Trust in, and value from, information systems

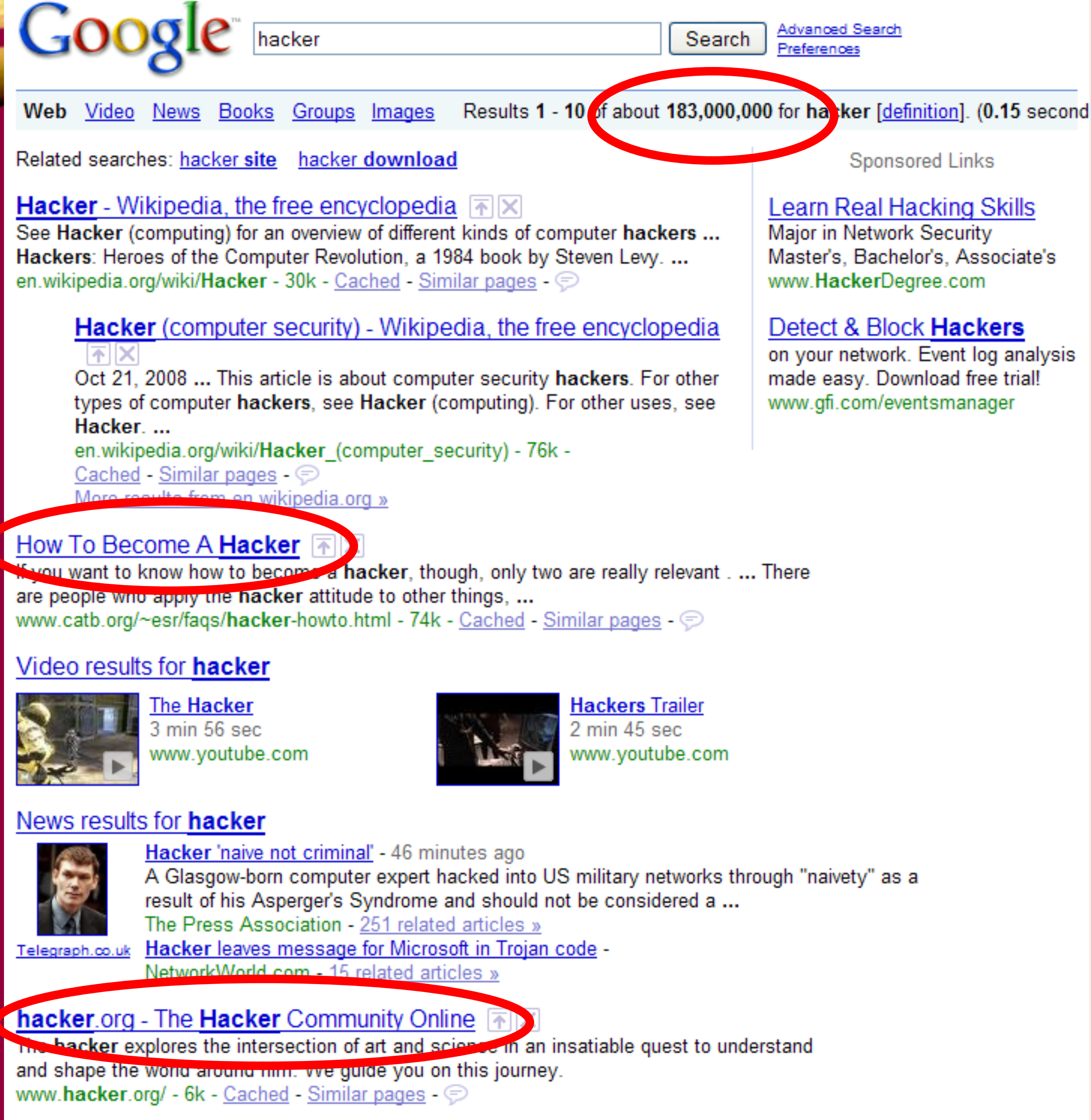
Trust in, and value from, information systems

TAXONOMY OF ATTACKS

Prof. Ing. Claudio CILLI, CISA, CISM, CRISC, CGEIT
cilli@di.uniroma1.it
http://dsi.uniroma1.it/~cilli

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

183,000,000



Results **1** - **10** of about **183,000,000** for **hacker** [definition]. (**0.15** second

Related searches: hacker **site** hacker **download**

Sponsored Links

Hacker - Wikipedia, the free encyclopedia
See **Hacker** (computing) for an overview of different kinds of computer **hackers** ... **Hackers**: Heroes of the Computer Revolution, a 1984 book by Steven Levy. ...
en.wikipedia.org/wiki/**Hacker** - 30k - Cached - Similar pages -

Hacker (computer security) - Wikipedia, the free encyclopedia
Oct 21, 2008 ... This article is about computer security **hackers**. For other types of computer **hackers**, see **Hacker** (computing). For other uses, see **Hacker**. ...
en.wikipedia.org/wiki/**Hacker**_(computer_security) - 76k - Cached - Similar pages -
More results from en.wikipedia.org »

How To Become A **Hacker**
If you want to know how to become a **hacker**, though, only two are really relevant . ... There are people who apply the **hacker** attitude to other things, ...
www.catb.org/~esr/faqs/**hacker**-howto.html - 74k - Cached - Similar pages -

Video results for **hacker**

The **Hacker**
3 min 56 sec
www.youtube.com

Hackers Trailer
2 min 45 sec
www.youtube.com

News results for **hacker**

Hacker 'naive not criminal' - 46 minutes ago
A Glasgow-born computer expert hacked into US military networks through "naivety" as a result of his Asperger's Syndrome and should not be considered a ...
The Press Association - 251 related articles »
Telegraph.co.uk

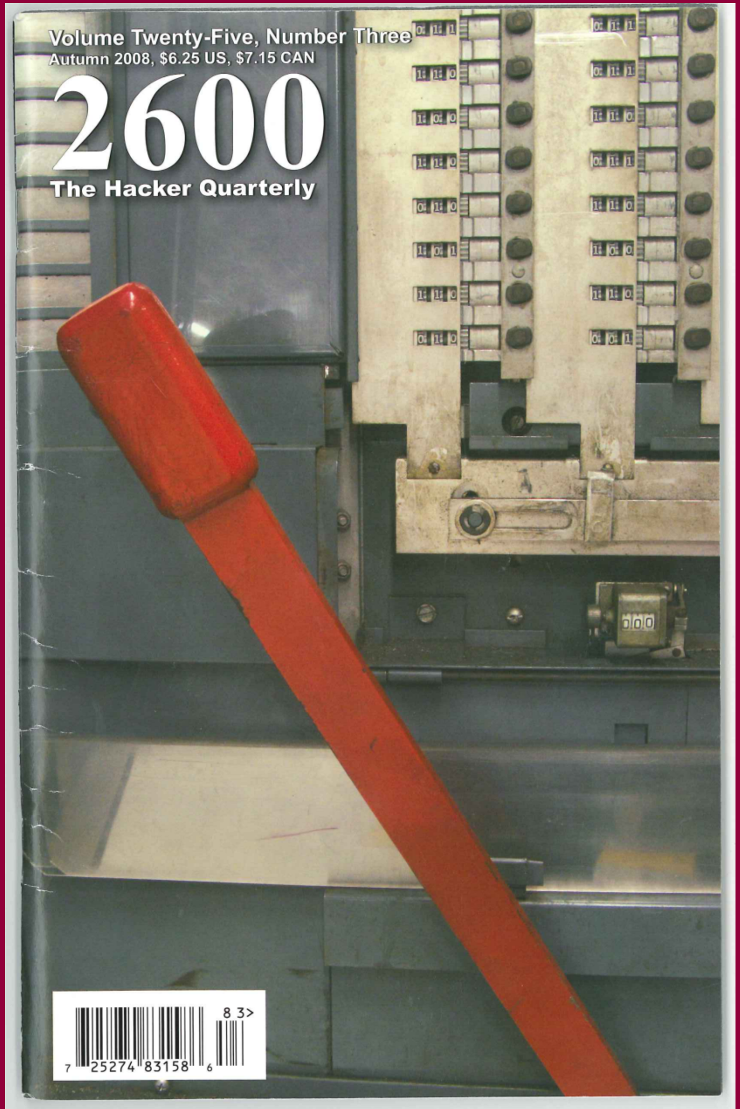
Hacker leaves message for Microsoft in Trojan code -
NetworkWorld.com - 15 related articles »

hacker.org - The **Hacker** Community Online
The **hacker** explores the intersection of art and science in an insatiable quest to understand and shape the world around him. We guide you on this journey.
www.**hacker**.org/ - 6k - Cached - Similar pages -

