ETHICAL HACKING AND CYBER SECURITY

P.Dinesh
Master of Computer Applications
Sree Ramakrishna Engineering College
Coimbatore, Tamilnadu.
dineshjoy@rediff.com

ABSTRACT—

"Ethical Hacking" which attempts to proactively Increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. Ethical hackers may beta test unreleased software, stress test released software, and scan networks of computers for vulnerabilities. Ethical hacking can be defined as the practice of hacking without no malicious intention, rather evaluate target system with a hackers perspectives. Hacking is a process to bypass the security mechanisms of an information system or network. In common usage, hacker is a generic term for a computer criminal. Hacking is an unprivileged usage of computer and network resources. The term "hacker" originally meant a very gifted programmer. In recent years though, with easier access to multiple systems, it now has negative implications.

Keywords —Ethical standards, Penetration, Exploits, Philosophy of Hacking, Vulnerability.

I. INTRODUCTION

This paper aims at putting forward the basic concept of ethical hacking and difference between a hacker and cracker, root philosophy of hacking, the approach that differs in the thought processes of hackers and programmers and reveals secretes of hacking under Linux domain. As we all are aware that data and Computer Communications are hot subjects and getting hotter every day. We see it when we turn on our television, cordless or cell phone, or the computer when we get our email. It has provided us lightning speed conveniences that our grandparents could only imagine when they went to the movies to see Buck Rogers or Dick Tracy. However, what they could not have imagined was the "dark side" that comes along with these technological advances. The rapid growth of the Internet has brought many constructive and valued

Solutions for our lives such as e-commerce, electronic communication, and new areas for research and information sharing. However, like many other technological advancements, there is also an issue of growing number of criminal hackers. Businesses are scared of computer experts who will penetrate into their web server and change their logo, steal their private emails or credit card numbers, or put in software that will quietly transmit their organization's data to somebody in another country. Hackers are commonly known as bad or terrible people in our society. They are also known as crackers or black hat guys. The reason is that majority of computer users are somehow victim of malicious activities by other users who are outstandingly experts in computers. The important thing to understand is not all the hackers are bad as some people are doing penetration of a system in the limits of ethical standards to understand the vulnerabilities in their system or their clients system, also called white hat hackers. Hence the term ―Ethical Standards actually refers to the consideration if the person performing hacking has a valid intention or not. If he or she just wants to access the target system with an illegal intention and misuse the data explored, can be termed as the cracker whereas the ethical hacker always intends for test that yields the vulnerabilities of the system as the output through the process of hacking. In ethical hacking, for example, a network administrator might use the encrypted password file and a "cracking" program to determine who has not picked a good password. The need is to train our computer science students with ethical hacking techniques, so that they can fight against criminal hackers. Because ethical hackers believe that one can best protect systems by probing them while causing no damage and subsequently fixing the vulnerabilities found.

II. ETHICAL HACKING

Today more and more software's are developing and people are getting more and more options in their present software's. But many are not aware that they are being hacked without their knowledge. One reaction to this state of affairs is a behavior termed "ETHICAL HACKING" which attempts to proactively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. A good ethical hacker should know the methodology chosen by the hacker like reconnaissance, host or target scanning, gaining access, maintaining access and clearing tracks.

The state of security on the Internet is bad and becoming worse. One reaction to this state of affairs is behavior termed "Ethical Hacking" which attempts to proactively increase security protection by identifying and patching known security vulnerabilities on systems owned by other parties. Ethical hackers may beta test unreleased software, stress test released software, and scan networks of computers for vulnerabilities. Previous work has emphasized ethical hacking as an altruistic behavior but we find ethical hackers act rationally, in self-interest, to secure systems that are within their own community (sometimes for pay)-networked systems are only as secure as the weakest system within perimeter defenses.

For ethical hacking we should know about the various tools and methods that can be used by a black hat hacker apart from the methodology used by them. From the point of view of the user one should know at least some of these because some hackers make use of those who are not aware of the various hacking methods to hack into a system. Also when thinking from the point of view of the developer, he also should be aware of these since he should be able to close holes in his software even with the usage of the various tools.

