PENETRATION TESTING METHODOLOGY
PTES – PENETRATION TESTING EXECUTION STANDARD

Shanawaz Mohammed

INTRODUCTION

Penetration tests (pen tests) have become a widely recognized approach for identifying and quantifying cyber risk. They actively attempt to 'exploit' vulnerabilities that reside in people, process and technology. Through pen testing, reports will be able to provide guidance around the vulnerability, impact, threat and the likelihood of a breach in an information asset. Penetration services provide extensive remediation guidance that can be used by risk professionals to instigate appropriate risk treatment plans.

Penetration tests can traditionally be run internally within an organization or externally from the internet. The appropriate vantage point for the testing should be determined by an organization's focus on risk. In addition, the two places for testing are not mutually exclusive. Organizations with a strong focus on risk management will most frequently conduct testing from both an internal and external perspective.

Internal Penetration Testing

This type of penetration testing engagement assesses security from the view of an individual that has physical access to the organization's buildings. Internal penetration tests are conducted from within an organization, through their wired or WIFI networks. The tests will identify whether it is possible to gain access to sensitive systems and data from devices that reside inside the corporate firewalls. Penetration tests are usually conducted without credentials, and determine whether a user with physical access to the organization could capture credentials and then escalate privileges to that of an administrator or super user.

External Penetration Testing

This type of assessment identifies vulnerabilities in infrastructure devices and applications that are accessible from the internet. External penetration tests assess devices and applications from the vantage point of an internet hacker, a competitor or a supplier with limited information about the internet facing environment. External penetration tests will assess the security posture of access routers, firewalls, Intrusion Prevention Systems (IPS) and Web Application Firewalls (WAFs), that protect the perimeter. In addition, they can provide assurance around the effective configuration of SIEM and log management technology. External tests will also provide the ability to assess security controls for applications that are published through the internet.

Penetration Testing Strategies

BLACK BOX TESTING: In a black box test, the client does not provide with information about their infrastructure other than their IP address space, their URL or even just the company name. In Black Box testing the environment is assessed as if they were an external attacker with no information about the infrastructure or application logic that they are testing. Black box assessments provide a simulation of how an attacker without any information, such as an internet hacker, organized crime or a nation a state could present risk to the environment.

GREY BOX TESTING: This type of assessment has many definitions to many people. It is in between black box and white box testing. In this scenario, the tester may receive architectural diagrams, credentials, demonstrations of the application, communication with the target, and much more. There are no strict constraints on what it does or does not have access to. In most testing scenarios, grey box testing is the preferred method. This is because the tester is not given everything (making them really try to break things), while giving him access to more of the application. Grey box tests can require very little information to perform. A tester really just needs to know the target URL(s) and have some credentials to access the application.

WHITE BOX TESTING: In this type of assessment, the tester is given a lot of information about the application. This will include credentials, architectural diagrams, source code, and any other information that will help get a full view of the system. There is nothing hidden from the tester for this assessment. White box, or authenticated tests, target the security of your underlying technology with full knowledge of your IT department. Information typically shared with the tester includes: network diagrams, IP addresses, system configurations and access credentials. This type of testing allows for different 'role-based' testing, allowing penetration testers to act as various individuals within, or connected to, an organization.

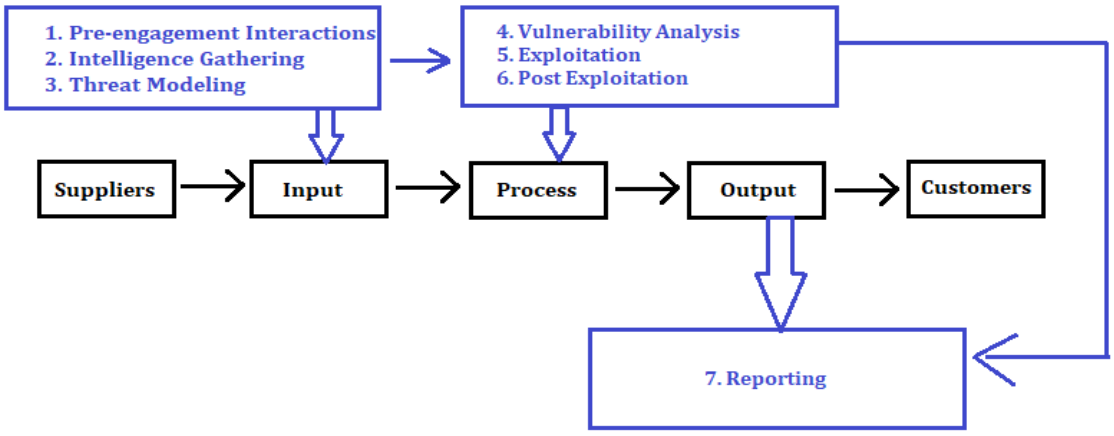
Pen Testing Methodology Overview:

