iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** VI **Month of publication:** June 2018

DOI: http://doi.org/10.22214/ijraset.2018.6261

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

Cyber Security and Ethical Hacking

P. Harika Reddy[1] Surapaneni Gopi Siva Sai Teja[2]
[1] *Student, Sreenidhi Institute Of Science and Technology, Hyderabad, India*

Abstract: Cyber Security and ethical hacking is the most emerging field in computer science. This paper gives vast information about what is ethical hacking, types and kinds of hackers in the present world .And phases of hacking by that what can a intruder answer.Footprinting methodologies and how to scan a target for finding the loopholes, how to gain access and maintain the access and also how to take measures to prevent from foot printing and scanning and clearing the tracks.

I. INTRODUCTION

In today's digital world, data rule. Cyber security has become a common term in recent years. Where many people spending a large amount of time in, exchanging information through media such as email and social media and performing banking operations and shopping online, it's not surprising that risks come with the digitalization of all your data. Cybercrime, Electronic Crime is where a computer or a mobile is the target of crime or is the means ratify to execute a crime. Cyber criminals are levering innovation at a stride which many target organizations and security hawker cannot possibly match. Most of these crimes are not new. Criminals simply overhaul different ways to undertake standard criminal activities such as fraud, theft, blackmail, and forgery, often involving the Internet. Secure trade secret, financial information, and your company's privilege is a compelling part of business strategy. Yet with the number of threats and the elegance of attacks increasing, it's a dreadful challenge. Companies that understand the value that security brings to the business also secure that they have a broad strategy in place and that they have the processes and procedures to back up their vision. The guiding principles for strategy are driven, in large part, by their data. Attaining vital resources and information in the network is the most challenging exploit for system trade. As business has wander to the digital world, criminals have, too. What has loom is a refined criminal ecosystem that has matured to the point that it functions much like any business management structure, quality control, and so on. While the hacking skills can be used for venomous purposes, this program provides you how to use the same hacking techniques to perform a white-hat, ethical hack, on your organization. You leave with the ability to significantly appraise and measure threats to information resources.

II. LITERATURE REVIEW

[10]Gary Hall - Erin Watson summarizes hacking is one of the most misunderstood cyber concepts. The majority of people think of hacking as something evil or illegal, but nothing could be farther from the truth. Indeed, hacking can be a real threat, but if you want to stop someone from hacking you, you must also learn how to hack.[12] Seth McKinnon gives abstract about methods and techniques such as penetration testing, Wi-Fi hacking and DOS attacks in order to provide a better understanding in how to hack and ultimately prevent your computer from being an easy target.[] Chuck East tom brings together up-to-the-minute coverage of all basic concepts, terminology, and issues, along with all the skills you need to get started in the field. Drawing on his extensive experience as a security instructor and consultant, East tom thoroughly covers core topics, such as vulnerability assessment, virus attacks, hacking, spyware, network defense, passwords, firewalls, VPNs, and intrusion detection. Computer Security Fundamentals, Second Edition is packed with tips and examples, all extensively updated for the state-of-the-art in both attacks and defense .This book will help you protect your systems and data and expand your career options [20].

III. ETHICAL HACKING

The noun "HACKER" refers to the person who finds weakness in the computer network for gaining the access. The verb "HACKING" describes modification in the technology for the offensive or the defensive purpose. The term "CRACKER" refers to person who uses his hacking skill for harmful purpose. The term "Ethical Hacker" refers to security professionals who apply their hacking skill for defensive purpose.

A. Types Of Hackers

There are three types of hackers

1) White Hat Hacker
2) Black Hat Hacker

3) Grey Hat Hacker

White hat hacker is one who does ethical hacking and writes the report for what he have done. Black hat hacker is one who does hacking for his own purpose.Grey hat hackers are the combination of both black hat and White hat hackers.

