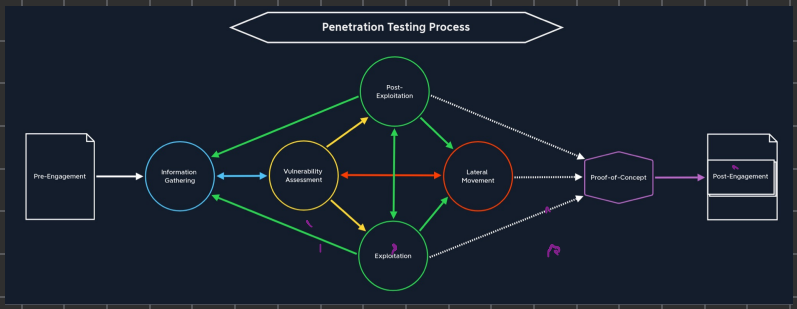
CPTS

1 Penetration Testing Process

A penetration testing process is defined by successive steps and events performed by the penetration tester to find a path to the predefined objective.



- These stages above are interdependent, disrupted and strictly defined.
- We will go through each of these stages later on and and learn TTP's (Tactic, Techniques and Procedures)

* Descriptions –

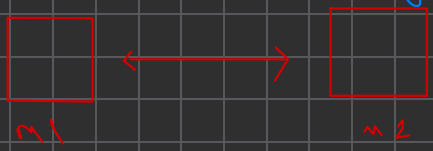
1. Pre-Engagement: Includes making of necessary documents, discuss the engagement with client and clarify question
2. Information gathering: We investigate the company's existing website we have been assigned to. We identify the technologies in use and learn how the web works.

3. Vulnerability Assessment: With the information, we look for known vulnerabilities.

4. Exploitation: After we have found potential vulnerability, we prepare our exploit code, tools and test the web server.

5. Post - Exploitation: Once we exploited the web server, we start into gathering from the inside and try to escalate our privileges.

6. Lateral Movement: We can move from one machine to another in a network using the info we gathered.



7. Proof of Concept: We create a proof of concept that there vulnerability exist

8. Post Engagement: Finally, the documentation is completed and presented to the client.

Pre Engagement

Components —

1. Scoping Questionnaire
2. Pre-Engagement meeting
3. Kick-off metting

i Documents —

Non-Disclosure Agreement

Unilateral

This type of NDA only one party to maintain confidentiality and allow the other party to share the info received with 3rd party.

Bilateral

It is most common type of NDA in which both parties agrees to maintain confidentiality

Multilateral

It is the commitment to confidentiality by more than two parties.

This also requires the preparation of several documents get signed by our clients as a consent. otherwise it will be a crime.

* Some of the documents are —

1. NDA	After initial contract
2. Scoping Questionnaire	Before Pre-Engagement meeting
3. Scoping Document	During "
4. Scope of Work	During "
5. Rules of Engagement	Before Kickoff meeting
6. Contractor Agreement (Physical)	"
7. Reports	During and after the conducted Penetration Test.

NOTE:

These documents should be reviewed by the lawyer after they have been prepared.

ii Scoping Questionnaire

We send a scoping questionnaire to client to have a better understand the services they ask seeking. We ask them choose from the below.

☐ Internal Vulnerability Assessment	☐ External Vulnerability Assessment
☐ Internal Penetration Test	☐ External Penetration Test
☐ Wireless Security Assessment	☐ Application Security Assessment
☐ Physical Security Assessment	☐ Social Engineering Assessment
☐ Red Team Assessment	☐ Web Application Security Assessment

We ask the client is the Pentest a Black Box, Gray Box or colnite box.

Would they like us to test a non-evasive, hybrid evasive (start quiet and becom louder eventually) or fully evasive.

Based on the information we received from the scoping questionnaire, we create an overview and summarize all information in the Scoping Document.

