How many hits does a search for the term 'Hacker' in Google reply with?

183,000,000
Welcome to DEFCON®, the Largest Underground Hacking Convention in ...

Information about the largest annual hacker convention in the US, including past speeches, video, archives, and updates on the next upcoming show as well as ...

www.defcon.org/
Kevin Mitnick  
January 21, 1995  
Compromised, DEC, IBM, HP, Motorola, PacBell, NEC, ...

Chen Ing-Hau, 24, Taiwan  
Arrested September 15, 2000  
CIH (Chernobyl) Virus

Jeffrey Lee Parson, 18, USA  
Arrested August 29, 2003  
Blaster Worm ('B' variants only), DDoS

Sven Jaschan, 18, Germany  
Arrested May 7, 2004  
NetSky (Sasser) Worm
Atilla Ekici, 21, Turkey
Arrested August 25, 2005
Operating Mytob and Zotob botnets

Farid Essebar, 18, Morocco
Arrested August 25, 2005
Mytob and Zotob (Bozori) Worms

Jeanson James Ancheta, 24, USA
Arrested November 3, 2005
Rxbot zombie networks for hire (spam and DDoS)
DDoS attacks bookmakers in October 2003

Extortion ($3 million gross)

Nine arrested on July 20 and 21, 2004

In October 2006, three were sent to prison

The two gang leaders and masterminds are still at large

On the Wanted List of the Federal Security Service (FSB) of the Russian Federation

Maria Zarubina and Timur Arutchev
• London branch of Japan’s Sumitomo Mitsui Bank
• Worked with insiders through Aharon Abu-Hamra, a 35-year-old Tel Aviv resident
• Injected a Trojan to gather credentials to a transfer system
• Attempted to transfer £220 million into accounts he controlled around the world
• £13.9 million to his own business account

Yaron Bolondi, 32, Israel
Arrested March 16, 2005
ALBERT GONZALEZ - SEGVEC, SOUPNAZI, J4GUAR

- Indicted on Aug 17, 2009
- Stole 130,000,000 credit card numbers
- Worked out of Miami - his one flaw
- Worked as an international organized cybercrime group
  - 3 in the Ukraine
    - Including Maksik who earned of $11m between 2004-2006
  - 2 in China
  - 1 from Belarus
  - 1 from Estonia
  - 1 from unknown location that goes by “Delperiao”
Lone Ranger  
Friends  
Criminal Gangs  
Criminal Organizations

CYBER CRIME TRENDS

<table>
<thead>
<tr>
<th>Year Range</th>
<th>Victim Loss</th>
<th>Criminal Gains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Before 2000</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>2000 - 2003</td>
<td>$200,000</td>
<td>$600,000</td>
</tr>
<tr>
<td>2003 - 2005</td>
<td>$800,000</td>
<td>$1,200,000</td>
</tr>
<tr>
<td>2005 to Present</td>
<td>$1,000,000</td>
<td>$12,000,000</td>
</tr>
</tbody>
</table>
C2C: MALWARE/PHISHING KIT - “ARMS SUPPLIERS”

- Criminal to Criminal - C2C
- Selling malware for "research only"
- Manuals, translation
- Support / User forums
- Language-specific
- Bargains on mutation engines and packers
- Referrals to hosting companies
- Generally not illegal
- Operate in countries that shield them from civil actions
- Makes it easy to enter the cybercrime market
# C2C - EXPLOIT - “INTELLIGENCE DEALERS”

![WabiSabi Labi Marketplace](image)

