International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 9 Issue 7 ǁ 2021 ǁ PP. 48-51

Penetration Testing and Vulnerability Assessment

Amey Kanunje, Sourabh Mahale, Niraj Khare, Pratik Daund
Prof. A.A.Deshmukh
Smt Kashibai Navle College of Engineering, Pune

Abstract-*Penetration testing, or pentesting, involves simulating real attacks to assess the risk associated with potential security breaches. On a pentest (as opposed to a vulnerability assessment), the testers not only discover vulnerabilities that could be used by attackers but also exploit vulnerabilities, where possible, to assess what attackers might gain after a successful exploitation.*

From time to time, a news story breaks about a major company being hit by a cyberattack. More often than not, the attackers didn't use the latest and greatest zero-day (a vulnerability unpatched by the software publishers). Major companies with sizable security budgets fall victim to SQL injection vulnerabilities on their websites, social-engineering attacks against employees, weak passwords on Internet-facing services, and so on. In other words, companies are losing proprietary data and exposing their clients' personal details through security holes that could have been fixed. On a penetration test, we find these issues before an attacker does, and we recommend how to fix them and avoid future vulnerabilities.

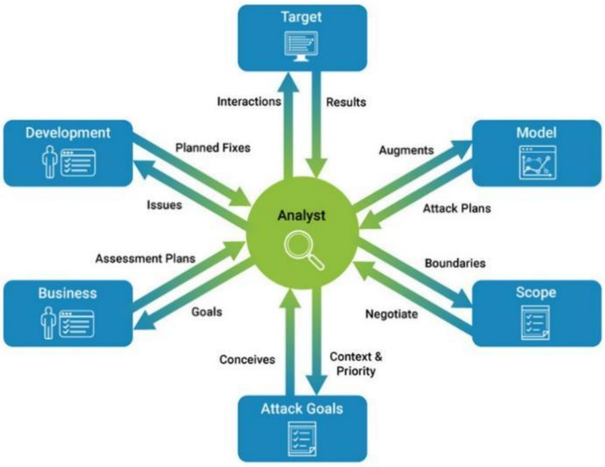
Index terms - *Penetration testing, vulnerabilities, exploit, attackers, injection, threats*

Date of Submission: 21-06-2021 Date of acceptance: 06-07-2021

I. INTRODUCTION

Penetration Testing, pen testing, or ethical hacking is 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. Those vulnerabilities may exist due to misconfiguration, insecure code, poorly designed architecture, or disclosure of sensitive information among other reasons. The output is an actionable report explaining each vulnerability or chain of vulnerabilities used to gain access to a target, with the steps taken to exploit them, alongside details of how to fix them and further recommendations. Each vulnerability discovered is assigned a risk rating which can be used to prioritise actionable remediation tasks. 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.

Figure[1]:Basic model of penetration testing



- Pre-engagement

Before the pentest begins, pentesters perform pre-engagement interactions with the client to make sure everyone is on the same page about the penetration testing. Miscommunication between a pentester and a client who expects a simple vulnerability scan could lead to a sticky situation because penetration tests are much more intrusive. The pre-engagement stage is when you should take the time to understand your client's business goals for the pentest. If this is their first pentest, what prompted them to find a pentester? What exposures are they most worried about? Do they have any fragile devices you need to be careful with when testing? (I've encountered everything from windmills to medical devices hooked up to patients on networks.) Ask questions about your client's business. What matters most to them? For example, to a top online vendor, hours of downtime could mean thousands of dollars of lost revenue. To a local bank, having online banking sites go down for a few hours may annoy a few customers, but that downtime wouldn't be nearly as devastating as the compromise of a credit card database. To an information security vendor, having their homepage plastered with rude messages from attackers could lead to a damaged reputation that snowballs into a major revenue loss. Other important items to discuss and agree upon during the preengagement
phase of the pentest include the following:

- SCOPE

What IP addresses or hosts are in scope, and what is not in scope? What sorts of actions will the client allow you to perform? Are you allowed to use exploits and potentially bring down a service, or should you limit the assessment to merely detecting possible vulnerabilities? Does the client understand that even a simple port scan could bring down a server or router? Are you allowed to perform a social-engineering attack?

