

# Offensive Security: Study on Penetration Testing Attacks, Methods, and their Types

1<sup>st</sup>Altynai AibekovaAsia Pacific University of Technology and Innovation Technology  
Park Malaysia2<sup>nd</sup> Vinesha SelvarajahAsia Pacific University of Technology and Innovation Technology  
Park Malaysia  
vinesha@apu.edu.my

**Abstract**—In the era of increasing growth of digitalization all information has become easily available through mobile and computer devices. This improvement has brought many useful and efficient technologies and services to peoples' lives which are Web Application, Cloud Computing, Online Communication platforms, E-Commerce, and far more. While some users access this information with only good intentions, some use it to identify ways to destroy or steal valuable data, documents of a website, or in a physical building. As it is well known the term penetration testing is also named ethical hacking. Penetration testing is a set of procedures that emulates the actions of potential hackers but instead of taking advantage of the breaches found, penetration testers document them and present practical advice on how to fix identified weaknesses in the system. This study aims to discuss the types, the strategies of penetration testing, the code of conduct of penetration testers, the advantages, and the methodology in performing penetration testing. The method of penetration testing includes six stages that will be further discussed in detail. This paper illustrates a practical exercise in the example of the Five86-1 machine in a CTF format and that is built with the purpose of learning and gaining experience in conducting ethical hacking. All the attacks demonstrated in the paper are done in Kali Linux operating system. Further, the impact and critical analysis of the attacks is covered in the paper.

**Keywords**—Attack stages, hacking method, Hacking tools, Penetration testing, CTF Challenge, Phishing, DoS, privilege escalation, Code of conduct.

## I. INTRODUCTION

Computers and technology have occupied our lives more than anything else, with the rapid growth of computers used daily enable us to stay informed to complete our tasks or do research. Peoples' lives can't be imagined without computers nowadays. Every day new attacks and new algorithms of the hacking system are being developed. And the companies deliberately collecting our data to provide their services leave no room for confidentiality, privacy, and more vulnerabilities that can be exposed to hackers. The demonstration of any personal data to the attacker could lead to consequences in the future therefore it is suggested to never reveal any of the laptop, computer, or software specifications. The following picture describes the stages in penetration testing as in fig 1.

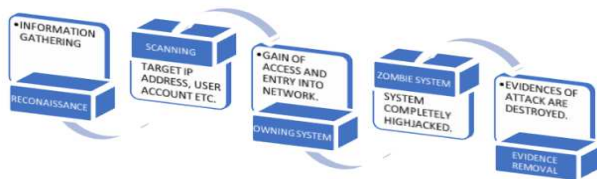


Fig. 1. Stages of hacking [7]

The idea of penetration testing is that legal penetration testers will come to a company and perform a test that could take from few days to few months. Within those six steps, it is possible to enhance the security of the IT infrastructure before malicious people hack the system. The idea of the organization's system being attacked by white hats has never been so exciting.

For this report, a vulnerable machine Five86-1 from vulnhub.com is used to hack into the target with the primary goal to obtain the flag.txt file. The machine was intentionally built to let newbies explore and understand the world of penetration testing. A range of different tools is used to hack into the machine for passing various stages of penetration testing.

The tools and methodologies that have been used for this attack are as follows:

Information gathering - to get the vulnerable IP address and check which ports are open.

- netdiscover
- Nmap

Enumeration:

- Experimenting with HTTP-based services.

Exploiting services such as:

- Exploiting OpenNetAdmin.
- Crack hashes with a hash cat
- Privilege escalation
- Abusing SUID

## II. MATERIALS AND METHODS

### A. Nmap Security Auditing Tool

Nmap is a highly functional tool that is used to scan the network for open connections. It determines the open ports, services that are running on these ports and shows the version of the operating system of the machine. This is also termed - fingerprinting.

It is a highly necessary tool for network administrators and to assess the security of network systems. Nmap tool is used for security, however, it is also liked to be used by hackers. For example, Nmap functions to detect unauthorized servers in the network are utilized by network administrators, but malicious actors will use Nmap to gather information of the victim's network configurations to prepare for an attack [6].

### B. Hash cat robust password recovery tool

Hash cat is the most powerful, advanced, and fastest password recovery application. There are five attacking modes analyze through 200 efficient hashing algorithms. Hash cat supports Linux and Windows operating systems, and on the CPU and GPU. This tool also enables to perform diverse and distributed cracking of passwords [6].

### C. Metasploit Framework

An ideal environment to execute, write, test exploits. Penetration testing is optimized by Metasploit because it is reliable and workable. Shellcodes are written in object-oriented programming languages such as Perl, Ruby, Python, C, and assembler. Metasploit is considered for buffer overflow testing and mainly exploits the vulnerability framework. It combines well-known vulnerabilities and shellcode commands to exploit them. Metasploit ensures easy and straightforward buffer overflow testing since the software is constantly updated [6].