### Current Bids

<table>
<thead>
<tr>
<th>Code</th>
<th>Time to Live</th>
<th>Title</th>
<th>System</th>
<th>Offer Type</th>
<th>Last Bid</th>
</tr>
</thead>
<tbody>
<tr>
<td>ZD-00000102</td>
<td>0d 15h 17m</td>
<td>SAP MaxDB</td>
<td>Linux</td>
<td>Auction</td>
<td>0 bids</td>
</tr>
<tr>
<td>ZD-00000140</td>
<td>0d 15h 17m</td>
<td>VanDyke V8Thil</td>
<td>Windows 2000</td>
<td>Auction</td>
<td>50000</td>
</tr>
<tr>
<td>ZD-00000144</td>
<td>0d 15h 17m</td>
<td>Norvell</td>
<td>Windows XP</td>
<td>Auction</td>
<td>5,000</td>
</tr>
<tr>
<td>ZD-00000133</td>
<td>0d 15h 17m</td>
<td>IBM</td>
<td>Windows XP</td>
<td>Auction</td>
<td>5,000</td>
</tr>
<tr>
<td>ZD-00000130</td>
<td>1d 15h 17m</td>
<td>Micros-world Anti-Virus</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000142</td>
<td>12d 15h 17m</td>
<td>Novell GroupWise</td>
<td>Web application</td>
<td>Auction</td>
<td>1,000</td>
</tr>
<tr>
<td>ZD-00000139</td>
<td>12d 15h 17m</td>
<td>Novell Collivery</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000138</td>
<td>12d 15h 17m</td>
<td>Novell OpenOffice</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000111</td>
<td>12d 15h 17m</td>
<td>Samba</td>
<td>Windows 2000</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000072</td>
<td>12d 15h 17m</td>
<td>DWSQLPro</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000083</td>
<td>12d 15h 17m</td>
<td>ClientX</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000085</td>
<td>12d 15h 17m</td>
<td>Vwrd Solutions BOCTFBrau</td>
<td>Windows XP</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000063</td>
<td>12d 15h 17m</td>
<td>MySQLigra</td>
<td>Web application</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000140</td>
<td>13d 15h 17m</td>
<td>RealNetworks Web Server</td>
<td>Linux</td>
<td>Auction</td>
<td>0</td>
</tr>
<tr>
<td>ZD-00000117</td>
<td>13d 15h 17m</td>
<td>MaxCalibre</td>
<td>Windows 2000</td>
<td>Auction</td>
<td>0</td>
</tr>
</tbody>
</table>
C2C: BOT MANAGEMENT- "TURN KEY WEAPONS SYSTEMS"

- 76service, Nuklus Team
- Botnet Dashboards
TYPES OF HACKER ATTACK

• Active Attacks
  • Denial of Service
  • Breaking into a site
    • Intelligence Gathering
    • Resource Usage
    • Deception

• Passive Attacks
  • Sniffing
    • Passwords
    • Network Traffic
    • Sensitive Information
  • Information Gathering
NETWORK HACKING
VARIOUS TYPES OF ATTACKS

• There are an endless number of attacks, which a system administrator has to protect his system from. However, the most common ones are:
  • Denial of Services attacks (DOS Attacks)
  • Threat from Sniffing and Key Logging
  • Trojan Attacks
  • IP Spoofing
  • Buffer Overflows
  • All other types of Attacks
• Definition:
  • An attacker alters his identity so that some one thinks he is some one else
  • Email, User ID, IP Address, ...
  • Attacker exploits trust relation between user and networked machines to gain access to machines

• Types of Spoofing:
  • IP Spoofing:
  • Email Spoofing
  • Web Spoofing
IP SPOOFING - FLYING-BLIND ATTACK

• Definition: Attacker uses IP address of another computer to acquire information or gain access

  Spoofed Address
  10.10.20.30

  Replies sent back to 10.10.20.30

  John
  10.10.5.5

  From Address: 10.10.20.30
  To Address: 10.10.5.5

  Attacker
  10.10.50.50

  Attacker changes his own IP address to spoofed address
  Attacker can send messages to a machine masquerading as spoofed machine
  Attacker can not receive messages from that machine
IP SPOOFING - SOURCE ROUTING

• Definition: Attacker spoofs the address of another machine and inserts itself between the attacked machine and the spoofed machine to intercept replies

Attacker intercepts packets as they go to 10.10.20.30

Spoofed Address
10.10.20.30

From Address: 10.10.20.30
To Address: 10.10.5.5

Replies sent back to 10.10.20.30

Attacker
10.10.50.50

John
10.10.5.5

• The path a packet may change can vary over time
• To ensure that he stays in the loop the attacker uses source routing to ensure that the packet passes through certain nodes on the network
EMAIL SPOOFING

• Definition:
  • Attacker sends messages masquerading as someone else
  • What can be the repercussions?