- The testing window

The client may want you to perform tests only du ring specific hours or on certain days.
Contact information
Whom should you contact if you find something serious? Does the client expect you to contact someone 24 hours a day? Do they prefer that you use encryption for email?

- A "get out of jail free" card

Make sure you have authorization to perform a penetration test on the target. If a target is not owned by the company (for instance, because it's hosted by a third party), make sure to verify that the client has formal approval from the third party to perform the penetration test. Regardless, make sure your contract includes a statement that limits your liability in case something unexpected happens, and get written permission to perform the test.
Finally, include a nondisclosure agreement clause in your contract. Clients will appreciate your written commitment to keep the penetrationtest and any findings confidential.

- Information Gathering

Next is the information-gathering phase. During this phase, you analyze freely available sources of information, a process known as gathering open source intelligence (OSINT). You also begin to use tools such as port scanners to get an idea of what systems are out there on the Internet or internal network as well as what software is running. Threat Modeling Based on the knowledge gained in the information-gathering phase, we move on to threat modeling. Here we think like attackers and develop plans of attack based on the information we've gathered. For example, if the client develops proprietary software, an attacker could devastate the organization by gaining access to their internal development systems, where the source code is developed and tested, and selling the company's trade secrets to a competitor. Based on the data we found during information gathering, we develop strategies to penetrate a client's systems.
Vulnerability Analysis Next, pentesters begin to actively discover vulnerabilities to determine how successful their exploit strategies might be. Failed exploits can crash services, set off intrusion-detection alerts, and otherwise ruin your chances of successful exploitation. Often during this phase, pentesters run vulnerability scanners, which use vulnerability databases and a series of active checks to make a best guess about which vulnerabilities are present on a client's system But th ugh vulnerability scanners are powerful tools, they can't full replace critical thinking, so we also perform manual analysis and verif results on our own in this phase as well.

- Exploitation

Now for the fun stuff: exploitation. Here we run exploits against the vulnerabilitie we've discovered (sometimes using a tool like Metasploit) in a attempt to access a client's systems. As you'll see, some vulnerabilities will be remarkably easy to exploit, such as logging in with default passwords.

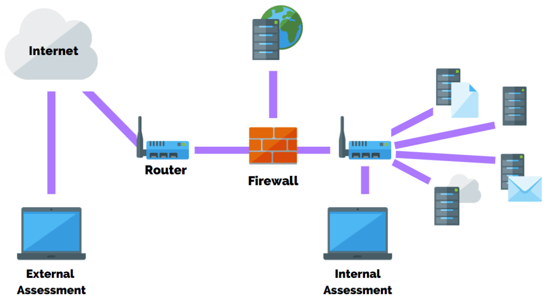
- Post Exploitation

Some say pentests truly begin only after exploitation, in the post-exploitation phase. You got in, but what does that intrusion really mean to the client? If you broke into an unpatched legacy system that isn't part of a domain or otherwise networked to high-value targets, and that system contains no information of interest to an attacker, that vulnerability's risk is significantl lower than i you were able to exploit a domain controller or a clie t's developmen system During pos exploitation, we gather information about the attacked system, look f r i teresting files, attempt to elevate our privileges where necessary, and so on. For example, we might dump password hashes to see if we can revers them or use them to access additional systems. We might also try to use the exploited machine to attack systems not previously available to us by pivoting into them.

- Reporting

The final phase of penetration testing is reporting. This is where we convey our findings to the customer in a meaningful way. We tell them what they're doing correctly, where they need to improve their security posture, how you got in, what you found, how to fix problems, and so on. Writing a good pentest report is an art that takes practice to master. You'll need to convey your findings clearly to everyone from the IT staff charged with fixing vulnerabilities to upper management who signs off on the changes to external auditors. For instance, if a nontechnical type reads, "And then I used MS08-067 to get a shell," he or she might think, "You mean, like a seashell?" A better way to communicate this thought would be to mention the private data you were able to access or change. A statement like "I was able to read your email," will resonate with almost anyone. The pentest report should include both an executive summary and a technical report, as discussed in the following sections.

Figure[2]:Internal and external pentest structure



II. TOOLS USED IN TEST

Whois – whois is website that can be accessed for free which contains all the important information about websites like its registrar, emails, contact numbers, etc. Kali linux has a cli tool for whois lookup.

Nslookup – nslookup is another great tool for finding nameserver, email servers and additional information about target. Its free and open source available for linux, windows, and macos .

