HACKING AND NETWORK SECURITY

J.MURALIDHARAN
RMD Engineering college
Department of Computer Science and Engineering
Kavaripettai-601206

ABSTRACT

HACKING –A vulnerable and also the almost brilliant task perform by an individual who are expert in programming and also in networking. Person who is totally immersed in computer technology and programming, and who likes to examine the code of programs to see how they work. Then uses his or her computer expertise for illicit purposes such as gaining access to computer systems without permission and tampering with programs and data. At that point, this individual would steal information and install backdoors, virus and Trojans. Hacker means cracker nowadays. Hack is nothing but Examine something very minutely, the rapid crafting of a new program or the making of changes to existing, usually complicated software**.**

Keywords: Hacking, Ethical Hacking, Attack types, hacks tools.

I.INTRODUCTION

But in the face of ethical hacking It is Legal. Permission is obtained from the target. Part of an overall security program. Identify vulnerabilities visible from Internet at particular point of time [1]. Ethical hackers possesses same skills, mindset and tools of a hacker but the attacks are done in a non destructive manner also Called – Attack & Penetration Testing. Before the penetration testing we want to do the following procedures: Identify the target system. Gathering Information on the target system. Finding a possible loophole in the target system. Exploiting this loophole using exploit code. Removing all traces from the log files and escaping without a trace.

Identify the target system Gathering Information on the target system. Finding a possible loophole in the target system. Exploiting this loophole using exploit code [2]. Removing all traces from the log files and escaping without a trace. Finding a possible loophole in the target system. Exploiting this loophole using exploit code. Removing all traces from the log files and escaping without a trace Ethical hackers possesses same skills, mindset and tools of a hacker but the attacks are done a Non-destructive manner also Called – Attack & Penetration Testing

II.HACKING

Hacking refers to an array of activities which are done to intrude someone else's personal information space so as to use it for malicious, unwanted purposes. Hacking is a term used to refer to activities aimed at exploiting security flaws to obtain critical information for gaining access to secured networks.

Boredom and drudgery are evil.

Hackers (and creative people in general) should never be bored or have to drudge at stupid repetitive work

Freedom is good Hackers are naturally anti-authoritarian.

Anyone who can give you orders can stop you from solving whatever problem you're being fascinated by Becoming a hacker will take intelligence, practice, dedication, and hard work.

III. BASIC HACKING SKILLS

Learn how to program.

This, of course, is the fundamental hacking skill. If you don't know any computer languages, you can't do hacking.

Get one of the open-source UNIX's and learn to use and run it

The single most important step any newbie can take towards acquiring hacker skills is to get a copy of Linux or one of the BSD-Unix's, install it on a personal machine, and run it.

Learn how to use the World Wide Web and write HTML.

To be worthwhile, your page must have *content* -- it must be interesting and/or useful to other hackers. When you start hacking the first thing you need to do is: to make sure the victim will not find out your real identity. So hide your IP by masking it or using a anonymous proxy server. This is only effective when the victim has no knowledge about computers and internet. Organizations like the F.B.I, C.I.A and such will find you in no time, so beware [3,4]. The best thing to do is using a dialup connection that has a variable IP address. Be smart, when you sign up for a internet dialup connection use a fake name and address. When hacking never leave traces of your hacking attempts, clear log files and make sure you are not monitored. So use a good firewall that keeps out retaliation hacking attempts of your victim.

IV.HOW IT IS POSSIBLE

A typical attacker works in the following manner: Identify the target system. Gathering Information on the target system. Finding a possible loophole in the target system exploiting this loophole using exploit code. Removing all traces from the log fi

A.DENAIL OF SERVICE

If an attacker is unsuccessful in gaining access, they may use readily available exploit code to disable a target as a last resort Techniques

- SYN flood
- ICMP techniques
- Identical SYN requests
- Overlapping fragment/offset bugs
- Out of bounds TCP options (OOB)
- DDoS

B.EXTERNAL HACKING

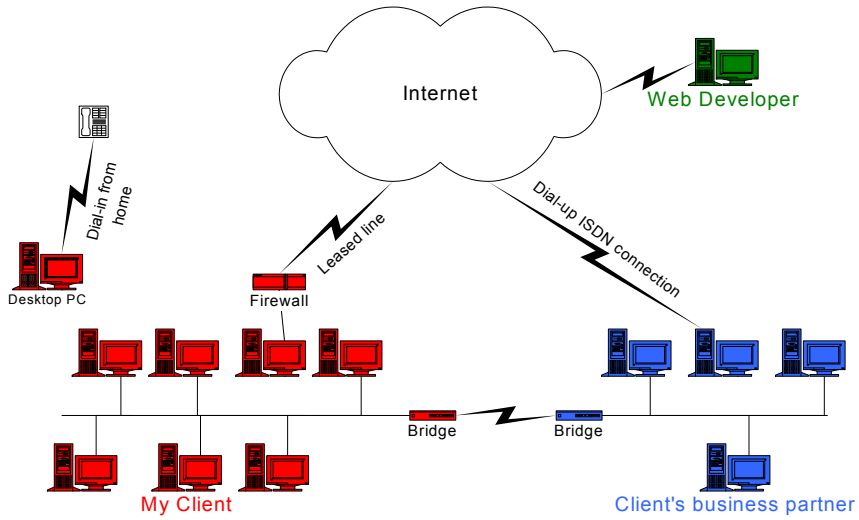


Fig 1: **EXTERNAL HACKING**

Collection of all discoveries made during evaluation. Specific advice on how to close the vulnerabilities. Tester's techniques never revealed. Delivered directly to an officer of the client organization in hard-copy form. Steps to be followed by clients in future.

