Ethical Hacking: Redefining Security in Information System

Sanchita Saha, Abhijeet Das, Ashwini Kumar, Dhiman Biswas and Subindu Saha

Abstract On defining the severe status of information security in the present world, we come across a very renowned technical term known as 'ethical hacking'. Ethical hacking refers to the art of unmasking the vulnerabilities and the weakness in a computer or an information system. The process involves duplication of intents and actions of other malevolent hackers. Ethical hacking can be also called as 'penetration testing', 'intrusion testing', or 'red teaming'. Talking about the term 'hacking', it is basically a challenging and an invigorating procedure to steal information from an unknown computer system or may be a device without the prior knowledge of the owner of that system. Now by the term 'ethical', we understand the process of hacking is done for an ethical purpose which will result in a boon for the society. An ethical hacker tries to recover or destroy the stolen information or data by the non-ethical hackers. The process of hacking can thus become a boon as well as a curse for the society, and it depends upon the intention of a hacker. This is no doubt that a very strong procedure and severely based on what way it is used. This paper elicits the various methodologies and concepts related to ethical hacking as well as the tools and software used in the process along with the future aspects and emerging technologies at this field.

Keywords Ethical · Security · Vulnerabilities · Hacker · Intrusion

S. Saha (✉) · A. Das · A. Kumar
Haldia Institute of Technology, Haldia, India
e-mail: sanchita.cse2007@gmail.com

A. Das
e-mail: abhijeetd720@gmail.com

A. Kumar
e-mail: ashwinikumaredu@gmail.com

D. Biswas
South Calcutta Polytechnic College, Kolkata, India
e-mail: bisdhi24@gmail.com

S. Saha
Institute of Engineering and Management, Kolkata, India
e-mail: subindu.saha@iemcal.com

© Springer Nature Singapore Pte Ltd. 2020

M. Chakraborty et al. (eds.), *Proceedings of International Ethical Hacking Conference 2019*, Advances in Intelligent Systems and Computing 1065, https://doi.org/10.1007/978-981-15-0361-0_16

1 Introduction

Ethical hacking can be defined as an ultimate security professional work commonly termed as 'white hat hacking'. Ethical hackers are well known to detect and exploit vulnerabilities and weakness out of various systems. An ethical hacker uses those skills in a legitimate and a lawful manner to find out the vulnerabilities existing in a system and fix them before the malicious activists try to break in through.

An ethical hacker role is similar to a penetration tester, but it involves bigger duties. They break into systems legally and ethically. This is the primary difference of legality between ethical hackers and non-ethical hackers.

Apart from testing processes, ethical hackers are associated with several other responsibilities. The main idea is to imitate a malicious hacker [1] at work, and rather than exploiting the susceptibilities for malicious purposes, they seek countermeasures to shore up the systems' defence. An ethical hacker might employ all or some of these strategies to enter into a system:

- Scanning Ports and Seeking Vulnerabilities: An ethical hacker uses port scanning tools like Nmap or Nessus to scan one's system and locate the open ports. The vulnerabilities with each of the ports can be studied and remedial actions can be taken.
- An ethical hacker examines the patch installations and creates prevention to save them getting exploited.
- The ethical hacker may get involved in social engineering concepts like dumpster diving rummaging through trash bins for passwords, sticky notes, charts, or other things with vital information [2] that can generate an attack (Fig. 1).

Fig. 1 A real-time image of threat model

Fig. 2 Threat model of ethical hacking

- An ethical hacker may also employ other social engineering techniques like shoulder surfing to gain access to crucial information or play the kindness card to trick employees to part with their password.
- An ethical hacker will attempt to evade intrusion prevention systems (IPS), intrusion detection systems (IDS), honeypots, and firewalls.
- Bypassing and cracking wireless encryption, sniffing networks and capture Web servers and Web applications.
- Ethical hackers may also handle issues related to device theft and employee fraud as well as solving the problems with locating the lost devices and unlocking through bypassing the password-protected devices and help the cyber units (Fig. 2).

A real-time image has taken for just to show that each and every second our personal information is compromised and how can we detect that well, by knowing the threats.

Therefore, we must be aware of the threat modelling.

Threat modelling helps us to know about the attacks and which appropriate steps can be taken in order to protect our information.

2 Types of Hacking

We can separate out hacking into different categories, based on what is being hacked. Here, it contains a set of examples:

- Website Hacking: Hacking a website means enchanting unauthorized control over a Web server and its related software such as databases and other interfaces.