### D. Hacking Methodology

Depending on the type of methodology and standards selected the results of the penetration testing will differ. Hence, the proposed methodology would guarantee successful penetration testing and is well suited to our case. From all 5 methodologies: OSSTMM, NIST, OWASP, ISSAF, and PTES. The Penetration Testing Execution Standard (PTES) is the one that will be followed during the penetration testing. This method provides guidelines for a structured approach of several phases to the penetration test. Phases consist of 7 sections: Planning, Information Gathering, Threat Modelling, Vulnerability Analysis, Exploitation, Post Exploitation, and Report Generation [11]. This method not only provides the post-exploitation phase but also enables testers to reevaluate the infrastructure after completing the reporting stage to ensure that clients have successfully fixed previously identified vulnerabilities [8]. PTES methodology was created to leverage key procedures that should be followed during a basic security test. The methodology itself does not define a fixed structure to perform a penetration test, but rather the steps that should commonly be followed [5]. The PTES also enables the steps to be customized based on the organization's specific needs and requirements. Hence for the organization that is going to have penetration testing, the following steps can be suggested:

1. Planning and Reconnaissance
2. Scanning
3. Exploitation
4. Maintaining Access
5. Removing Tracks
6. Report generation

The PTES could use other resources and incorporate other frameworks for example from OWASP for web application testing.

This method allows achieving outstanding results and guarantees successful penetration testing with helpful recommendations.

1) *Planning and Reconnaissance*: The first phase is planning and information gathering. Planning also known as the pre-phase which begins by identifying the test's scope. The area of infrastructure that needs to be tested is outlined by the client. For example, the client wants the red team to perform social engineering tests or only tests in the internal network. It is very important to get precise directions and not spend time on a network that is not within the scope of the test. As there are often critical systems, testers do not want to take them down as in fig 2.

**In range**  
192.168.1.0/24  
192.168.2.0/24  
192.168.5.0/24

**Out of range**  
192.168.3.0/24  
192.168.4.0/24 – critical servers

Fig. 2. Within and out of range network addresses [3]

Having defined the scope, now both parties should define the expectation, objectives, goals, and legal implications in the contract. In case of unforeseen events that may happen during the test in the network, the testers want to be free from these liabilities. Therefore, the clients must fulfil the pen testers' requirements to proceed with the testing. Testers will not commence any of their operations unless clients have backed up all their network services or signed with the agreement to proceed without any backup of some services.

Now it is time to work on reconnaissance. At this phase, testers and hackers will understand the target and the idea behind this phase is to gain as much information as possible [3-4].

These are the most popular tools used for reconnaissance. The first tool is the search engine like Google, Yahoo, Shodan, DuckDuckGo, and so forth. They are used to collect information about the system or web application of the target. The name of the website or system is entered in a search engine. Then entered the URL of the website using which other information like the IP address, range, and many more can be obtained.

The next tool is NSLookup is used to get the domain name and the IP address map of the target.

WHOis Lookup is a browser-based query and response tool, and it is mainly used to get the registration and delegation details of the target. All this information will play a vital role when trying to hack the application or server.

2) *Scanning*: In this phase, a scan of the network is carried out to see which points hackers and penetration testers can enter from and whether these points are blocked or open. It is needed to find a safe way to enter the system and perform the attack. In other words, hackers look for points that have weak security or vulnerabilities and where they can hack the infrastructure from.

The area covered at this phase also includes threat identification that is categorized into internal and external

threats. Internal threats are the employees, vendors, management, etc. External threats stem from network protocols, ports, web applications, traffic of the network, etc. The information collected during scanning mode are active ports and active hosts, and these are the ports and hosts that are life running in the target network. Threat actors would want to hack into one of the targets that are live and running. Next are the services, for instance, security services: firewall, Intrusion Detection attackers become more careful with those systems in place. From there onwards, malicious individuals want to collect information about vulnerable applications and operating systems. It means the applications or an operating system that are being used by the target are unpatched or outdated. Hence, malicious parties can use these weaknesses to hack into the organization. Examples of the most popular vulnerability scanner tools include OpenVAS, Nikto, Wireshark, and Nessus.

3) *Exploitation*: It is the step where the tester or hacker takes advantage of the weakness or loophole of the target and compromises it. Different exploitation tools can be used to penetrate the organization's IT infrastructure. At this stage tester or hacker will select an attack, they have decided on demonstrating the following attacks

1. DDoS
2. Phishing Attack
3. SQL injection
4. Malware
5. Wireless network attacks

Depending on the weaknesses found it is important to select the appropriate attacks. By launching the attack, they gain access to the target system. There are some of the most popular tools used for exploitation: BeEF, Metasploit, and SQLMap.

4) *Maintaining Access*: It is the phase, where the hacker installs software or makes changes on the target such that they can connect back to the compromised system later in time.

By completing this step, the ethical hacker maintains a connection with the target. So that if there is a need to access the system again later in time there is no need to start the attack from the scratch.

There are different ways to maintain the access:

1. Install Backdoors used to bypass login or authentication.
2. Create new Users/Escalate Privileges to login to the target system without being detected.
3. Privilege escalation is used to obtain superuser privileges to run certain system commands or services on the target.
4. Install Rootkits, software used to enable access to the target.
5. Trojans

Some of the well-known tools used to maintain access are: Powersploit is mainly used for Windows OS.

Weeveily is a PHP web shell that can be used to install stealth backdoors or to manage web accounts. Dns2tcp.

5) *Removing Tracks*: After managed to maintain control over the target, the next step is to keep the strategic plan and actions confidential. In this phase, all details about the identity of the hacker and how the exploit has been carried out are erased. If this part is not completed the hacker can be caught. Tracks can be removed by clearing the cache and cookies. Then, tampering log files by deleting them. Attackers can also close ports or stop the services that they might have started to install backdoors, rootkits, or any other services.