With the growth of the Internet, computer security has become a major concern for businesses and governments. They want to be able to take advantage of the Internet for electronic commerce, advertising, information distribution and access, and other pursuits, but they are worried about the possibility of being "hacked." At the same time, the potential customers of these services are worried about maintaining control of personal information that varies from credit card numbers to social security numbers and home addresses.

In their search for a way to approach the problem, organizations came to realize that one of the best ways to evaluate the intruder threat to their interests would be to have independent computer security professionals attempt to break into their computer systems. This scheme is similar to having independent auditors come into an organization to verify its bookkeeping records. In the case of computer security, these "tiger teams" or "ethical hackers" would employ the same tools and techniques as the intruders, but they would neither damage the target systems nor steal information. Instead, they would evaluate the target systems' security and report back to the owners with the vulnerabilities they found and instructions for how to remedy them.

This method of evaluating the security of a system has been in use from the early days of computers. In one early ethical hack, the United States Air Force conducted a "security evaluation" of the Multics operating systems for "potential use as a two-level (secret/top secret) system."Their evaluation found that while Multics was "significantly better than other conventional systems," it also had "vulnerabilities in hardware security, software security, and procedural security" that could be uncovered with "a relatively low level of effort." The authors performed their tests under a guideline of realism, so that their results would accurately represent the kinds of access that an intruder could potentially achieve. They performed tests that were simple information-gathering exercises, as well as other tests that were outright attacks upon the system that might damage its integrity. Clearly, their audience wanted to know both results. There are several other now unclassified reports that describe ethical hacking activities within the U.S. military.

A) HACKER

A hacker is a person intensely interested in the arcane and recondite workings of any computer operating system. Hackers are most often programmers. As such, hackers obtain advanced knowledge of operating systems and programming languages. They might discover holes within systems and the reasons for such holes. Hackers constantly seek further knowledge; freely share what they have discovered, and never intentionally damage data.

B) CRACKER

A cracker is one who breaks into or otherwise violates the system integrity of remote machines with malicious intent. Having gained unauthorized access, crackers destroy vital data; deny legitimate users service, or cause problems for their targets. Crackers can easily be identified because their actions are malicious.

III. Ethical Hackers Activity

A) Remote Network

This test simulates the intruder launching an attack across the Internet. The primary defenses that must be defeated here are border firewalls, filtering routers, and Web servers.

B) Remote Dial-Up Network

This test simulates the intruder launching an attack against the client's modem pools. The primary defenses that must be defeated here are user authentication schemes. These kinds of tests should be coordinated with the local telephone company.

C) Local Network

This test simulates an employee or other authorized person who has a legal connection to the organization's network. The primary defenses that must be defeated here are intranet firewalls, internal Web servers, server security measures, and e-mail systems.

D) Stolen Laptop Computer

In this test, the laptop computer of a key employee, such as an upper-level manager or strategist, is taken by the client without warning and given to the ethical hackers. They examine the computer for passwords stored in dial-up software, corporate information assets, personnel information, and the like. Since many busy users will store their passwords on their machine, it is common for the ethical hackers to be able to use this laptop computer to dial into the corporate intranet with the owner's full privileges.

E) Social Engineering

This test evaluates the target organization's staff as to whether it would leak information to someone. A typical example of this would be an intruder calling the organization's computer help line and asking for the external telephone numbers of the modem pool. Defending against this kind of attack is the hardest, because people and personalities are involved.

F) Physical Entry

This test acts out a physical penetration of the organization's building. Special arrangements must be made for this, since security guards or police could become involved if the ethical hackers fail to avoid detection. Once inside the building, it is important that the tester not be detected. Such a document could be found by digging through trash cans before the ethical hack or by casually picking up a document from a trash can or desk once the tester is inside.

G) The Havij

Havij is an automated SQL Injection tool that helps penetration testers to find and exploit SQL Injection vulnerabilities on a web page.

It can take advantage of a vulnerable web application. By using this software user can perform back-end database fingerprint, retrieve DBMS users and password hashes, dump tables and columns, fetching data from the database, running SQL statements and even accessing the underlying file system and executing commands on the operating system.

