A Study on Penetration Testing Using Metasploit Framework

Aradhya Tandon, BCA Scholar, Invertis University, Bareilly India, aradhyatandon9@gmail.com
Dr. Siddharth Pandey, Assistant Professor, Invertis University, Bareilly India, siddharth.p@invertis.org

Abstract— In today's digital era, the Internet has made the life of humans much easier not only in personal but also in professional aspect thereby increasing security risks. Cybercriminals exploit vulnerabilities to gain unauthorized access, leading to malicious activities and data breaches. In this paper, we will discuss about the Metasploit Framework tool, a widely used tool among ethical hackers and security experts to perform activities i.e., from Scanning to exploiting the systems. It allows security teams to simulate real-world attacks, helping organizations identify weak points before malicious hackers do and fix them to prevent future attacks.
Keywords—Vulnerability Assessment, Penetration Testing, Web Application Penetration Testing

1. Introduction

In recent years, IT industries are adding more features and accessibility in the existing applications and producing new applications for the benefit of the customers as well as employees. These additional functionalities boost up the Hackers for always seeking for the vulnerability by which they can exploit and can perform some activities like stealing private and confidential data, getting access to user bank accounts and so on. The engineers are giving their best to cover all the vulnerabilities by which they can stop the Hackers. However, vulnerabilities are not limited and can be accidentally elicited in systems or resources that are operative for an extended period. To stop the intruder activities, the companies are using a testing named as Pen-testing which is discussed in the next section.

2. Penetration Testing

Penetration Testing, also called Pen-testing or Ethical Hacking, is a method of identifying security vulnerabilities in computer systems, networks, or web applications that hackers might exploit. It can be performed manually or through automated tools. The process includes collecting information about the target, identifying possible entry points, attempting to exploit them, and reporting the results. As IT companies are creating more rich-featured apps, Pen-testing helps in proactively identifying and fixing weaknesses before hackers can exploit them.

2.1. History of Penetration Testing

The concept of penetration testing can be traced back to ancient times, when armies would conduct mock battles and strategic simulations to anticipate enemy tactics. This early form of security assessment was a way to understand vulnerabilities and potential breaches—much like penetration testing in the digital age.

In the 1960s, as computer systems became more complex and multi-user environments emerged, the need for formal digital security testing grew. This era saw the birth of "Tiger Teams," government and military groups tasked with probing systems for weaknesses. In 1971, the U.S. Air Force commissioned security testing of time-shared computer systems, marking one of the earliest documented instances of penetration testing in the tech world.

The 1980s saw further involvement from the U.S. military, with the Navy testing how easily terrorists could infiltrate naval bases. During this period, the U.S. government also began taking legal action against malicious hacking, resulting in the 1986 Computer Fraud and Abuse Act. This legislation acknowledged the need for ethical hacking, provided it occurred within formal agreements between the hacker and the client organization. In the 1990s, penetration testing became more refined and widely recognized. In 1995, Dan Farmer and Wietse Venema published a ground breaking paper, "Improving the Security of Your Site by Breaking Into It," which highlighted the role of the "uebercracker"—a highly advanced hacker capable of bypassing top-level security undetected. That same year, John Patrick of IBM coined the term "ethical hacking," emphasizing the need for organizations to assess their own security through the eyes of a hacker.

By the 2000s, penetration testing had matured into a structured discipline. The Open Web Application Security Project (OWASP) published its Testing Guide in 2003, setting the first industry best practices. This was followed in 2009 by the Penetration Testing Execution Standard (PTES), which provided a standardized methodology for professional testing services.

Today, penetration testing is a vital component of cybersecurity strategy. By 2013, enterprise security spending had surpassed $6 billion, reflecting the growing demand for skilled ethical hackers. Organizations now recognize the

importance of proactively defending against sophisticated cyber threats, relying on penetration testing to identify and address vulnerabilities before they can be exploit

2.2. Types of Penetration Testing Approaches

Whenever you talk about penetration testing, it comes to clearly three fronts; namely black box, white box and grey box testing. The approaches mainly depend on the level of access and knowledge granted to the tester. From how testing is undertaken, it directly affects the critical factors that help in simulating real scenarios of their world's threats.

2.2.1. Black Box Testing

In Black Box testing, the tester operates without any prior knowledge of the internal systems, network architecture, or source code of the target system. This method simulates an external attacker trying to gain unauthorized access. The tester relies on publicly available information and tools to gather intelligence and attempt exploitation. This is best suited for evaluating the organization's defences and response to external threats.

2.2.2. White Box Testing

White Box testing, on the other hand, provides the tester with full access and detailed internal knowledge of the system. This includes access to source code, system configurations, and network maps. White Box testing allows for deep analysis of potential security flaws and is typically used for code review and configuration auditing. This is usually done in a development or quality assurance environment where the intent is to expose possible vulnerabilities prior to their deployment.

2.2.3. Grey Box Testing

Grey Box testing is a combination approach that provides the tester with partial system knowledge. This may include limited access credentials, internal documentation, or basic network details. It aims to simulate an attack by a malicious insider or a hacker who has already breached certain layers of the security perimeter. Grey Box testing is a balance between depth of testing and real-world relevance, making it one of the most practical and commonly used methods in enterprise environments.

3. Penetration Testing Outcomes and Result Analysis

3.1. Information Gathering: This phase focuses on gathering all information related to server like what is correct domain of web server and how many sub-domains are connected to this domain. Is any firewall is setup for web server or not? In our information gathering phase, we have found that web server's IP - **192.168.72.131**. For detection of firewall, the tool **WAFW00F** (Web Application Firewall Detection Tool) is used.

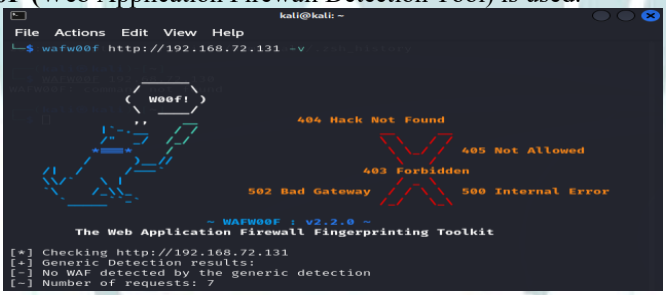

Figure 1: The result showed that no firewall was detected on the target server.

3.2. Scanning: In the Scanning Phase, use Nmap to identify open ports and discover services running on the target machine. First, perform a TCP SYN Scan using -sS to check for open ports on the target IP 192.168.72.131: nmap -sS 192.168.72.131

```
└─$ nmap -sS 192.168.72.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 11:54 EDT
Nmap scan report for 192.168.72.131
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
```

Figure 2: This command helps us determine which ports are open on the target

Next, focus specifically on port 80 (HTTP), as it is commonly used for web servers, which are often targeted for exploits. To obtain in-depth information regarding the services available on port 80, we use the below Nmap command with the -A flag, which would turn on service version detection, OS detection, as well as script scanning: nmap -A -p 80 192.168.72.131

```
└─$ nmap -A -p 80  192.168.72.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-04-14 12:55 EDT
Nmap scan report for 192.168.72.131
Host is up (0.0018s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
MAC Address: 00:0C:29:45:A8:B0 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.75 ms 192.168.72.131

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.25 seconds
```

Figure 3: Detailed data on the web server installed on port 80, such as its version, operating system, and vulnerabilities.

3.3. Discover Vulnerabilities: In the Vulnerability Discovery Phase, employ Searchsploit to find known vulnerabilities related to the Apache 2.2.8 web server installed on the target system. The focus here is to particularly look for PHP-related vulnerabilities using the following command: searchsploit Apache 2.2.8 | grep php

```
┌──(kali㉿kali)-[~]
└─$ searchsploit Apache 2.2.8 | grep php
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin  | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote C | php/remote/29316.py
```

Figure 4: Identification of Vulnerabilities

These vulnerabilities indicate that the target server, running Apache 2.2.8 with a vulnerable version of PHP, is susceptible to remote code execution and command injection through the cgi-bin script.

