Overview of Penetration Testing Methodologies and Tools

November 2018

CS479 – Introduction to Cyber Security

Bilkent University

Emre Yüce, Phd

Corporate Cyber Sec. Services Team Leader @HAVELSAN

Overview

- What is penetration testing?
- Vulnerability Assessment vs. Pentesting
- Pentesting Methodology
  - Pre-engagement Phase
  - Engagement Phase
  - Post-engagement Phase
- Tools and Resources

What is Penetration Testing?

- Penetration testing (pentesting), or ethical hacking
- Responsible disclosure
- The process of assessing an application or infrastructure for vulnerabilities in an attempt to exploit those vulnerabilities, and circumvent or defeat security features of system components through rigorous manual testing.
- Vulnerabilities may exist due to
  - misconfiguration,
  - insecure code,
  - poorly designed architecture, or
  - disclosure of sensitive information among other reasons.

What is Penetration Testing?

- The output is an actionable report explaining
  - Each vulnerability or chain of vulnerabilities used to gain access to a target,
  - The steps taken to exploit them,
  - Details of how to fix them and
  - Further recommendations.
- Each vulnerability discovered is assigned a risk rating which can be used to priorities actionable remediation tasks.

Vulnerability Assessment vs. Pentest

	Vulnerability Assessment	Pentest
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly or after significant changes.	At least annually and upon significant changes.
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.
Reports	Potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability.	Description of each vulnerability verified and/or potential issue discovered. More specific risks that vulnerability may pose, including specific methods how and to what extent it may be exploited.
Duration	Relatively short amount of time, typically several seconds to several minutes per scanned host.	Engagements may last days or weeks depending on the scope of the test and size of the environment to be tested. Tests may grow in time and complexity if efforts uncover additional scope.

Pentesting Methodology

- Pre-engagement phase: Negotiation (scope, type etc.)

- Engagement phase:
  - Reconnaissance
  - Scanning & Enumeration
  - Gaining Access
  - Maintaining Access
  - Covering Tracks

- Post-engagement phase: Reporting, verification.

