ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 2, pp: (183-189), Month: April-June 2014, Available at: www.researchpublish.com

HACKING METHODS, TECHNIQUES AND THEIR PREVENTION

R. Sushmitha [#1], D. Venkatasubramanian [#2], R.Shyam Sundar[#3]

Student[#1] Professor[#2] student[#3]
CSE Department, Saveetha School Of Engineering, Saveetha University, Thandalam , chennai ,India

Abstract: **Some of the problems with respect to computer security have received considerable academic attention in recent days in cyber security has become a top priority for many organizations. Two main categories of hackers have evolved: the Open Source and Free Software group and the Security Hackers group. This paper details more about the notable groups and individuals.**

Keywords: **Hacking, hacker, etiquette, ethics, groups of hacking, m'category' of hackers, methods of hacking, security, hacking tools.**

1. INTRODUCTION

Computer hacking means someone alters computer hardware or software such that it can change the original content. The people who hack computers are known as hackers. Hackers are the experts who had learnt about the computer and the working of the computer.

2. HACKER ETIQUETTE

Hacker Ethic may be a term that was 1st utilized in Hackers: Heroes of the pc Revolution written by Yankee journalist Steven Levy in 1984. The ideology behind hacker ethics came from the values of the hackers at the university computer science Laboratory. The key points square measure:

•"Access to computers - and something which could teach you one thing concerning the method the planet works -Should be unlimited and total. Invariably yield to the active Imperative!"

•"All data ought to be free."

•Mistrust authority- promotes decentralization."

• Hackers ought to be judged by their hacking, not imitative criteria like degrees, age, race, or position."

• "You will produce art and sweetness on a pc."

•"Computers will modification your life for the higher."

3. ETHICS

The Jargon File, a wordbook of hacker slang created in 1975 from multiple technical cultures, conjointly provides a definition of hacker ethic.

1. "The belief that information-sharing may be a powerful positive smart, which it's associate moral duty of hackers to share their experience by writing ASCII text file code and facilitating access to data and to computing resources where doable."

2. "The belief that system-cracking for fun and exploration is ethically OK as long because the cracker commits no thievery, vandalism, or breach of confidentiality." A lot of typically, hacker ethic "is that just about all hackers square

measure actively willing to share technical tricks, software, and probably computing resources with different hackers".

4. HACKING GROUPS

The two classes of hacker's area unit Open supply and free computer code cluster and therefore the second is security Hackers cluster.

4.1. OPEN SUPPLY AND FREE COMPUTER CODE HACKERS

Hackers UN agency see the look of the computer code as associate degree sort and that they build the program simply. This cluster was developed within the 1960's by educational hackers those area unit operating with minicomputers within the field of technology. It became a lot of what we all know because the free computer code and open supply movement in 1990's.The hackers people who belong to the open supply and free computer code class named as white hat hackers. Hackers beneath this cluster add the open and blow over their real name. Usually they appear down for security hackers and consult with them as kooky. Programmer's people who area unit operating within the educational culture can modify existing code or the resources to attain their finish goal. Most of the contributors belong to the present cluster. Example Linux creator LINUS TORVALDS and DENNIS RITCHIE and KEN THOMPSON creator of C programming. A number of the foremost common free computer code merchandise that exists area unit given below.

Free Software	Description
Linux	OS
Eclipse	Java based Integrated Development Environment
Mozilla	Internet browser
Firefox	Lightweight browser
Wireshark	Network protocol analyzer
Thunderbird	Redesign of Mozilla mail component
Openoffice	Complete office suite
My SQL	Relational database management system

4.2. SECURITY HACKERS

Security hacker's square measure the class of hackers prefers to be uncommunicative. Typically they use associate degree alias to hide their true identity. Hackers within the security hacking class square measure known as black hat hackers operating with unwell intensions. Some teams and people but might higher be classified as gray hat hackers. The cluster was at the start developed within the context of phreaking, the social group curious about the general public phone networks, throughout the 1960's and also the personal computer bulletin board system (BBS) scene of the 1980's.

5. HACKING METHODOLOGY

The method of hacking is worn out 5 phases. The phases are a unit.

- Information gathering
- Scanning and enumeration
- Gaining access
- Maintaining access
- Covering tracks

5.1. INFORMATION GATHERING

This part includes survey and foot printing. This part is preparation part that is employed to assemble the data the

maximum amount as potential past to AN attack. The offender tries to search out and exploit a ambiguity by distinguishing patterns of behavior of individuals or systems. Here non-intrusive ways area unit used for making a map of AN organization's network. The ways area unit,

- Target system
- Network design
- Application sort
- Operating system and version
- Server sorts
- Physical location

5.2. SCANNING AND ENUMERATION

During this part, the offender acknowledges target system's informatics address and determines whether or not a system is on the network and additionally they're accessible. additionally this part helps to spot the known security loopholes in keeping with system and repair version and defines a user account or system account to be used in hacking the target system. Most account rights will then be exaggerated to permit the account with a lot of access than it had been antecedently granted.