- Network Hacking: Hacking a network means gathering information about a network by using different tools like Telnet, nslookup, ping, TRACERT, and netstat, with the resolved to harm the network system and hamper its operation.
- Email Hacking: This contains getting unauthorized access on an email account to using it.
- Password Hacking: This is the process of recuperating secret passwords from data that has been stored in or diffused by a computer system.
- Computer Hacking: This is the process of stealing computer ID and password [3] by applying hacking methods and getting unauthorized access to a computer system.
- Ethical Hacking: Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed on it. It is very much comparable to penetration testing.

2.1 Penetration Testing

This is basically a replicated cyber-attack against your computer system to check for the exploitable susceptibilities present in the system. In the context of Web application security, penetration testing is commonly used to enhance a Web application firewall (WAF).

Penetration testing comprises the attempted piercing of any number of application systems, (e.g. application protocol interfaces (APIs), front-end/back-end servers) to uncover vulnerabilities, such as unsensitized inputs that are susceptible to code injection attacks (Fig 3).

The pen testing process can be broken down into the following five stages:

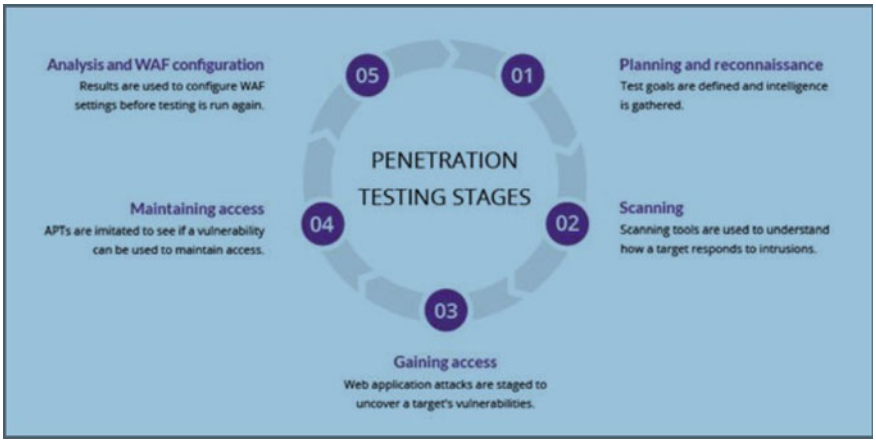

Fig. 3 Penetration testing stages of ethical hacking

2.1.1 Planning and Reconnaissance

- The scope and goals of a test, including the systems to be addressed and the testing methods to be used, are significant.
- Intelligence (e.g. network and domain names, mail server) is required to better understand how a target works and its probable vulnerabilities.

2.1.2 Scanning

The next is to understand how the goal application will respond to various invasion attempts. This is characteristically done using:

- Static analysis: Reviewing an application's code to estimate the way it performs while running. Tools can scan the whole of the code in a single pass.
- Dynamic analysis: Reviewing an application's code in a running state. This is a more real way of scanning [4], as it delivers a real-time view into an application's performance.

2.1.3 Gaining Access

This phase uses Web application attacks, such as cross-site scripting, SQL injection, and back doors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, stealing data, intercepting track, etc., to understand the damage they can cause.

2.1.4 Maintaining Access

The target of this stage is to see if the vulnerability can be used to achieve a tenacious presence in the exploited system long enough for a bad actor to gain in-depth access. This concept is to imitate unconventional persistent threats, which often remain in a system for months in order to steal an organization's most crucial data.

2.1.5 Analysis

The results of the penetration test are then assembled into a report listing:

- Precise susceptibilities that were exploited.
- Delicate data that was accessed.
- The certain amount of time the pen tester was able to remain undetected in the system.

The above information is scrutinized by security personnel to help configure an enterprise's WAF settings and other application security solutions to patch susceptibilities and protect against future attacks.

3 Tools Used for Ethical Hacking

3.1 Nmap

Nmap or a Network Mapper is a free open-source tool which widely used in the purpose of network detection and security checking. It was originally built to scan large networks, but it can work equally for single hosts as well. It makes it easy for the network administrators for the tasks such as network inventory, monitoring host, or service up-time and upgrade schedules managing service. Nmap [5] works well in the well-known operating systems such as the Windows, Mac OS X, as well as it is already installed in Kali Linux platform and BackTrack.