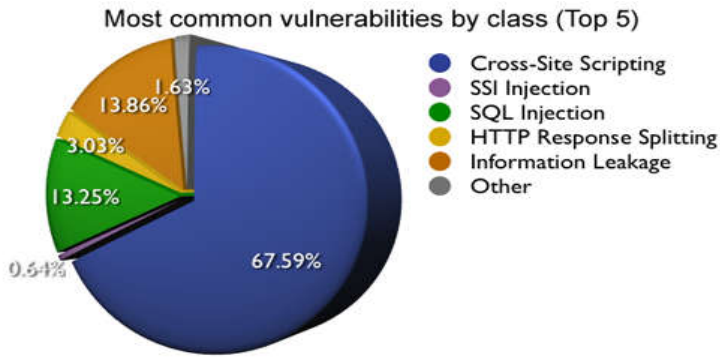
Although, it is impossible to stop clients from Port Scanning your network [5], however, it is advisable to take all possible measures against possible attackers. Some useful Anti-Port Scanning software available are: Scaled (A Unix based Port Scan Detector & Logger) Black ICE (A Windows based Port Scan Detector & Logger)

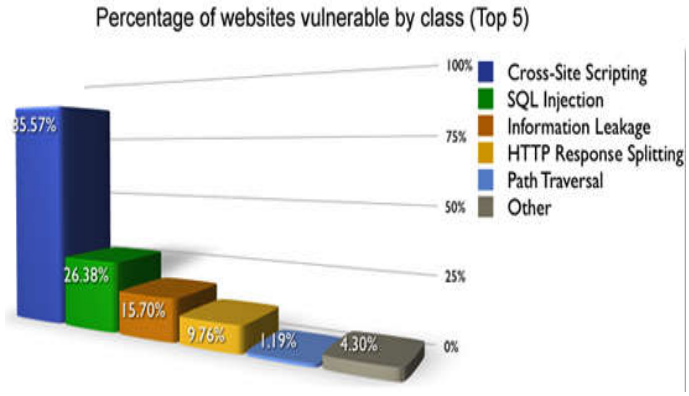
Snort: A packet sniffer cum IDS. Abacus Port sentry: Capable of Detecting both normal and stealth port scanning attempts. Other than the above tools, it is always advisable to disable as many services as possible. In other words, one should try to close as many ports as possible, without compromising on the services offered by that system.

C.FINAL REPORT

Collection of all discoveries made during evaluation Specific advice on how to close the vulnerabilities. Testers techniques never revealed. Delivered directly to an officer of the client organization in hard-copy form. Steps to be followed by clients in future.

V.NETWORK SECURITY





The Internet Control Message Protocol (ICMP) is the protocol used for reporting errors that might have occurred while transferring data packets over networks [6] Extremely Useful in Information Gathering. Originally, designed for network diagnosis and to find out as to what went wrong in the data communication.

Can be used to find out the following:

Host Detection
Operating System Information
Network Topography Information Below is sample output of a PING command executed on a Windows machine
C:\WINDOWS>ping www.yahoo.com Below some sample security codes will be available:

Pinging **www.yahoo-ht3.akadns.net** [69.147.96.15] with

32 bytes of data:

- Reply from 69.147.96.15 : bytes=32 time=163ms TTL=61
- Reply from 69.147.96.15 : bytes=32 time=185ms TTL=61
- Reply from 69.147.96.15 : bytes=32 time=153ms TTL=61
- Reply from 69.147.96.15 : bytes=32 time=129ms TTL=61

V I.ADVANTAGES

  - To make security stronger (Ethical Hacking)
  - Hack other systems secretly
  - Providing more jobs in security fields
- Easily economical state will be improved in an individual

VII.DISADVANTGES

- Just for fun
- Show off
- Steal important information
- Destroy enemy's computer network during the war

VIII.FUTURE SCOPE

- Phishing Method Brute Force Hack.
- Fake Login Hack. Cookie Steal Hack.
- Web Mail Hack
- Those are some of the already existed process. Through cloud hacking we can secure private functions in advanced hacking.

IX.CONCLUSION

As we are all living in the Silicon Valley hacking also plays vital role in software stream Even a coin has two sides also the hacking too. Grey hat hackers are mostly falls on ethical hacking which is legal and also permit table my paper has an innovative approach in order to hack safely in an unpredictable environment with safe keys .If this pear been practically successful all Indians will become professional hackers in Day today life within a year.

EXTERNAL REFERENCES

[1]" Engineering in Medicine and Biology Society",2008. EMBS 2008. 30th Annual International Conference of the IEEE

[2] Henry Markram, "The Blue Brain Project", NatureReviews Neuroscience 2006 February.

[3] Simulated brain closer to thought BBC News 22April 2009.

[4] ETHICAL HACKING Kaashiv infotech solutiondfrom pdf 2015

[5] HACKING from Kaashiv INFOTECH SOLUTIOND pdf 2016

[6] CCNA CISCO NETWORK SECURITY kaashiv infotech 2010