Learn Real Hacking Skills
Major in Network Security
Master's, Bachelor's, Associate's
www.**Hacker**Degree.com

Detect & Block **Hackers**
on your network. Event log analysis made easy. Download free trial!
www.gfi.com/eventsmanager

2600 – THE HACKER QUARTERLY CONFERENCES


Volume Twenty-Five, Number Three
Autumn 2008, $6.25 US, $7.15 CAN
2600
The Hacker Quarterly

- Black Hat

- 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/ -

HACKERS - FIRST GENERATION – LONE WOLF

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

CYBER CRIMINALS - "PROOF OF CONCEPT" FOR MAKING $

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)

CYBER GANGS – ONLINE EXTORTION

- 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

CYBER CRIME GOES BIG TIME

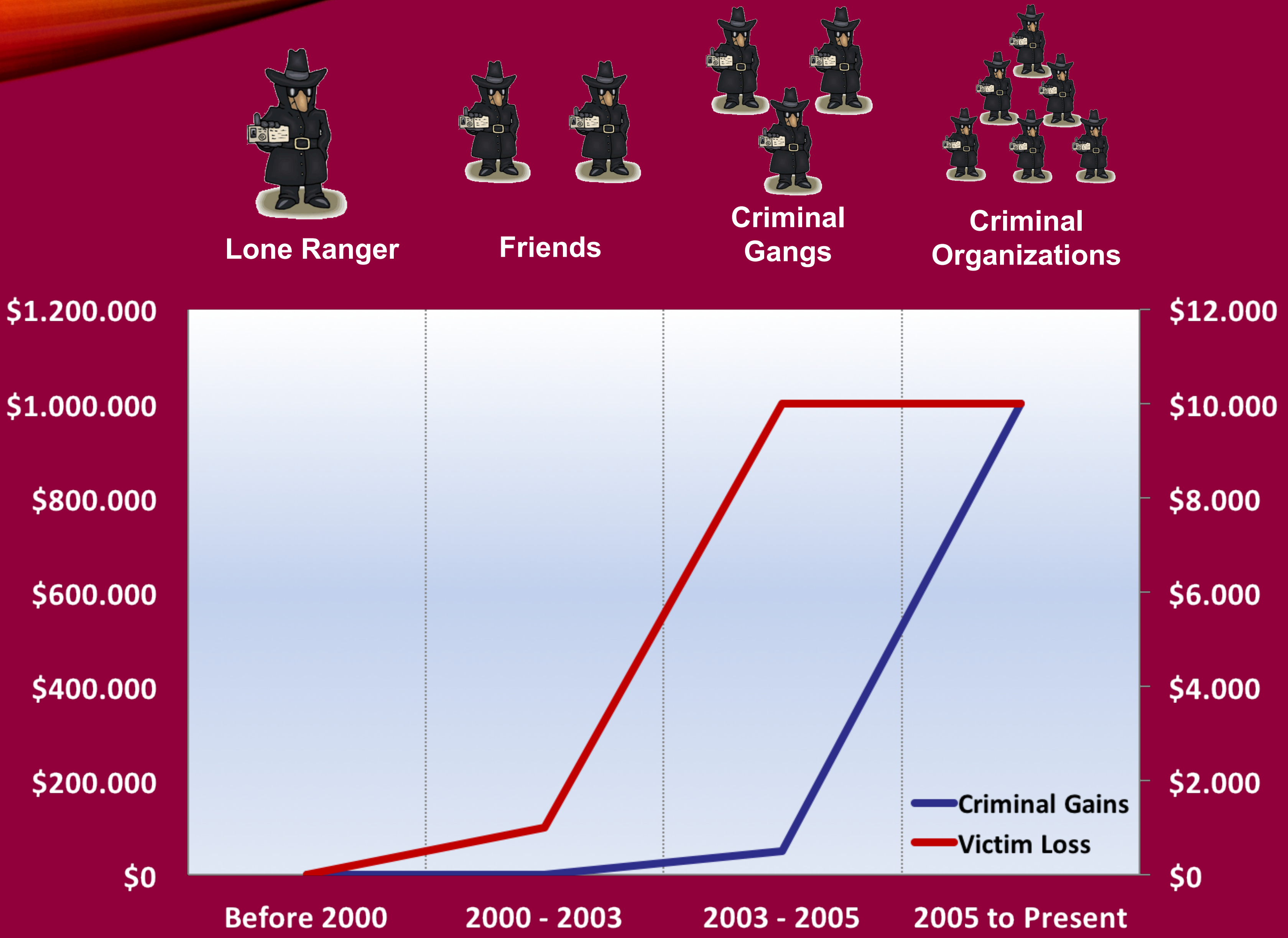
- London branch of Japan's Sumitomo Mitsui Bank
- Worked with insiders through Aharon Abu-Hamra, a 35-year-old Tel Aviv resident
- Injected a Trojan to gather credentials to a transfer system
- Attempted to transfer £220 million into accounts he controlled around the world
- £13.9 million to his own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