Nmap basically uses the raw IP packets to determine these various terminologies used in cybersecurity.

- The hosts which are available on the network.
- The operating systems they are running on.
- The services offered by those hosts.
- The type of firewalls in use and other such characteristics.

3.2 Burp Suite

A Burp Suite is a popular platform that is widely used for performing security testing of Web applications. It has several tools that works with the collaboration of whole testing process support, from initial mapping and analysis of an application's attack surface, to finding and manipulating security vulnerabilities. Burp Suite [6] can be easily operated on and it provides the administrators full control to combine advanced manual techniques with automation for effectual testing. Burp Suite can be simply configured, and it contains specific features to assist even the most experienced testers with their work (Fig. 4).

This is an original screenshot of the working tool Burp Suite along with the XAMPP control panel opened on the window.

Step 1: Go to proxy tab and then select Intercept → click on Intercept and make it enable.
Step 2: Open Web browser and open any website to capture its traffic and vulnerabilities.
Step 3: The vulnerabilities are detected in the Burp Suite Panel.

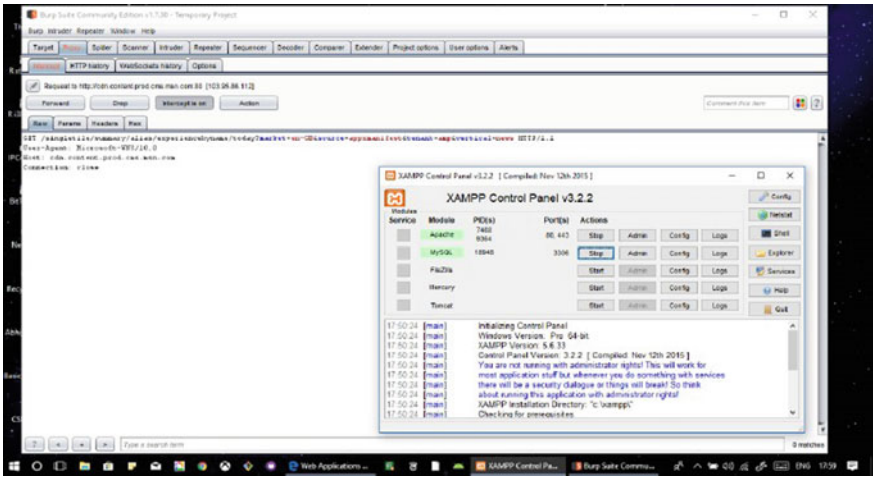

Fig. 4 Working tool of Burp Suite along with XAMPP control panel

3.3 Maltego

Maltego [7] is an interactive data mining tool which extracts directed graphs for link analysis. For online investigations, this tool verdicts the relationship between pieces of information from numerous sources which are located on Internet (Fig. 5).