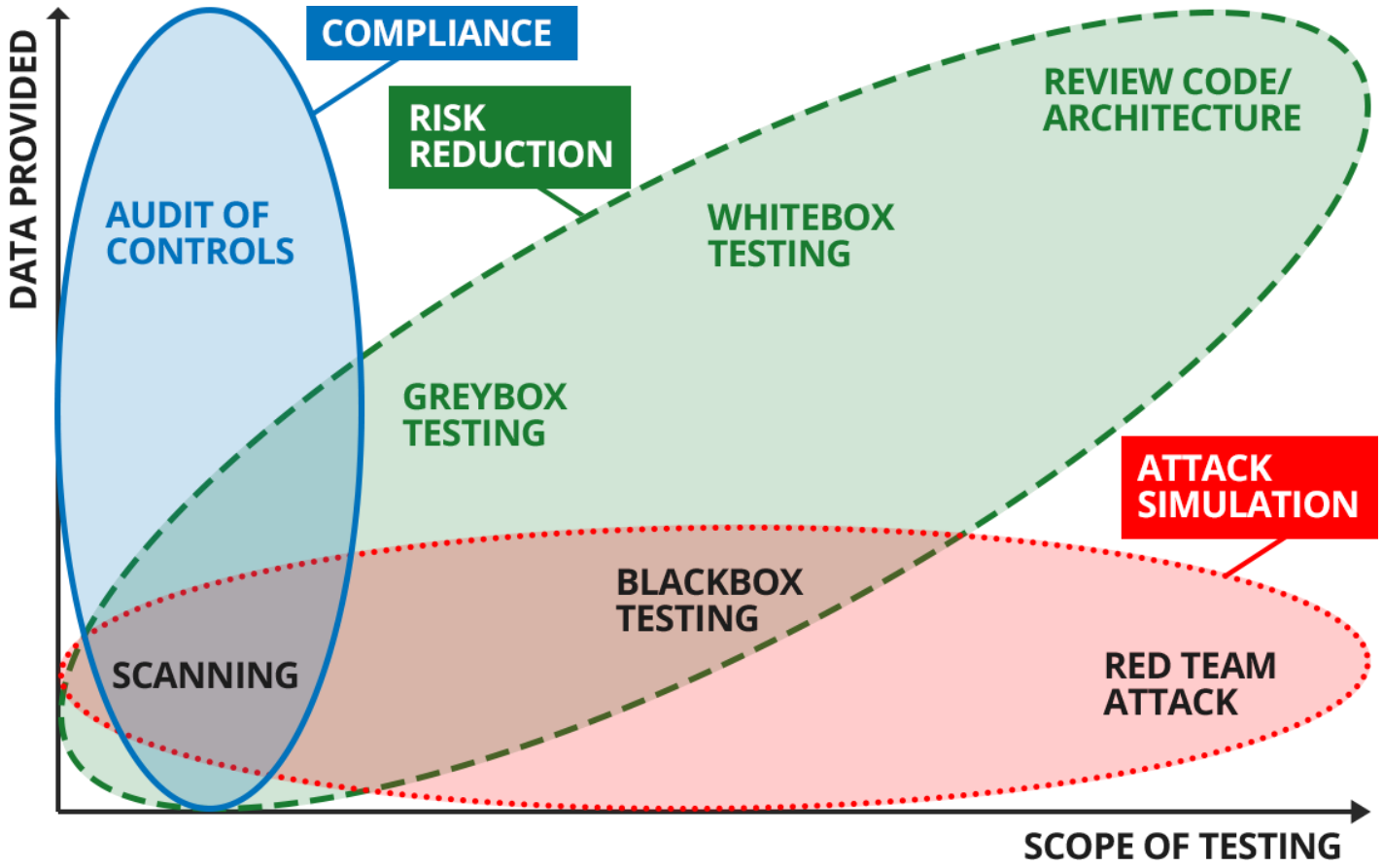
Pre-engagement phase

Understand Business Requirements

- This is the most important part of the engagement.
- You must have a clear understanding of why the customer requires the penetration test?
- Part of a new launch? Or compliance driven?
- The answers to these types of questions will guide you through how the rest of the engagement is approached.

Define the Scope

- Understand what the client wants
  - Black, gray, white box testing or red teaming
  - Announced – unannounced
  - Internal – External



Define the Scope

- How long assessment will take
- What to expect from the assessment
- Client contacts from project manager to network admins in case of emergencies
- Remember to log everything
- Secure communication with clients
- Clear definition of what is allowed and what isn’t allowed in the rules of engagement

Non-Disclosure Agreement (NDA)

- A legal contract
- between at least two parties
- outlines
  - confidential material,
  - knowledge, or
  - Information
- the parties wish to share with one another for certain purposes,
- wish to restrict access to or by third parties.

Get Authorization

- The actions performed during a penetration test would normally be considered illegal without prior authorization.
- This can land you in some legal hot water unless you have your “Get Out of Jail Free” paperwork signed off.

Agree on Timing

- There may be certain times in an organization where the risk of interference or downtime is considered a higher consequence; such as
  - periods of high utilization or
  - when project implementations and upgrades are taking place.
- Make sure you agree on an acceptable time window to perform the penetration test.