!!! Pre-Engagement Meeting

This meeting discusses all relevant and essential components with the customer before the pentest. This will also pose as the Scope of Work or Contract

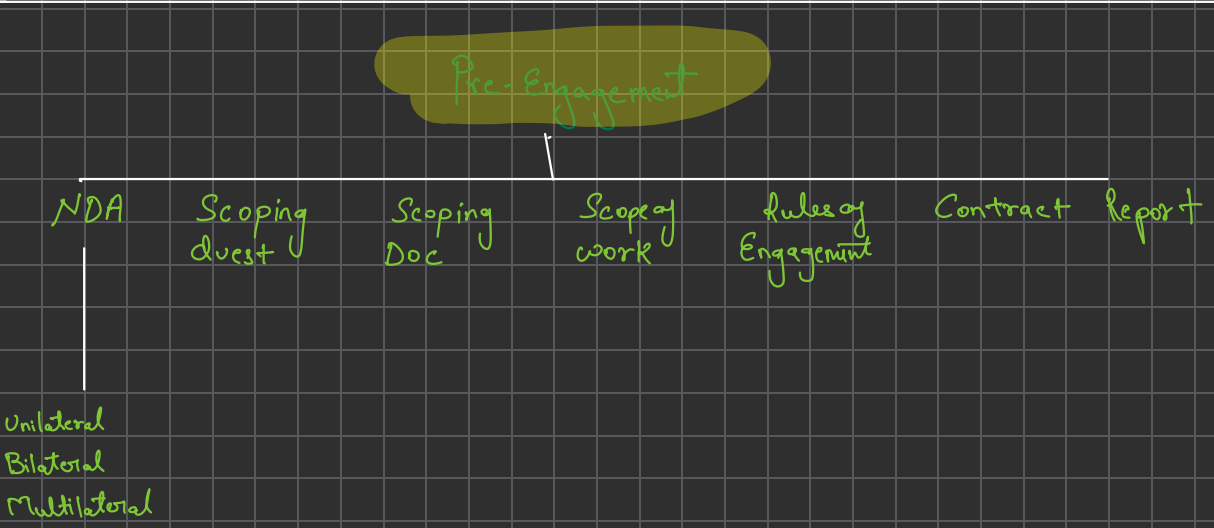
Contract - Checklist

Checkpoint	Description
□ NDA	Non-Disclosure Agreement (NDA) refers to a secrecy contract between the client and the contractor regarding all written or verbal information concerning an order/project. The contractor agrees to treat all confidential information brought to its attention as strictly confidential, even after the order/project is completed. Furthermore, any exceptions to confidentiality, the transferability of rights and obligations, and contractual penalties shall be stipulated in the agreement. The NDA should be signed before the kick-off meeting or at the latest during the meeting before any information is discussed in detail.
□ Goals	Goals are milestones that must be achieved during the order/project. In this process, goal setting is started with the significant goals and continued with fine-grained and small ones.
□ Scope	The individual components to be tested are discussed and defined. These may include domains, IP ranges, individual hosts, specific accounts, security systems, etc. Our customers may expect us to find out one or the other point by ourselves. However, the legal basis for testing the individual components has the highest priority here.
□ Penetration Testing Type	When choosing the type of penetration test, we present the individual options and explain the advantages and disadvantages. Since we already know the goals and scope of our customers, we can and should also make a recommendation on what we advise and justify our recommendation accordingly. Which type is used in the end is the client's decision.
□ Methodologies	Examples: OSSTMM, OWASP, automated and manual unauthenticated analysis of the internal and external network components, vulnerability assessments of network components and web applications, vulnerability threat vectorization, verification and exploitation, and exploit development to facilitate evasion techniques.
□ Penetration Testing Locations	External: Remote (via secure VPN) and/or Internal: Internal or Remote (via secure VPN)
□ Time Estimation	For the time estimation, we need the start and the end date for the penetration test. This gives us a precise time window to perform the test and helps us plan our procedure. It is also vital to explicitly ask how time windows the individual attacks (Exploitation / Post-Exploitation / Lateral Movement) are to be carried out. These can be carried out during or outside regular working hours. When testing outside regular working hours, the focus is more on the security solutions and systems that should withstand our attacks.
□ Third Parties	For the third parties, it must be determined via which third-party providers our customer obtains services. These can be cloud providers, ISPs, and other hosting providers. Our client must obtain written consent from these providers describing that they agree and are aware that certain parts of their service will be subject to a simulated hacking attack. It is also highly advisable to require the contractor to forward the third-party permission sent to us so that we have actual confirmation that this permission has indeed been obtained.
□ Evasive Testing	Evasive testing is the test of evading and passing security traffic and security systems in the customer's infrastructure. We look for techniques that allow us to find out information about the internal components and attack them. It depends on whether our contractor wants us to use such techniques or not.
□ Risks	We must also inform our client about the risks involved in the tests and the possible consequences. Based on the risks and their potential severity, we can then set the limitations together and take certain precautions.
□ Scope Limitations & Restrictions	It is also essential to determine which servers, workstations, or other network components are essential for the client's proper functioning and its customers. We will have to avoid these and must not influence them any further, as this could lead to critical technical errors that could also affect our client's customers in production.
□ Information Handling	HIPAA, PCI, HITRUST, FISMA/NIST, etc.
□ Contact Information	For the contact information, we need to create a list of each person's name, title, job title, e-mail address, phone number, office phone number, and an escalation priority order.
□ Lines of Communication	It should also be documented which communication channels are used to exchange information between thecustomer and us. This may involve e-mail correspondence, telephone calls, or personal meetings.
□ Reporting	Apart from the report's structure, any customer-specific requirements the report should contain are also discussed. In addition, we clarify how the reporting is to take place and whether a presentation of the results is desired.
□ Payment Terms	Finally, prices and the terms of payment are explained.

based on this, the Rules of Engagement are created.

iv Kick-off meeting

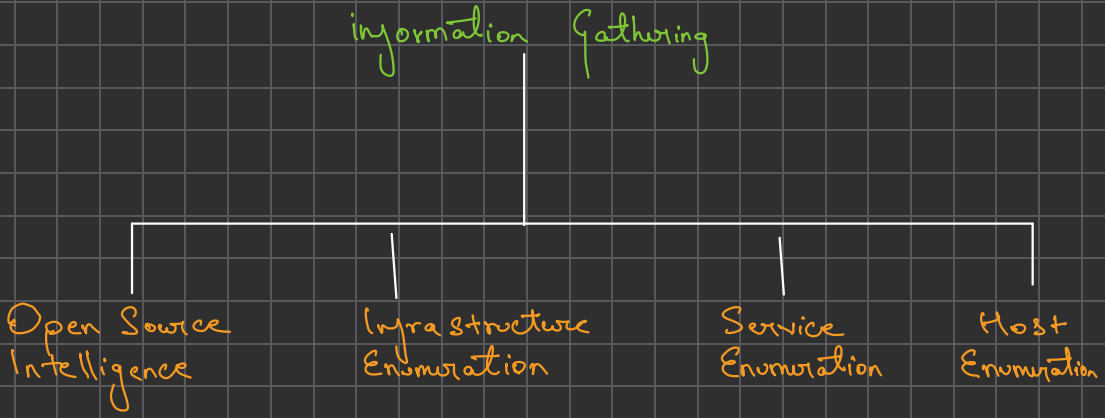
- Usually occurs at a meeting in a scheduled time where usually PoC, client devs, sys admins, pentesting team.
- If a critical vulnerability is found, the pentesting activities will be paused and notification report will be generated.
- We must also inform our customers about potential risks during a pentest. (Risks include many log entries and alarms or that we may accidently lock some users.)



Information Gathering

- Once All the parties have signed the contract, the process of info gathering begins.
- This phase is considered as the cornerstone of the penting process

However, we can divide them into four categories



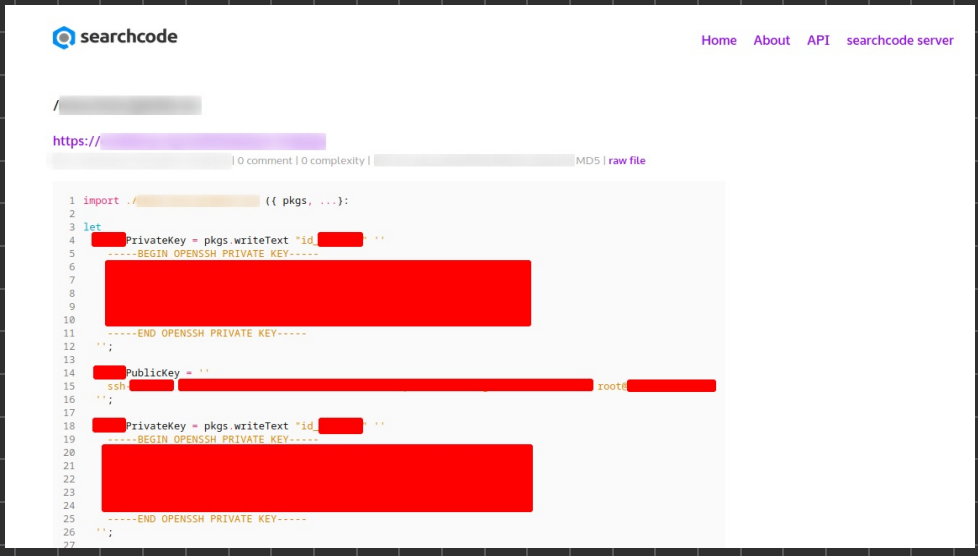
All four categories must be performed by us for each pentest.