6) *Reporting*: The final phase of ethical hacking is reporting. Testers are going to document and inform the client organization of what happened. The red teamers report everything that was performed for example, what was the strategy, plan, weaknesses found on the testing network, which attacks were used to hack the target, and how the team has gained control over the system. The reporting also mentions certain precautions and recommendations that the target can take to improve security [12] as in Table 1.

TABLE I. SOME OF THE TOOLS USED IN PENETRATION TESTING [1]

|                             |  |
|-----------------------------|--|
| Port Scanners               | Nmap, Superscans, Angry IP Scanner, Nikto, Unicornscan, Autoscan.  |
| Packet Sniffers             | Wireshark, TCPdump, Ethercap, Dsniff, EtherApe.  |
| Vulnerability Exploitation  | Metasploit, Sqlmap, Sqlninja, Social Engineer Toolkit, Netsparker, BeEF, Dradis.                           |
| Vulnerability Scanners      | Nessus, OpenVAS, Nipper, Retina, QualysGuard, Nexpose.   |
| Hacking Operating System    | Backtrack5r3, Kalilinux, SE Linux, Knoppix, Backbox linux, Pentoo, Matriux, Krypton, NodeZero, Blackbuntu. |
| Intrusion Detection Systems | Snort, Netcap  |

TABLE II. PENETRATION TESTING TOOLS [10]

| Name of Tool | Specific Purpose  | Cost | Portability  |
|--------------|---|------|--|
| Nmap         | <ul style="list-style-type: none"><li>• Network scanning</li><li>• Port Scanning</li><li>• OS detection</li></ul>   | Free | Linux, Windows, Free BSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga |
| Hping        | <ul style="list-style-type: none"><li>• Port scanning</li><li>• Remote OS fingerprinting</li></ul>  | Free | Linux, Free BSD, NetBSD, OpenBSD, Solaris, Mac OS X, Windows                             |
| SuperScan    | <ul style="list-style-type: none"><li>• Detect open TCP/UDP ports determine which services are running on those ports</li><li>• Run queries like whois, ping and hostname lookups</li></ul> | Free | Windows 2000/XP/ Vista 7   |
| Xprobe2      | <ul style="list-style-type: none"><li>• Remote active OS fingerprinting</li><li>• TCP</li></ul>   | Free | Linux  |

|                         |  |   |   |
|-------------------------|--|---|---|
|                         | fingerprinting <ul style="list-style-type: none"> <li>• Port scanning</li> </ul>   |   |   |
| pOf                     | <ul style="list-style-type: none"> <li>• OS fingerprinting</li> <li>• Firewall detection</li> </ul>  | Free  | Linux, Free BSD, NetBSD, OpenBSD, Mac OS X, Solaris, AIX, Windows   |
| Httpprint               | <ul style="list-style-type: none"> <li>• Web server fingerprinting</li> <li>• Detect web enabled devices (e.g. wireless access points, routers, switches, modems) which do not have a server banner string</li> <li>• SSL detection</li> </ul> | Free  | Linux, Mac OS X, Free BSD, Win32, (command line and GUI)  |
| Nessus                  | <ul style="list-style-type: none"> <li>• Detect network vulnerabilities that allow remote cracker to control or access sensitive data</li> <li>• Detect misconfiguration, default password and denial of service</li> </ul>                    | Free for Personal edition, Non enterprise edition | Mac OS X, Linux, Free BSD, Oracle Solaris, Windows, Apple   |
| Shadow Security Scanner | <ul style="list-style-type: none"> <li>• Detect network Vulnerabilities, audit proxy and LDAP servers</li> </ul>   | Free trial version                                | Windows but scan servers built on any platform  |
| Iss Scanner             | <ul style="list-style-type: none"> <li>• Detect network vulnerabilities</li> </ul>   | Free trial version                                | Windows 2000 Professional with SP4, Windows Server 2003 Standard with SOI, Windows XP Professional with SP1a                                |
| GFI LAN guard           | <ul style="list-style-type: none"> <li>• Detect network vulnerabilities</li> </ul>   | Free trial version                                | Windows server 2003/2008 Windows 2000 Professional, Windows 7 Ultimate/ Vista Business/XP Professional/Small Business Server 2000/2003/2008 |
| Brutus                  | <ul style="list-style-type: none"> <li>• Telnet, ftp and http password cracker</li> </ul>  | Free  | Windows 9x/NT/2000  |
| Metasploit Framework    | <ul style="list-style-type: none"> <li>• Develop and execute exploit code against remote target</li> <li>• Test vulnerability of computer architecture</li> </ul>  | Free  | All versions of Unix and Windows  |

As shown in Table 2, the tools have been defined as how each of them can be used to fulfil a specific penetration testing activity. Moreover, important information such as the cost and the OS type that each tool supports has also been provided.

Table II illustrates the description of each tool of what specific task each tool can perform in Web Application penetration testing. As well as the details about the cost of the tool and what OS version has been provided.

During the process of defining the scope and objectives of the penetration testing, two things should be considered such as penetration testing strategies and penetration testing types as in Table 3.