The power of Havij that makes it different from similar tools is its injection methods. The success rate is more than 95% at injection vulnerable targets using Havij.

The user friendly GUI (Graphical User Interface) of Havij and automated settings and detections makes it easy to use for everyone even amateur users.

H) The Hide IP

Just like my IP address, your IP address is unique and assigned to your computer by your ISP. Hackers may use your IP address to track you back to your computer. But if you are able to hide your IP address, your online security and privacy is greatly enhanced. Each time you connect to the Internet with Hotspot shield, you get a new US IP address to mask your actual IP address and surf the Internet anonymously--completely protected from hackers and snoopers.

Hotspot Shield VPN essentially changes your IP address by replacing it with an IP address belonging to one of our servers. Thus, when you get a free US IP address, you can browse the Internet as a user from the United States or other countries of your choosing with our premium Elite service. Therefore, hackers are not able to locate you or your computer. Unlike your ISP, Hotspot Shield VPN does not track and does not record your web activities.

I) CCproxy

CCProxy is easy-to-use and powerful proxy server software. CCProxy can support broadband, DSL, dial-up, optical fiber, satellite, ISDN and DDN connections, it helps you build your own proxy server and share Internet connection within the LAN efficiently and easily. CC Proxy Server can act as an HTTP, mail, FTP, SOCKS, news, telnet and HTTPS proxy server. It features powerful account management functions, including Internet access control, bandwidth control, Internet web filtering, content filtering and time control. It also provides web caching, online access monitoring, access logging and bandwidth usage statistics functions.

As Window proxy server software, CCProxy is compatible with Windows 7/8, Windows Server 2008, Windows Server 2003, Windows XP and Vista. Many people use CCProxy for Windows internet sharing such as Windows XP Internet sharing, Win 7/8 Internet sharing and so on. CCProxy can act as web proxy software, which enables you to browse web pages, download files and send and receive e-mails via web browsers such as IE, Chrome, and Firefox etc. The web caching function of web proxy server can increase the Internet surfing speed. CCProxy provides powerful management functions including several ways to control the Internet access on the LAN. They are IP address, IP range, MAC address, User Name/Password and group. It can also merge with Windows Active Directory.

J) The Zone Alarm Security

ZoneAlarm is a personal firewall software application originally developed by Zone Labs. It includes an inbound intrusion detection system, as well as the ability to control which programs can create outbound connections.

In ZoneAlarm, program access is controlled by way of "zones", into which all network connections are divided. The "trusted zone" generally includes the user's local area network and can share resources such as files and printers, while the "Internet zone" includes everything not in the trusted zone. The user can specify which "permissions" to give to a program before it attempts to access the Internet or, alternatively, ZoneAlarm will ask the user to give the program permission on its first access attempt.

THE KEY LOGGER

The term ‘key logger’ it is neutral, and the word describes the program’s function. Most sources define a key logger as a software program designed to secretly monitor and log all keystrokes. This definition is not altogether correct, since a key logger doesn’t have to be software – it can also be a device. Key logging devices are much rarer than key logging software, but it is important to keep their existence in mind when thinking about information security.

Legitimate programs may have a key logging function which can be used to call certain program functions using “hotkeys,” or to toggle between keyboard layouts (e.g. Keyboard Ninja). There is a lot of legitimate software which is designed to allow administrators to track what employees do throughout the day, or to allow users to track the activity of third parties on their computers. However, the ethical boundary between justified monitoring and espionage is a fine line. Legitimate software is often used deliberately to steal confidential user information such as passwords.

Most modern key loggers are considered to be legitimate software or hardware and are sold on the open market. Developers and vendors offer a long list of cases in which it would be legal and appropriate to use key loggers, including:

•Parental control: parents can track what their children do on the Internet, and can opt to be notified if there are any attempts to access websites containing adult or otherwise inappropriate content;

•Jealous spouses or partners can use a key logger to track the actions of their better half on the Internet if they suspect them of "virtual cheating";

•Company security: tracking the use of computers for non-work-related purposes, or the use of workstations after hours;

•Company security: using key loggers to track the input of key words and phrases associated with commercial information which could damage the company (materially or otherwise) if disclosed;

•Other security (e.g. law enforcement): using key logger records to analyze and track incidents linked to the use of personal computers;

However, the justifications listed above are more subjective than objective; the situations can all be resolved using other methods. Additionally, any legitimate key logging program can still be used with malicious or criminal intent. Today, key loggers are mainly used to steal user data relating to various online payment systems, and virus writers are constantly writing new key logger Trojans for this very purpose.