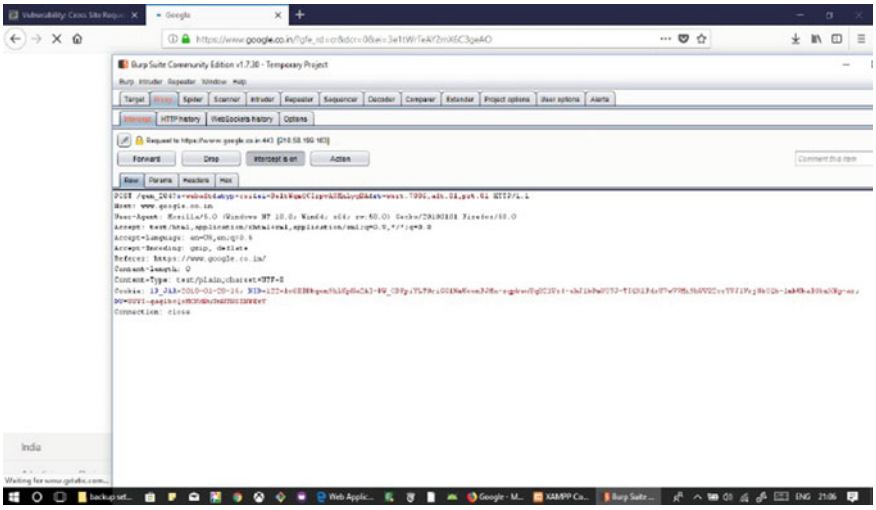

Fig. 5 Vulnerability detection in Burp Suite panel

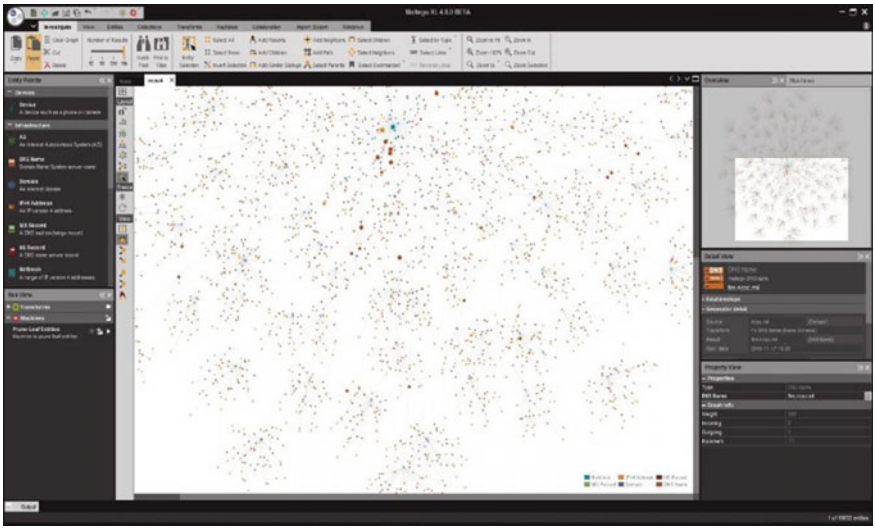

Fig. 6 A directed graph of Maltego for link analysis

- It uses the idea of transmutes to automate the process of interrogating different data sources, and this information is then displayed on a node-based graph suited for performing link analysis.
- Presently, there are three versions of the Maltego client namely Maltego CE, Maltego Classic, Maltego XL.
- All these Maltego clients come with access to a library of standard transforms for the discovery of data from an eclectic range of public sources that are usually used in online digital forensics and online investigations (Fig. 6).
- Because Maltego can effortlessly integrate with nearly any data source, many data vendors have chosen to use Maltego as a delivery platform for their private data. This also means Maltego can be adapted to someone's own, unique supplies (Fig. 7).

3.3.1 What Does Maltego Do?

The focus of using Maltego is evaluating real-world relationships between information and knowledge which is publicly accessible on the Internet. This includes footprinting Internet infrastructure as well as information gathering about the people and the corresponding organization.

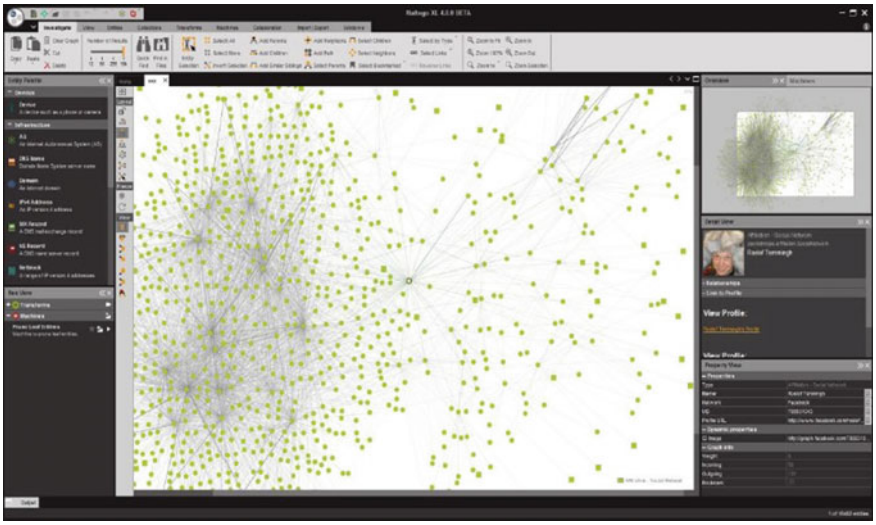

Fig. 7 A node-based graph suited for performing link analysis

Maltego can determine the relationships between the following things:

a. People:
   - Names.
   - Email addresses.
   - Aliases.

b. Social networks (groups of people).
c. Organizations.
   - Websites.
   - Domain.
   - DNS names.
   - Net blocks.
   - IP addresses.

d. Affiliations.
e. Documents and files.