Theharvester – theHarvester is a tool that can be used to find subdomains, users, emails, phone numbers, name servers, etc. It is a very powerful tool in recon phase. It is free and open source available for linux, windows and mcos.

Maltego – maltego is another powerful tool that can be used for information gathering and it also offers a simple and unique gui to the user which makes it more interactive and simple to use. It is also available for linux, windows and macos however only the community edition if free, the professional edition is paid.

Netcat – netcat is another powerful tool. It is often referred as the swiss army knife of networking.

Nmap – nmap also known as the network mapper is a powerful tool used to scan all the ports on the target system and gain more information about services running on the target system.

Exploitdb – exploitdb is the exploit databse that contains all the exploits. It is a very important tool that is used in vulnerability analysis phase to search for exploits.

Metsploit-framework – Metsploit framework is the most advanced framework offered by rapid7 which can be used to enumerate, search exploits, create exploits and payloads, deploy exploits on the target system.

Burpsuite - for pentesting web applications, Burp Suite is your go-to tool. Incorporating not only vulnerability scanning but Fully Proxy capturing and command injection services as well. Burps UI is fully optimized for the working professional with built-in profiles to allow you to save your configurations on a per-job basis.

III. RESULT AND FINDING OF TEST

The result of the test must include the detailes analysis of the vilnerabilities found. This is the main and the most significant difference between pentest and security audit. The threats found must be properly reported to the organisation so that they can make necessary changes to patch the vulnerability in their systems.

The solutions implemented will be dependent on the vulnerabilities identified, the loss to the company if conditions triggering the vulnerability occurred, and the cost (and effectiveness) of the available solutions. One solution might require that a new system running a web server must pass a vulnerability test before the web port is opened at the firewall. Another solution might require that all mail within the domain is sent to a central mail system and delivered to local host systems by the central mail server. Enforcement of the existing policy might be the only condition required to address certain vulnerabilities.

In the case of desktop security, remote administration software might be already prohibited at the company. But a better job needs to be done to ensure compliance.

There might also be vulnerabilities that can be addressed by applying the most recent version of the application or operating system patch. The results of the report should be closely guarded. If the information fell into the wrong hands, or an unauthorized individual, the organisation may face problems, hence the confidentiality of the report must be ensured.

IV. CONCLUSION

With the on going digitalization, everything is coming online on the internet and as we all know internet is not a very secured platform. Hence to ensure the integrity and confidentiality of your valuable data measures must be taken. With the increasing news of cyber attacks, cyber threats and data leaks we must ensure that our valuable data is safe. Penetration testing is the a comprehensive method to identify vulnerabilities in the system. It can offer benifits such as prevention od confidential data leaks, finiancial loss of business organizations, consumers and shareholders; preserving the corporate image of organization and protectively analyzing and eliminating the threats and vulnerabilities in the organizations systems and network. The tester may choose to perform white box, black box, grey box tests or internal,external testing depending upon the objectives of the test and organization. This paper conveys the important information about the scope, phases and importance of penetration testing.The test phase is done in four phases that is information gathering, vulnerability analysis, exploitation and post exploit phase. All of these phases can be done manually or using automated tools.

REFERENCES

[1]. Shinde, P. and Ardhapurkar, S. (2016). Cyber security analysis using vulnerability assessment and penetration testing. 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave).

[2]. Cwe.mitre.org. (2019). CWE -Common Weakness Enumeration. [online] Available at: https://cwe.mitre.org/ [Accessed 15 Mar. 2019].

[3]. Owasp.org. (2019). Top 10-2017 Top 10 - OWASP. online] Available at: https://www.owasp.org/index.php/Top_10-2017_Top_10 [Accessed 15 Mar. 2019].

[4]. Pranathi, K., Kranthi, S., Srisaila, A. and Madhavilatha, P. (2018). Attacks on Web Application Caused by Cross Site Scripting. 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA).

[5]. Shebli, H. and Beheshti, B. (2018). A study on penetration testing process and tools. 2018 IEEE Long Island Systems, Applications and Technology

[6]. Conference (LISAT).

[7]. Taha, T. and Karabatak, M. (2018). A proposed approach for preventing cross-site scripting. 2018 6th International Symposium on Digital Forensic and Security (ISDFS).