• Types of Email Spoofing:
  • Create an account with similar email address
    • Sanjaygoel@yahoo.com: A message from this account can perplex the students
  • Modify a mail client
    • Attacker can put in any return address he wants to in the mail he sends
  • Telnet to port 25
    • Most mail servers use port 25 for SMTP. Attacker logs on to this port and composes a message for the user.
WEB SPOOFING

• Basic
  • Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com

• Man-in-the-Middle Attack
  • Attacker acts as a proxy between the web server and the client
  • Attacker has to compromise the router or a node through which the relevant traffic flows

• URL Rewriting
  • Attacker redirects web traffic to another site that is controlled by the attacker
  • Attacker writes his own web site address before the legitimate link

• Tracking State
  • When a user logs on to a site a persistent authentication is maintained
  • This authentication can be stolen for masquerading as the user
SESSION HIJACKING

• Definition:
  • Process of taking over an existing active session

• Modus Operandi:
  • User makes a connection to the server by authenticating using his user ID and password.
  • After the users authenticate, they have access to the server as long as the session lasts.
  • Hacker takes the user offline by denial of service
  • Hacker gains access to the user by impersonating the user
SESSION HIJACKING

• Attacker can
  • monitor the session
  • periodically inject commands into session
  • launch passive and active attacks from the session

Bob telnets to Server
Bob authenticates to Server
Bob
Server
Attacker
Die!
Hi! I am Bob
DENIAL OF SERVICE (DOS) ATTACK

• Definition:
  • Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it

• Types:
  • Crashing the system or network
    • Send the victim data or packets which will cause system to crash or reboot
  • Exhausting the resources by flooding the system or network with information
    • Since all resources are exhausted others are denied access to the resources
  • Distributed DOS attacks are coordinated denial of service attacks involving several people and/or machines to launch attacks
DENIAL OF SERVICE (DOS) ATTACK

• Types:
  • Ping of Death
  • SSPing
  • Land
  • Smurf
  • SYN Flood
  • CPU Hog
  • Win Nuke
  • RPC Locator
  • Jolt2
  • Bubonic
  • Microsoft Incomplete TCP/IP Packet Vulnerability
  • HP Openview Node Manager SNMP DOS Vulnerability
  • Netscreen Firewall DOS Vulnerability
  • Checkpoint Firewall DOS Vulnerability
BUFFER OVERFLOW ATTACKS

- This attack takes advantage of the way in which information is stored by computer programs.
- An attacker tries to store more information on the stack than the size of the buffer.
- How does it work?

<table>
<thead>
<tr>
<th>Bottom of Memory</th>
<th>Normal Stack</th>
<th>Fill Direction</th>
<th>Top of Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer 2</td>
<td></td>
<td></td>
<td>Local Variable 2</td>
</tr>
<tr>
<td>Buffer 1</td>
<td></td>
<td></td>
<td>Local Variable 1</td>
</tr>
<tr>
<td>Return Pointer</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function Call</td>
<td></td>
<td></td>
<td>Arguments</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bottom of Memory</th>
<th>Smashed Stack</th>
<th>Fill Direction</th>
<th>Top of Memory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buffer 2</td>
<td></td>
<td>Buffer 1 Space</td>
<td>Overwritten</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return Pointer</td>
<td></td>
</tr>
<tr>
<td>Machine Code:</td>
<td></td>
<td></td>
<td>Overwritten</td>
</tr>
<tr>
<td>execve(/bin/sh)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>New Pointer to</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exec Code</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Function Call</td>
<td></td>
<td></td>
<td>Arguments</td>
</tr>
<tr>
<td>Arguments</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
• Programs which do not have a rigorous memory check in the code are vulnerable to this attack
• Simple weaknesses can be exploited
  • If memory allocated for name is 50 characters, someone can break the system by sending a fictitious name of more than 50 characters
• Can be used for espionage, denial of service or compromising the integrity of the data