3.4 Metasploit

Metasploit [8] gives information about security susceptibilities, and it is mainly used as a tool for developing and executing exploit code against a remote target machine.

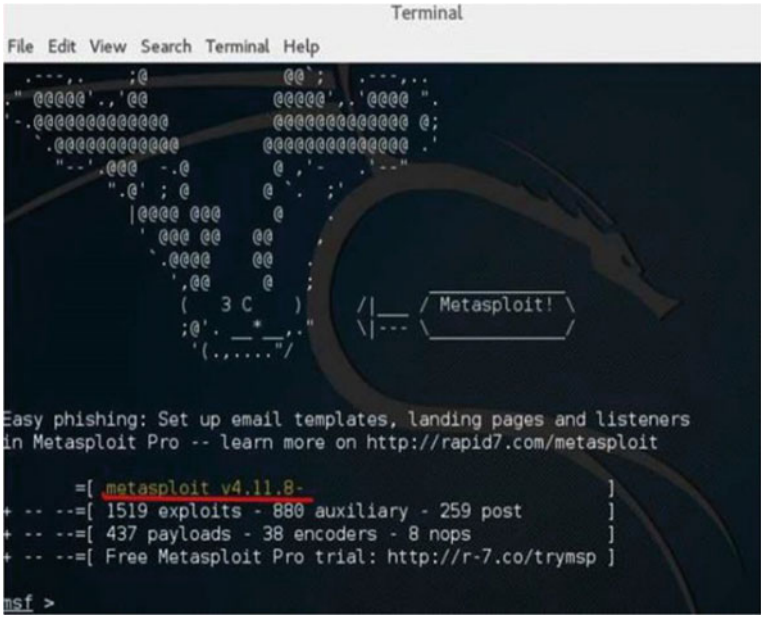

Fig. 8 Metasploit framework for exploitation and testing

- First, open the Metasploit Console in Kali. Then move to Applications → Exploitation Tools → Metasploit.
- Then, the following screen appears (Fig. 8). If we want to find out the exploits related to Microsoft, the command can be msf → search name: Microsoft type: exploit (Fig. 9), where search is the command, name denotes the name of the object that we are looking for, and type denotes the particular kind of script we are in search of.
- Module or platform provides the information regarding the author name, vulnerability reference, and the payload restriction.

This is an example of how to see exploits related to Microsoft, and there are many commands in Metasploit framework for exploitation and testing, which can be checked using help command.

3.5 Armitage

Armitage [9] GUI for Metasploit is an accompaniment tool for Metasploit. It envisions targets, recommends exploits, and exposes the advanced post-exploitation features (Fig. 10).