IV. KINDS OF HACKERS

A. Coders

Coders are the one who writes code. Coder come under grey hat because they write code for white hat hackers and black hat hackers

B. Admins

Admins manages the code. They comes under white hat hackers. Actually coders are great than admins because admin just manages the code written by the coder

C. Script Kiddies

They are the one who can read blogs make use of tips find in internet. They doesn't know anything they are like small kid searches everything in web every step. Script kiddies comes under black hat hackers

D. Hacktivist

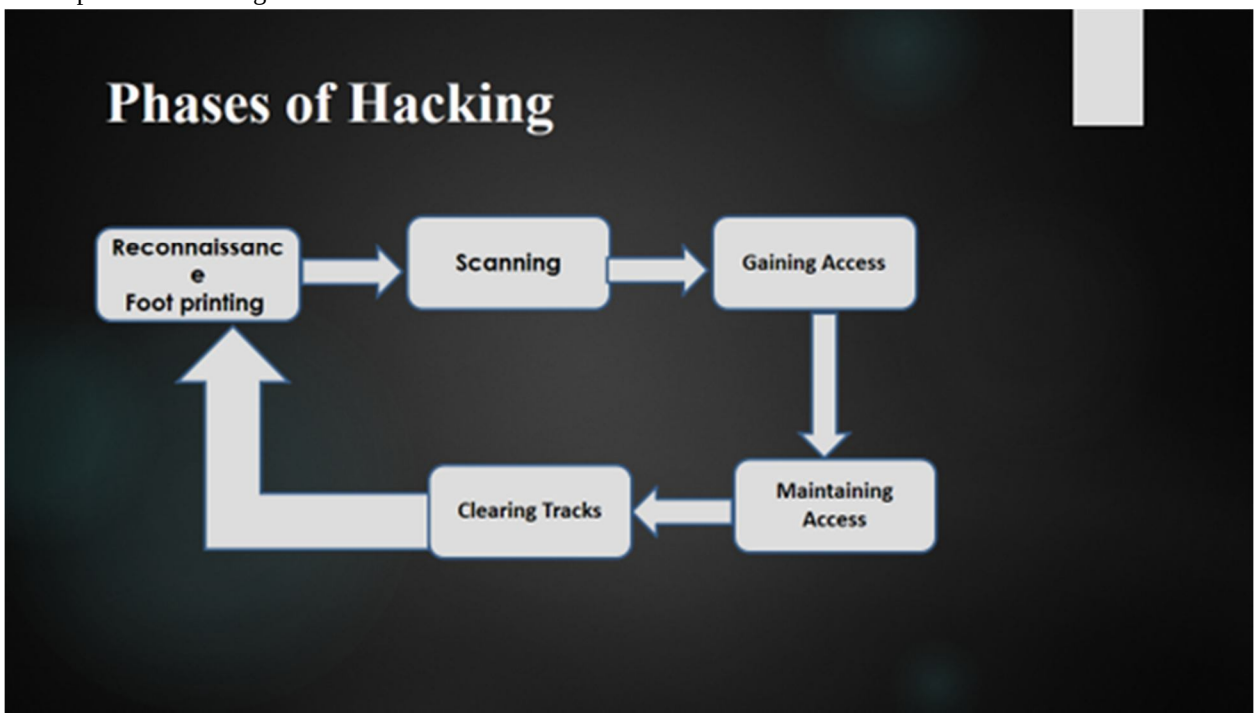
Hacktivist are the group of hackers coming for a cause. The cause may be good or bad. They come under black hat hackers.

E. Suicidal Hackers

They knows how to be secured and wanted to reveal his name and details after they are done with hacking. Suicidal hackers comes under black hat hackers.

V. PHASES OF HACKING

There are five phases in hacking.



Ethical Hackers try to answer

A. What can the outsider person see on target system? (Reconnaissance and scanning phase
B. What can the outsider person do with that information? (Gaining and maintaining access phase
C. Does anyone at the target notice the intruder's attempt or success? Reconnaissance and Covering Track phase)

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue VI, June 2018- Available at www.ijraset.com

VI. PHASE-1(FOOTPRINTING)

Foot printing is gathering information about the target as much as possible. We can gather information in many ways. Here are the methodologies for the foot printing.

A. Foot printing using Search Engines.

We can gather information about the target using the following search engines.
-> Google
-> Yahoo
-> Bing etc.

B. Email Foot Printing

To extract information from email header like sender and receiver mail address, timestamp, ip addresses and Sending unexciting mail to server.

C. Foot Printing Using Google

We use google dorks/google operators to find sensitive information and hidden urls

1) Site: (Google dorks
2) Inurl:, intext
3) Filetype:, intitle

D. DNS record

Connection between domain to server is DNS

1) A, AAAA
2) Cname, MX, SR
3) NS etc.