TABLE III. WEB APPLICATION PENETRATION TESTING TOOLS [10]

| Name of Tool                  | Specific Purpose  | Cost              | Portability   |
|-------------------------------|---|-------------------|---|
| Nmap                          | Find web server   | Free              | Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga |
| Fiddler                       | A web debugging proxy   | Free              | Windows XP/2K3/Vista/2K8/Win7/Win 8<br>Microsoft, Net Framework v2.0 or later                     |
| Nikto                         | Identifies web server type, version, add-on and other interesting files, performs quick analysis of web server and applications and common server and software misconfigurations, default files and programs, insecure files and programs and outdated servers and programs | Open Source       | Windows, Mac OS X, Linux and Unix (including RedHat, Solaris, Debian, Knoppix etc.,)              |
| WebScarab                     | Interceptor, identifies new URLs on the test target, session ID analyzer, parameter fuzzer  | Free              | All platforms that support Java in any version not older than 1.4                                 |
| W3af                          | Vulnerability tester, Interceptor, Fuzzer   | Open source       | Linux, Windows XP, Windows Vista, Open BSD and any platform that supports python                  |
| Firefox Extension-Firebug     | Inline editing, for breaking forms, messing with JavaScript, making rogue sites and man-in-the-middle components  | Free              | Any platforms that support Firefox  |
| Firefox Extension-TestGen4web | Record and playback clicks during surfing   | Free              | Any platform that support Firefox 1.5 beta  |
| Centric Hailstorm             | Web Vulnerability Scanner   | 1 week trial free | Windows 7 Pro or Windows XP Professional with   |

|                      |   |   | Service pack 3   |
|----------------------|---|---|--|
| Core Impact          | Identify, Validate and exploit vulnerabilities, test web application for XSS, Reflective XSS, SQL Injection, Blind SQL Injection, Remote Inclusion for PHP applications | Commercial  | Windows 7, Windows Vista, Windows Server 2008 SP2, Windows Server 2003 SP2 |
| Nessus 4             | Detect vulnerabilities that allow remote cracker to control or access sensitive data, misconfiguration, default password and denial of service                          | Free for personal edition, non-enterprise edition | Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows, Apple                   |
| Metasploit Framework | Develop and execute exploit code against a remote target machine. Test vulnerability of computer system   | Free  | All versions of Unix and Windows   |

### E. Penetration Testing Strategies

Penetration testers follow one of the penetration testing strategies: black box, white box, and grey box.

In black-box penetration testing, the team has no prior information from the target. In this case, the testers have to discover loopholes from scratch. The penetration testers involved in the black box are closer to simulating the actions of a real attacker, it is also known as the blind test strategy.

White box ethical hackers, on the other hand, are provided with the necessary information from the organization. Testers work together with the organization to conduct targeted testing on the corporate system. This strategy provides more accurate and tailored results for a specific network component as all the details are disclosed to testers before the test.

Gray box testers receive partial information about the target, and they need to collect the rest of the information on their own before they can conduct the test [2].

### F. Penetration Testing Types

There are three levels to test in the penetration testing: the physical level of the system, the logical level of the system, and the workflow of the system. These three areas form the types of penetration testing which are network, application, and social engineering.

Network penetration testing is a process to safely identify flaws and vulnerabilities in the architecture, operation of the network. Testers aim to penetrate the target by launching exploits and analyzing whether network devices and connections are prone to any attacks.

Application penetration testing employs simulated attacks to reveal the efficiency of the application's security. Even with

organizations implementing firewall and monitoring systems, the applications can still be hacked as traffic can be allowed to pass through the firewall.

Social engineering makes use of psychological schemes to trick people into revealing information about an organization and its computer systems. Social engineering testings are performed in the organization to determine the level of security awareness among the staff that manages the target system. This test is useful to check the ability of the organization to prohibit unauthorized access to its information system [10].

### G. The Code of Conduct of An Ethical Hacker

- The data privacy and confidentiality of any organization must be outlined and determined before hacking and should not violate their rules and regulations.
- Sustaining transparency before and after the hacking with the clients and owners of the organization.
- Having very clear intentions that to never harm the client or organization.
- Always stay within the assigned target area while performing ethical hacking and do not go beyond components that are not specified in the agreement.
- Not to reveal the information found during the hacking to other parties after the completion of hacking. This information must be kept confidential [1], [13].

## III. RESULTS AND DISCUSSION

To hack this machine a good knowledge of Linux commands is required, in this paper, the main tool will be the Metasploit framework and will run hash cat and Nmap execution commands. This box is great for students and anyone new to penetration testing. The difficulty level is considered intermediate.

To perform the penetration testing on the virtual machine Five86-1 – Kali Linux Operating System must be installed in the system.