This is because the info gathering is the main component that will lead to finding vulns.

* lets see each phase one-by-one deeply-

OSINT

- Lets assume our client wants us to see what info we can find about his company on the internet.
- The OSINT is a process for finding publicaly available information.
- These information can be events and happenings, connections employees.
- We can use some resources like the GitHub, stack overflows.
- Public posted passwd and SSH Keys can be crucial for us too.

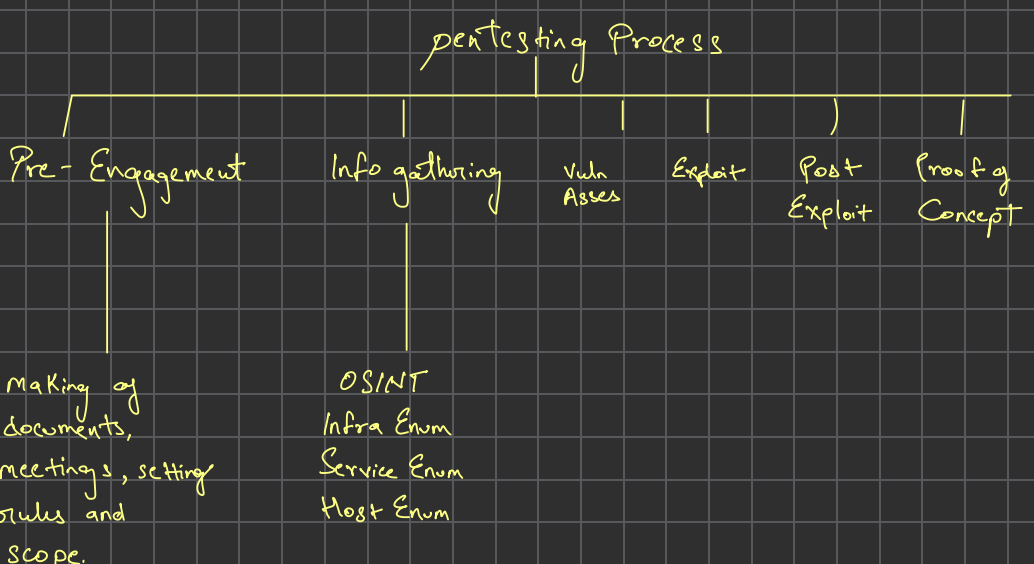


ii Infrastructure Enumeration

- During this phase, we try to map the client's infrastructure with some active scans. We use services like DNS, name servers, mail servers, web servers. We try to make accurate list of live hosts and compare them to our scope.

- We also try the Evasive Testing. A testing in which we determine the company's firewalls, WAF's which gives us an understanding what could trigger the alarm.

- If we are performing the infrastructure enumeration from the internal environment, we can perform a password spraying attack. An attack in which we use one valid password and try to authenticate much services as possible from it.



iii Service Enumeration

- We identify the version of the services running on the target machine.
- It is crucial to find what version, what information it provides us.
- This will help us to know if the services running on the target machine is up to date or outdated.

iv. Host Enumeration

- We try to identify the targets or hosts operating system they are running, which services are running and the versions.
- From internal perspective, we will find services that are not accessible from the outside, Therefore, many admins think that the server is safe as it is not accessible directly from the internet.
- We also try to figure out what role does a particular host play in a network. How and to what it communicates, and of course the port No.!!

Vulnerability Assessment

Vulnerability assessment is a phase where we take very crucial analytical decisions which are based on the findings of Information Gathering phase.

Analysis can be very complicated, as many interdependencies plays a significant role.
There are 4 types of analysis.

1. Descriptive: It is essential in any data analytics. Helps to detect possible error in data collection

2. Diagnostic: It analyses causes, affects, how it happened and why it happened. With the subtle difference that we try to find for developments

3. Predictive: By analyzing the past and current data sets, we can predict and anticipate the outcome of futures possibilities

4. Prescriptive: Aims to narrow down what actions to prevent for triguring futures problems or process.

i Vuln Research and analysis-

- This is a part of descriptive analysis where we try to find out the network hosts known vulnerabilities which are already published with the CVE and and exploit guidance.
- This is where diagnostic and predective analysis takes place in the same time. Here once we found out the known CVE, we can diagnose the functionality and with the PoC.

ii Assessment of Possible Attack Vendors -

- This is a kind of predictive analysis where we actual test the machine with the already known vulnerabilities.
- We predict the possible attack vendors with the knowledge of known CVEs.
- We try to mimic the target machine as much as possible on our local machine.