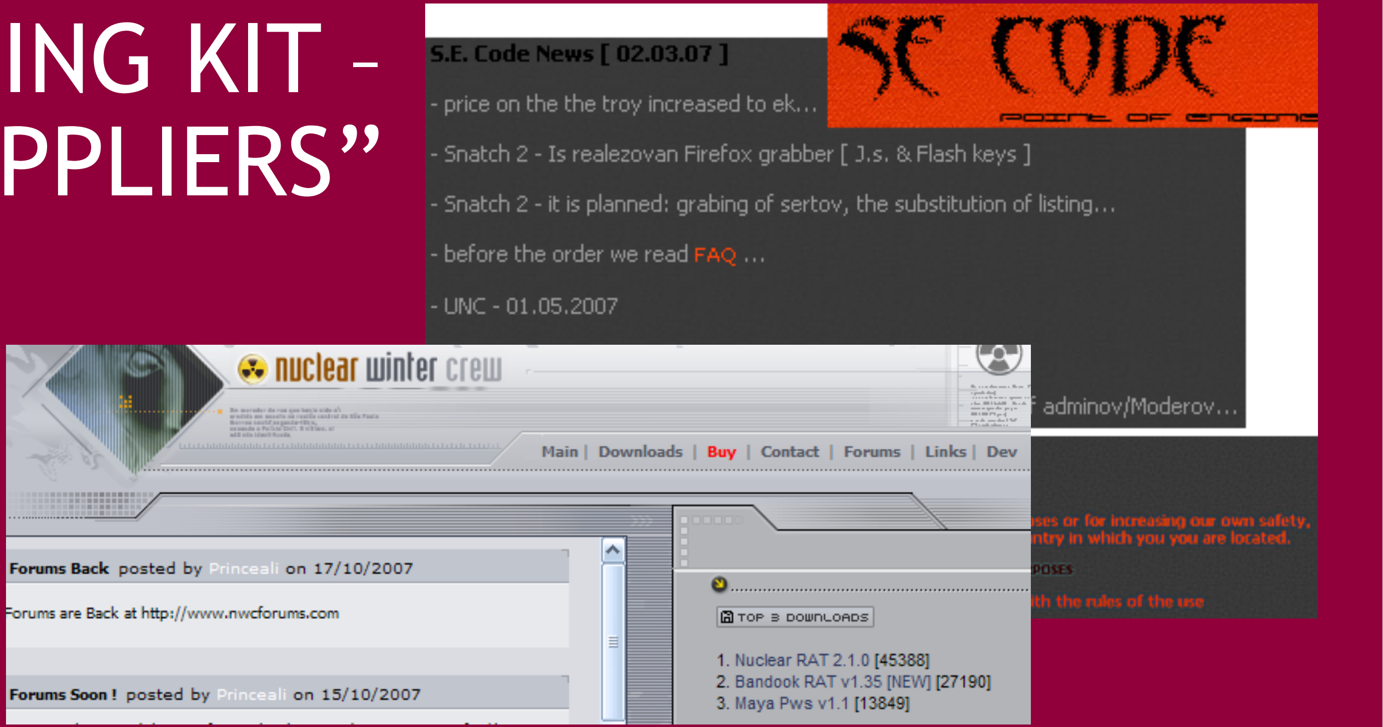
CYBER CRIME TRENDS



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



S.E. Code News [02.03.07]

- price on the the troy increased to ek…

- Snatch 2 - Is realezovan Firefox grabber [J.s. & Flash keys]

- Snatch 2 - it is planned: grabing of sertov, the substitution of listing…

- before the order we read FAQ …

- UNC - 01.05.2007

f adminov/Moderov…

ses or for increasing our own safety, ntry in which you you are located.

POSES

ith the rules of the use

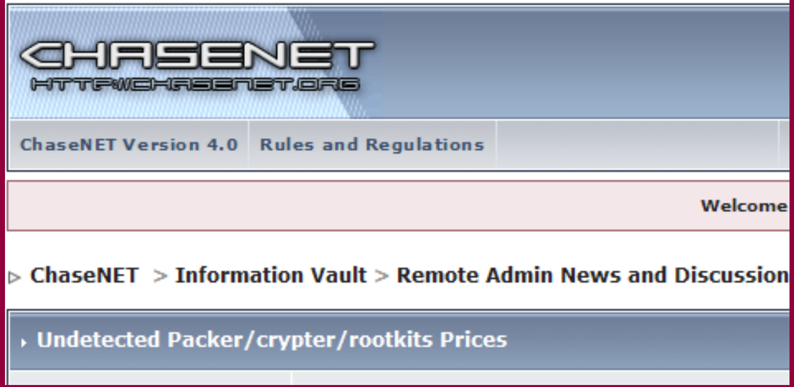
Forums Back posted by Princeali on 17/10/2007

Forums are Back at http://www.nwcforums.com

Forums Soon ! posted by Princeali on 15/10/2007

TOP 3 DOWNLOADS

1. Nuclear RAT 2.1.0 [45388]
2. Bandook RAT v1.35 [NEW] [27190]
3. Maya Pws v1.1 [13849]

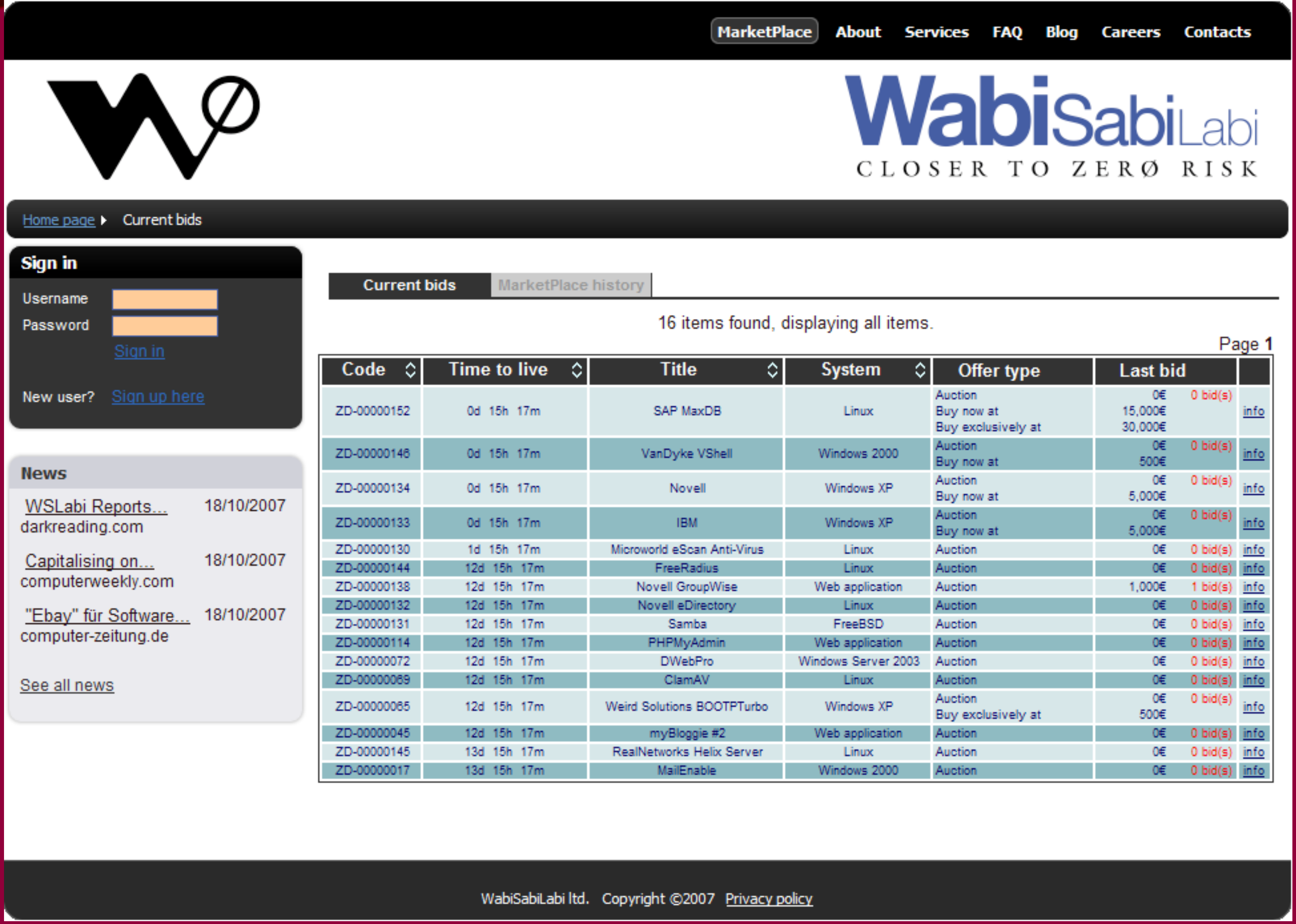


Welcome

ChaseNET > Information Vault > Remote Admin News and Discussion

Undetected Packer/crypter/rootkits Prices

C2C – EXPLOIT – “INTELLIGENCE DEALERS”



News

WSLabi Reports... 18/10/2007
darkreading.com

Capitalising on... 18/10/2007
computerweekly.com

"Ebay" für Software... 18/10/2007
computer-zeitung.de

See all news

16 items found, displaying all items.