### A. Reconnaissance phase

This phase begins with scanning the target by using the command and scanning the subnet. As can be seen, there are port 22, 80 are open as in fig 3.

```
root@kali:~# nmap -A 10.0.0.156 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-27 22:10 EST
Nmap scan report for 10.0.0.156
Host is up (0.020s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u1 (protocol 2.0)
|_ ssh-hostkey:
|_ 2048 69:e6:3c:bf:72:f7:a8:08:f9:d9:f4:1d:08:e2:3c:bd (RSA)
|_ 256 4b:9e:c7:1e:9f:5b:d3:ce:fc17:56:f2:fe:42:ab:dc (ECDSA)
|_ 256 ae:0a:9e:92:64:5f:86:20:c4:11:44:e8:58:32:c5:05 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_ http-robots.txt: 1 disallowed entry
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-title: Site doesn't have a title (text/html).
10000/tcp open  http     MiniServ 1.920 (Webmin httpd)
|_ http-title: Site doesn't have a title (text/html; Charset=iso-8859-1)
MAC Address: 3C:6A:A7:B4:C2:29 (Intel Corporate)
Device type: general purpose
Running: Linux 3.2-4.9
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Fig. 3. Nmap scan on the target

### B. Enumeration

After having a look at /ona catalog. The activity known as website enumeration is taking place next because as seen earlier



the port 80 TCP is open. Let us enter the target IP address and /ona to view the webserver as in fig 4.

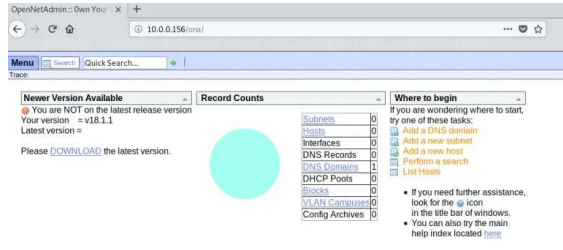


Fig. 4. /ona redirected to a vulnerable webserver

After clicking the Menu button, the version of the webserver has appeared. It is 18.1.1 OpenNetAdmin and it is a vulnerable webserver. The exploit for this server is to be typed in

Google. After founding the exploit, press the import button and begin the download process. After that, the new module is added and copied into the desired location and this module will be saved as 47772.rb.

### C. Exploitation



Fig. 5. The image shows the steps of command to execute to add the exploit into the Metasploit.

The Metasploit is launched and 47772 exploit is used to open the meterpreter session. Next, RHOST and LHOST IP addresses will be set as in fig 5- fig 10.

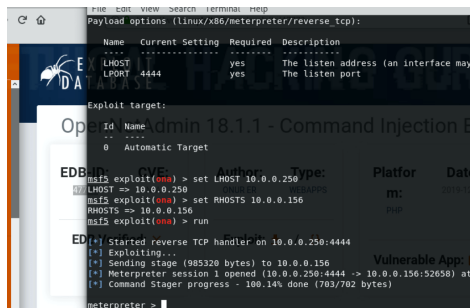


Fig. 6. Exploit the 47772 with msfconsole

Once the shell has been created, the shell upgrade to the python module will commence for spawning a new bash process with better control. The command in the image below.



Fig. 7. To get a better control upgrading it to the python module

### D. Dictionary Attack

The webserver's typical user is www-data to run the server that is currently used.

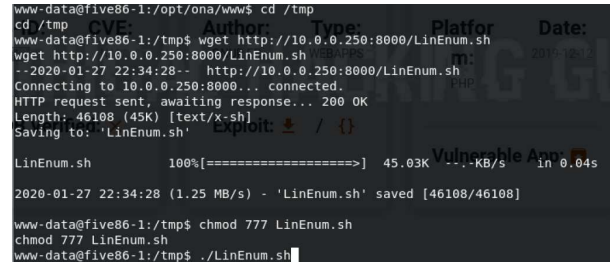


Fig. 8. Chmod 777 to the LinEnum.sh

Permit files with 777 chmod and runs it on the shell. The output reveals there is hashed password in the .htpasswd file.

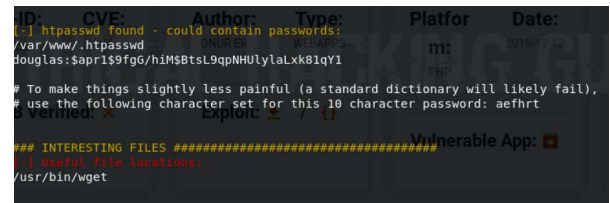


Fig. 9. The file is hidden, and the message alert is received

According to the given message it can be used to generate a wordlist of passwords based on the 6 symbols.



Fig. 10. decrypted the hash and picked up the password

Now it is time to launch crunch and add the command: crunch 10 10 aefhrt > wordlist.txt. The password for the user douglas has been obtained which is "fatherrrrr". When looking at the sudo -l for douglas user it is seen douglas user has sudo privileges to run /bin/cp binary for user jen as in fig11.

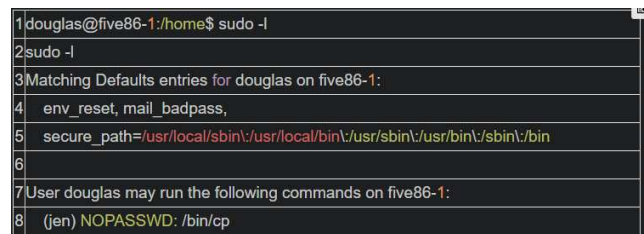


Fig. 11. The commands above will help us to exploit the /bin/cp binary when logged in as jen user to the target

### E. Privilege Escalation

Next, the necessary files can be copied by using an SSH keypair. A key phrase is not needed, thus users can just press enter twice as in fig 12 - fig 16.

