
- Limited network access and limited storage access are also common in compliance driven assessments. PCI DSS–compliant organizations have often isolated their card processing systems on a separate network with distinct infrastructure, which means that access to the environment via the network and the ability to access storage or other underlying services may be highly restricted.

Questions

1. What term describes a document created to define project-specific activities, deliverables, and timelines based on an existing contract?
A. NDA
B. MSA
C. SOW
D. MOD

2. What type of language is WSDL based on?
A. HTML
B. XML
C. WSML
D. DIML

3. Which of the following types of penetration test would provide testers with complete visibility into the configuration of a web server without having to compromise the server to gain that information?
A. Black box
B. Gray box
C. White box
D. Red box

4. What type of legal agreement typically covers sensitive data and information that a penetration tester may encounter while performing an assessment?
A. A noncompete
B. An NDA
C. A data security agreement
D. A DSA

5. Which of the following threat actors is the most dangerous based on the adversary tier list?
A. APTs
B. Hacktivists
C. Insider threats
D. Organized crime

6. During a penetration test, Alex discovers that he is unable to scan a server that he was able to successfully scan earlier in the day from the same IP address. What has most likely happened?
A. His IP address was whitelisted.
B. The server crashed.
C. The network is down.
D. His IP address was blacklisted.

7. What does an MSA typically include?
A. The terms that will govern future agreements
B. Mutual support during assessments
C. Micro-services architecture
D. The minimum service level acceptable

8. While performing an on-site penetration test, Cassandra plugs her laptop into an accessible network jack. When she attempts to connect, however, she does not receive an IP address and gets no network connectivity. She knows that the port was working previously. What technology has her target most likely deployed?
A. Jack whitelisting
B. Jack blacklisting
C. NAC
D. 802.15

9. What type of penetration test is not aimed at identifying as many vulnerabilities as possible And instead focuses on vulnerabilities that specifically align with the goals of gaining control of specific systems or data?
A. An objectives-based assessment
B. A compliance-based assessment
C. A black-team assessment
D. A red-team assessment

10. During an on-site penetration test, what scoping element is critical for wireless assessments when working in shared buildings?
A. Encryption type
B. Wireless frequency
C. SSIDs
D. Preshared keys

11. What type of adversary is most likely to use only prewritten tools for their attacks?
A. APTs
B. Script kiddies
C. Hacktivists
D. Organized crime

12. During a penetration test specifically scoped to a single web application, Chris discovers that the web server also contains a list of passwords to other servers at the target location.
After he notifies the client, they ask him to use them to validate those servers, and he proceeds to test those passwords against the other servers. What has occurred?
A. Malfeasance
B. Pivoting
C. Scope creep
D. Target expansion

13. Lucas has been hired to conduct a penetration test of an organization that processes credit cards. His work will follow the recommendations of the PCI DSS. What type of assessment is Lucas conducting?
A. An objectives-based assessment
B. A red-team assessment
C. A black-team assessment
D. A compliance-based assessment

14. The penetration testing agreement document that Greg asks his clients to sign includes a statement that the assessment is valid only at the point in time at which it occurs. Why does he include this language?
A. His testing may create changes.
B. The environment is unlikely to be the same in the future.
C. Attackers may use the same flaws to change the environment.
D. The test will not be fully comprehensive.

15. What penetration testing strategy is also known as "zero knowledge" testing?
A. Black box testing
B. Grey box testing
C. Red-team testing
D. White box testing

16. Susan's organization uses a technique that associates hosts with their public keys. What type of technique are they using?
A. Key boxing
B. Certificate pinning
C. X.509 locking
D. Public key privacy

17. Charles has completed the scoping exercise for his penetration test and has signed the agreement with his client. Whose signature should be expected as the counter signature?
A. The information security officer
B. The project sponsor
C. The proper signing authority
D. An administrative assistant

18. Elaine wants to ensure that the limitations of her red-team penetration test are fully explained. Which of the following are valid disclaimers for her agreement? (Choose two.)
A. Risk tolerance
B. Point-in-time
C. Comprehensiveness
D. Impact tolerance

19. During the scoping phase of a penetration test, Lauren is provided with the IP range of the systems she will test, as well as information about what the systems run, but she does not receive a full network diagram. What type of assessment is she most likely conducting?

A. A white box assessment
B. A crystal box assessment
C. A gray box assessment
D. A black box assessment

20. What type of assessment most closely simulates an actual attacker's efforts?

A. A red-team assessment with a black box strategy
B. A goals-based assessment with a white box strategy
C. A red-team assessment with a crystal box strategy
D. A compliance-based assessment with a black box strategy