If we are unable to detect any known vulnerabilities on the environment, its okay to return back to the Info Gathering phase

Remember, Info gathering is most crucial part of the pentesting process and you'll be going back and forth to this process.

Information Gathering ⟷ Vulnerability Assessment

Exploitation

- During this phase, we look for the weaknesses that can be adopted to our use cases for desired role. The development or choosing of exploits may takes place in this phase.

- Suppose, we found 2 vulnerabilities while Vuln Assessment phase, We will need to Prioritize the Possible Attack It depends on these three factors.

  → Probability of Success
  We will assess the probability of success and check the CVSS scores.

  → Complexity
  We will compare how complex the attack is while performing. Lesser the complex, more points in favour of that particular exploit.

  → Probability of Damage
  In this, we assess and compare whether the attack have a potential to damage the client environment. Lesser the damage, more points in favour.

Prioritization Example

Factor	Points	Remote File Inclusion	Buffer Overflow
1. Probability of Success	10	10	8
2. Complexity - Easy	5	4	0
3. Complexity - Medium	3	0	3
4. Complexity - Hard	1	0	0
5. Probability of Damage	-5	0	-5
Summary	max. 15	14	6

Based on the above example, we would prefer the remote file inclusion attack. It is easy to prepare and execute and should not cause any damage if approached carefully.

Post Exploitation

The post exploitation stage aims to obtain sensitive information from a local perspective and business related information that in most cases requires higher privileges than a standard user.

This stage includes —

→ Evasive Testing: If a skilled administrator monitors the systems, any change or any single command could trigger the alarm that will give us away.

→ Information Gathering: Since we are into new environment, we need to get familiar with the new environment and the perspective. Thus, we will repeat the process of Info Gathering, Vuln Assessment and Exploit.

→ Pillaging: It is the stage where we examine the role of the host in the corp network. We understand the role of system, how the different components in the network communicate with each other.

→ Persistence: Our next step is maintaining access to the system. Suppose if the project is taking a more than a week, we need to have our foothold on the system where we can access it easily.

→ Priv Esc: In most cases, it is a significant step. It represents a critical moment that can open door for us.

→ Data Exfiltration: Some clients will want to check if it is possible to exfiltrate personal informations on our local system. Security Systems like DLP (Data loss Prevention) and EDR (Endpoint Detection and Response) help detect and prevent data exfiltration.

Proof of Concept

It is a project management term which serves as a proof that a project is feasible in principle.

It serves as a decision making basis for the further course of action. At the same time, it enables risks to be identified and minimised.

In conclusion, POC holds the info about vulns found, how they were found with the scripts and codes with step by step guidance.

Post-Engagement

The post engagement is the last phase of the pentesting. After completing the assessments and making of POC, the Post-Engagement takes place.

✳ Following are the components of Post Engagement.

- **Clean Up**: After testing, we should perform a necessary cleanup, such as tools/scripts uploaded on the target system. We should make a very detailed document if we are uploading or removing an uploaded files, we should document these
- **Documentation and Reporting**: Before disconnecting from the clients environment completely, we should check if we have enough documentation for all the findings. This includes command output, screenshots, lists of affected hosts etc, And we should not contain any PII's found during the project.
- **Report Review and Meeting**: Typically this includes the same folks from the client and the firm performing the assessment. During this meeting, we will not read the entire report word-by-word to client but explain briefly about the findings.

- **Delivery Acceptance:** Generally, we deliver a report marked DRAFT and give the client a chance to review and comment. Once the client has submitted feedback, we can issue them a new report marked as FINAL.

- **Post-Remediation Testing:** In this phase, we will review any documentation provided by the clients showing evidence of remediation or just a list of remediated findings. As a pentester, we will need to serve as a third party and maintain a degree of independence and serve as a trusted advisor by giving general remediation advice.

- **Data Retention:** As a tester, we will have a very large amount of client-specific data such as scan results, log outputs, credentials and screenshots. The destruction of data may vary from country to country or firm to firm. Some may destroy it or some may store it in a very secure manner with encryption.

- **Close out:** At this stage, we finally close the project and ensure that the systems used to connect with client has been entirely wiped and data is destroyed, making sure that byt over data is secured.
