IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

HACKING WITH KALI LINUX

Aditya Kumar, Anku Mishra

Student, Student,
Computer Science Engineering,
[1]SRM University, Delhi-NCR , India

Abstract: Ethical hacking, the word in itself is a big confusion for people to comprehend because it's hacking yet it is ethical. Let me explain it with one example, in today's war-torn era, arms and ammunition are of huge importance for national security. But the arms and ammunition can not be considered as elements of evil destruction, what should be considered as evil is the intention of people who are using it. In the end, ethical hacking is also a skill set just like other skills used in the industry. In future there will be high demand for protecting the confidential data whether it is government body or private firm or it belongs to particular individual. Theft and leakage of confidential data is becoming a major issue in present scenario.

I. Introduction

The trend of hacking came to existence only after Internet was introduced (JANUARY 1, 1983), before internet, electronic signals were captured and decrypted by evil persons. As we all can see, only 40 years have passed since invention of internet. Though its adolescence period is over, internet is in very immature phase. We need to do more research in this domain and invent advance technologies to provide safety measures for internet users. As more and more people are connecting to internet from all parts of world.
Internet is huge and it can broadly be categorized into 3 parts. Not many people are aware of all 3 of these parts, mainly due to lack of interest I believe.

(a) Surface Web: Surface web is everything that you can search and explore on your internet browser, example: YouTube, Twitter, E-books, Articles etc.
(b) Deep Web: Deep web are websites that is not shown by search engines or they are protected by passwords.
(c) Dark Web: Dark web is filled with websites that are encrypted and it also carries private databases. It is usually accessed by (TOR) the onion router.

So many things are happening in dark web. Dark web provides anonymity. Dark web carries marketplaces for purchasing and selling illegal products and services. Crypto Mixers are used for breaking blockchains of crypto-currencies. Evil hackers can be hired for malicious activity.

Kali Linux is an operating system used for penetration testing and digital forensic. It was first released in March 2013 by offensive security. It carries many tools for penetration testing and has its own server called Apache2. Most of the times it is seen that flaw and vulnerability present in website is because of bad practices of web developer.

2 LITERATURE REVIEW AND RELATED WORKS

SECURITY BASES:

1.) Authentication: It will address the question: - "who are you?" It is the process of identifying uniquely customers, applications, and services.
2.) Authorization: It will address the question: - "What can you do?" It is the process that controls resources and operations, the user is allowed to access.

3.) Non-Repudiation: It will keep the record of activities performed by specific user and ensures that user cannot refuse to perform that operation.

4.) Privacy/Confidentiality: It ensures that data is kept private and cannot be viewed by unauthorized users or intruders. Encryption is used to enforce confidentiality.

5.) Integrity: It ensures that data is protected and cannot be altered or modified.

6.) Availability: It means data will remain available to legitimate users.

NEED FOR WEB APPLICATION SECURITY: -

The growth and advancements of internet has created huge impact on how we communicate and operate in present day leading to generation of lots of sensitive information. For example: e-commerce websites, bank services, social networking web etc.

TYPES OF PENETRATION TESTING: -

There are 3 types of penetration testing.

1.) Black Box Testing: Tester has no idea about the system he will be testing. Major priority is given to gathering information about target network and system.

2.) White Box Testing: Tester is provided with complete range of information about system and network infrastructure such as OS details, IP address etc. We try to measure the damage inflicted by someone who is part of the organization.

3.) Grey Box Testing: Tester is usually provided with partial or limited information about system. We try to simulate the attack done by someone who is not part of organization.

7 STAGES OF PENETRATION TESTING:

1.) Planning And Preparation: In planning stage goals and objectives of pen testing is decided.

2.) Reconnaissance: The tester starts by analyzing the available information and if needed requests for more information such as system description, network plans.

3.) Discovery: Scanning targets assets for discovering vulnerability. Some tools have their own databases giving details of latest vulnerability.

4.) Analyzing Information and Risks: Before penetrating the system, tester will analyze the information. Because of large number of system and size of infrastructure it is extremely time consuming.

5.) Active Intrusion Attempts: In this step we measure the extent to which the potential vulnerability possesses actual risk.

6.) Final Analysis: It considers all step conducted till that time. It also evaluates vulnerability presents in form of potential risk. It recommends to eliminate the vulnerability.