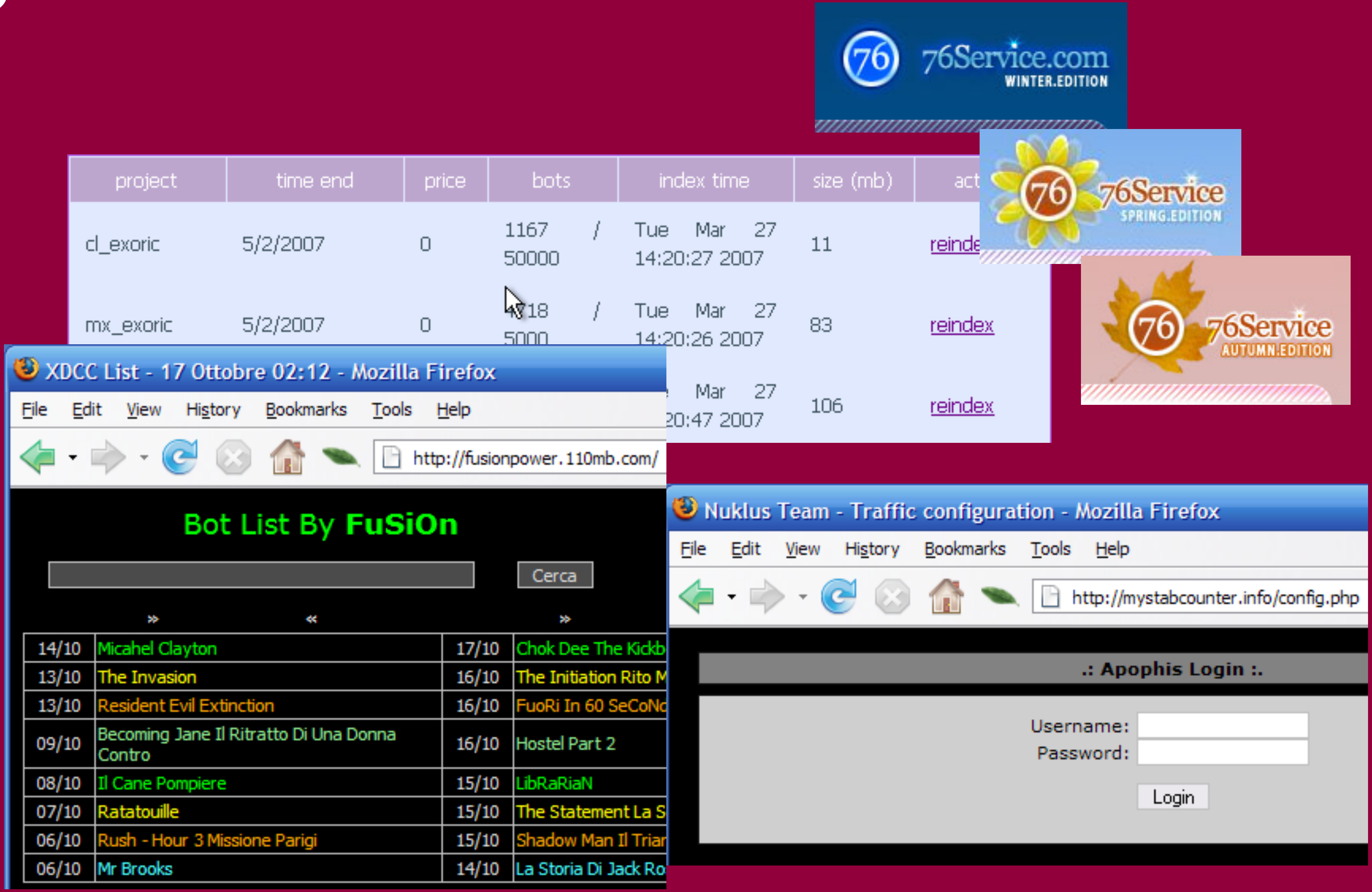
Page **1**

Code	Time to live	Title	System	Offer type	Last bid	
ZD-00000152	0d 15h 17m	SAP MaxDB	Linux	Auction Buy now at Buy exclusively at	0€ 0 bid(s) 15,000€ 30,000€	info
ZD-00000146	0d 15h 17m	VanDyke VShell	Windows 2000	Auction Buy now at	0€ 0 bid(s) 500€	info
ZD-00000134	0d 15h 17m	Novell	Windows XP	Auction Buy now at	0€ 0 bid(s) 5,000€	info
ZD-00000133	0d 15h 17m	IBM	Windows XP	Auction Buy now at	0€ 0 bid(s) 5,000€	info
ZD-00000130	1d 15h 17m	Microworld eScan Anti-Virus	Linux	Auction	0€ 0 bid(s)	info
ZD-00000144	12d 15h 17m	FreeRadius	Linux	Auction	0€ 0 bid(s)	info
ZD-00000138	12d 15h 17m	Novell GroupWise	Web application	Auction	1,000€ 1 bid(s)	info
ZD-00000132	12d 15h 17m	Novell eDirectory	Linux	Auction	0€ 0 bid(s)	info
ZD-00000131	12d 15h 17m	Samba	FreeBSD	Auction	0€ 0 bid(s)	info
ZD-00000114	12d 15h 17m	PHPMyAdmin	Web application	Auction	0€ 0 bid(s)	info
ZD-00000072	12d 15h 17m	DWebPro	Windows Server 2003	Auction	0€ 0 bid(s)	info
ZD-00000069	12d 15h 17m	ClamAV	Linux	Auction	0€ 0 bid(s)	info
ZD-00000065	12d 15h 17m	Weird Solutions BOOTPTurbo	Windows XP	Auction Buy exclusively at	0€ 0 bid(s) 500€	info
ZD-00000045	12d 15h 17m	myBloggie #2	Web application	Auction	0€ 0 bid(s)	info
ZD-00000145	13d 15h 17m	RealNetworks Helix Server	Linux	Auction	0€ 0 bid(s)	info
ZD-00000017	13d 15h 17m	MailEnable	Windows 2000	Auction	0€ 0 bid(s)	info

WabiSabiLabi ltd. Copyright ©2007 Privacy policy

C2C: BOT MANAGEMENT– “TURN KEY WEAPONS SYSTEMS”

- 76service, Nuklus Team
- Botnet Dashboards



project	time end	price	bots	index time	size (mb)	act
cl_exoric	5/2/2007	0	1167 / 50000	Tue Mar 27 14:20:27 2007	11	reinde
mx_exoric	5/2/2007	0	1718 / 5000	Tue Mar 27 14:20:26 2007	83	reindex
				Mar 27 20:47 2007	106	reindex

XDCC List - 17 Ottobre 02:12 - Mozilla Firefox

http://fusionpower.110mb.com/

Bot List By FuSiOn

»	«		»
14/10	Micahel Clayton	17/10	Chok Dee The Kickb
13/10	The Invasion	16/10	The Initiation Rito M
13/10	Resident Evil Extinction	16/10	FuoRi In 60 SeCoNd
09/10	Becoming Jane Il Ritratto Di Una Donna Contro	16/10	Hostel Part 2
08/10	Il Cane Pompiere	15/10	LibRaRiaN
07/10	Ratatouille	15/10	The Statement La S
06/10	Rush - Hour 3 Missione Parigi	15/10	Shadow Man Il Trian
06/10	Mr Brooks	14/10	La Storia Di Jack Ro

Nuklus Team - Traffic configuration - Mozilla Firefox

http://mystabcounter.info/config.php

.: Apophis Login :.