Other notes

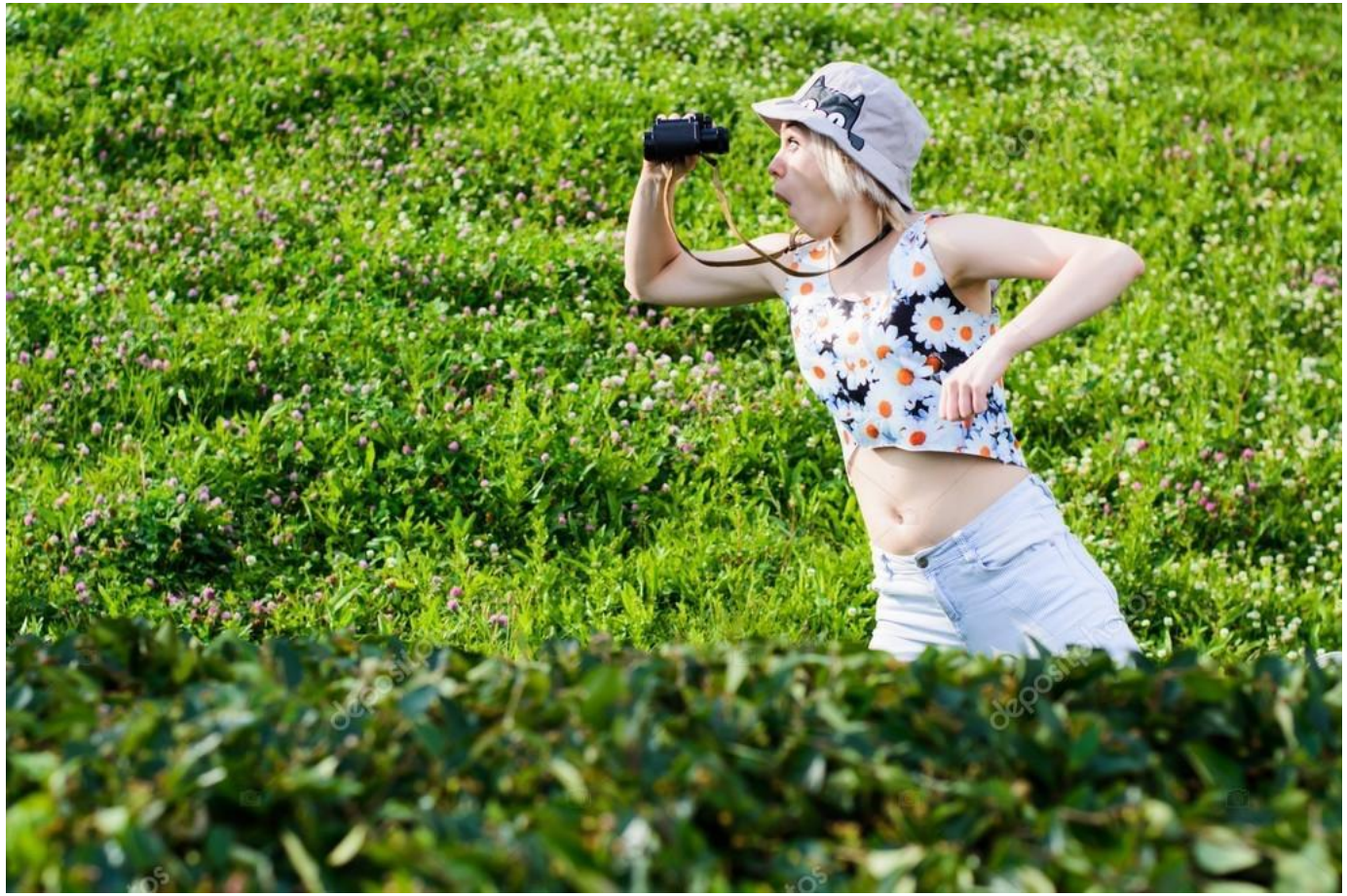
- Whitelist Source IPs
- Confirm internal contacts available

- ***People*** – to ensure that there is adequate education and awareness;
- ***Process*** – to ensure that there are adequate policies and standards and that people know how to follow these policies;
- ***Technology*** – to ensure that the process has been effective in its implementation.

- You need to think like a hacker.

Engagement phase

Reconnaissance



Reconnaissance

- Review Past Threats and Vulnerabilities
- Gathering information passively
- Not actively scanning or exploiting anything
- Harvesting information
  - Bing, google, yahoo, yandex
  - Way back machine (archive)
  - Social media etc.

Scanning & Enumeration

- Target discovery
- Enumerating
- Vulnerability mapping

Tools

- Maltego
- Recon-ng
- Theharvester
- Nmap

Gaining Access

- Mapped vulnerabilities
- Important to penetrate gaining user and escalating privileges
- Try multiple vectors. This is actually a decently easy part
  - Web application
  - Wi-Fi
  - Social engineering
- Research

Maintaining Access

- Keeping account access
- Privilege escalation
- Pivoting to own all

Tools

- Metasploit
- Post scripts

Covering Tracks

- Removing tools
- Backdoors
- Clearing logs
- Windows security, application and system logs
- Linux /var/log/*
- Remove audit logs carefully!!!!!