The methodology followed for penetration testing is PTES, by pentest-standard.org. The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the

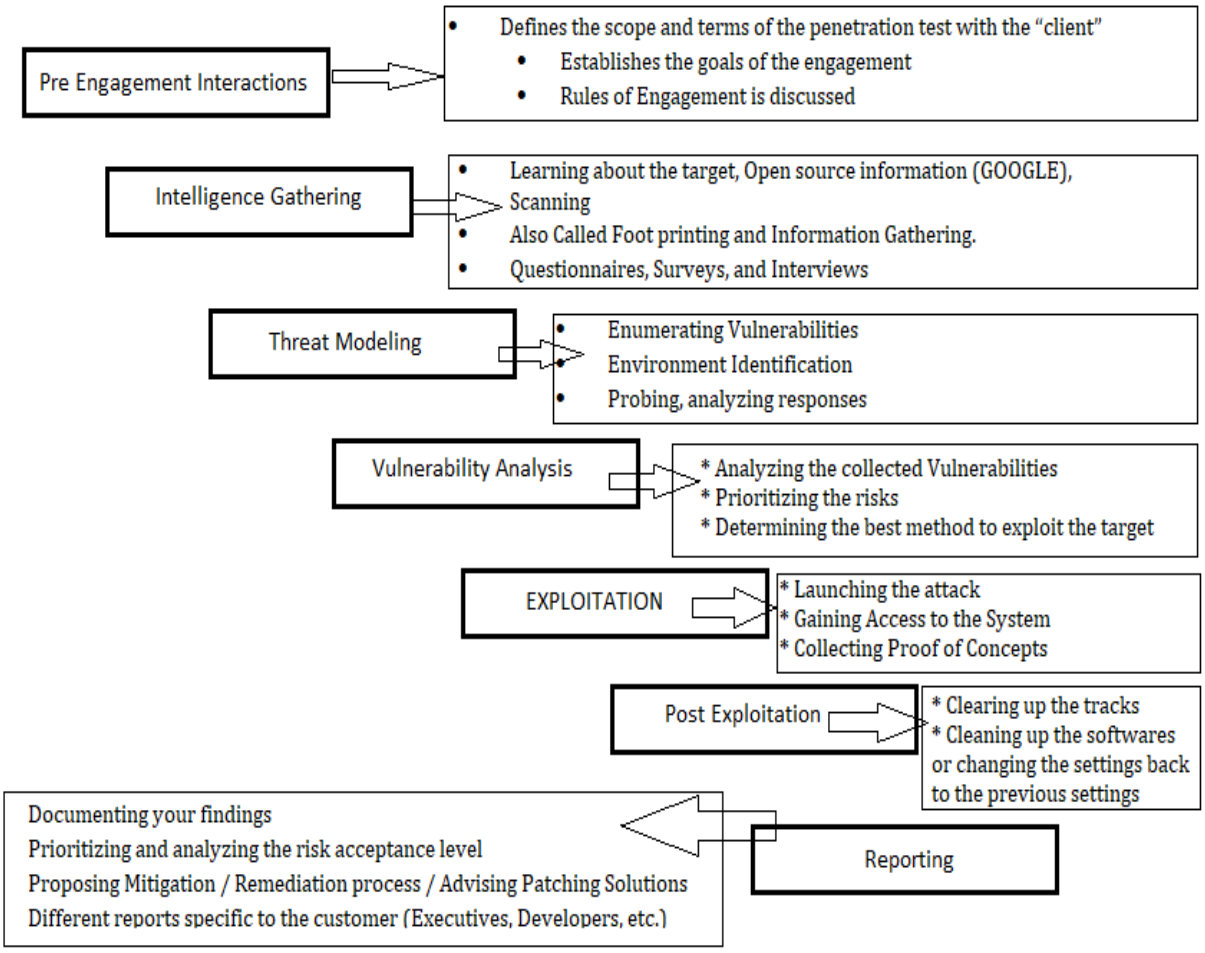
reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

Following are the main sections defined by the standard as the basis for penetration testing execution:

1. Pre-engagement Interactions ------ Scoping
2. Intelligence Gathering ---------- Reconnaissance and Enumeration
3. Threat Modeling ---------- Mapping and Service Identification
4. Vulnerability Analysis ---------- Vulnerability Assessments
5. Exploitation ---------- Service Exploitation
6. Post Exploitation ---------- Pivoting, maintaining access, & clearing tracks.
7. Reporting ---------- Reporting & remediation.