```
douglas@fife86-1:/home/$ ssh-keygen -b 2048
ssh-keygen -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key (/home/douglas/.ssh/id_rsa):

/home/douglas/.ssh/id_rsa already exists.
Overwrite (y/n)? y
y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/douglas/.ssh/id_rsa.
Your public key has been saved in /home/douglas/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:S5XidPgoA7F3/hPEb1CPU0ig7YciH3AfcSFO5aNAId douglas@fife86-1
The key's randomart image is:
[RSA 2048]-----
+.o.o E++X+O=+
|O..+.*.X..B.
|..oo.o=B*o.
|O..+oo+.o.
|.. So
|...
|o
```

Fig. 12. Generating ssh key pair

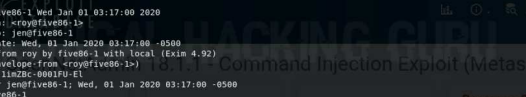
By changing the directory, a new pair of the key is created. All SSH keypairs will be stored in the `./ssh` folder and they contain public and private files. Connection to the host is done via SSH by using a keypair.

```
douglas@liveB6-1:/home$ cp /home/douglas/.ssh/id_rsa.pub /tmp/authorized_keys
cp /home/douglas/.ssh/id_rsa.pub /tmp/authorized_keys
douglas@liveB6-1:/home$ chmod 777 /tmp/authorized_keys
chmod 777 /tmp/authorized_keys
douglas@liveB6-1:/home$ sudo -u jen /bin/cp authorized_keys /home/jen/.ssh
sudo -u jen /bin/cp authorized_keys /home/jen/.ssh
/bin/cp: cannot stat 'authorized_keys': No such file or directory
douglas@liveB6-1:/home$ sudo -u jen /bin/cp /tmp/authorized_keys /home/jen/.ssh
sudo -u jen /bin/cp /tmp/authorized_keys /home/jen/.ssh
douglas@liveB6-1:/home$ ssh jen@127.0.0.1
ssh jen@127.0.0.1
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is SHA256:ae9ZGwKrvGggzH21BjQ23GmqV8eD5CzW0nUq8PBRYM.
Are you sure you want to continue connecting (yes/no)? yes
yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
jen@liveB6-1:~$ cat /etc/passwd
jen:x:1000:1:4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u2 (2019-11-11) x86_64
jen:jen:/home/jen:/bin/bash

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/*copyright.
```

Fig. 13. Jen user mail file

From the above image, a person logged in as jen and opened a mail file from the webserver.



roy@five06-1/var/mails cat jen  
cat jen  
From roy@five06-1 Wed Jan 01 03:17:00 2020  
Return-path: <roy@five06-1>  
Envelope-to: <jen@five06-1>  
Delivery-date: Wed, 01 Jan 2020 03:17:00 -0500  
Received: From roy by five06-1 with local (Exim 4.92)  
(envelope-from <roy@five06-1>)  
id 1m2ZC-0001PU-E1  
for <jen@five06-1>; Wed, 01 Jan 2020 03:17:00 -0500  
To: <jen@five06-1>  
Subject: Monday Moss  
MIME-Version: 1.0  
Content-Type: text/plain; charset=UTF-8  
Content-Transfer-Encoding: 8bit  
Message-ID: <1m2ZC-0001PU-E1@five06-1>  
From: Roy Treiman <roy@five06-1>  
Date: Wed, 01 Jan 2020 03:17:00 -0500  
EDB Verified: X  
Exploit: 0 / 1  
Vulnerable App: 0

As you know, I'll be on the "customer service" course on Monday due to that incident on Level 4 with the accounts people.

But anyway, I had to change Moss's password earlier today, so when Moss is back on Monday morning, can you let him know that his password is now **FireFire!**

Fig. 14. The new email reveals to us the password which is Fire!Fire!

The next step is to log in with another user moss and use the Fire!Fire! password. Doing some more steps for Linux privilege escalation it is possible to run the SUID in the /upyourgame with the privileges of sudo.

[illegible]

Fig. 15. The “upyourgame” in the highlighted text implies escalate privileges to root

```
moss@five86-1:~/games$ ./upyourgame
./upyourgame
Would you like to play a game? y
y
Could you please repeat that? y
y
Nope, you'll need to enter that again. y
OpenNetAdmin 18.1.1 - Comma
You entered: No. Is this correct? n
n
EDB-ID: CVE: Author: Type:
y 2020 N/A UNUR ER WEBAPPS
Made in Britain.
# whoami
whoami
root
EDB Verified: ✕ Exploit: 📄 / {}
# cd /root
cd /root
# ls
ls
flag.txt
# cat flag.txt
cat flag.txt
8f3b38dd95eccf600593da4522251746
#
```

Fig. 16. Flag.txt revealed

Finally, after typing the flag.txt with its content has been collected. The mission of hacking this box has been achieved.

#### F. DoS Attack

The next attack to launch is a Denial of Service (DoS) attack against the company's webserver to shut it down or heavily slow down the operation of the web application. DoS attacks utilize different flooding methods to send data packets which are: HTTP flood, ICMP ping, SYN Flood, Ping of Death, UDP Flood, and others. For this demonstration, the UDP flood is going to be used. The goal of this type of flood is to overwhelm the server memory and CPU. The UDP protocol can communicate without a TCP connection in other words establishing a 3-way handshake is not required.

A UDP flood does not exploit any vulnerability but it aims to create and forward a huge number of UDP packets from compromised IP addresses to the target webserver. By doing so a web application will become unreachable or very slow to the clients who want to learn some information from their website. This type of traffic cannot be processed by the server and leads it to consume a large amount of bandwidth. In the reconnaissance phase, Nmap script or whois tool will be used to discover the IP address of the target, and Nmap tool is used to identify which ports are open. To perform this attack the ports 80 or 53 should be opened as in fig 17 and fig 18.

In Linux OS hpin3 tool can be utilized to generate UDP floods:

```
root@kali:~# hping3 --flood --rand-source --udp -p TARGET_PORT TARGET_IP
```

HPing XXXX.XXX.XXX.XXX (eth0 XXXX.XXX.XXX.XXX): udp mode set, 28 headers + 0 data bytes  
hping in flood mode, no replies will be shown

Fig. 17. hping3 tool a code to execute DoS attack [9]

Where --flood: the packets will be sent as quickly as possible.

--rand source: insert any source address

--udp: is for the UDP mode

-p : port 80 is the port UDP runs on

Lastly, key in the target's port and IP address [9].

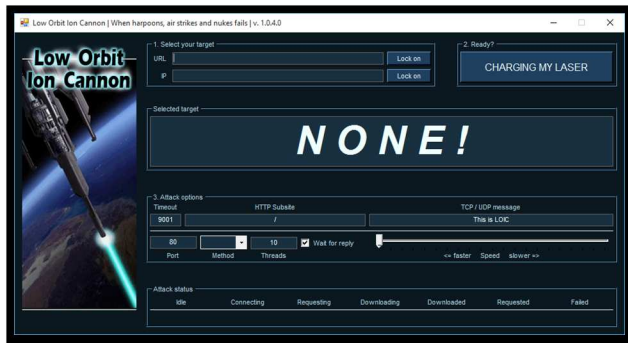


Fig. 18. Low Orbit Ion Cannon tool [9]

The GUI version of the tool to perform DoS is available too and it is called Low Orbit Ion Cannon (LOIN). It provides an easier and user-friendly interface for the testers.

The attack is started by setting the target's IP address 192.168.120.20 and port set to 80 with the method type UDP. After that, press the "CHARGING MAH LASER" to begin the flooding. Even though the tested system has Firewall and DMZ implemented these security services will not prevent DoS as simply they will fail to withstand the data load due to having limited bandwidth. A vast number of organizations' firewalls have around from 1 – 5 Gbps bandwidth provided by their ISPs. However, the normal size of a DoS attack usually starts from 6.65 Gbps which means the firewall bandwidth can quickly become overwhelmed while the attack continues to proceed to damage the web services. The attack will not stop unless stopped by the tester or reached the limit when the server is down, even with the cloud protection the successful launch of the attack might result in data or property theft during the incident.

### G. Critical Analysis

1) *Benefits of Penetration Testing from Business Perspective:* Penetration testing aids to protect organizations from potential failures through averting financial charges; ensuring diligence and compliance to industry regulators; maintaining the organization's reputation and image, along efficiently resolving information security investment.

After a security breach, organizations attempt to recover from it by spending millions of dollars, such as remediation efforts, notification cost, declined productivity and loss of revenue. According to the CSI study, the cost of recovery alone is estimated to be \$167,713.00 per incident. A great benefit of penetration testing is that it can identify and address risks before a security breach occurs, thus financial loss due to a security breach is eliminated. Industries such as HIPAA, PCI DSS, and others have mandated regulatory requirements for computing systems. Not complying with their requirements can result in the

organization receiving heavy fines, sanctions, imprisonment, or the organization ceases to operate in the market. Penetration testing being a proactive service provides organizations to stay up to par and pass auditing or compliance aspects of regulations [10].

2) *Disadvantages of Penetration Testing:* Penetration testing does not have any disadvantages but sometimes it leads to failures and faults which can be interpreted as data breaches when the data exposed can be leaked thus harm personal privacy and sensitive information. Working while cybercriminals threatening persons with fear for their lives or their lives of families for money. Moreover. The errors and failures in the systems may result in corruption of systems if not handled properly. In addition, data used for harmful and malicious purposes by penetration testers. The next disadvantage that is one of their main constraints is lack of reliability, organizations may not trust the ethical hacker. Furthermore, hiring such specialists can be expensive due to their specialized work. Lastly, if someone has hacked the system it becomes very time-consuming and frustrating [7].

3) *Impact of Hacking Computer Services:* The impact of compromising a person's laptop by establishing a Metasploit attack in the company can lead to serious damage to the company. The password and email will be leaked as shown in our demonstration. Just the fact of sharing with someone a password is wrong itself. The worst comes to worst the attacks based on password stealing and data leakage will surely lead to customers' loss and completely ruined reputation. Some companies even may go bankrupt because many people started not trusting them. Newly created malicious payloads in the Metasploit framework can be launched and bypass modern antivirus or prevention systems that opens door to Zero-day attacks. Releasing a patch for those attacks can take up to years and many systems will have a risk to be exposed to those vulnerabilities.