E. Whois

WHOIS query gives information such as creation, updation, expiry, dates of the domain, contact details of admin and names server information Who is (site)

F. Network Foot Printing

We get information like no of devices connected, host details, ip addresses, mac addresses etc. Tools used for network foot printing are:

1) angry ip scanne
2) Advanced ip scanner

G. Social engineering

Art of convincing a person to fall into the trap or to reveal confidential information. The ways to gather information are
Eavesdropping
Shoulder suffering
Dumpster diving etc.

H. Competitive Intelligence

The process of gathering information about target either online or offline
->Website/online database checking
-> Trademarks and patents
-> Press and newspaper releases
->Customers and vender interviews
->Social engineering employees etc.

VII. PHASE-II(SCANNING)

In this phase by doing the scanning of the target we can find the loop holes present in it.They are three scans.

A. Port Scan

Port scan used to find open ports, closed ports and filtered ports

B. Network Scan

Network scan used to find out the topologies of network.

C. Web Application Scan

Web application scan used to find out the vulnerabilities present in a website
Tools used for the scanning are:
Acunetix
Nmap
Nessus
Measures to protect from Scanning
By using firewalls and using packet filtering
By closing unwanted ports

VIII. PHASE-III(GAINING ACCESS)

Once done with the second phase that is scanning if any holes are present and found they are open we enter through that hole, this is gaining access. In this process vulnerabilities are located.

A. Vulnerability Testing

1) Directory traversa
2) Sql injection
3) Cross Site Scripting
4) Session hijacking
5) Cross Site Request ForgeryDenial of Service

IX. PHASE-IV(MAINTAINING ACCESS)

One the hacker gained the access into the system he will not leave any evidence. After gaining access, the hacker keep some backdoors to enter into the system when he needs access in this owned system in future.Metasploit is the tool in this process.

X. PHASE-V(CLEARING TRACKS)

Once we are able to gain and maintain the access we need to cover the tracks. This is the final stage of the hacking. In this goal is to erase all the things which we done in the above phases.