3.4. Exploitation: The exploitation phase of the penetration test is performed by targeting a known vulnerability in the PHP CGI implementation, which allows command injection via specially crafted HTTP requests. The exploit is carried out using the Metasploit Framework, targeting port 80 of the target host (192.168.72.131).

Steps to execute remote code and gain shell access:

msf > use exploit/multi/http/php_cgi_arg_injection

msf6 exploit(multi/http/php_cgi_arg_injection) > show options
msf6 exploit(multi/http/php_cgi_arg_injection) > set RHOST 192.168.72.131
msf6 exploit(multi/http/php_cgi_arg_injection) > exploit

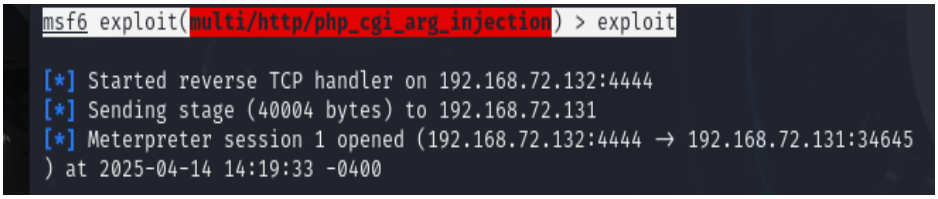

Figure 5: It shows how Successful Exploitation is achieved

After successful exploitation, a Meterpreter session is established. The following post-exploitation commands are used to verify access:
meterpreter > sysinfo
meterpreter > getuid

Figure 6: It depicts how to establish a session

This confirms successful remote code execution and access to the target host (192.168.72.131) via HTTP (port 80) by exploiting the PHP CGI Argument Injection vulnerability.
The PHP CGI Argument Injection vulnerability exploit via the php_cgi_arg_injection exploit on the target host (192.168.72.131) through port 80 was successful. This resulted in the creation of a Meterpreter session. System information was obtained, verifying access as user www-data, leading to complete control of the vulnerable system.
To generate a penetration testing report, compile all findings from the information gathering, scanning, vulnerability discovery, and exploitation phases into a structured format. Use tools like Metasploit's output, Nmap results, and Searchsploit findings, and summarize them along with exploitation results and recommended mitigations to create a comprehensive report.

4 Future Scope

4.1. Integration of Artificial Intelligence and Machine Learning

In the coming years, AI and ML will have a revolutionary impact on penetration testing. These technologies can help automate various phases of the testing process, such as reconnaissance, vulnerability detection, and exploit prioritization. AI-based tools would be adaptive to new threats more easily and would give an ethical hacker the chance to simulate complex attack scenarios without spending so much effort in manual operations.

4.2. Focus on Cloud and Containerized Environments

As these organizations move most of their structures to the cloud and increasingly use containerization tools such as Docker and Kubernetes, the practice of penetration tests would also need to adapt. Future pen tests would be facing challenge after specific challenges on the uniqueness of cloud-native environments in terms of misconfigurations, identity management issues, and insecure APIs.

4.3. Integration with DevSecOps

Penetration testing is expected to become an essential component of the DevSecOps pipeline. Automatic security tests would then be part of the CI/CD process, ensuring that holes in the security layer get detected early and fixed within the development lifecycle. This would enable a shift toward delivering secure software quickly.

4.4. Evolution of Automated Penetration Testing Tools

Tools like Metasploit will continue to evolve, offering more modules, better exploit coverage, and integration with third-party platforms. The future will likely see the development of more intuitive and scalable testing tools that support hybrid environments (on-premise + cloud) and offer real-time collaboration features.

4.5. Integration with Threat Intelligence Platforms

Future pen-testing frameworks may integrate with real-time threat intelligence feeds to simulate the latest and most relevant attack vectors. This helps ensure that penetration tests are up-to-date with emerging threats, zero-day vulnerabilities, and tactics used by advanced persistent threat (APT) groups.