Furthermore, many key loggers hide themselves in the system (i.e. they have rootkit functionality), which makes them fully-fledged Trojan programs.

As such programs are extensively used by cyber criminals, detecting them is a priority for antivirus companies. Kaspersky Lab's malware classification system has a dedicated category for malicious programs with key logging functionality: Trojan-Spy. Trojan-Spy programs, as the name suggests, track user activity, save the information to the user's hard disk and then forward it to the author or 'master' of the Trojan. The information collected includes keystrokes and screen-shots, used in the theft of banking data to support online fraud.

KEYLOGGERS ARE A THREAD

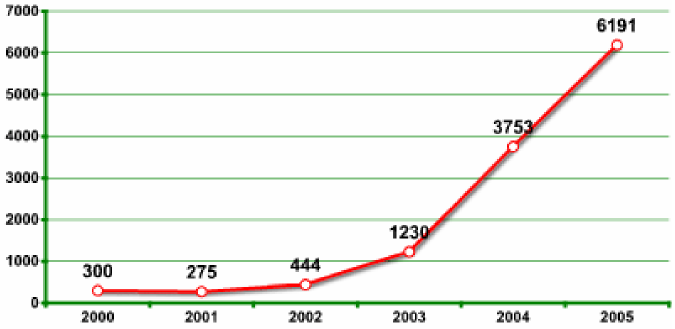
Unlike other types of malicious program, key loggers present no threat to the system itself. Nevertheless, they can pose a serious threat to users, as they can be used to intercept passwords and other confidential information entered via the keyboard. As a result, cyber criminals can get PIN codes and account numbers for e-payment systems, passwords to online gaming accounts, email addresses, user names, email passwords etc.

Once a cyber criminal has got hold of confidential user data, s/he can easily transfer money from the user's account or access the user's online gaming account. Unfortunately access to confidential data can sometimes have consequences which are far more serious than an individual's loss of a few dollars. Key loggers can be used as tools in both industrial and political espionage, accessing data which may include proprietary commercial information and classified government material which could compromise the security of commercial and state-owned organizations (for example, by stealing private encryption keys).

Key loggers, phishing and social engineering (see 'Computers, Networks and Theft') are currently the main methods being used in cyber fraud. Users who are aware of security issues can easily protect themselves against phishing by ignoring phishing emails and by not entering any personal information on suspicious websites. It is more difficult, however, for users to combat key loggers; the only possible method is to use an appropriate security solution, as it's usually impossible for a user to tell that a key logger has been installed on his/ her machine.

According to Christine Hoepers, the manager of Brazil's Computer Emergency Response Team, which works under the aegis of the country's Internet Steering Committee, key loggers have pushed phishing out of first place as the most-used method in the theft of confidential information. What's more, key loggers are becoming more sophisticated – they track websites visited by the user and only log keystrokes entered on websites of particular interest to the cyber criminal.

In recent years, we have seen a considerable increase in the number of different kinds of malicious programs which have key logging functionality. No Internet user is immune to cyber criminals, no matter where in the world s/he is located and no matter what organization s/he works for.



Increased Use Of Key loggers

FIREWALL

A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Firewall Configuration

Firewalls can be configured by adding one or more filters based on several conditions as mentioned below

IP Addresses

In any case if an IP address outside the network is said to be unfavorable, then it is possible to set filter to block all the traffic to and from that IP address. For example, if a certain IP address is found to be making too many connections to a server, the administrator may decide to block traffic from this IP using the firewall.