• Examples
  • NetMeeting Buffer Overflow
  • Outlook Buffer Overflow
  • AOL Instant Messenger Buffer Overflow
  • SQL Server 2000 Extended Stored Procedure Buffer Overflow
PASSWORD ATTACKS

• A hacker can exploit a weak passwords & uncontrolled network modems easily

• Steps
  • Hacker gets the phone number of a company
  • Hacker runs war dialer program
    • If original number is 555-5532 he runs all numbers in the 555-55xx range
    • When modem answers he records the phone number of modem
  • Hacker now needs a user id and password to enter company network
    • Companies often have default accounts e.g. temp, anonymous with no password
    • Often the root account uses company name as the password
    • For strong passwords password cracking techniques exist
PASSWORD SECURITY

- Password hashed and stored
  - Salt added to randomize password & stored on system
- Password attacks launched to crack encrypted password

![Diagram of password security process](image)
PASSWORD ATTACKS - TYPES

• Dictionary Attack
  • Hacker tries all words in dictionary to crack password
  • 70% of the people use dictionary words as passwords

• Brute Force Attack
  • Try all permutations of the letters & symbols in the alphabet

• Hybrid Attack
  • Words from dictionary and their variations used in attack

• Social Engineering
  • People write passwords in different places
  • People disclose passwords naively to others

• Shoulder Surfing
  • Hackers slyly watch over peoples shoulders to steal passwords

• Dumpster Diving
  • People dump their trash papers in garbage which may contain information to crack passwords
DENIAL OF SERVICES (DOS) ATTACKS

• DOS Attacks are aimed at denying valid, legitimate Internet and Network users access to the services offered by the target system

• In other words, a DOS attack is one in which you clog up so much memory on the target system that it cannot serve legitimate users

• There are numerous types of Denial of Services Attacks or DOS Attacks
DOS ATTACKS: PING OF DEATH ATTACK

• The maximum packet size allowed to be transmitted by TCP\IP on a network is 65,536 bytes.

• In the Ping of Death Attack, a packet having a size greater than this maximum size allowed by TCP\IP, is sent to the target system.

• As soon as the target system receives a packet exceeding the allowable size, then it crashes, reboots or hangs.

• This attack can easily be executed by the ‘ping’ command as follows:
  • ping -l 65540 hostname
DOS ATTACKS: SMURF ATTACKS

• In SMURF Attacks, a huge number of Ping Requests are sent to the Target system, using Spoofed IP Addresses from within the target network

• Due to infinite loops thus generated and due to the large number of Ping Requests, the target system will crash, restart or hang up
THREATS FROM SNIFFERS AND KEY LOGGERS

• Sniffers: capture all data packets being sent across the network in the raw form.
  • Commonly Used for:
    • Traffic Monitoring
    • Network Trouble shooting
    • Gathering Information on Attacker.
    • For stealing company Secrets and sensitive data.

• Commonly Available Sniffers
  • tcpdump
  • Ethereal
  • Dsniff
THREATS FROM SNIFFERS: WORKING & COUNTERMEASURES

• Working
  • Sniffers work along with the NIC, capturing all data packets in range of the compromised system.

• Countermeasures
  • Switch to Switching Networks. (Only the packets meant for that particular host reach the NIC)
  • Use Encryption Standards like SSL, SSH, IPSec
THREATS FROM KEY LOGGERS

• Key loggers: Record all keystrokes made on that system and store them in a log file, which can later automatically be emailed to the attacker

• Countermeasures
  • Periodic Detection practices should be made mandatory
  • A Typical Key Logger automatically loads itself into the memory, each time the computer boots
  • Thus, the start up script of the Key Logger should be removed
TROJAN ATTACKS

• Trojans: act as a RAT or Remote Administration Tool, which allow remote control and remote access to the attacker
  • Working:
    • The Server Part of the Trojan is installed on the target system through trickery or disguise
    • This server part listens on a predefined port for connections
    • The attacker connects to this Server Part using the Client part of the Trojan on the predefined port number
    • Once this is done, the attacker has complete control over the target system
TROJAN ATTACKS: DETECTION AND COUNTERMEASURES