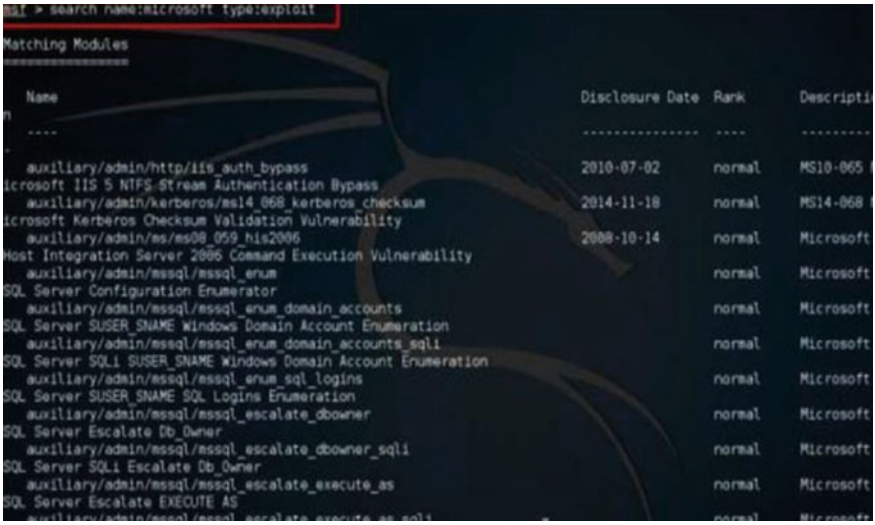

Fig. 9 Metasploit framework for exploitation and testing using help command

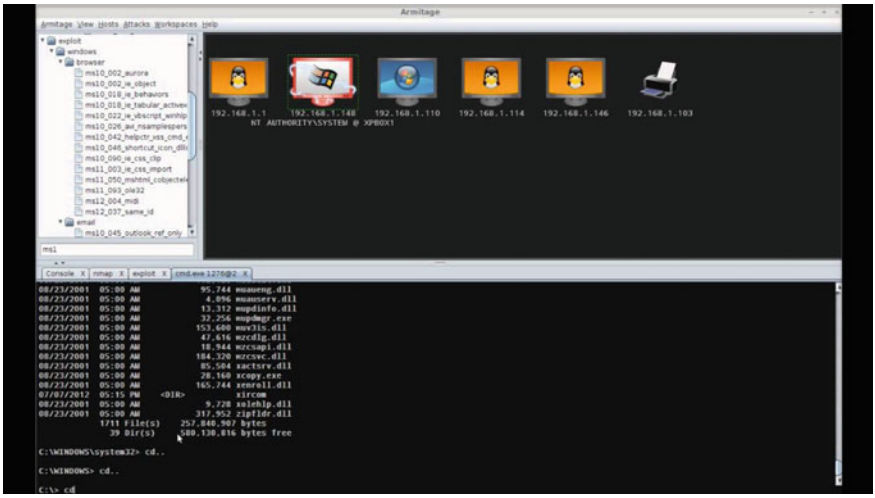

Fig. 10 An Armitage GUI for Metasploit

- Connect to Armitage, and it will list all the discovered machines to be exploited. Hacked target is shown in red colour with a storm with it.
- After having to target hack, just right-click on it and continue the exploration.

3.6 Hydra [10]

Login cracker tools that supports numerous protocols (Cisco auth, CVS, FTP, Cisco enable, HTTP(S)-FORM-GET, HTTP(S)-FORM-POST, HTTP(S)- GET, HTTP(S)-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MySQL, NNTP, Oracle SID, PC Anywhere, PC-NFS, POP3, PostgreSQL, RDP, Rexec, Rlogin, Rsh, SIP, SMB(NT), SMTP, SMTP Enum, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Telnet, VMware-Auth, VNC, and XMPP) to attack.

- It will open terminal console (Fig. 11). In this case, we will brute force FTP service of Metasploitable machine, which has MAC Address CA: 01:17: A8:00:08 (Fig. 12).
- We have created in Kali a word list with extension first in the path user (Fig 13).