Domain Names

Since it is difficult to remember the IP addresses, it is an easier and smarter way to configure the firewalls by adding filters based on domain names. By setting up a domain filter, a company may decide to block all access to certain domain names, or may provide access only to a list of selected domain names.

Ports/Protocols

Every service running on a server is made available to the Internet using numbered ports, one for each service. In simple words, ports can be compared to virtual doors of the server through which services are made available. For example, if a server is running a Web (HTTP) service then it will be typically available on port 80. In order to avail this service, the client needs to connect to the server via port 80. Similarly different services such as Telnet (Port 23), FTP (port 21) and SMTP (port 25) services may be running on the server. If the services are intended for the public, they are usually kept open. Otherwise they are blocked using the firewall so as to prevent intruders from using the open ports for making unauthorized connections.

Specific Words Or Phrases

A firewall can be configured to filter one or more specific words or phrases so that, both the incoming and outgoing packets are scanned for the words in the filter. For example, you may set up a firewall rule to filter any packet that contains an offensive term or a phrase that you may decide to block from entering or leaving your network.

Hardware vs. Software firewall

Hardware firewalls provide higher level of security and hence preferred for servers where security has the top most priority whereas, the software firewalls are less expensive and are most preferred in-home computers and laptops. Hardware firewalls usually come as an in-built unit of a router and provide maximum security as it filters each packet in the hardware level itself even before it manages to enter your computer. A good example is the Linksys Cable/DSL router.

SQL INJECTION

SQL Injection is one the common Web application vulnerability that allows an attacker to inject malicious SQL command through Parameter or any Input box that is connected to Website Database. In SQL Injection an attacker finds (SQLi) vulnerability and Inject Malicious code through various techniques and Hack the website Database this is called SQL Injection attack Exploiting DB (Database) and also SQL Injection Vulnerability Exploitation. Using SQL Injection attack method an attacker can get complete DB of website - User ID and Password can be exploded, an attacker can also shut down My SQL Server. An attacker can modify content of website & bypass login.

SQL Injection is a type of web application security vulnerability in which an attacker is able to submit a database SQL command which is executed by a web application, exposing the back-end database. A SQL Injection attack can occur when a web application utilizes user-supplied data without proper validation or encoding as part of a command or query. The specially crafted user data tricks the application into executing unintended commands or changing data. SQL Injection allows an attacker to create, read, update, alter, or delete data stored in the back-end database. In its most common form, a SQL Injection attack gives access to sensitive information such as social security numbers, credit card number or other financial data. According to Vera code's State of Software Security Report SQL Injection is one of the most prevalent types of web application security vulnerability.

Key Concepts Of A Sql Injection Attack

SQL injection is a software vulnerability that occurs when data entered by users is sent to the SQL interpreter as a part of an SQL query

Attackers provide specially crafted input data to the SQL interpreter and trick the interpreter to execute unintended commands.

Attackers utilize this vulnerability by providing specially crafted input data to the SQL interpreter in such a manner that the interpreter is not able to distinguish between the intended commands and the attacker's specially crafted data.

The interpreter is tricked into executing unintended commands. A SQL Injection attack exploits security vulnerabilities at the database layer. By exploiting the SQL injection flaw, attackers can create, read, modify, or delete sensitive data.

The Most Prevalent Type Of Application Security Vulnerability

With over 20% of all web vulnerabilities being attributed to SQL Injection, this is the 2nd most common software vulnerability and having the ability to find and prevent SQL injection should be top of mind for web developers and security personnel. In general, a SQL Injection attack exploits a web application which does not properly validate or encode user-supplied input and then uses that input as part of a query or command against a back-end database.

An attacker using SQL Injection may enter "some data or 1=1". If the web application does not properly validate or encode the user-supplied data and sends it directly to the database, the reply to the query will expose all ids in the database since the condition "1=1" is always true. This is a basic example, but it illustrates the importance of sanitizing user-supplied data before using it in a query or command.