• Detection & Countermeasures
  • Port Scan your own system regularly
  • If you find a irregular port open, on which you usually do not have a service running, then your system might have a Trojan installed
  • One can remove a Trojan using any normal Anti-Virus Software
INTERNET APPLICATION SECURITY
INTERNET APPLICATION HACKING
STATISTICS

• WHID (Web Hacking Incident Database) annual report for 2007 67% percent of the attacks in 2007 were "for profit" motivated. And it targeted the Web-Applications

• Acunetix, a leading vendor of web application security solutions, revealed that on average 70% of websites are at serious and immediate risk of being hacked. Every 1500 lines of code has one security vulnerability. (IBM LABS)

• 3 out of 4 websites are Vulnerable to attack. (Gartner Report)

• Most popular attacks are against web server (incident.org)
WEB APPLICATION ARE THREE-TIER APPLICATION

- Three-tier application
OVERVIEW OF INTERNET SECURITY
GENERAL HACKING METHODS

• A typical attacker works in the following manner:
  • Identify the target system
  • Gathering Information on the target system
  • Finding a possible loophole in the target system
  • Exploiting this loophole using exploit code
  • Removing all traces from the log files and escaping without a trace
FUNDAMENTAL METHODOLOGY TO DO ANY WEB-APPLICATION ASSESSMENT

• Foot printing  
  • Discovery of Web application
• Profiling
• Getting Real Attack Points
• Exploit the system
• Finding the defend mechanism and approach for them
WHY VULNERABLE?

- Poor Web Application coding
- Insecure deployment of web application
- Insufficient input validation
- No web traffic filtering
- Web application attributes are not guarded well. For example Query String
WEB APPLICATION SECURITY CONSORTIUM (WASC) STATISTICS
VULNERABILITY

Percentage of websites vulnerable by class (Top 5)

- Cross-Site Scripting: 35.57%
- SQL Injection: 26.38%
- Information Leakage: 15.70%
- HTTP Response Splitting: 9.76%
- Path Traversal: 4.30%
- Other: 1.19%

0% 100% 25% 50% 75% 100%
CLASSES OF ATTACKS

• Authentication
  • The Authentication section covers attacks that target a web site's method of validating the identity of a user, service or application

• Authorization
  • The Authorization section covers attacks that target a web site's method of determining if a user, service, or application has the necessary permissions to perform a requested action

• Client-side Attacks
  • The Client-side Attacks section focuses on the abuse or exploitation of a web site's users

• Command Execution
  • The Command Execution section covers attacks designed to execute remote commands on the web site. All web sites utilize user-supplied input to fulfill requests.

• Logical Attacks
  • The Logical Attacks section focuses on the abuse or exploitation of a web application's logic flow
ATTACK TECHNIQUES
(HACKING TECHNIQUES)

• **Brute Force**
  A Brute Force attack is an automated process of trial and error used to guess a person's username, password, credit-card number or cryptographic key

• **Cross-site Scripting**
  Cross-site Scripting (XSS) is an attack technique that forces a web site to echo attacker-supplied executable code, which loads in a user's browser

• **SQL Injection**
  SQL Injection is an attack technique used to exploit web sites that construct SQL statements from user-supplied input

• **XPath Injection**
  XPath Injection is an attack technique used to exploit web sites that construct XPath queries from user-supplied input
HI, WHAT ARE YOU DOING?

SECURE BROWSING

INTERESTING

BUT THE COMPUTER IS SWITCHED OFF

AS I'VE SAID: SECURE BROWSING

SECURE BROWSING
THANKS FOR YOUR ATTENTION!

• Prof. Claudio Cilli, CISA, CISM CRISC, CGEIT
• Università degli Studi di Roma "La Sapienza"
• http://dsi.uniroma1.it/~cilli
• https://www.linkedin.com/in/claudiocilli/
• claudio.cilli@uniroma1.it