PTES mapping with SIPOC



Seven Steps of PTES

The first three steps of the PTES, which are pre engagement interactions, intelligence gathering and threat modeling will be acting as the inputs from the suppliers. Then the process of vulnerability assessments, exploiting the weaknesses found through vulnerability analysis and gathering proof of concepts will help in preparing the reports. These reports are the outcomes of the SIPOC model. These reports help in prioritizing the risks, understanding the security posture of the organization and mitigating any existing vulnerabilities in the system. These reports cover different segments of audience from executives to application owners. The reports are broken into two sections for executives and technical people. These reports include, tools used during pen testing and recommendations for patch management team. PTES is regarded as the Successful standards for security.

PTES – Penetration Testing Execution Standard

Penetration Testing Methodologies and Standards

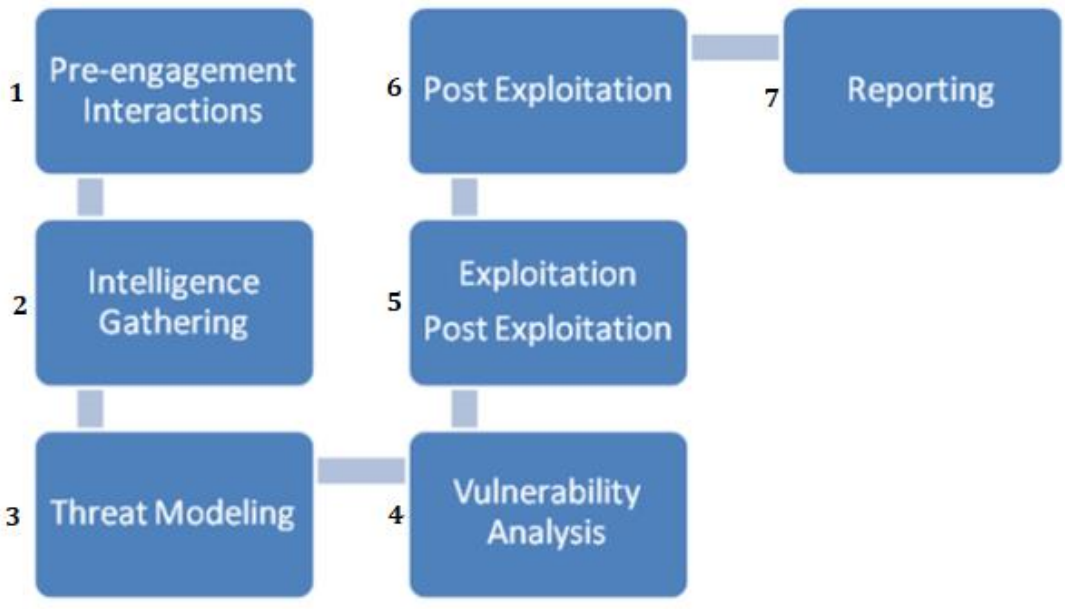
The penetration testing execution standard covers everything related to a penetration test. From the initial communication, information gathering it also covers threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation.

The penetration testing execution standard consists of seven phases:

PTES defines a baseline for the minimum that is required for a basic pen test, as well as several advanced scenarios that provide more comprehensive activities required for organizations with higher security needs.

1. Pre-engagement Interactions:

In this phase, we prepare and gather the required tools, OS, and software to start the penetration testing. Whereas selecting the tools required during a penetration test depends on



several factors such as the type and the depth of the engagement.

There are some common and basic tools that are compulsory to complete penetration testing with the expected results, include:

- **VMware:** VMware enables us to run multiple instances of the operating system on a single workstation.
- **Linux Based Operating System**: As Linux is the most recommended OS for penetration testing, mostly penetration testing is carried on Linux based system (Kali Linux).
- **Windows-Based Operating System:** Windows based OS is required for certain tools to be used. Many commercial tools or Microsoft-specific network assessment and penetration tools are available that run cleanly on the platform.
- **Wifi Adapter:** An 802.11 USB adapter allows the easy connection of a wireless adapter to the penetration testing system. The 802.11 USB adapter is recommended as other don't support the required functions (Wireless Testing)
- **Spectrum Analyzer:** A spectrum analyzer is a device used to examine the spectral composition of some electrical or optical waveform. A spectrum analyzer is used to determine whether or not a wireless transmitter is working according to defined standards
- **Series of software:** The software requirements are based upon the engagement scope. However, some commercial and open source software that could be required to conduct a full penetration test properly are listed below:
    - Maltego
    - Nessus
    - Nexpose
    - Rainbow Crack
    - Dnsmap
    - The Social Engineering Toolkit (SET)
    - The Metasploit Toolkit
    - Dnsrecon