Sql Dork

```
inurl:adminlogin.aspx
inurl:admin/index.php
inurl:administrator.php
inurl:administrator.asp
inurl:login.asp
inurl:login.aspx
```

THE CLICKJACKING

Click jacking attack allows to perform an action on victim website, Mostly Facebook and Twitter accounts are targetable. When an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top level page. Thus, the attacker is "hijacking" clicks meant for their page and routing them to other another page, most likely owned by another application, domain, or both. Click jacking is a term first introduced by Jeremiah Grossman and Robert Hansen in 2008 to describe a technique whereby an attacker tricks a user into performing certain actions on a website by hiding clickable elements inside an invisible iframe.

Using a similar technique, keystrokes can also be hijacked. With a carefully crafted combination of style sheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker. At present this attack mostly uses on social network websites like Face book and twitter, Because this attack is used by convinced victim for click on the link and Social Network website might be very useful for attack on victim.

The Phishing

The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is bogus and set up only to steal the user’s information. Phishing scams are not limited to the internet. Some phishers use the telephone to make requests for information. If you get a call from your banking institution asking for personal information, hang up and call your bank directly.

Dns Hijacking

Unauthorized modification of a DNS server or change of DNS address that directs users attempting to access a web page to a different web page that looks the same, but contains extra content such as advertisements, is a competitor page, a malware page, or third-party search page.DNS hijacking is also now being done by some of the large ISPs such as Comcast as a method to linking users to their own search pages when they visit a webpage that no longer exists. Many claim this is to improve the users experience; however, this can also be another great source of extra revenue since they control the site and get paid off any advertisements. Currently all countries in the world have no laws against an ISP doing this to its users.

Brute Force

A password and cryptography attack that does not attempt to decrypt any information, but continue to try a list of different passwords, words, or letters. For example, a simple brute-force attack may have a dictionary of all words or commonly used passwords and cycle through those words until it gains access to the account. A more complex brute-force attack involves trying every key combination in an effort to find the correct password that will unlock the encryption. Due to the number of possible combinations of letters, numbers and symbols, a brute force attack can take a long time to complete. The higher the type of encryption used (64-bit, 128-bit or 256-bit encryption), the longer it can take.

Although a brute-force attack may be able to gain access to an account eventually, these attacks can take several hours, days, months, and even years to run. The amount of time it takes to complete these attacks is dependent on the complexity of the password, the strength of the encryption, how well the attacker knows the target, and the strength of the computer(s) being used to conduct the attack.

To help prevent dictionary brute-force attacks many systems will only allow a user to make a mistake in entering their username or password three or four times. If the user exceeds these attempts, the system will either lock them out of the system or prevent any future attempts for a set amount of time.

Brute Force was a game originally developed and released for the PC in 2000 and later released for the Xbox gaming console in 2003 by Microsoft Game Studios. Brute Force was a third-person shooter and consisted of multiple characters, each with their own strengths and capabilities. The game was set in the year 2340, and the object was to find several other characters who were loyal to the Confederation. These other characters became part of the Brute Force team, which fought against aliens, outcasts and mercenaries. From day one, the game was very popular, breaking several Xbox sales records, as well as beating out sales of the game Halo.

Hacking In Linux Operating Systems

In the last decade the open source movement has been a vital source of innovation affecting software development .However, open source community practices have provoked a Debate on software quality namely, is open source software‘s quality better than that of its closed source counterpart? Studies have attempted to correlate metrics with software performance or validate that metrics can actually predict software systems ‘fault proneness.

Open Source Software

Where you can define closed-source software as a product created using traditional software development methods, the definition of open source software isn‘t always straightforward. This is because a software product can take at least three paths to become open source. For example, a collaborating open source community developed the Linux kernel; an individual created PGP (Pretty Good Privacy) and the Mozilla browser were

Originally developed as proprietary software. One implication of this is that any conclusions about

Linux might not hold true for all open source products. But being an initiative taker, open source

Communities make society Linux strong system software. A hacker always needs to figure out the vulnerabilities in the victim system.

A) Local Access Control in Linux Environment

From a Physical Security (PHYSSEC) perspective, problems do not really begin until attackers have their hands on a machine. Having suitable access controls to prevent direct access and policies in place to prevent social engineering will help ensure that attackers are kept at a safe distance. Linux is a robust OS, but it is still vulnerable to hardware dangers that may lead to damage on its physical drives or power losses that may cause data corruption. Therefore, in addition to access controls, server rooms should include the following items to ensure integrity and availability and provide protections from power outages, power anomalies, floods, and so on.