Username:
Password:

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

SPOOFING

- 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

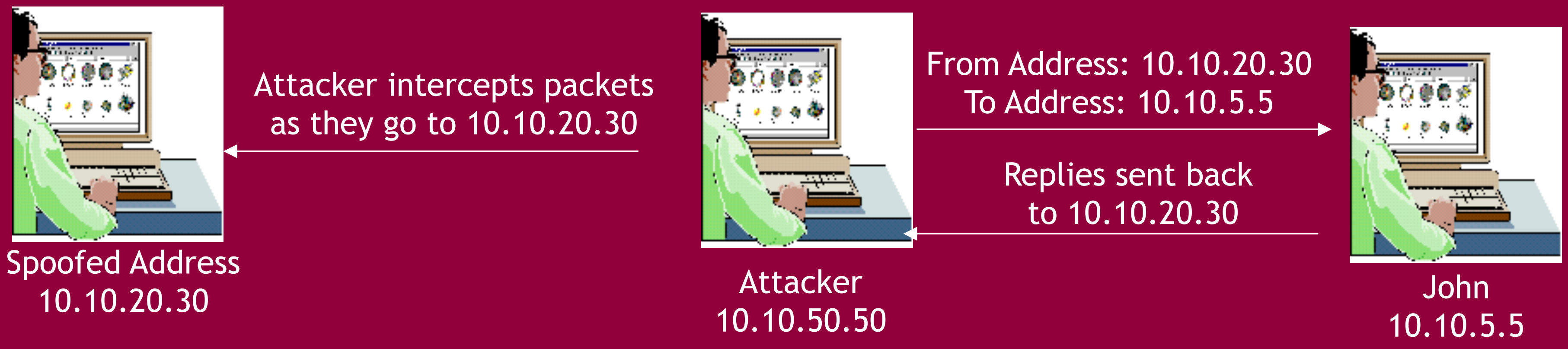
From Address: 10.10.20.30
To Address: 10.10.5.5

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

Attacker
10.10.50.50

From Address: 10.10.20.30
To Address: 10.10.5.5

Replies sent back to 10.10.20.30

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 some one 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

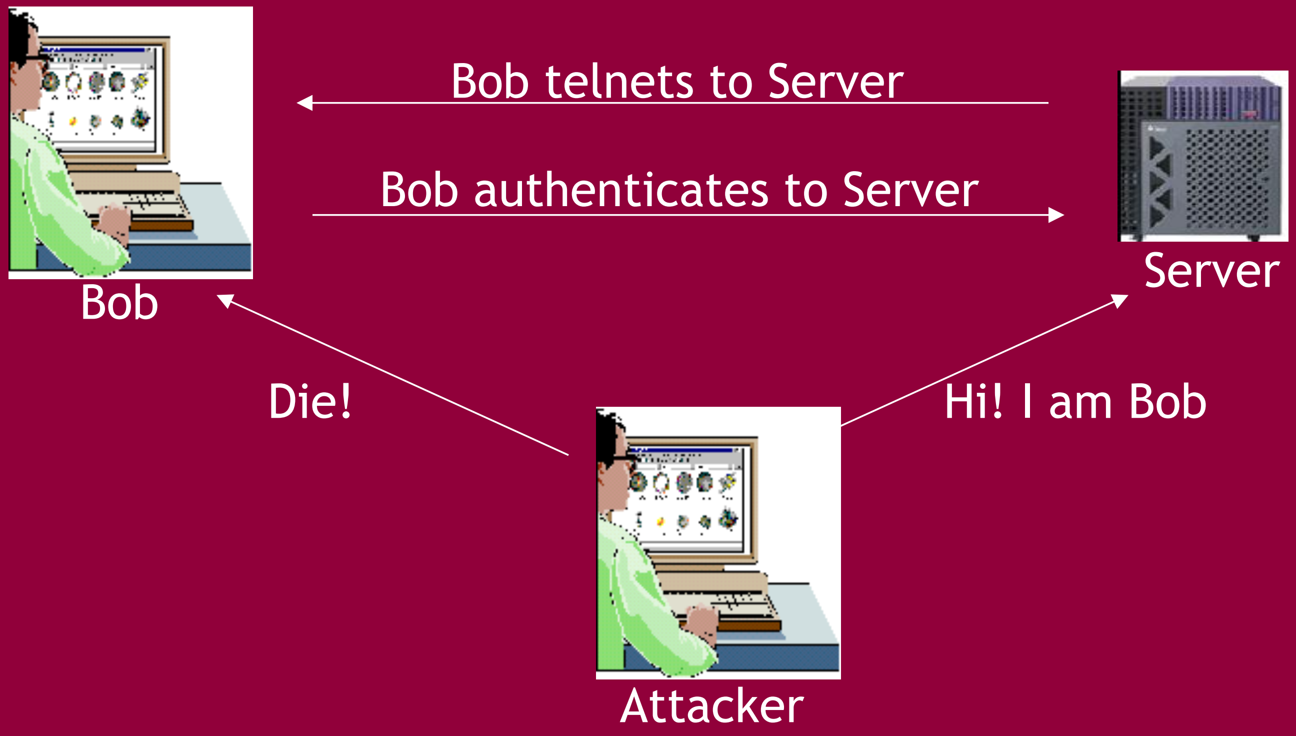
- Basic
  - Attacker registers a web address matching an entity e.g. votebush.com, geproducts.com, gesucks.com
- Man-in-the-Middle Attack
  - Attacker acts as a proxy between the web server and the client
  - Attacker has to compromise the router or a node through which the relevant traffic flows
- URL 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

Die!

Hi! I am Bob

Attacker

DENIAL OF SERVICE (DOS) ATTACK

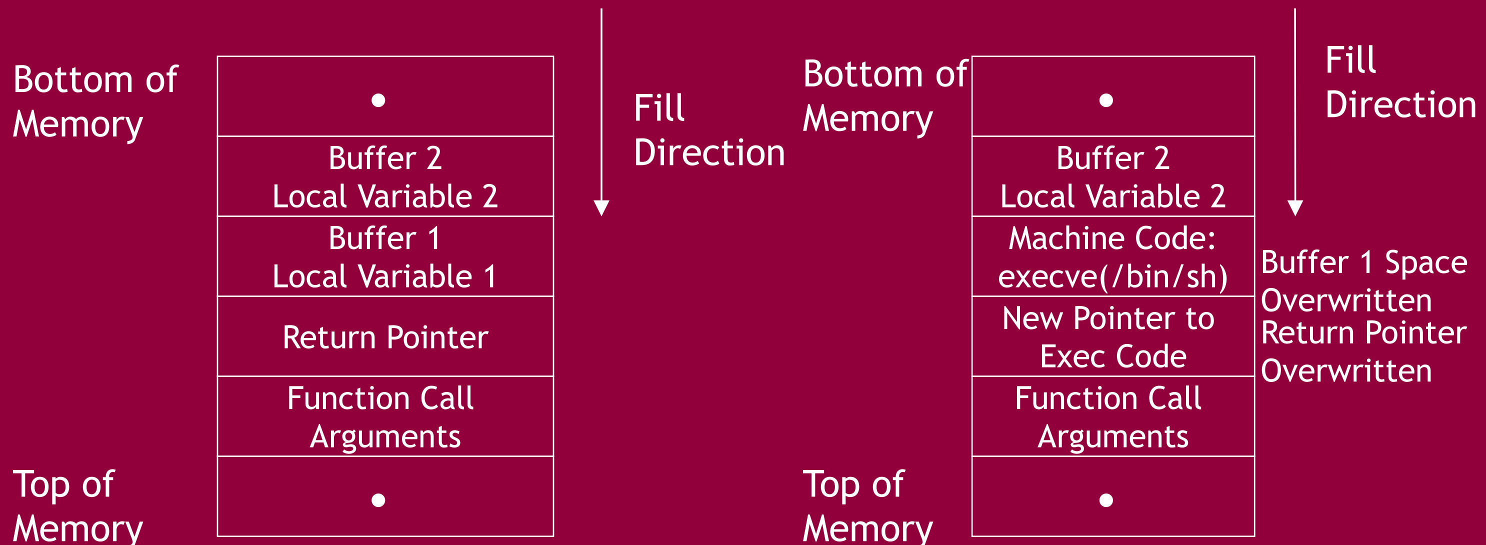
- Definition:
  - Attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the system so that no one else can use it
- Types:
  - Crashing the system or network
    - Send the victim data or packets which will cause system to 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 Vulneability
  - 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?