7.) Report Preparation: It starts with description of testing procedure, followed by analysis of vulnerability and risk. The high order risk and critical vulnerability must have priority followed by lower order.

DARK WEB: -

Darknet Services: - According to the latest report released by UNITED NATIONS OFFICE OF DRUG AND CRIMES, the top 3 services provided by darknet are as follows:

1.) Illicit Marketplace
2.) Cryptocurrencies
3.) Illicit products

As anonymization technology is getting more popular, more users are interacting with illicit darknet marketplaces. The number of these marketplaces have increased from 1 in 2011 to 118 in 2019. Most often you will find cryptocurrencies usage for transaction on these marketplaces as they provide anonymity.

Bitcoin is very popular cryptocurrency used in darknet and most of the times, transaction made by bitcoin are traceable. For this purpose, only

Crypto-Mixers are used.

Crypto mixers will generally break the block chain of transaction. This is done by mixing traceable bitcoin with fresh non traceable bitcoin in a particular wallet and send back random non traceable bitcoin. One can think of it as money laundry by eliminating the traceable link between two wallets.

There are different kinds of products and services provided by darknet. One can purchase ransomware and malware as a service. Drugs ranging from prescribed one to steroids and ecstasy stimulants are sold on different marketplaces.

3 PROBLEMS AND PROPOSED SOLUTION

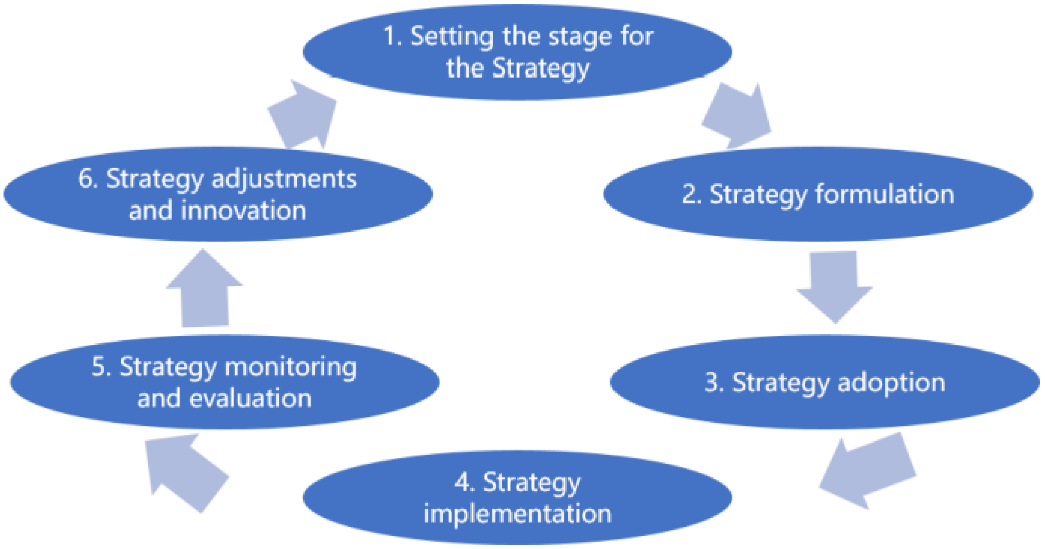
Mobility: After COVID-19, many private firms have adopted the use of internet in their businesses. With greater mobility and wide network access, number of employees working remotely have increased. But this network is less secure, due to this many confidential data is vulnerable for exploitation.

Connectivity: As internet services are getting cheaper, more people are using internet for electronic communication and transaction but the standards of security of the devices and networks are low. This increases the chances of people becoming victim of cybercrime and fraud.

Legislation and Jurisdiction: Sometimes cybercrime involves people of different countries working together. This creates so much chaos as different countries have different laws and the activity which is crime in one country may not be a crime in other country.

Under-Reporting: In many cases it is observed that companies and individuals have ignored cybercrime offences. Because of the failure of reporting cybercrime offenses there is lack of information on how these criminals operate and coordinate among themselves.

Cybercrime Strategy:


1. Setting the stage for the Strategy
2. Strategy formulation
3. Strategy adoption
4. Strategy implementation
5. Strategy monitoring and evaluation
6. Strategy adjustments and innovation

A cybercrime strategy should support counter-terrorism and provide solutions for eliminating money laundering efforts. Cybercrime strategy should work on international level so that different countries can coordinate with each other. The strategy should have relevant phases of procedures which can be accomplished in given time frame.