2. Intelligence Gathering:

In this phase, the information or data or intelligence is gathered to assist in guiding the assessment actions. The information gathering process is conducted to gather information about the employee in an organization that can help us to get access, potentially secret or private "intelligence" of a competitor, or information that is otherwise relevant to the target.

- OSINT, Open source Intelligence, using DNS records from WHOIS lookups, and openly available resources like google, Shodan.io, duck duck go, bing, aol, yahoo, etc.
- Port Scanners like, NMAP, Angry IP Scanner, SuperScan, etc.
- Banner grabbing tools like Netcat,

3. Threat Modeling:

Threat modeling is a process for optimizing network security by identifying vulnerabilities and then defining countermeasures to prevent, or mitigate the effects of threats to the system. The threat modeling is used to determine where the most effort should be applied to keep a system secure. This is a factor that changes as applications are added, removed, or upgraded or user requirements are evolved. Primarily Threat modeling is analysis which exposes possible threat vectors, leading to better understanding of a system, asset, or attacker for defensive purposes. Basically, this step is to model all the collected information from the previous two phases of PTES.

Hence this phase does not require any tools, but few models are suggested by MICROSOFT called STRIDE. **STRIDE model** is a classification schemes for **characterizing known threats** according to the kinds of exploit that are used (or motivation of the attacker). STRIDE is acronym formed from the first letter of each of the following categories.

- **Spoofing Identity**
- **Tampering with Data**
- **Repudiation**
- **Information Disclosure**
- **Denial of Service**
- **Elevation of Privilege**

Another such model for threat modeling is DREAD. **DREAD** is a classification scheme **for quantifying, comparing and prioritizing the amount of risk** presented by each evaluated threat. The DREAD acronym is formed from the first letter of each category below. DREAD modeling influences the thinking behind setting the risk rating, and is also used directly to sort the risks. The DREAD algorithm, shown below, is used to compute a risk value, which is an average of all five categories.

Risk_DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

- **Damage Potential -** If a threat exploit occurs, how much damage will be caused?
- **Reproducibility -** How easy is it to reproduce the threat exploit?
- **Exploitability** - What is needed to exploit this threat?
- **Affected Users** - How many users will be affected?
- **Discoverability -** How easy is it to discover this threat?

Combination of STRIDE and DREAD will help in characterizing known threats and quantifying the risk value.

4. Vulnerability Analysis:

Vulnerability Analysis is used to identify and evaluate the security risks posed by identified vulnerabilities. The Process of vulnerability is divided into two steps, Identification and Validation.

- **Identification**: Discovering the vulnerability is the main task in this step.
- **Validation**: In this step, we reduce the number of identified vulnerabilities to only those that are actually valid.

Tools used for Vulnerability Analysis are:

- Nessus,
- Acunetix,
- Burp suite Professional
- Core IMPACT
- IBM AppScan
- HP Fortify/ Web Inspect
- Qualys Guard
- Open VAS
- Appspider
- Tools from RAPID 7 (Nexpose, Metasploit pro, App Spider)

5. Exploitation:

After finding the vulnerabilities, we try to exploit those vulnerabilities to breach the system and its security. For the Exploitation we use different framework and software that are recommended for exploitative purpose and are freely available. Some of the most recommended tools include:

- Core IMPACT
- BURP SUITE PRO
- SAINT Scanner and Exploit
- Metasploit Framework
- SQL Map
- Canvas
- Social Engineering Toolkit
- Netsparker

Combination of two or more tools may also be used for exploitation.

6. Post-Exploitation:

In the Post-exploitation phase, we determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machine's usefulness in further compromising the network. This phase also includes, clearing all the tracks and uninstalling all the tools that were installed as a part of exploitation. This phase highly relies on ROE (Rules of Engagement). This phase speaks about how to report an event, or any incidents that requires immediate action.