Bottom of Memory

•

Buffer 2
Local Variable 2

Buffer 1
Local Variable 1

Return Pointer

Function Call Arguments

•

Top of Memory

Fill Direction

Normal Stack

Bottom of Memory

•

Buffer 2
Local Variable 2

Machine Code:
execve(/bin/sh)

New Pointer to Exec Code

Function Call Arguments

•

Top of Memory

Fill Direction

Buffer 1 Space Overwritten

Return Pointer Overwritten

Smashed Stack

BUFFER OVERFLOW ATTACKS

- Programs which do not 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

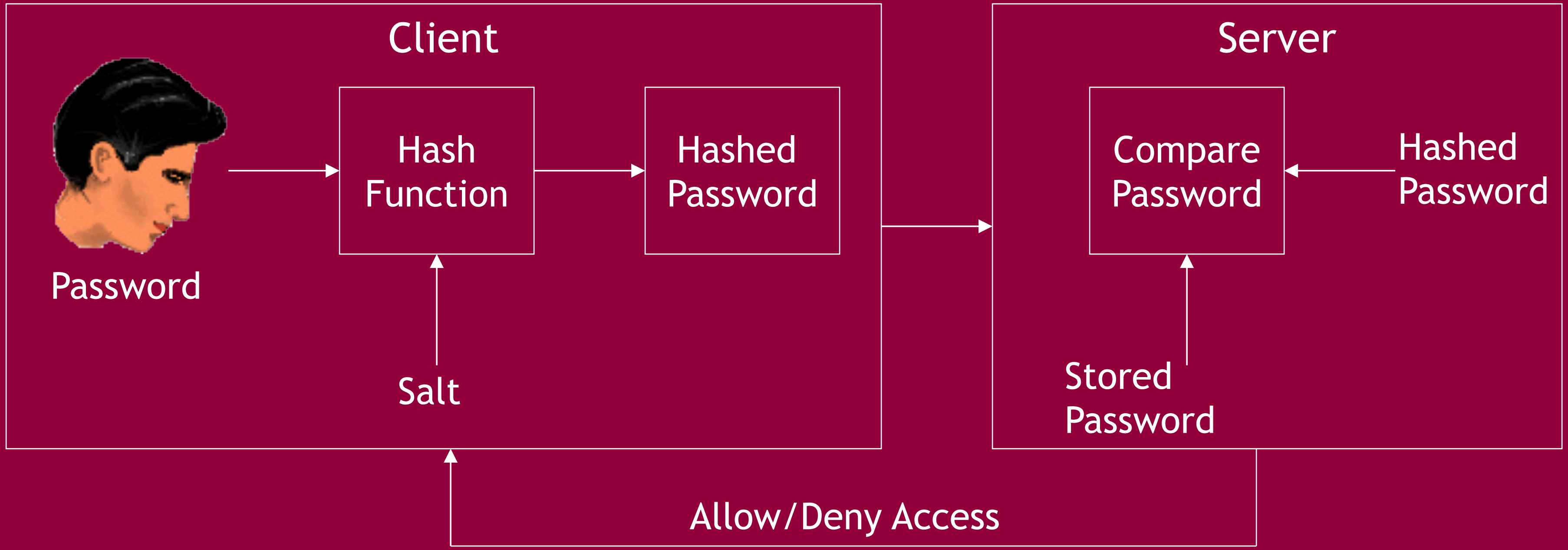
- Examples
  - NetMeeting Buffer Overflow
  - Outlook Buffer Overflow
  - AOL Instant Messenger Buffer Overflow
  - SQL Server 2000 Extended Stored Procedure Buffer Overflow