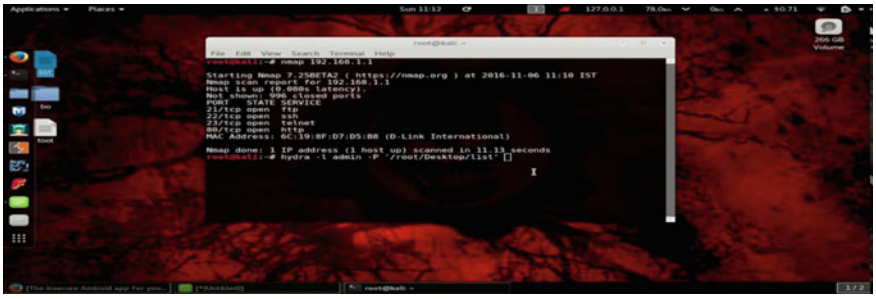

Fig. 11 Hacking router password using HYDRA

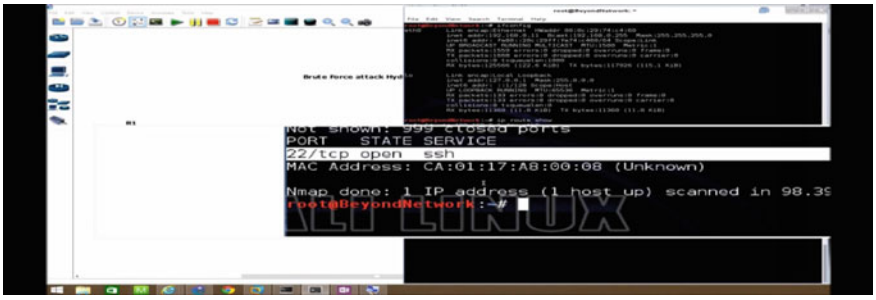

Fig. 12 Hacking MAC address using HYDRA

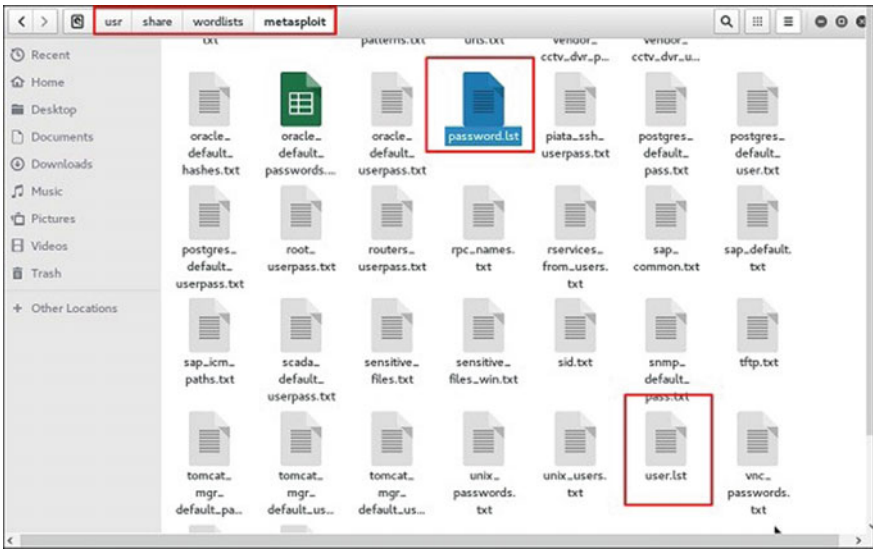

Fig. 13 A word list generation in Kali with extension

- The command is as follows: hydra-l/user/share/word lists/Metasploit/user-P/user/share/word lists/Metasploit/passwords ftp://192.168.2.58 V where V is the user name and password while trying (Fig. 14 and Table 1).
- As shown in the following, the user name and password are new local admin and $uP3r5ekrItpass, respectively.

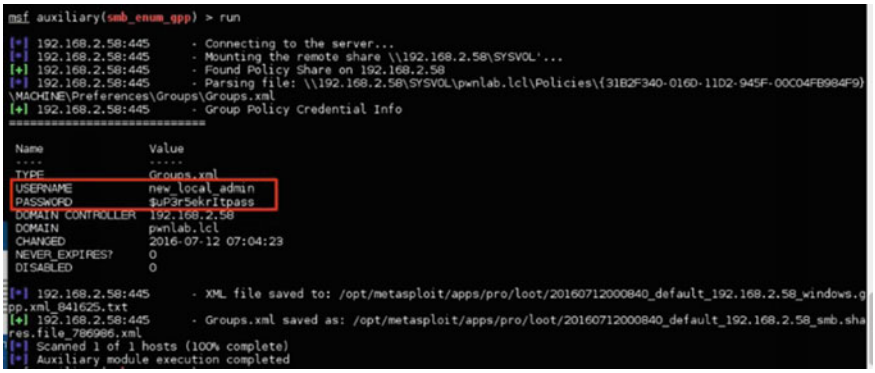

Fig. 14 Track username and password

Table 1 Features of the tools used are shown as follows

Tools	Features
Nmap	• It is a network scanner tool which is free and open source • It is connected to a network/host and discovers open ports (responding to TCP and ICMP requests) • It points out hosts answering to network requests • It gives the host details (like network and OS details) • It can discover application running and its details • It is used to scan huge networks consisting of thousands of machines
Burp Suite	• It is a Java-based Web penetration testing framework • It helps to identify vulnerabilities and verify attack vectors that are affecting Web applications • It acts as 'man in the middle', capturing and analysing requests to and from the target Web application to be analysed • It can be paused, manipulated, and replay individual HTTP requests in order to analyse potential parameters or injection points. Those can be specified for manual as well as automated fuzzing attacks to discover potentially unintended application behaviours, crashes, and error messages
Maltego	• It is generally used for open-source intelligence and forensics • It helps to discover data in visual formats using built-in libraries of transforms • It permits creating custom entities apart from the entities that it provides • It analyses social, computer, or any real-world relationships from data sources, DNS records, search engines, API, social network, and various meta-data
Metasploit	• It is used to check security vulnerabilities and also for penetration testing IDS signature development • It includes anti-forensic and evasion tools, which are built on its framework • To choose an exploit and payload, some information about the target system is needed, such as operating system version and installed network services • It can be gleaned with port scanning and OS fingerprint tools such as Nmap • It can import vulnerability scanner data and compare the identified vulnerabilities to existing exploit modules for accurate exploitation
Armitage	• It is a graphical cyber-attack management tool under Metasploit framework • It visualizes the potential exploits and recommends too • It is used to access the advanced features of Metasploit • A user may launch scans and exploits, get exploit recommendations, and use the advanced features of the Metasploit Framework's metaoperator
Hydra	• It includes many login protocols like FTP, SMB, POP3, IMAP, VNC, and SSH • It is known as paralyzed network logon cracker • It is used for brute-force attack on any protocol like password and username guessing if any field is provided, cracking login credentials, etc. • A very well-known and respected network logon cracker (password cracking tool) which can support many different services