5.3. GAINING ACCESS

During this section of hacking, hackers exploit exposures exposed throughout the survey and scanning section. They may gain access through dissimilar path like,

- Direct access to a private laptop
- Local space network
- Internet

A common exposure includes stack primarily based buffer overflow, denial of service and hijacking session that has the most objective to realize the possession of the system. Once the system has been hacked, the system management is below the hacker and that they use the system as they need.

5.4. MAINTAINING ACCESS

Once gaining access, hackers keep the access for his or her future activities. They will even harden the system and shield their access with backdoors rootkits and Trojans to forestall different hackers. Once the hacker owns the system, they will use it as a base to launch further attacks within which the cooperated system is additionally referred to as zombies.

5.5. COVERING TRACKS

In this section hackers would take away all traces of the attack like log files, alarms to safeguard themselves. The purpose of this to avoid detection by protective personnel to continue exploitation the compromised system and take away proof of hacking to avoid action.

6. WEB APPLICATION TESTING

On-line services, net applications are developed and deployed with smallest attention given to security risks, leading to a shocking range of company sites that are at risk of hackers. Outstanding sites from variety of regulated industries together with money services, government, healthcare, and retail, are probed daily. The implications of a security breach are great: loss of revenues, harm to believability, legal liability, and loss of client trust. Software system most at risk of these styles of attacks includes:

•User interface code: This can be to supply the planning and feel of the location

•Web server: This supports the physical communication between the user's browser and therefore the net applications

•Frontend applications: This interfaces directly with the interface code, and backend systems

7. SECURITY PLAN

A Web Application Security method is enforced exploitation four key guidelines:

7.1. Understand

Perform security audits and defect testing throughout the appliance life cycle. Production applications are a clear 1st place to implement regular audits and analysis to see security and compliance risk to a corporation. At constant time, don't forget that the appliance development life cycle is that the piece of land for the defects that cause the risks. Playacting security testing throughout the appliance development life cycle at key points throughout the varied stages from development to QA to Staging can scale back prices and considerably scale back your on-line risk.

7.2. Communicate

When risks and security defects are known, it's imperative to induce the proper data to the proper neutral. Development has to perceive what these vulnerabilities and compliance exposures are in development terms. this suggests providing details around however the attack works and steerage on rectification. There are many smart sources each on-line and in security testing tools for developers. Similarly, QA should be ready to perform delta, trend and multivariate analysis on the protection defects similar to they are doing for performance and practicality flaws. Exploitation their existing strategies and metrics they, alongside Product Management, will properly priorities and monitor the defect rectification method further as accurately assess unleash political campaign. Finally, with the ever-increasing range and scope of state and internal laws and policies, groups from Security, Risk, Compliance, and analysis & Development have to be compelled to communicate and validate application risks against these terribly real business drivers.

7.3. Train

Guarantee correct coaching of developers. This doesn't essentially mean that with coaching the codes they write are going to be safer. However the a lot of developers perceive however net servers and browsers communicate and act, and therefore the protocols employed in web communications, the a lot of possible they're to create applications that aren't at risk of attacks.

7.4. Measure

For any method to achieve success there has to be criteria by that to live the successes or failures of the procedures enforced. Organizations use trending and defect rectification analysis metrics to spot areas and problems to focus on; there may well be a particular security defect sort that keeps cropping up which may then be known and prohibited through targeted education and coaching to acknowledge recurrent risks with a specific infrastructure product or seller. Ultimately, measurement and analyzing scan results can contribute to a discount in liability and risk led to by implementing an online application security set up.

8. HACKINGPROTECTION TECHNIQUES

In relevance numerous hacking activities, a number of the suggested protection techniques area unit

8.1. SECURITY INFRASTRUCTURE

One amongst the foremost common infrastructures for imposing info security is that the firewall, that aims at proscribing the access of incoming and departing traffic through configuration of rule sets.

8.2. INTRUSION DETECTION SYSTEM

It protects a network by grouping info from a spread of system and network supply, so analyzing the data for potential security issues. It provides time period observation and analysis of user and system activity. In general, there are a unit 2 styles of IDS, specifically Network Intrusion Detection System (NIDS) monitors multiple hosts by examining network traffic at the network boundaries and Host Intrusion Detection System (HIDS) will monitor one host by analyzing application logs, filing system modification like word file and access management lists.

8.3. CODE REVIEW

For any self-developed applications like internet applications, AN freelance code review on the programs ought to be

conducted severally from the appliance development so as to make sure no security flaw is disclosed from the codes that area unit visible to the general public, and proper error handling and input validation are implemented within the code.

8.4. SECURITY PATCHES

Several service suppliers, together with package vendors and package suppliers compromise with security patches once their weakness of the package or package was found. The installation of up-to-date protective patches is incredibly vital since these weaknesses area unit sometimes noted to the general public.