7. Reporting:

In this phase, we report the findings in a way that is understandable and acceptable by the organization that owns that system or hardware. It includes the defects that allow an attacker to violate an explicit (or implicit) security policy to achieve some impact (or consequence). In particular, defects that allow intruders to gain increased levels of access or interfere with the normal operation of systems are vulnerabilities.

There are different types of reporting that depends on the genre of authority to which we are reporting.

- **Executive Level Reporting**
  - Business Impact

- Customization
- Talking to the business
- Affect bottom line
- Strategic Roadmap
- Maturity model
- Appendix with terms for risk rating

- **Technical Reporting**
  - Identify systemic issues and technical root cause analysis
  - Maturity Model
  - Technical Findings
    - Description
    - Screenshots
    - Ensure all PII is correctly redacted
    - Request/Response captures
    - PoC examples
    - Ensure PoC code provides benign validation of the flaw
  - Reproducible Results
    - Test Cases
    - Fault triggers
  - Incident response and monitoring capabilities
    - Intelligence gathering
    - Reverse IDS
    - Pentest Metrics
    - Vulnerability Analysis
    - Exploitation
    - Post-exploitation
    - Residual effects (notifications to
    - 3rd parties, internally, LE, etc…)
  - Common elements
    - Methodology
    - Objective(s)

- Scope
- Summary of findings
- Appendix with terms for risk rating

Social Engineering

Social engineering engagements, and assessments help in understanding and increasing the security posture and reduce the risk of insider threat attacks. The phrase social engineering covers a multitude of different types of tests, ranging from services conducted over the internet, through to services conducted over the phone or physically on site. An element of social engineering should be conducted in all penetration tests, due to the fact that humans are involved in all security processes. As reported by Marie Keyworth, from BBC, that in the last two years there has been a spike in social engineering fraud, with reported losses in 2015 doubling to nearly $1bn (£675m) - though, by comparison, global credit card fraud was $16bn last year.

To focus on the technology alone, results in an incomplete security assessment. The intent behind a penetration test should be to identify the risk that is presented by a certain type of asset, connection or activity. Therefore, to fully address all of the elements that feed into that risk, human aspects need to be considered while conducting Penetration testing.

Some of the high profile security breaches that occurred in recent times were instigated through social engineering exploits. Users were targeted through spear phishing emails, and through clicking on a link, opening an attachment or browsing to a website, providing a backdoor into the corporate environment for an attacker to exploit. Through conducting spear phishing attacks and other social engineering tests, an organization can get a feel for how susceptible its employees are to compromise.

In almost all instances employees will provide the weakest link in any organization's security arsenal. As a consequence, social engineering tests that feed directly into security awareness training programs provide a direct mechanism for organizations to tackle this vulnerability. The human element will always pose a risk to organizations, however through considered social engineering and targeted security training, organizations can help to reduce the risk of employees exploited through malicious content.

Vishing:

A type of fraud where criminals persuade victims to hand over personal details or transfer money, over the telephone. They have a number of techniques at their disposal, such type of fraud is called "vishing".

- Information: the criminals already have your name, address, phone number, bank details - essentially the kind of information you would expect a genuine caller to have.
- Urgency: You are made to believe your money is in danger and have to act quickly - fear often leads people into acting without thinking
- Phone spoofing: The phone number appears as if it's coming from somewhere else, so when you pick up the phone you already believe the caller because the number is convincing
- Holding the line: In some cases, the criminals can hold your telephone line, so if you hang up to call back the bank, you can get put straight back to the fraudsters.
- Atmosphere: You hear a lot of background noise so it sounds like a call center rather than a guy in a basement - they either do have a call center, or are playing a sound effects CD

Phishing:

Phishing emails can look very convincing, copying branding and 'spoofing' email addresses to make them look genuine.

How to Identify:

- Hover the mouse over the link and the URL details will come up and will show if it's valid, or taking you somewhere unrecognizable
- If in doubt, don't click on the link
- Open up a new web page in your browser, go to the website, log in that way and see if you have a notification there
- If an email looks genuine then contact the sender through their official website
- Never using telephone numbers or links provided in the email

Smishing:

"Smishing" is SMS phishing where text messages are sent trying to encourage people to pay money out or click on suspicious links. Sometimes attackers try to get victims on the phone by sending a text message asking them to call a number, in order to persuade them further. Unsolicited text messages from unknown numbers should raise alarm bells, but often banks do text their customers

for a variety of reasons. In that case, you should call the bank using a number from a bank statement or a verified source, not a text message.

Tools for Social engineering: KALI LINUX comprises of a pre-configure framework for conducting Social engineering attack, called “Social Engineering Toolkit or setoolkit”.