4 Advantages of Ethical Hacking

Millions of systems are hacked every second for the monetary as well as economic benefits resulting in a slowdown in the growth of a country. Hacking is a process which requires high profile techniques to catch the data theft and fraud. These techniques may or may not be within the permissions of the cyber laws. Benefits of ethical hacking are noticeable, but many are overlooked. The benefits include:

- National security breaches and fighting against terrorism.
- To prevent malicious hackers from gaining access to the computer system.
- Having acceptable pre-emptive measures in place to prevent security breaches.

5 Limitations of Ethical Hacking

An ethical hacker should know the consequences of illegal hacking into a system. Ethical hacking is usually conducted in a systematized manner, usually as part of a penetration test or security audit. The ethical hacker uses the knowledge they have when they are involved in malevolent hacking activities. This also referred to as intrusion testing, penetration testing, and red teaming. The ethical hacker generally sends and place spiteful code, viruses, malware, and other harmful things on a computer system.

6 Conclusion

Information is the most valuable strength of any organization. Hacking is the activity through which intruders are trying to gain access to the system to steal personal/corporate data. Everyone should pay much attention so that security measures can be strong to protect the confidentiality and integrity. Ethical hacking identifies and rectifies weaknesses of the computer system by describing the process of hacking in a decent manner. It protects the privacy of the organization and informs the hardware and software vendors of the identified weakness. Ethical hacking thus improves the security of the network or system.

References

1. Kumar, D., Agarwal, A., Bhardwaj, A.: Ethical hacking. Int. J. Eng. Comput. Sci., **4**(4), 11466–11468 (2015)
2. Sahare, B., Naik, A., Khandey, S.: Study of ethical hacking. Int. J. Comput. Sci. Trends Technol. (IJCST) **2**(4) (2014)

3. Munjal, M.N.: Ethical hacking: an impact on society, cyber times. Int. J. Technol. Manag. **7**(1) (2014)
4. Utkarsh, K.: System security and Ethical hacking. Int. J. Res. Eng. Adv. Technol. (IJREAT) **1**(1) (2013)
5. Juneja, G.K.: Ethical hacking: a technique to enhance information security. Int. J. Innov. Res. Sci., Eng. Technol. **2**(12) (2013)
6. Tekade, A.P., Gurjar, P., Ingle, P.R., Meshram, B.B.: Ethical hacking in linux environment. Int. J. Eng. Res. Appl. (IJERA) **3**(1), 1854–1860 (2013). ISSN: 2248-9622
7. Begum, S., Kumar, S.: Ashhar: a comprehensive study on ethical hacking. Int. J. Eng. Sci. Res. Tecgnology, **3** (2016). ISSN: 2277-9655
8. Ajinkya, A.F., Kashikar, A.G., Zunzunwala, A.: Ethical hacking. Int. J. Comput. Appl. (0975–8887), **1**(10), 14–20 (2010)
9. Whitman, M.E., Mattord, Herbert, J.: Management of Information Security, Boston, Massachusetts: Thomson Course Technology, pp. 363–375 (2004)
10. Smith, B., Yurcik, W., Doss, D.: Ethical hacking: the security justification. In: Proceedings of the Ethics of Electronic Information in the 21st Century Symposium (EEI21), Inc. Publishers, University of Memphis, Memphis TN USA (2001)
11. Satapathy, S., Patra, R.R.: Ethical hacking. Int. J. Sci. Res. Publ. **5**(6) (2015)
12. Mukhopadhyay, R., Nath, A.: Ethical hacking: scope and challenges in 21st century. Int. J. Innov. Res. Adv. Eng. (IJIRAE) **1**(11) (2014). ISSN: 2349-2163