9. TOP TEN HACKING TOOLS

Commonly, a hacker knows the usage of tools. Some hacker writes their own tools. Here are the top TEN best hacking tools listed below:

- Nmap
- Wireshark
- Cain and abel
- Metasploit
- Burp suite
- Aircrack-ng
- Nessus
- THC hydra
- Hping3
- Putty

9.1. Nmap

This is often additionally referred to as because the Swiss knife of hacking. This is often largely employed in the foot printing section to scan the ports of the remote laptop for locating out ports is open.

9.2. Wireshark

This captures all networks traffic prying a network adapter. It analyze for juicy information like usernames and passwords. To perform network troubleshooting network directors is employed.

9.3. Cain and abel

This could be wont to crack window watchword. It additionally performs man within the middle attacks, capture network passwords etc.

9.4. Metasploit

It's a large info of exploits. It's the final word hacking tool which will enable to "hack" a laptop. It's best to use metasploit below Linux.

9.5. Burp suite

Burpsuite may be a net proxy tool that is employed to check the net application security. This could brute force any login type in a very browser. One will edit or modify information before causation to the server. This tool is below windows and Linux environments

9.6. Aircrack-ng

Aircrack-ng may be a set of tools wont to crack wireless fidelity passwords. This additionally comes below Linux setting.

9.7. Nessus

This is often a comprehensive automatic weakness scanner. One ought to provide information processing address as input

and it'll scan that address to seek out the weakness therein system.

9.8. THC Hydra

This is often a quick watchword cracker tool. It cracks passwords of remote systems through the network. It will crack passwords of the many protocols as well as ftp, http, etc. there's Associate in Nursing choice to provide a lexicon file it contains attainable passwords. It comes below Linux setting.

9.9. Hping3

Hping3 sends custom ICMP, UDP or communications protocol packets so displays any replies. This tool is extremely helpful once attempting to trace route/ping/probe hosts that have firewalls obstruction traditional pings. This comes below windows and Linux.

9.10. Putty

It's not a hacking computer code by itself; it's an awfully great tool for hacker. It's a shopper for SSH and telnet, which may be won't to connect with remote computers. The use putty after you needs to attach to your return machine from your Windows laptop. It may also be wont to perform SSH tunneling to bypass firewalls.

10. WIRELESS NETWORK SEARCHING

Even though the wrongdoer collects tidy quantity of data concerning a wireless network through sniffing, while not revealing his wireless presence in the slightest degree, there are a unit items that will still be missing. The wrongdoer then sends unnaturally created packets to a target that trigger helpful responses. This activity is understood as searching or active scanning.

The target might realize that it's being probed, it'd even be a honey pot target fastidiously created to lure the wrongdoer. The wrongdoer would try and minimize this risk.

10.1 Detection of SSID

Detection of SSID is often potential by merely sniffing Beacon frames as describe during a previous section.

If Beacon transmission is disabled, and therefore the wrongdoer doesn't want to with patience sit up for a voluntary Associate Request to seem from a legitimate station that already features a correct SSID, or Probe Requests from legitimate stations, he can resort to searching by injecting a research Request frame that contains a spoofed supply raincoat address. The Probe Response frame from the APs can contain, within the clear, the SSID and alternative data kind of like that within the Beacon frames were they enabled. The wrongdoer sniffs these Probe Responses and extracts the SSIDs.

Some models of APs have associate degree choice to disable responding to Probe Requests that don't contain the right SSID. During this case, the wrongdoer determines a station related to the AP, and sends the station a cast Disassociation frame wherever the supply raincoat address is about thereto of the AP. The station can send an Association Request that exposes the SSID.

10.2. Detection of APs and stations

Every AP could be a station, so SSIDs, raincoat addresses area unit gathered as delineated on top of. Certain bits within the frames establish that the frame is from associate degree AP. If we tend to assume that WEP is either disabled or cracked, the wrongdoer may collect the informatics addresses of the AP and therefore the stations.

10.3. Detection of searching

Detection of searching is feasible. The frames that associate degree wrongdoer injects may be detected by the intrusion detection systems (IDS) of hardened wireless local area network. There's GPS-enabled instrumentation which will establish the physical coordinates of a wireless device through that the probe frames area unit being transmitted.

REFERENCES

[1] http://www.gangte.net/2013/09/top-10-best-hacking-tools.html

[2] http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm

[3] http://ito.hkbu.edu.hk/eng/publication/newsletter/is_newsletter/professional/Issue_11_HackingProtection/JUCC%20Newsletter-IT-11%20HackingProtection.pdf

[4] http://www.cse.wustl.edu/~jain/cse571-07/ftp/hacking_orgs.pdf

[5] http://www.nebhe.org/info/pdf/tdbank_breakfast/Fraud_Prevention_and_Detection.pdf

[6] http://www.cs.berkeley.edu/~bh/hacker.html

[7] http://whatishacking.org/

[8] http://stackoverflow.com/questions/449421/what-is-the-legal-definition-of-hacking

[9] http://www4.ncsu.edu/~kksivara/sfwr4c03/projects/YamKhadduri-Project.pdf

[10] http://www.iss.net/security_center/advice/Underground/Hacking/default.htm