Post-engagement phase

Post-engagement Phase

- Report writing
  - Any issues occur? Could they have been prevented? Can it be fixed?
- Did you get what you wanted from the engagement?
- Get feedback for yourself
  - Any new tools added or methodologies?
  - Possible new techniques?
- Was the customer satisfied?
- Verification

Reporting

- It is the last thing the customer sees. Make it the best thing they see
- Customers are paying for quality
- Different reports for various teams
  - Executive Summary
  - Detailed Summary

Validation Test

- At least one re-test should be offered by the penetration tester as part of an engagement.
- The client should request that a re-test is performed as soon as they have completed remediation tasks.
- The re-test will test for the vulnerabilities discovered in the initial test in order to validate whether they have been successfully remediated.

Tools and Resources

Toolset

- Kali Linux – The new backtrack
- Use your methodology to help build this
- Recon, Scanning, Exploitation, Post exploitation
- Become familiar with those tools
- Change it up to add more to your collection

Toolset

- Recon-ng / Theharvester
- Burpsuite
- Nmap / p0f / ncat
- Nessus / CoreImpact / Acunetix / Saint
- Arachni / Vega / Metasploit / Websecurify
- Python / Bash
- Keepnote / Lair / etherpad / (armitage *testing*)
- Sqlmap
- Google

Toolset

- Nmap
  - A host discovery and port scanner in order to “map” out the a network.
  - Host fingerprinting, service detection, and vulnerability scanning — effectively enumerating all services running on any given host(s) including vulnerabilities detected on them.
- Netcat
  - The swiss army knife of the network,
  - Terminal connectivity, chat sessions, file transfers, port redirection,
  - Launching forward and reverse shells on connect.

Toolset

- Burp Suite
  - A web application intercepting proxy which is capable of spidering and downloading a website,
  - Modifying web requests on the fly,
  - Fuzzing user input fields and values,
  - Analyzing session token ID randomness,
  - Automatically scanning HTTP requests for vulnerabilities.
  - It is used mainly in web and mobile application penetration tests where web requests are sent to a server.

Toolset

- SQLMap
  - Automatic database takeover tool.
  - Identify SQL injection vulnerabilities,
  - Exploit them in order to download entire databases,
  - Launch commands remotely, and spawn a remote OS shell.
- Nessus
  - A vulnerability scanner
  - Detect missing patches, vulnerabilities which can be used as a basis to launch an exploit against in order to gain quick access.

Toolset

- Metasploit
  - Exploit framework used to set up and launch exploits at vulnerable hosts.
  - It can also be used for enumeration tasks as well as a listener for incoming reverse shells and meterpreter shells.
- Python
  - Master at least one high level scripting language.
  - Easy to write and well adopted within penetration testing and exploit development circles.

Toolset

- Bash
  - Learning the bash shell and how to script with associated linux command line tools during a penetration test is essential.
  - You should be able to quickly put together custom scripts to filter and format data for presentation or input into another tool.
- Google
  - Open source information that will prove interesting during a penetration test
  - The discovery of potentially sensitive documents that shouldn’t be publicly searchable.
  - Google Hacking Database (GHDB):
    - https://www.exploit-db.com/google-hacking-database/

CVE – CVSS – NVD

- CVE is a list of entries—each containing an identification number, a description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE does not provide severity scoring or prioritization ratings for software vulnerabilities.
- CVSS
  - operated by the Forum of Incident Response and Security Teams (FIRST)
  - used to score the severity of software vulnerabilities identified by CVE Entries.
- NVD
  - NIST
  - provides a free CVSS calculator for CVE Entries.

Other Tests

- Social engineering
- DDoS attacks

Warning !!!

- Make sure you do everything as discussed and set out within the agreed scope.
- Make sure you do get authorization signed off to perform the penetration test.
- Do not ever perform a penetration test without prior approval.
- Do not perform testing outside of the agreed scope of the test.

- Penetration testing has numerous components
- It’s not always about hacking it’s about research and business
- Make sure you are niche at what you do. Know your target and field
- Always improve your methods while helping your client improve their infrastructure
- “Don’t learn to hack, hack to learn”

Resources

- Open Web Application Security Project (OWASP) Testing Guide
  - https://www.owasp.org/images/1/19/OTGv4.pdf
- PCI Penetration Testing Guidance
  - https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf
- https://www.coresentinel.com/definitive-guide-penetration-testing/