Console Access

Stealing data using a Bootable Linux CD:

1. Reboot the system and configure it to boot from the CD-ROM.
2. Boot into the bootable Linux distro.
3. Open a root command shell.
4. Create a mount point by typing mkdir mountpoint, which will create a directory called mount point.
5. This is where the file system will be mounted.
6. Determine the type of hard disks (SCSI or IDE) on the system. [sda, sdb, sdc, and so on for SCSI, & hda, db,

Hdc, and so on for IDE] to determine the disk type, type fdisk –l or look through the output of the dmesg command.

7. Determine the partition on the disk to be mounted. Partitions on the disk are represented as sda1, sda2, sda2, and so on.
8. Identifying the correct partition that contains the /etc/shadow file (always the root ?/? partition). It is usually one of the first three partitions.
9. Type mount /dev/sda# mountpoint, where /dev/sda# is your root partition (sda1, sda2, sda3,…), and mountpoint is the directory you created.
10. Change to the /etc directory on your root partition by typing cd mountpoint/ etc
11. Use your favorite text editor (such as vi) to pen the etc/shadow file for editing.
12. Scroll down to the line containing the root's information, which looks something

Like: root: qDlrwz/E8RSKw:13659:0:99999:7: 13. Delete everything between the first and second colons, so the line, resembles this one: root:: 13659:0:99999:7:::

14. Save the file and exit you editor.
15. Type cd to return to the home directory.
16. Type umount mountpoint to unmount the target file system.
17. Type reboot to reboot the system and remove the bootable Linux distribution CD from the drive.
18. Now the system can be accessed as root with no password (or the known password).

IV CONCLUSION

Testing is an essential part of any data security program. If corrective action is taken and there is proper distribution of the lesson learned, then an ethical hack can reduce the potential exposure of the company to criminal hackers. The effort, however, must be done in a manner that does not expose the company to unnecessary liability. It is important to understand factors such as what data is exposed, what techniques will be employed, identifying the applicable legal obligations, and the implications of who will conduct the test and what will be done with the results. With a sufficient amount of analysis and preparation, risks can be addressed without compromising the efficacy of the testing, while preserving the mission of the information security program. Information security and legal functions can work together to create a process that is the most effective for the organization. In this case, an ounce of prevention may not only be worth a pound of cure, but also millions of dollars of avoidable liability risk.

REFERENCES

1. Packet Sniffing: A Brief Introduction DECEMBER 2002/JANUARY 2003 0278-6648/02/$17.00 © 2002 IEEE
2. PERVASIVE computing published by the IEEE CS n 1536-1268/08/$25.00 © 2008 IEEE
3. Teaching Students to Hack: Ethical Implications in Teaching Students to hack at university level
4. What Hackers Learn that the Rest of Us Don ‘t ‖ , THE IEEE COMPUTER SOCIETY,1540-7993/07/$25.00 © 2007 IEEE.
5. Ethical Hacking: The Security Justification Redux by Bryan Smith WilliamYurcikDavid Doss Illinois State University, 0-7803-7824-0/02/%10.00 62002 IEEE.
6. Network Viruses: Their Working Principles and Marriages with Hacking Programs by Yanjun Zuo and Brajendra Panda Computer Science & Computer Engineering Department University of Arkansas, ISBN 0-7803-7808-3/03/$17.00 0 2003 IEEE.
7. Hacking Exposed in Linux 3rd Edition by ISECOMM Tata McGrawHill Publication
8. Linux 101 Hacks: Practical Foundation to built strong foundation in Linux by Ramesh Natarajan.
9. John Cherllo, “Hack Attacks Testing”.
10. Peter Gregory,” Computer Viruses for Dummies”
11. Stuart McClure, Joel Scambray and George Kurtz, “Hacking exposed: network security secrets & solutions”, Fifth Edition.
12. Mark Ludwig ,“The Giant Black Book of Computer Virus”