## IV. CONCLUSIONS

The article pays primary focus on the important event known as penetration testing which is essential in securing valuable information assets of the organization and making sure it meets the requirements of the regulator's compliance. Different types of penetration testing and the strategies of penetration testing have been discussed before moving to the information-gathering phase. The paper has demonstrated few attacks that can be potentially dangerous if security measures in the organizations are not in place or contain flaws and vulnerabilities. This article illustrates many free online tools with necessary information on how to use them to carry out a specific task or step in the penetration testing, even dedicated beginners can practice with these tools to extract information for their benefits. Thus, the advantages of conducting testing and hiring penetration testers is vital, who will be able to safeguard the information that poses a risk to be exploited or become a threat. The number of cyber-attacks is increasing daily and becoming more sophisticated, thus it is a necessity to let penetrating testing teams hack the organization's system before actual hackers compromise or



destroy the valuable information of the organization. It can be concluded that penetration testing with its corresponding methodology is an important step taken in the process of defending the entire information infrastructure in the organization. Through the research, it was confirmed that numerous free tools can be used to perform penetration testing.

#### ACKNOWLEDGEMENTS

The author would like to express sincere gratitude and deep appreciation to Dr. Vinesha Selvarajah for her valuable advice, comments, and active cooperation towards completing the article. The author also would like to acknowledge the contributions of her family and friends as necessary support to move forward. Without the help of all these people, the paper could not have been completed.

#### REFERENCES

- [1] A. Gupta and A. Anand, "Ethical hacking and hacking attacks", *International Journal of Engineering and Computer Science*, vol. 6, pp. 21042-21050, 2017. [Online] Available at: [https://www.researchgate.net/publication/316431977\\_Ethical\\_Hacking\\_and\\_Hacking\\_Attacks](https://www.researchgate.net/publication/316431977_Ethical_Hacking_and_Hacking_Attacks) [Accessed 30 April 2021].
- [2] A. Rahman, S. Rasel, A. Norman and S. Alim, "Vulnerability assessments in ethical hacking", *American Journal of Engineering Research (AJER)*, vol. 5, pp. 1-5, 2016. [Online] Available at: [http://www.ajer.org/papers/v5\(05\)/A05050105.pdf](http://www.ajer.org/papers/v5(05)/A05050105.pdf) [Accessed 30 April 2021].
- [3] Cyberx, "7 Penetration testing phases to achieve amazing results", n.d. [Online] Available at: <https://cyberx.tech/penetration-testing-phases/> [Accessed 01 March 2021].
- [4] Cybervie.com, "Phishing attack – step by step demo using Kali Linux free tool!", n.d. [Online] Available at: [Phishing Attack - Step by step Demo using Kali Linux Free Tool \(cybervie.com\)](#) [Accessed 01 March 2021].
- [5] D. Gkoutzamanis, "Five penetration testing frameworks and methodologies", 2020. [Online] Available at: <https://cisotimes.com/five-top-penetration-testing-frameworks-and-methodologies/> [Accessed 01 March 2021].
- [6] D. Son "Top 9 Best Tool for Penetration Tester", 2017. [Online] Available at: [Top 9 Best Tool for Penetration Tester • Penetration Testing \(securityonline.info\)](#) [Accessed 21 February 2021].
- [7] D. Kumar, Y. Khera, Sujay, N. Garg, P. Jain, "Towards the impact of hacking on cyber security", 2018. [Online] Available at: [https://www.researchgate.net/publication/326812925\\_TOWARDS\\_THE\\_IMPACT\\_OF\\_HACKING\\_ON\\_CYBER\\_SECURITY](https://www.researchgate.net/publication/326812925_TOWARDS_THE_IMPACT_OF_HACKING_ON_CYBER_SECURITY) [Accessed 30 April 2021].
- [8] EC-Council, "5 Penetration testing methodologies and standards for better ROI", n.d. [Online] Available at: <https://blog.eccouncil.org/5-penetration-testing-methodologies-and-standards-for-better-roi/> [Accessed 01 March 2021].
- [9] G. Sagoglu, "How to perform DDoS test as a pentester", 2016. [Online] Available at: <https://pentest.blog/how-to-perform-ddos-test-as-a-pentester/> [Accessed 01 March 2021].
- [10] G. Bacudio, X. Yuan, B. T. B. Chu and M. Jones, "An Overview of Penetration Testing", *International Journal of Network Security & Its Applications*, vol.3, pp. 19-38, 2011. [Online] Available at: [https://www.researchgate.net/publication/274174058\\_An\\_Overview\\_of\\_Penetration\\_Testing](https://www.researchgate.net/publication/274174058_An_Overview_of_Penetration_Testing) [Accessed 30 April 2021].
- [11] N. J. Hout, "Standardized penetration testing? Examining the usefulness of current penetration testing methodologies", 2019. [Online] Available at: (PDF) [Standardised Penetration Testing? Examining the Usefulness of Current Penetration Testing Methodologies \(researchgate.net\)](#) [Accessed 01 March 2021].
- [12] Packtpub.com, "The mobile application penetration testing methodology", n.d. [Online] Available at: [The mobile application penetration testing methodology - Mobile Application Penetration Testing \(packtpub.com\)](#) [Accessed 21 February 2021].
- [13] R. Johansen, "Ethical hacking code of ethics: security, risk & issues", 2017. [Online] Available at: [Ethical Hacking Code of Ethics: Security, Risk & Issues - Panmore Institute](#) [Accessed 01 March 2021].