4 METHODOLOGY:

There are 5 phases of ethical hacking, they are as follows: -

a.) Reconnaissance: In this phase, hacker will try to collect as much information as possible.

b.) Scanning and Enumeration: In this phase, hacker will scan the network of organization and gather information about different services running on the victim machine. What ports are open, and what kind of devices are connected to the network.

c.) Gaining Access: In this phase, hacker will try to penetrate the network. Hacker will use different tools and techniques to bypass security, such as ARP spoofing, DNS spoofer etc.

d.) Maintaining Access: In this phase, hacker will run malicious program such as backdoors, virus, trojan etc. so that next time when hacker needs to gain unauthorized access of victim machine, it does not have to start from beginning.

e.) Covering Tracks: At this phase, hacker will eliminate all the traces so that it cannot be suspected for the crime it committed.

Threat Modeling: It is an approach to spot and diagnose the threats and vulnerability of system. In broader terms, it is a risk management approach which mainly focuses on analysis of network and application security.

5 IMPLEMENTATION

There are different kinds of tools used in different phases of hacking.
Information Gathering (Reconnaissance): There are 2 types of information gathering. Active and Passive information gathering. In passive reconnaissance, hacker will collect information without directly involving with victim. It will collect information from other sources and websites like 'WhoIsLookUp'. In active reconnaissance hacker will directly interact with victim. Social engineering can be considered as active reconnaissance.

Scanning and Enumeration: In this phase, hacker will scan the network and victim machine. Nmap scan, Service scan, Version scan and Port scanning are techniques used for this purpose. This will give us detailed information about open ports and services running on the machine.

a.) db_nmap => stores scanned result in database.
b.) Nmap -P 80 scanme.nmap.org => shows the services running on port 80.
c.) Nmap -sV -P 80 scanme.nmap.org => shows the version of services running.
d.) nmap -O [IP address] => tells the operating system running on host machine.
e.) netdiscover -r [IP address] => It gives all the client present in the network.

Gaining Access: In this phase hacker will perform different attacks on victim machine based on the information collected so far. 'Man In The Middle' attack is very popular attack these days. Its types are as follows:

a.) ARP Spoofing
b.) DNS Spoofing
c.) Rouge Access Point

Various techniques are used in these types of MITM attacks, such as
a.) Packet Sniffing
b.) SSL Striping

Packet Sniffing:
a.) "airodump-ng --bssid[mac address] --channel --write[file name] interface" => this command will store the data sniffed from victim mac address in a file.
b.) "aireplay-ng --deauth -a[mac address] -c[station] interface" => this command will disconnect victim from network for given time frame.
c.) "BetterCap" is an inbuilt tool of Kali Linux used for packet sniffing. It is having a great graphical user interface and can also be accessed by terminal window.

WEP Cracking:
WEP is an encryption protocol used by many devices. We can bypass WEP protocol by following steps: -
a.) Capture large number of data packets using airodump-ng.

"airodump-ng --bssid[mac address] --channel --write[file name] interface"
b.) Analyze the packets which were captured using airocrack-ng.

"aircrack-ng [captured file]"

Monitor Mode [MAC address changer]:
Monitor mode is used by hackers to change its own mac address so that they can cover their tracks. This helps in increasing anonymity. Series of commands are used to do that.
a.) ifconfig [interface] down
b.) iwconfig [interface] mode monitor
c.) ifconfig [interface] up

These commands are used for linux based operating system. In python programing this can be achieved by using subprocess module.

ARP Spoofing: It is a man in the middle attack which is used to send broadcast messages to devices present in the network. The main ideology is to fool the victim and router. Hacker will tell the victim that he is router and it will tell the router that he is the victim. With this hacker will get in middle of victim and router.

a.) For router: “arpspoof -i[interface] -t[gateway IP] [hacker IP]”
b.) For victim: “arpspoof -i[interface] -t[client IP] [hacker IP]”

To let the packet pass through hacker machine, he needs to give permission for that. “echo 1 > proc/sys/net/ipv4/Ip-forward” following command should be executed in hacker machine.