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



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

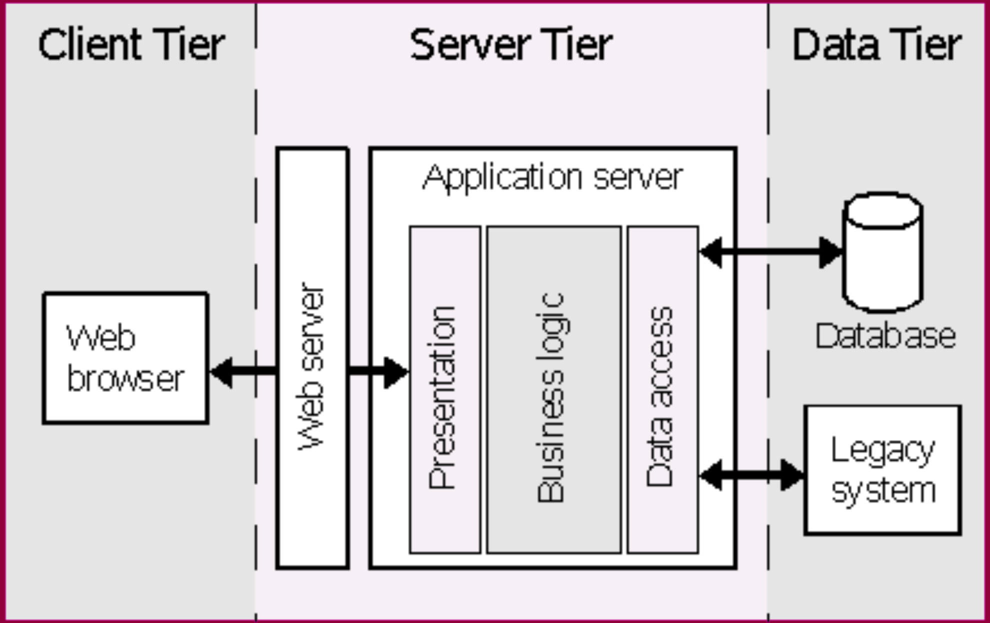
INTERNET APPLICATION SECURITY

INTERNET APPLICATION HACKING STATISTICS

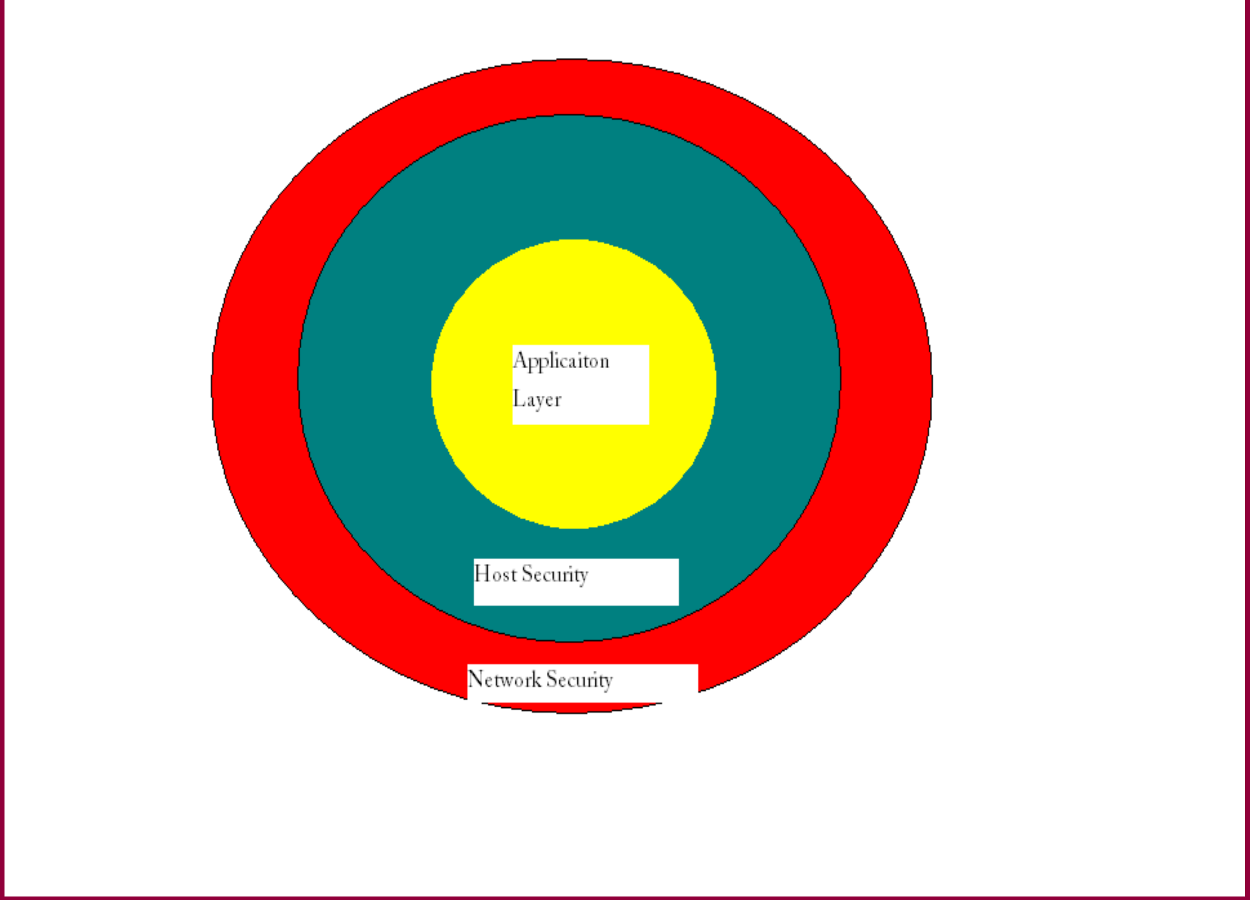
- **WHID (Web Hacking Incident Database) annual report for 2007** 67% percent of the attacks in 2007 were "for profit" motivated. And it targeted the Web-Applications
- Acunetix, a leading vendor of web application security solutions, revealed that on average 70% of websites are at serious and immediate 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