4.6. Enhanced Legal and Ethical Frameworks

AAs penetration testing is increasingly being adopted, legal certainty regarding what constitutes approved testing will become paramount. Future prospect involves more defined laws and ethical standards worldwide to enable testers and organizations to make assessments without infringing on the law.

4.7. Penetration Testing-as-a-Service (PTaaS)

The rise of cloud-based platforms is giving birth to the concept of PTaaS, where organizations can subscribe to penetration testing services on-demand. This model allows for scalable, recurring tests without the need for in-house security experts, making it accessible to small and medium-sized businesses.

5. Conclusion

Penetration testing is a very effective way of finding and fixing vulnerabilities within an organization's systems. It reduces financial loss, enforces regulatory compliance, preserves stakeholders' faith, and protects the firm's reputation. Black box, white box, or grey box testing techniques can be used depending on the extent of access provided to the tester. In addition, Moreover, testing can be classified as internal or external depending on the source of the simulated threat and the particular security objectives. The main categories of penetration testing include network-based, application-level, and social engineering attacks.

This research outlined a structured three-phase methodology: preparation, execution, and analysis. The execution phase involves information gathering, vulnerability scanning, and exploitation performed either manually or by using automated tools. By this structured process, penetration testing allows organizations to actively improve their security stance

In a constantly evolving cyber threat landscape, regular penetration testing becomes essential. Organizations must adopt it as a part of their routine security strategy to maintain robust defences against increasingly sophisticated attacks. Through the use of tools such as Metasploit, combined with systematic testing practices, cybersecurity teams can stay ahead of threats and protect critical digital assets.

References

[1] Pawan Kasarani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lakendra Kumar Tiwari, A Study on Penetration Testing Using Metasploit Framework.
[2] Sudhanshu Raj, Navpreet Kaur Walia, A Study on Metasploit Framework: A Pen-Testing Tool
[3] Metasploit, "Metasploit Framework User Guide," Amyotrophy. Lateral Scler. Off. Publ. World Fed. Neurol. Res. Gr. Mot. Neuron Dis., vol. 11, no. 1–2, pp. 38–45, 2010, [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/20184514.
[4] U. Timalsina and K. Gurung, "Use of Metasploit Framework in Kali Linux Metasploit Framework with Kali Linux," *Penetration Tester's Guide*, San Francisco: No Starch Press, vol. 4, no. April 2015, pp. 0–8, 2017, doi: 10.13140/RG.2.2.12377.93284.
[5] D. Kennedy, J. O'Gorman, and D. Kearns, Metasploit - The Penetration Tester's Guide, San Francisco: No Starch Press, 2011.
[6] Georgia Weidman, *Penetration Testing: A Hands-On Introduction to Hacking*, San Francisco: No Starch Press, 2014.
[7] Filip Holík, J. Horalek, Ondrej Marik, Sona Neradova, Stanislav Zitta, Effective penetration testing with Metasploit framework and methodologies, DOI:10.1109/CINTI.2014.7028682, Corpus ID: 18909293
[8] Sivamanikanta Malkapurapu, Mohamed Addelshafea Mousa Abbas, Pranjit Das, Exploring the Capabilities of the Framework for Effective Penetration Testing, DOI: 10.1007/978-981-99-6755-1_35, In book: Data Science and Network Engineering
[9] Aaryen Toggi; Bhavna Bose; Dharini Naidu; Raghav Srivastava, Metasploit Based Automated Penetration Testing Using Reinforcement Learning, **2024** First International Conference for Women in Computing (InCoWoCo), 14-15 November 2024, **DOI:** 10.1109/InCoWoCo64194.2024.10863399
[10] Seema Rani, Ritu Nagpal, PENETRATION TESTING USING METASPLOIT FRAMEWORK: AN ETHICAL APPROACH, International Research Journal of Engineering and Technology (IRJET), Volume: 06 Issue: 08 | Aug 2019