Maintaining Access: In gaining access phase hacker will send malicious programs such as payloads and backdoors. This will make easier for hacker to invade victim machine in future. Malwares are designed to infiltrate and adversely effect computer system without owner’s consent.
Keylogger is a virus used to capture all the keystrokes made by victim. There are 2 variants of keylogger at present times. First one is a simple keylogger which will store the keystrokes in a text file on victim machine. Second one is a keylogger which will store the keystrokes and can directly send that to email of hacker. Second variant saves a lot of times for hacker.
Many times backdoors can be found in open ports and services they are running. For example if a service in running on some port and the version of service is outdated, then there are chances that it consist of loopholes which can be exploited by black hat hackers.
Ransomware are malware which will infect the database of particular organization and it will encrypt all the data present inside. The only person who can decrypt the data is hacker itself and he will decrypt the data only after achieving what he wanted.

Covering Tracks: In this phase hacker will try to hide its intrusion from victim machine. Use of increased anonymity helps in doing so. Anonymity can be achieved by changing mac address, using tor browser etc. Leaving things as they were before intrusion after achieving the goal.
Sometimes using post exploitation tools helps in increasing the time frame before malicious activity goes undetected.

6 CONCLUSION AND FUTURE SCOPE

We tried to keep this paper resourceful and touched many aspects of hacking. We tried to implement many theories into practical demonstration. In future more research will be done on this field since data is generated every second on different parts of world, and privacy is major issue in internet. More advanced technologies are yet to be invented to safeguard user’s interest. Better security protocols and network infrastructure is needed. Restriction should be made on dark web users.

ACKNOWLEDGMENT

We would also like to express our special thanks to Ms. Shruthy Govindan , Assistant Professor and Project Supervisor of SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for his insight and knowledge on the subject, who imbued us with the feeling to work assiduously.

We feel compelled to articulate our thankfulness to Dr. Jitendra Singh, and Dr. Rakesh Kumar Yadav, Project Coordinators, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for there enlightening dexterity which was truly a perennial source of inspiration.

We would like to express our hearty gratitude to respected Director, Dr. S. Vishwanathan, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, under whose unconditional support, we were able to work on our project work.

We would like to express our hearty gratitude to Dr. D. K. Sharma, Dean, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for his helpful guidance and support.

Also, we extend our sincere regards and thanks to Dr. R. P. Mahapatra, Head of the Department, Computer Science and Engineering, & Dean Admission, SRM Institute of Science and Technology, Delhi-NCR Campus, Modinagar, for his suggestions and motivation for completing this project.

We are also indebted to all the teaching and non-teaching staff members of our college for helping us directly or indirectly by all means throughout the course of our study and project work.

Finally, we take this opportunity to thank our parents, family members and friends for their moral support and help and extended thanks to our well-wishers.
.

REFERENCES

1. Interpol – Cyber Strategy Guide Book. (April-2021)
2. United Nations Office of Drug And Crime – Darknet Cybercrime Threats to Southeast Asia. (2020)
3. IEEE – penetration testing using ethical hacking (Rina Elizabeth Lopez de Jimenez Escuela de Computacion Itca-Fepade Santa Tecla, EI Salvador)
4. Kali Linux – WILEY PUBLICATION, Author – Gus Khawaja

5. Penetration Testing with Kali Linux by OFFENSIVE SECURITY
6. International Journal of Advanced Research In Engineering And Technology. (IJARET 2020)
7. A Survey of Ethical Hacking – American University of Beirut, Electrical And Computer Engineering Department. (MARCH-2021)
8. Offensive Security: Ethical Hacking Methodology On Web 1 Carrera de Ingeniería en Telecomunicaciones, Universidad Técnica del Norte, Av. 17 de Julio 5-21 y Gral. José María Córdova, 100105 Ibarra, Ecuador
9. Training network managers in ethical hacking techniques to manage resource starvation attacks: Kemal Hajdarevic, Indira Avdagic faculty of electrical engineering university of Sarajevo
10. Ethical Hacking: The security justification by Brian Smith Illinois university.
11. Scoping the ethical principles of cybersecurity fear appeals, by DUPUIS Marc and Renaud Karen
12. Proceedings of international ethical hacking conference 2018 by Chakraborty Mahuya, Satyajit Balas and Valentina Emilia.
13. Analysis to determine the scope and challenging responsibility of ethical hacking, by Vignesh and Rohini.
14. Scope and limitation of ethical hacking and information security. By M Mohan and R Sri Kumar