Applicaiton Layer

Host Security

Network 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

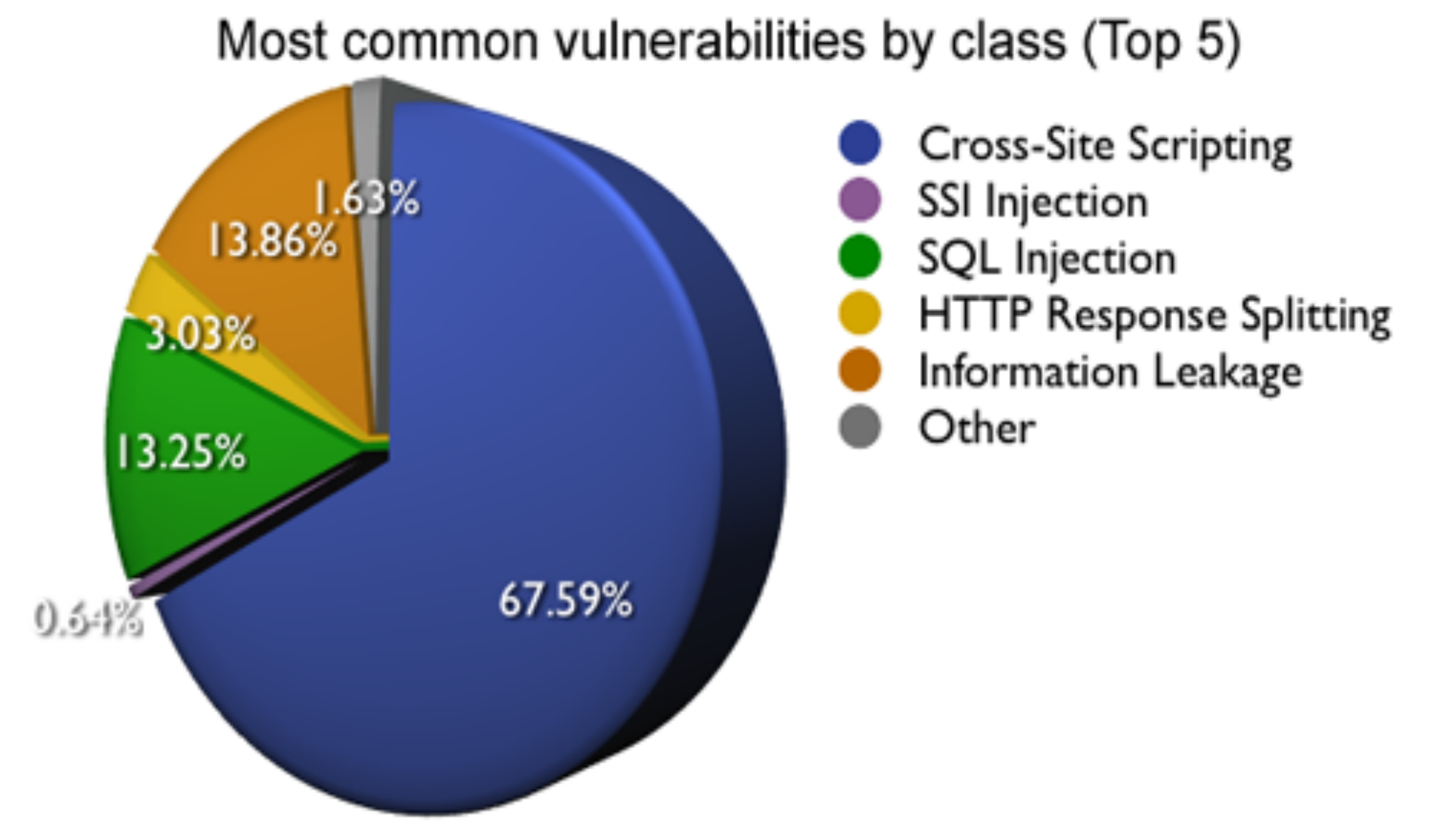
FUNDAMENTAL METHODOLOGY TO DO ANY WEB-APPLICATION ASSESSMENT

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

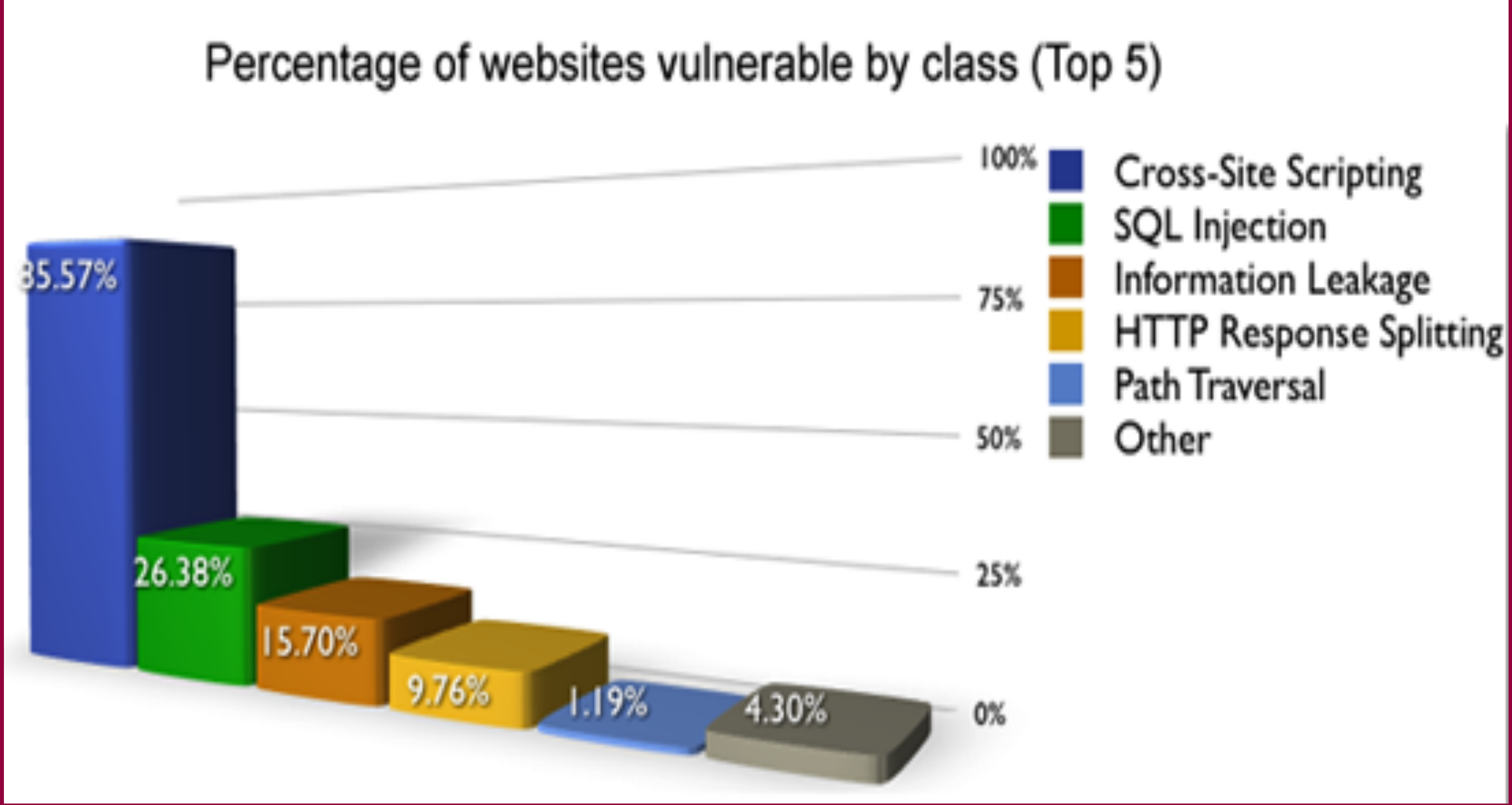
WHY VULNERABLE?

- 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

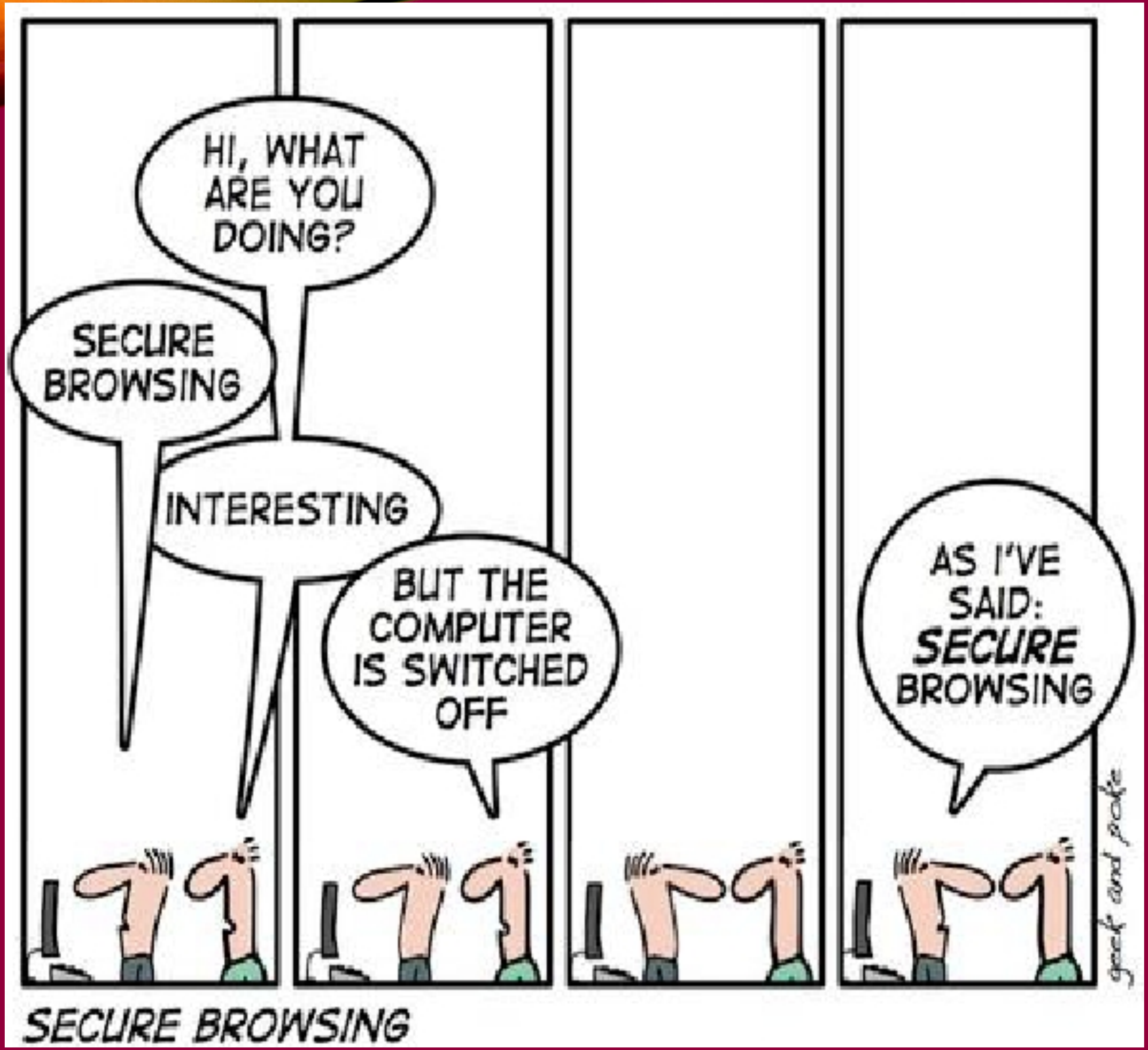


CLASSES OF ATTACKS

- 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
geek and poke
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

QUESTIONS?