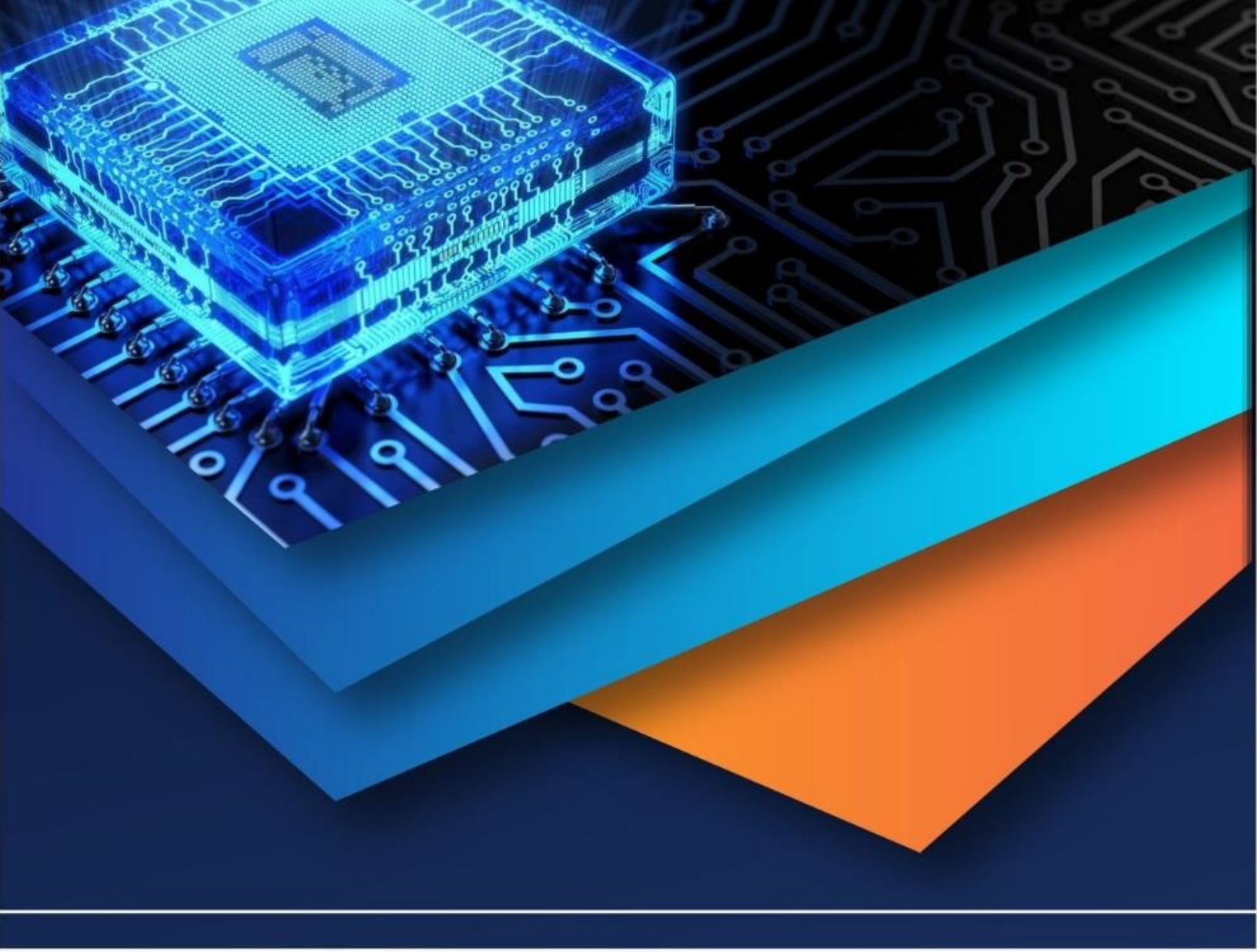
XI. CONCLUSION

This paper gives complete view about what is ethical hacking, difference between hacker, cracker and ethical hacker types and kinds of hackers and penetration testing. Discusses phases of hacking, methodologies of foot printing and scanning, finding vulnerabilities in a website using scanning, maintaining access and gaining access.

REFERENCES

[1] Asthana, N. C., and Priyamvada Asthana. Cyber Security, Cyber Attacks and Hacking. Pointer Publishers, 2013
[2] Hall, Gary, and Erin Watson. Hacking: Computer Hacking, Security Testing, Penetration Testing and Basic Security. CreateSpace Independent Publishing Platform, 2016
[3] Asthana, N. C., and Priyamvada Asthana. Cyber Security, Cyber Attacks and Hacking. Pointer Publishers, 2013
[4] Anto, Y. The Art of Hacking: Self Paced Training Kit for Cyber Security Professionals. LAP LAMBERT Academic Pub., 201
[5] Ethical Hacking & Cyber Security Course : A Complete Package." Udemy, 24 June 2018, www.udemy.com/ethical-hacking-cyber-security-course/.
[6] Cyber Security Standards." Wikipedia, Wikimedia Foundation, 19 June 2018, en.wikipedia.org/wiki/Cyber_security_standards.
[7] "What Is Cybersecurity? - Definition from WhatIs.com." SearchSecurity, TechTarget, searchsecurity.techtarget.com/definition/cybersecurity

[8] What Is Cyber Security?" Digital Guardian, 6 Apr. 2018, digitalguardian.com/blog/what-cyber-security.
[9] What Is Ethical Hacking and an Ethical Hacker?" Computer Hope, 27 June 2017, www.computerhope.com/jargon/e/ethihack.htm
[10] Mathew, Thomas. Ethical Hacking: Student Courseware. OSB Publisher, 2003.
[11] Jones, Don. "Ethical Hacking." Pluralsight, Pluralsight, 20 May 2015, www.pluralsight.com/blog/tutorials/learning-path-ethical-hacking.
[12] Holt, Thomas J., and Bernadette H. Schell. Hackers and Hacking: a Reference Handbook. ABC-CLIO, LLC, 2013
[13] TutorialsPoint. "Ethical Hacking & Cyber Security." Www.tutorialspoint.com, Tutorials Point, 10 Oct. 2017, www.tutorialspoint.com/ethical_hacking_and_cyber_security/index.asp.
[14] Ethical Hacking & Cyber Security Workshop." IHackers,ihackers.co.in/ethical-hacking-cyber-security-workshop/.
[15]]Sinha, Sanjib. Beginning Ethical Hacking with Python. Apress, 2017.
[16] Practical Cyber Security and Ethical Hacking." Fundraising and Development | UCSD Extension, extension.ucsd.edu/courses-and-programs/practical-cyber-security-and-ethical-hacking.
[17] Eckovation." Eckovation : Social Learning Platform, eckovation.com/course/ethical-hacking-and-cyber-security.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY