# Ethical Hacker :

# Anatomia di un Hacking


***Relatore***

***Francesco Arruzzoli***

# Chi sono gli ethical hacker ?

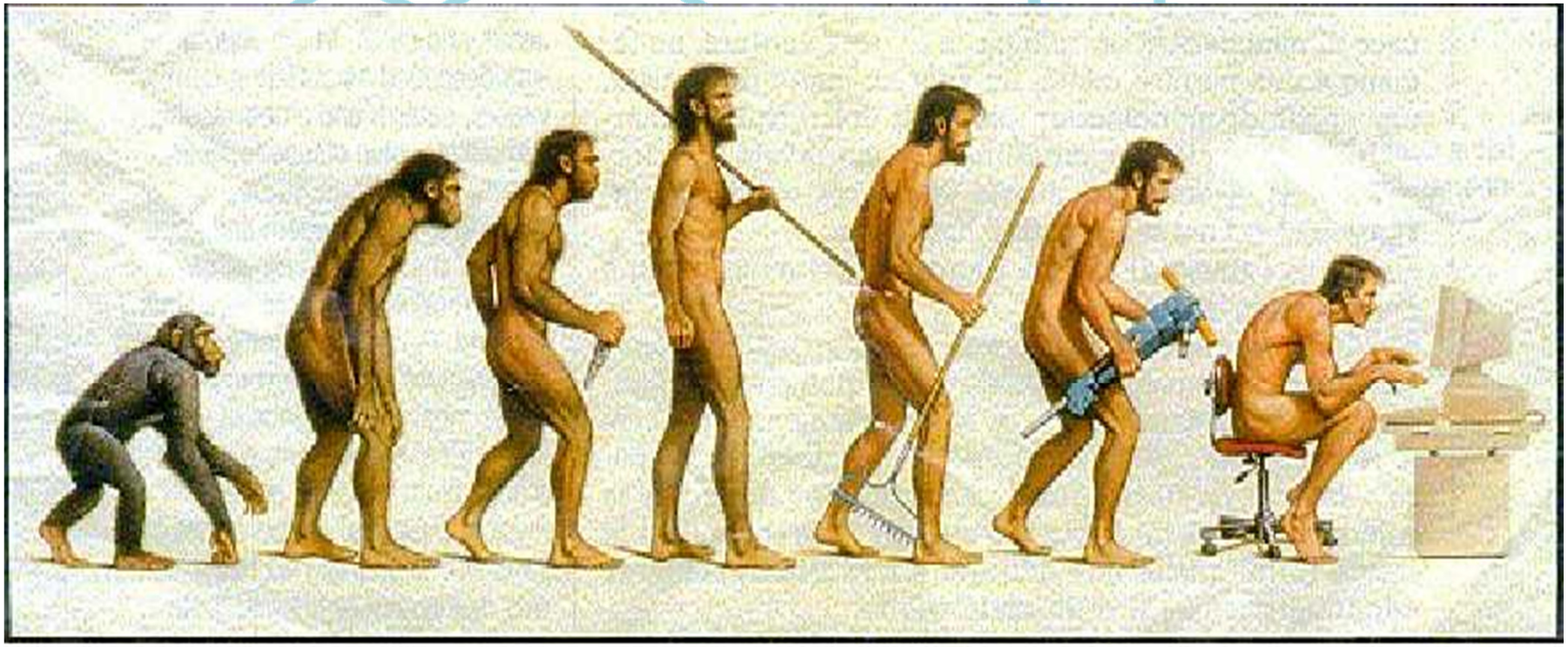
**Gli ethical hacker sono professionisti ICT multidisciplinari (forti competenze nello sviluppo software, nell'area sistemistica e nel networking) con diversi anni di esperienza lavorativa e una particolare conoscenza delle influenze dell'ICT nei comportamenti e nelle dinamiche sociali (ad es. Social Engineering).** Il modus operandi degli ethical hacker combina le metodologie e tecniche di protezione con quelle utilizzate per violare la sicurezza dei sistemi affrontando la problematica da entrambi le parti : difensore – attaccante, lo scopo finale è unicamente quello di migliorare la sicurezza dei sistemi informatici nel rispetto dei regolamenti e della legge.

# Il campo di battaglia

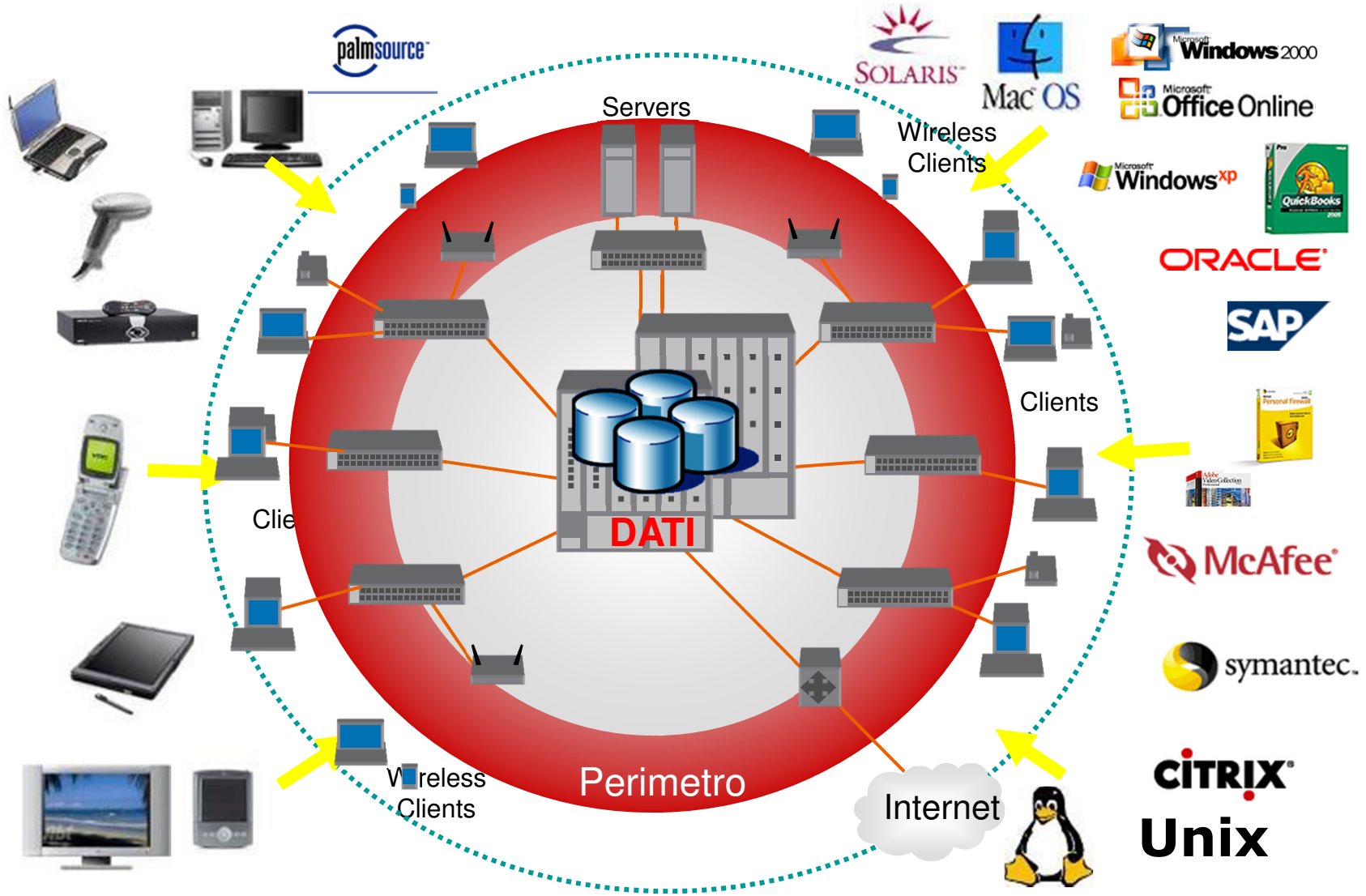
# Tecnologia invasiva

Casa

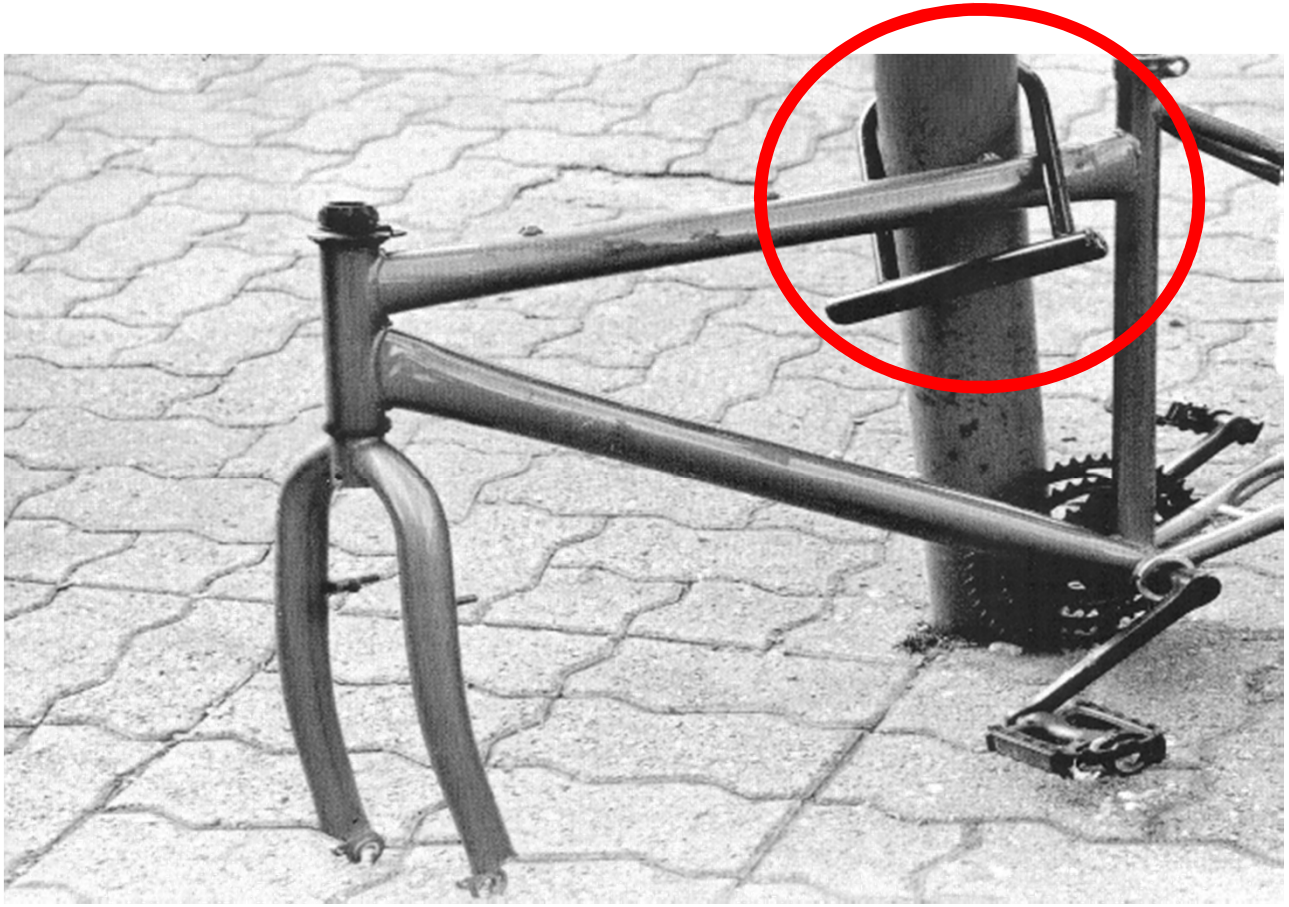
Ufficio



# Tecnologie


palmsource
SOLARIS
Mac OS
Windows 2000
Microsoft Office Online
Windows xp
QuickBooks
ORACLE
SAP
McAfee
symantec.
CITRIX
Unix
Servers
Wireless Clients
Clients
Clie
DATI
Perimetro
Wireless Clients
Internet

# I prodotti funzionano molto spesso egregiamente….

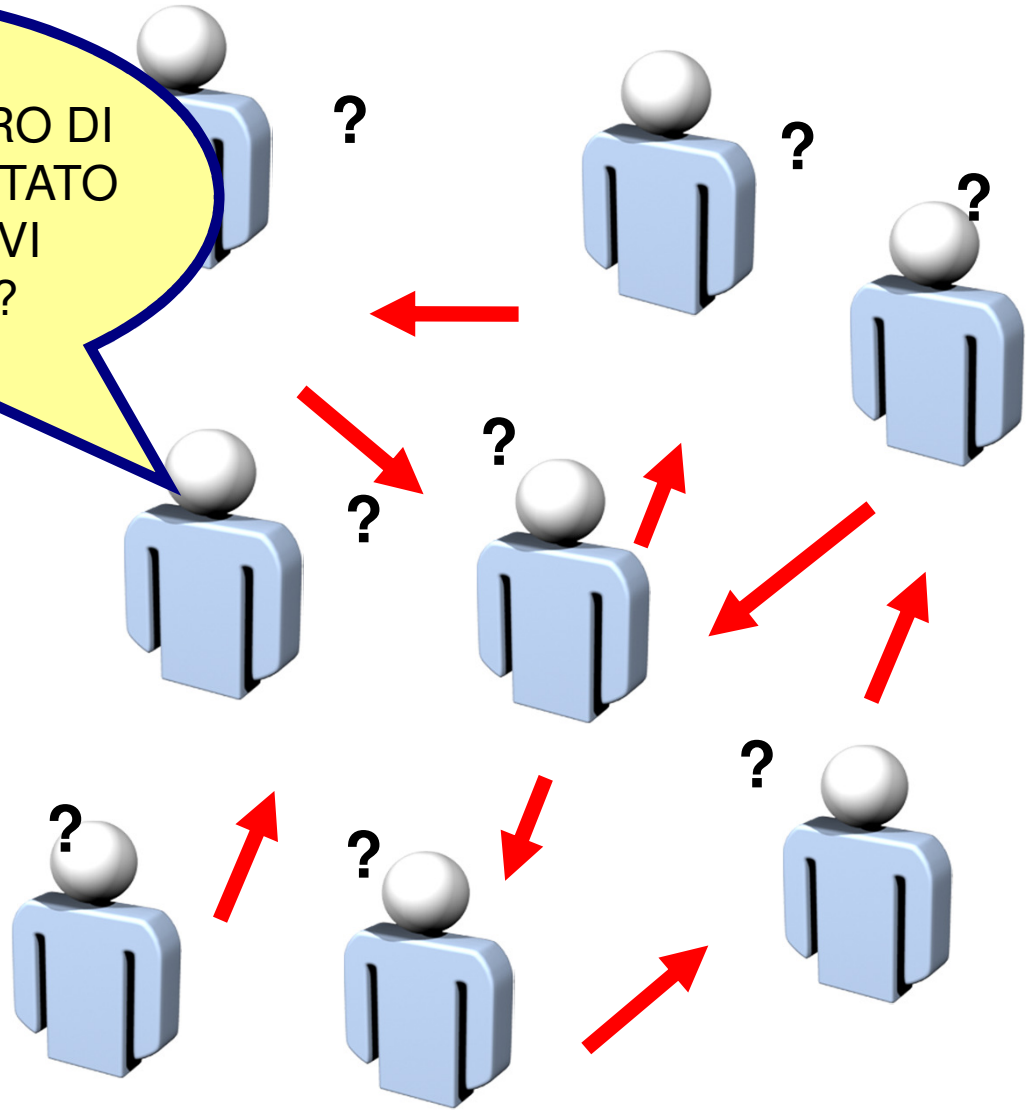


# ma da soli non bastano.

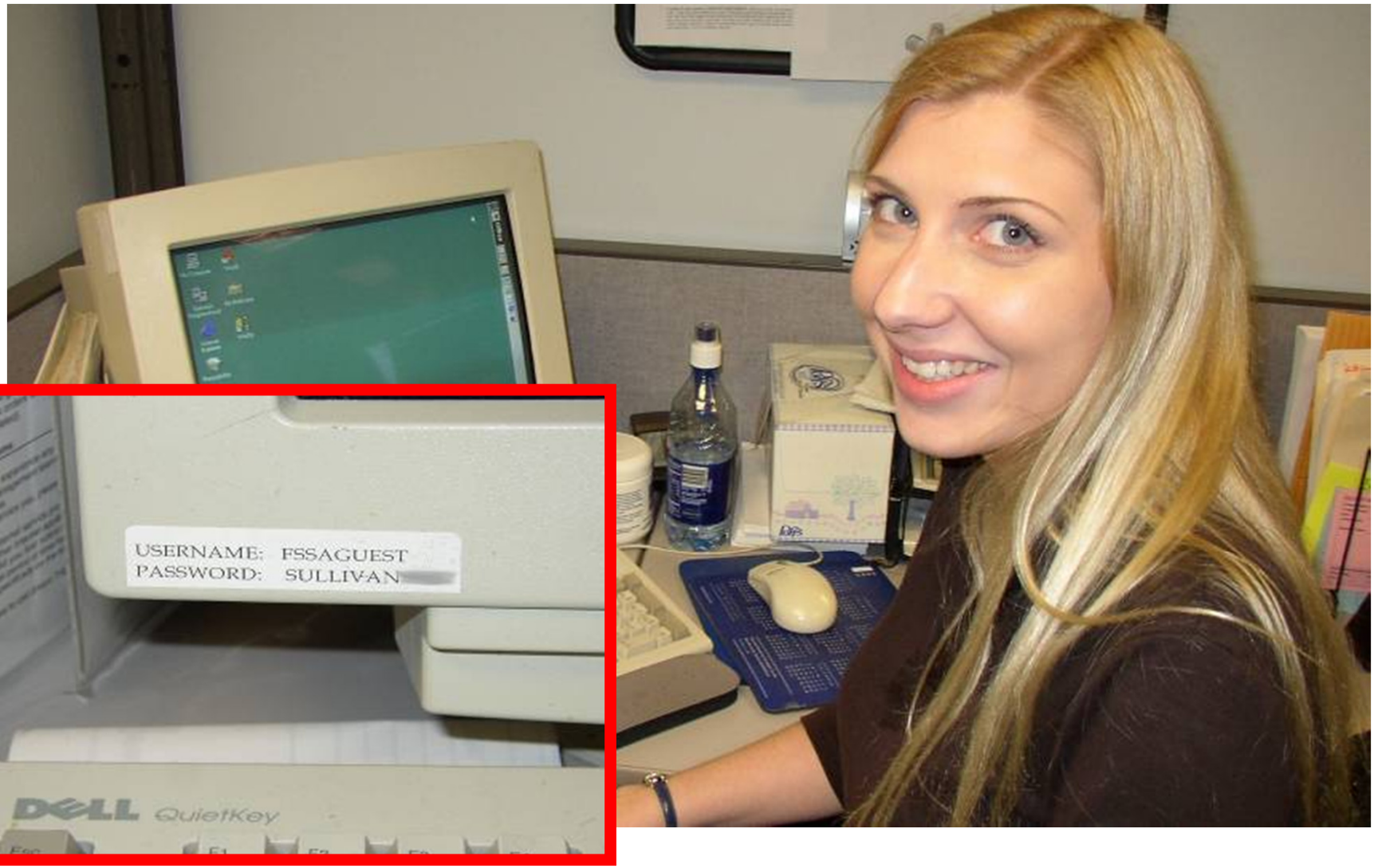
# PROCESSI ORGANIZZATIVI

MA IL VECCHIO NASTRO DI BACKUP CHE HAI GETTATO VIA, NON LO DOVEVI CANCELLARE TU ?

**DATI**



# LE PERSONE



## Un recente esempio di Social Engineering

**Nel 2006 la sicurezza informatica una nota società di credito è stata sottoposta ad un penetration test da parte di auditor esterni che hanno utilizzato un semplice ma geniale trucco per entrare nel sistema informativo dell'azienda, hanno disseminato lungo il perimetro dell'edificio della società 20 chiavette usb contenenti, documenti divertenti, immagini accattivanti, finte email personali, giochi e naturalmente un Trojan costruito ad HOC per catturare ed inviare le password degli utenti…**

# …RISULTATO..

**..15 CHIAVETTE SU 20 SONO STATE UTILIZZATE SUI COMPUTER AZIENDALI, POCHI MINUTI DOPO L'INIZIO DELLA GIORNATA LAVORATIVA I TROJAN HANNO COMINCIATO A SPEDIRE AGLI AUDITOR DATI E INFORMAZIONI CLASSIFICATE COME CONFIDENZIALI.**

# La sicurezza dei sistemi dipende da:

# Tecnologia, Processi, Persone e …


# Informazione

## La condivisione delle informazioni richiede una comprensione comune e costante di cosa le informazioni significhino.

Adolf Hitler

Partito Nazista

**La svastica è un simbolo universalmente conosciuto e molto antico**, se ne trova traccia in Asia, in Mongolia, in India e anche nell'America centrale. La simbologia della svastica si puo' osservare anche sulle grandi statue d'oro dei *Buddha*, al centro del suo petto La simbologia della svastica deriva dalla lingua sanscrito e lo si ritrova nelle antiche scritture indiane e cinesi e **fa parte dei simboli rappresentanti la sapienza** .

# Unicode: La nuova torre di Babele

**Unicode** è una codifica per rappresentare caratteri latini, greci, ebraici, arabi, cirillici, etc. Cfr. ASCII (7 bit, 128 caratteri), ISO-Latin-1 (8 bit, 256 caratteri). Lo scopo di Unicode è stilare una lista di tutti i caratteri delle lingue del mondo, come i caratteri arabi (ש), le nostre classiche lettere "latine" (a, b, c), i caratteri russi (cirillico: Й), i caratteri greci (Σ) e tutti i caratteri degli altri paesi del mondo. L'esigenza di Unicode è nata dal voler scrivere documenti leggibili in ogni paese, indipendentemente dal software utilizzato.

**I caratteri a, c, e, o, p, y sono omografi dei cirillici a, c, e, o, p, y, anche se la pronuncia differisce.**

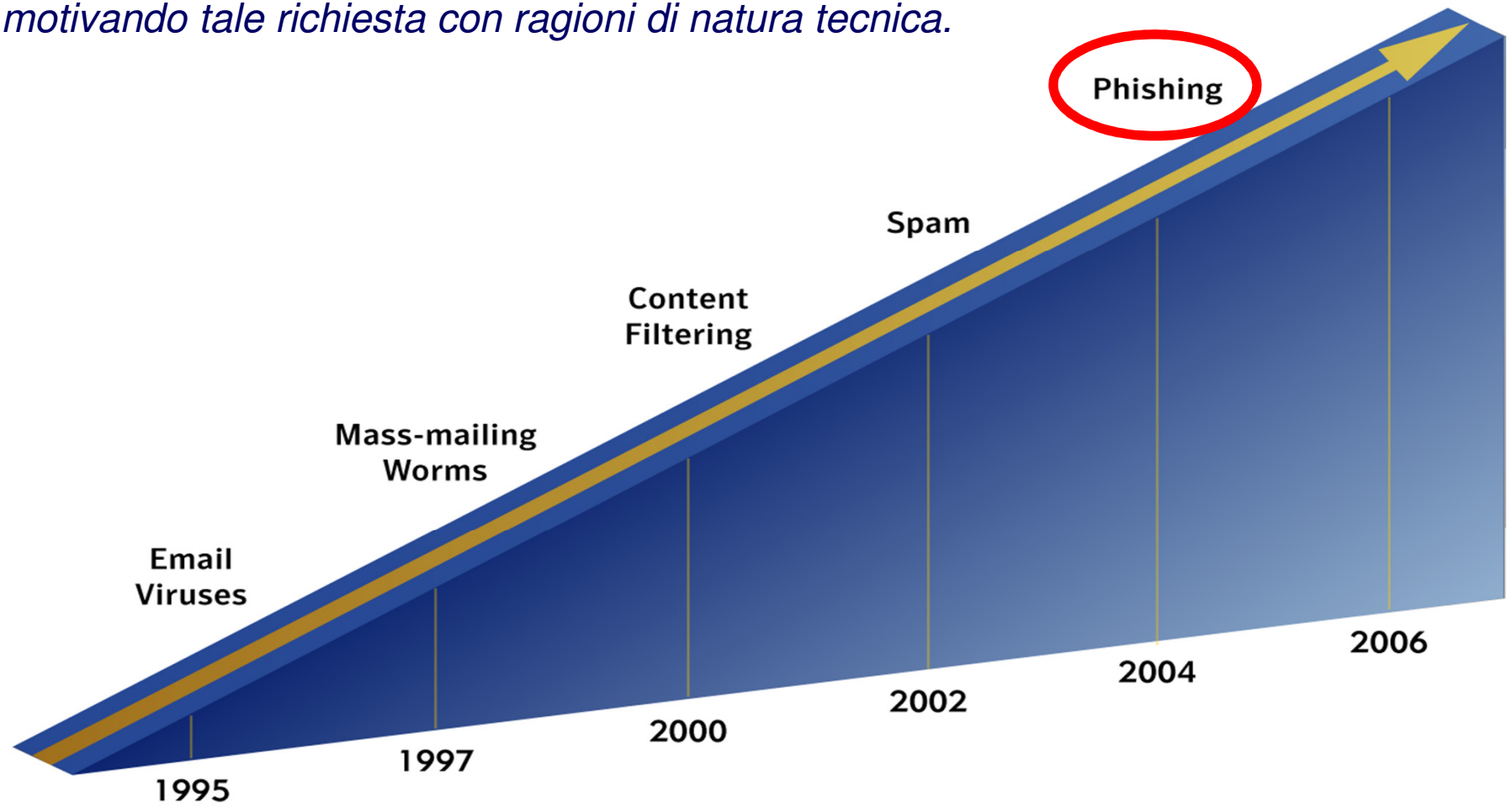
Nel 2002 due studenti dell'Israel Institute of Technology (Evgeniy Gabrilovich e Alex Gontmakher) registrano www.microsoft.com, utilizzando al posto delle o il carattere cirillico o, per dimostrare le loro tesi sull'omografia. L'operazione viene effettuata regolarmente dal provider register.com :

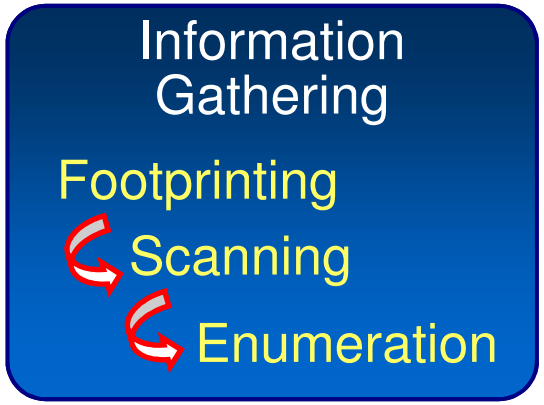
**Indirizzo originale : www.microsoft.com**

**Indirizzo omografico : www.microsoft.com**

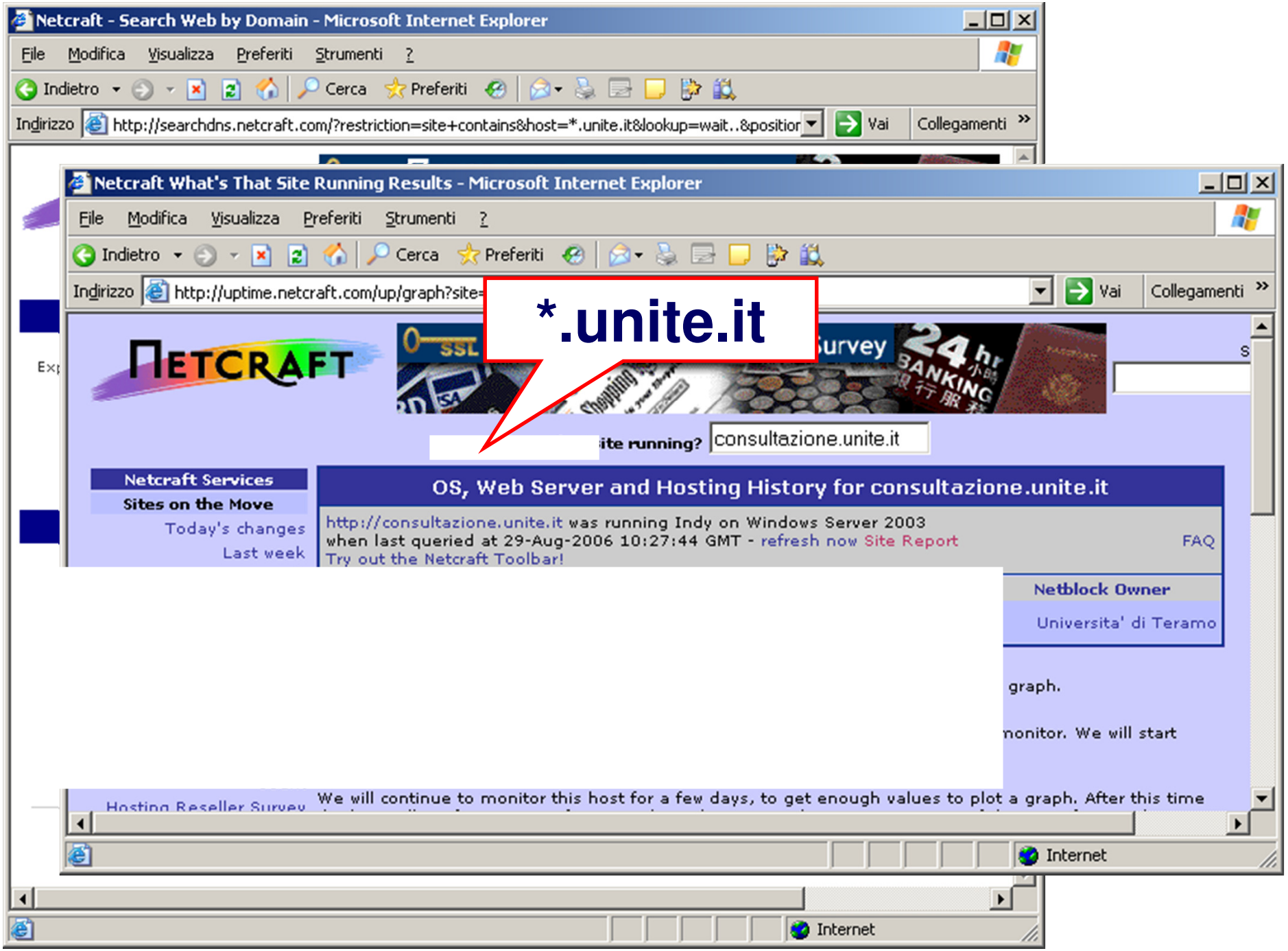
# La parola phishing deriva dall'unione delle parole inglesi "password", "harvesting" e "fishing".

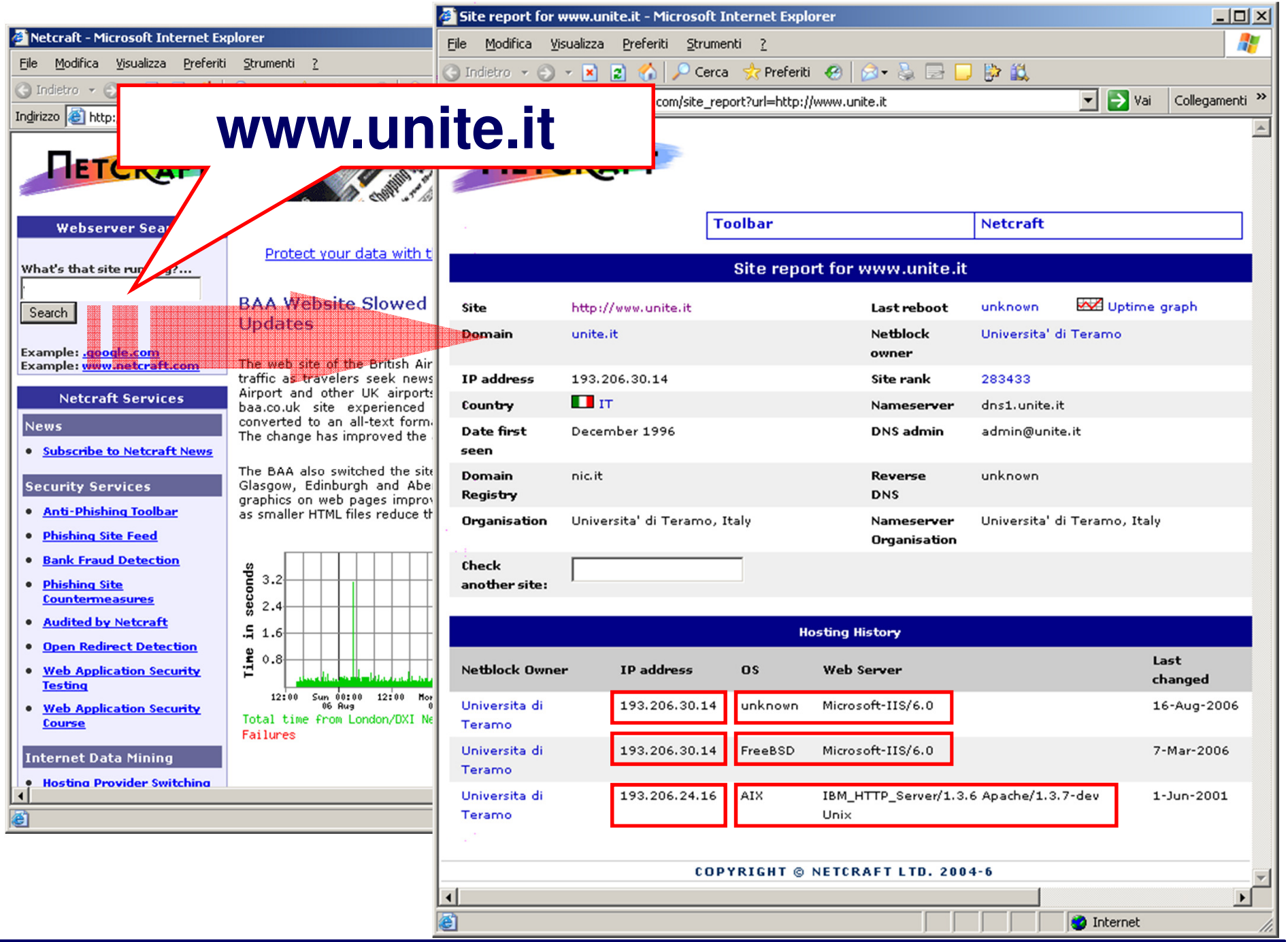
*La frode viene realizzata generalmente attraverso l'invio di e-mail contraffatte con la grafica ed i loghi ufficiali di aziende ed istituzioni opportunamente creati per apparire autentici, che invitano il destinatario a fornire informazioni, spesso motivando tale richiesta con ragioni di natura tecnica.*

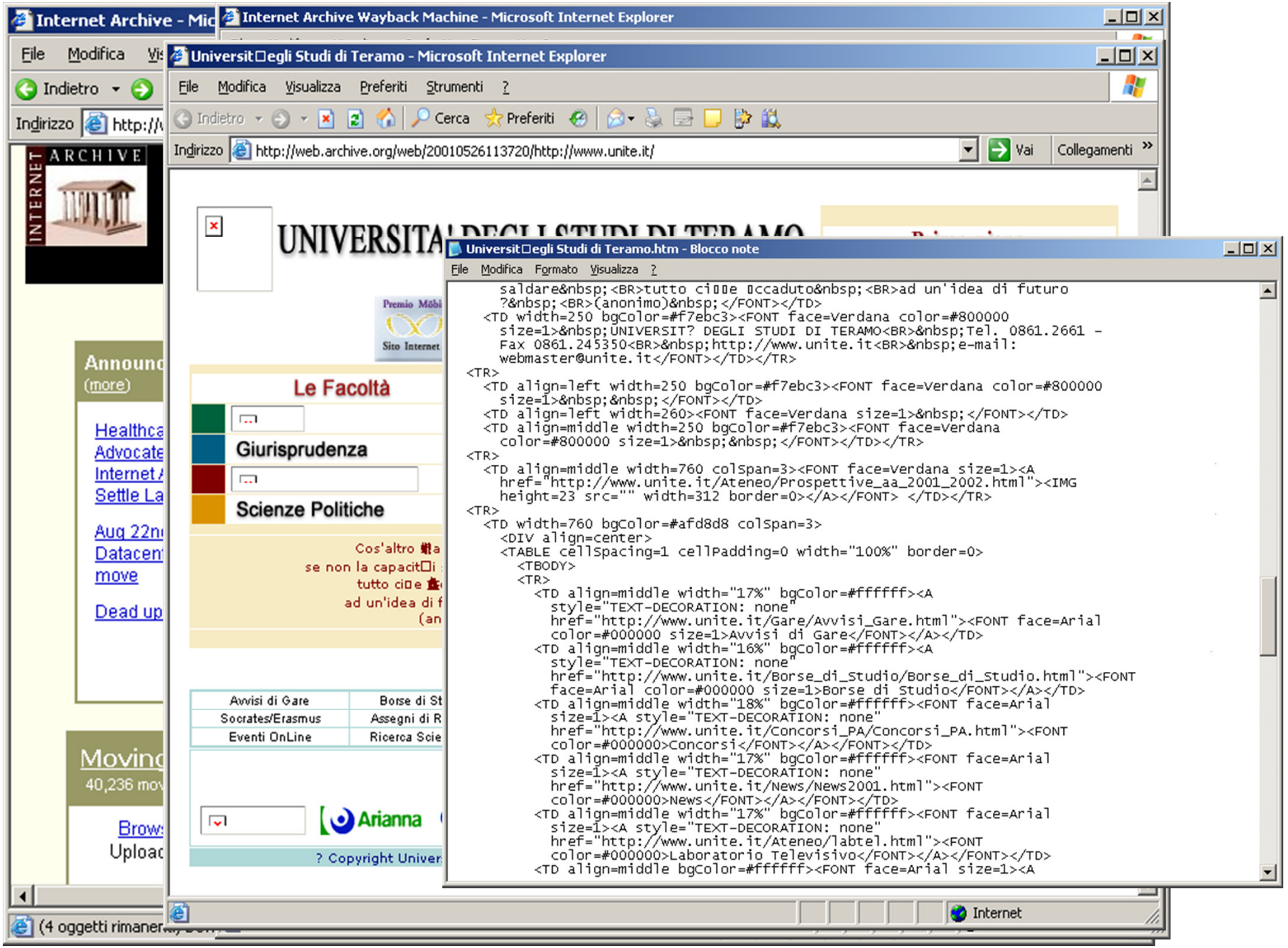


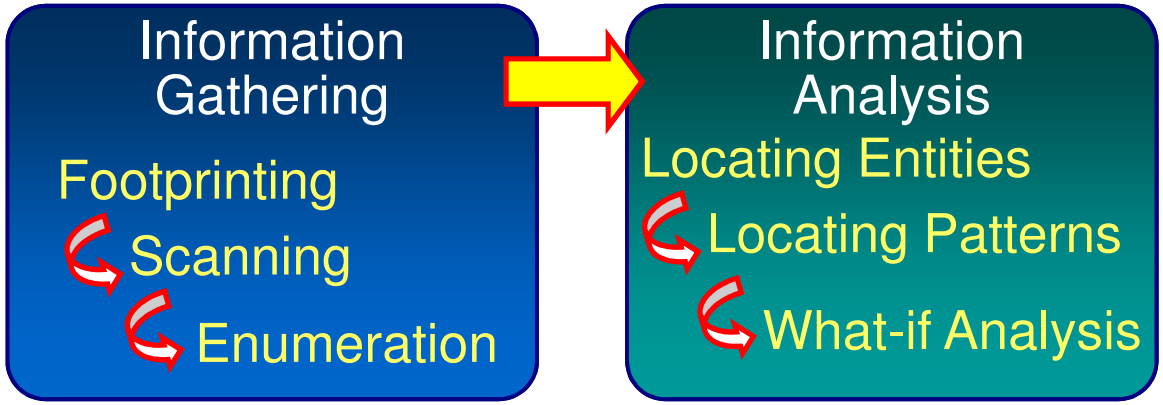



# Strategia di un Hacking

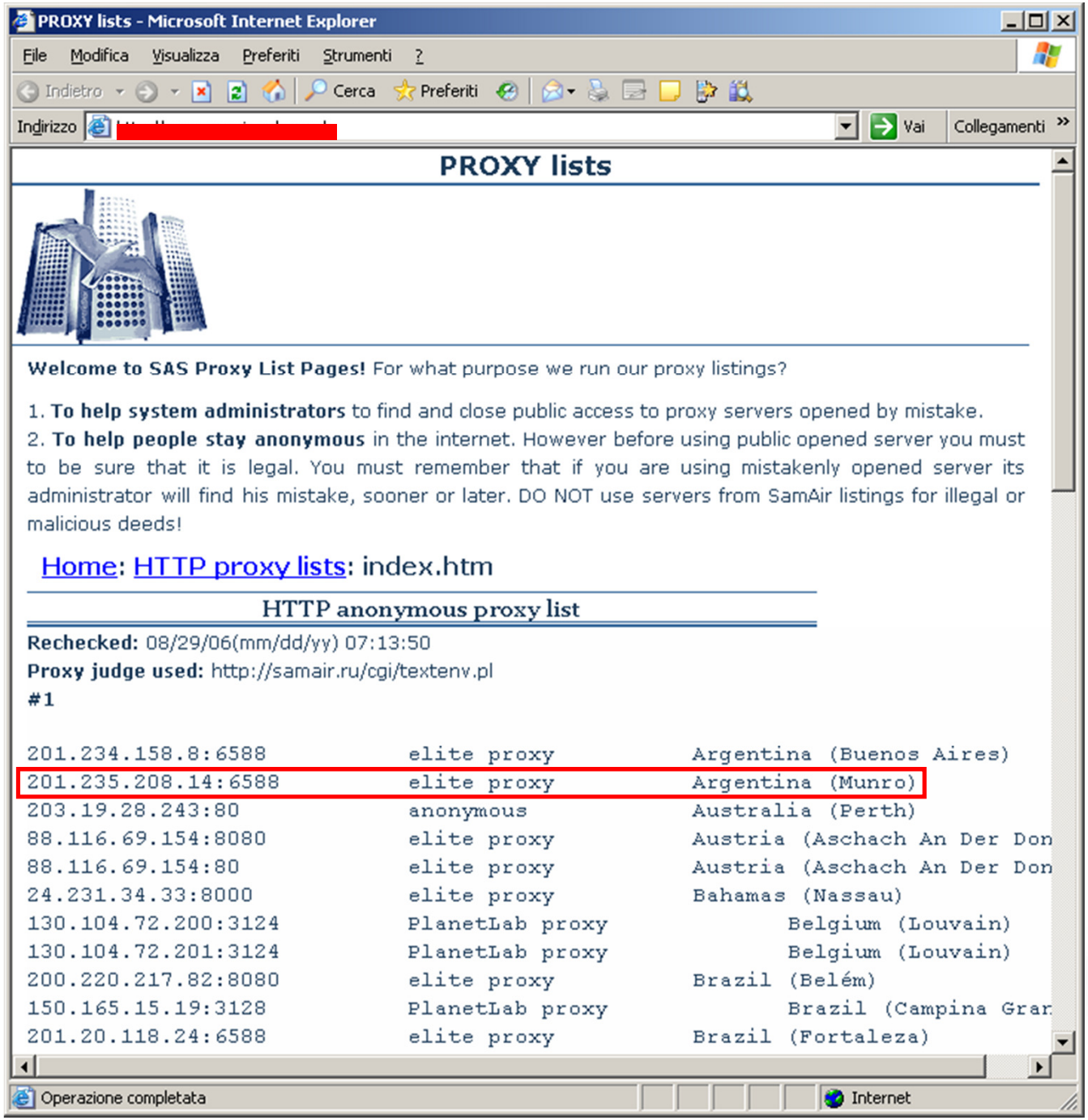

Netcraft - Search Web by Domain - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo http://searchdns.netcraft.com/?restriction=site+contains&host=*.unite.it&lookup=wait..&position
Vai Collegamenti
Netcraft What's That Site Running Results - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo http://uptime.netcraft.com/up/graph?site=
Vai Collegamenti
*.unite.it
NETCRAFT
consultazione.unite.it
Netcraft Services
Sites on the Move
Today's changes
Last week
OS, Web Server and Hosting History for consultazione.unite.it
http://consultazione.unite.it was running Indy on Windows Server 2003
when last queried at 29-Aug-2006 10:27:44 GMT - refresh now Site Report
Try out the Netcraft Toolbar!
FAQ
Netblock Owner
Universita' di Teramo
graph.
monitor. We will start
We will continue to monitor this host for a few days, to get enough values to plot a graph. After this time
Internet
Internet

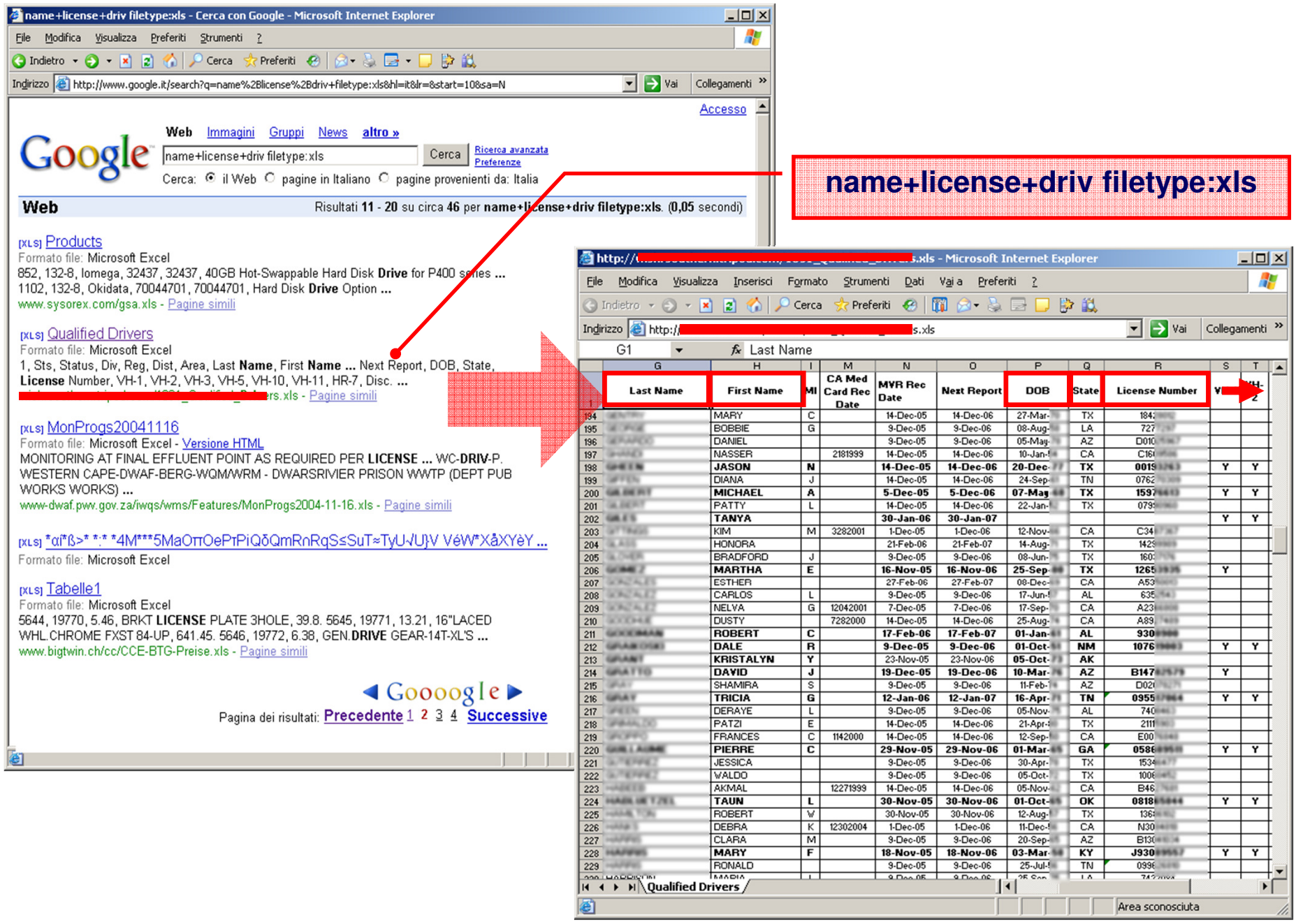

www.unite.it
Netcraft - Microsoft Internet Explorer
Site report for www.unite.it - Microsoft Internet Explorer
Webserver Search
Netcraft Services
News
Subscribe to Netcraft News
Security Services
Anti-Phishing Toolbar
Phishing Site Feed
Bank Fraud Detection
Phishing Site Countermeasures
Audited by Netcraft
Open Redirect Detection
Web Application Security Testing
Web Application Security Course
Internet Data Mining
Hosting Provider Switching
Toolbar
Netcraft
Site report for www.unite.it
Site http://www.unite.it
Last reboot unknown
Uptime graph
Domain unite.it
Netblock owner Universita' di Teramo
IP address 193.206.30.14
Site rank 283433
Country IT
Nameserver dns1.unite.it
Date first seen December 1996
DNS admin admin@unite.it
Domain Registry nic.it
Reverse DNS unknown
Organisation Universita' di Teramo, Italy
Nameserver Organisation Universita' di Teramo, Italy
Check another site:
Hosting History
Netblock Owner
IP address
OS
Web Server
Last changed
Universita di Teramo
193.206.30.14
unknown
Microsoft-IIS/6.0
16-Aug-2006
Universita di Teramo
193.206.30.14
FreeBSD
Microsoft-IIS/6.0
7-Mar-2006
Universita di Teramo
193.206.24.16
AIX
IBM_HTTP_Server/1.3.6 Apache/1.3.7-dev Unix
1-Jun-2001
COPYRIGHT © NETCRAFT LTD. 2004-6


Internet Archive - Mic
Internet Archive Wayback Machine - Microsoft Internet Explorer
Universit□egli Studi di Teramo - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo http://web.archive.org/web/20010526113720/http://www.unite.it/
Vai Collegamenti
UNIVERSITA
Le Facoltà
Giurisprudenza
Scienze Politiche
Avvisi di Gare
Socrates/Erasmus
Eventi OnLine
Arianna
Universit□egli Studi di Teramo.htm - Blocco note
File Modifica Formato Visualizza ?
saldare <BR>tutto ci□□e □ccaduto <BR>ad un'idea di futuro
? <BR>(anonimo) </FONT></TD>
<TD width=250 bgColor=#f7ebc3><FONT face=Verdana color=#800000
size=1> UNIVERSIT? DEGLI STUDI DI TERAMO<BR> Tel. 0861.2661 -
Fax 0861.245350<BR> http://www.unite.it<BR> e-mail:
webmaster@unite.it</FONT></TD></TR>
<TR>
<TD align=left width=250 bgColor=#f7ebc3><FONT face=Verdana color=#800000
size=1>  </FONT></TD>
<TD align=left width=260><FONT face=Verdana size=1> </FONT></TD>
<TD align=middle width=250 bgColor=#f7ebc3><FONT face=Verdana
color=#800000 size=1>  </FONT></TD></TR>
<TR>
<TD align=middle width=760 colSpan=3><FONT face=Verdana size=1><A
href="http://www.unite.it/Ateneo/Prospettive_aa_2001_2002.html"><IMG
height=23 src="" width=312 border=0></A></FONT> </TD></TR>
<TR>
<TD width=760 bgColor=#afd8d8 colSpan=3>
<DIV align=center>
<TABLE cellSpacing=1 cellPadding=0 width="100%" border=0>
<TBODY>
<TR>
<TD align=middle width="17%" bgColor=#ffffff><A
style="TEXT-DECORATION: none"
href="http://www.unite.it/Gare/Avvisi_Gare.html"><FONT face=Arial
color=#000000 size=1>Avvisi di Gare</FONT></A></TD>
<TD align=middle width="16%" bgColor=#ffffff><A
style="TEXT-DECORATION: none"
href="http://www.unite.it/Borse_di_Studio/Borse_di_Studio.html"><FONT
face=Arial color=#000000 size=1>Borse di Studio</FONT></A></TD>
<TD align=middle width="18%" bgColor=#ffffff><FONT face=Arial
size=1><A style="TEXT-DECORATION: none"
href="http://www.unite.it/Concorsi_PA/Concorsi_PA.html"><FONT
color=#000000>Concorsi</FONT></A></FONT></TD>
<TD align=middle width="17%" bgColor=#ffffff><FONT face=Arial
size=1><A style="TEXT-DECORATION: none"
href="http://www.unite.it/News/News2001.html"><FONT
color=#000000>News</FONT></A></FONT></TD>
<TD align=middle width="17%" bgColor=#ffffff><FONT face=Arial
size=1><A style="TEXT-DECORATION: none"
href="http://www.unite.it/Ateneo/labtel.html"><FONT
color=#000000>Laboratorio Televisivo</FONT></A></FONT></TD>
<TD align=middle bgColor=#ffffff><FONT face=Arial size=1><A
Internet



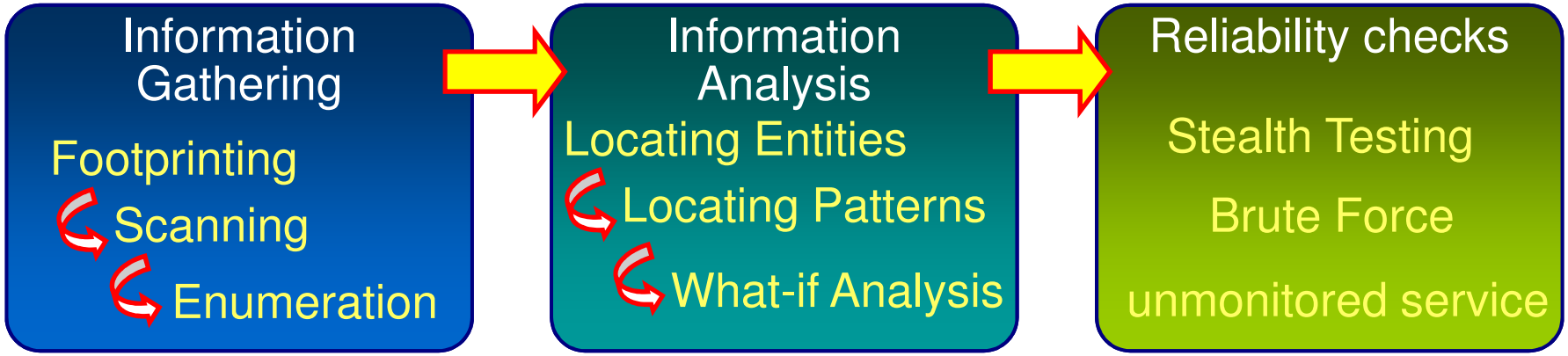

# Strategia di un Hacking


PROXY lists - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo Vai Collegamenti
PROXY lists
Welcome to SAS Proxy List Pages! For what purpose we run our proxy listings?
1. To help system administrators to find and close public access to proxy servers opened by mistake.
2. To help people stay anonymous in the internet. However before using public opened server you must to be sure that it is legal. You must remember that if you are using mistakenly opened server its administrator will find his mistake, sooner or later. DO NOT use servers from SamAir listings for illegal or malicious deeds!
Home: HTTP proxy lists: index.htm
HTTP anonymous proxy list
Rechecked: 08/29/06(mm/dd/yy) 07:13:50
Proxy judge used: http://samair.ru/cgi/textenv.pl
#1
201.234.158.8:6588 elite proxy Argentina (Buenos Aires)
201.235.208.14:6588 elite proxy Argentina (Munro)
203.19.28.243:80 anonymous Australia (Perth)
88.116.69.154:8080 elite proxy Austria (Aschach An Der Don
88.116.69.154:80 elite proxy Austria (Aschach An Der Don
24.231.34.33:8000 elite proxy Bahamas (Nassau)
130.104.72.200:3124 PlanetLab proxy Belgium (Louvain)
130.104.72.201:3124 PlanetLab proxy Belgium (Louvain)
200.220.217.82:8080 elite proxy Brazil (Belém)
150.165.15.19:3128 PlanetLab proxy Brazil (Campina Gran
201.20.118.24:6588 elite proxy Brazil (Fortaleza)
Operazione completata
Internet


name+license+driv filetype:xls - Cerca con Google - Microsoft Internet Explorer
http://www.google.it/search?q=name%2Blicense%2Bdriv+filetype:xls&hl=it&lr=&start=10&sa=N
Google
name+license+driv filetype:xls
Cerca
Web
Risultati 11 - 20 su circa 46 per name+license+driv filetype:xls. (0,05 secondi)
[XLS] Products
Formato file: Microsoft Excel
852, 132-8, Iomega, 32437, 32437, 40GB Hot-Swappable Hard Disk Drive for P400 series ...
1102, 132-8, Okidata, 70044701, 70044701, Hard Disk Drive Option ...
www.sysorex.com/gsa.xls - Pagine simili
[XLS] Qualified Drivers
Formato file: Microsoft Excel
1, Sts, Status, Div, Reg, Dist, Area, Last Name, First Name ... Next Report, DOB, State, License Number, VH-1, VH-2, VH-3, VH-5, VH-10, VH-11, HR-7, Disc. ...
[XLS] MonProgs20041116
Formato file: Microsoft Excel - Versione HTML
MONITORING AT FINAL EFFLUENT POINT AS REQUIRED PER LICENSE ... WC-DRIV-P. WESTERN CAPE-DWAF-BERG-WQM/WRM - DWARSRIVIER PRISON WWTP (DEPT PUB WORKS WORKS) ...
www-dwaf.pwv.gov.za/iwqs/wms/Features/MonProgs2004-11-16.xls - Pagine simili
Formato file: Microsoft Excel
[XLS] Tabelle1
Formato file: Microsoft Excel
5644, 19770, 5.46, BRKT LICENSE PLATE 3HOLE, 39.8. 5645, 19771, 13.21, 16"LACED WHL.CHROME FXST 84-UP, 641.45. 5646, 19772, 6.38, GEN.DRIVE GEAR-14T-XL'S ...
www.bigtwin.ch/cc/CCE-BTG-Preise.xls - Pagine simili
Pagina dei risultati: Precedente 1 2 3 4 Successive
name+license+driv filetype:xls
Microsoft Excel
Qualified Drivers
Area sconosciuta

# Carta di credito “legale”


Novelty Id: Italy Novelty ID Card Template Italy Driver License Sample - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro Cerca Preferiti
Indirizzo
Vai Collegamenti
ABOUT US
HOME
F.A.Q.
TESTIMONIALS
ORDER
CONTACT US
About Us
Home
Faq Answers
Testimonials
Australia Cards
Canada Cards
United States Cards
Student Cards
International Cards
Custom Design Cards
Adoption Certificates
Baptism Certificates
Birth Certificates
Death Certificates
Italy
ORIGINAL FORMAT
Order now
ORIGINAL PRODUCT DESIGNS USING A SIMPLE CARD CREATION PROCESS
Photograph
Full Name
Unique Number
Bar Codes
Signature Strip
Magnetic Strip
Holographic Image
UV Lighting
Security Seals
Biometric Data Storage
Internet




# Strategia di un Hacking

Reliability checks

Stealth Testing

Brute Force

unmonitored service

# PRINCIPALI TOOLS IN RETE :

**Dig** – discover the topology of all externally facing servers of a company. This includes redundant web servers, mail servers, load balancers, and firewalls.

**Fping** – PING UTILITY MOLTO VELOCE PER SCOPRIRE SERVER CONNESSI IN RETE.

**Nmap** – APPLICAZIONE MULTIFUNZIONALE PER L'ANALISI DELLA RETE .

**SuperScan** –TCP PORT SCANNER

**Queso** –APPLICAZIONE PER IDENTIFICARE IL SISTEMA OPERATIVO IN USO (SPESSOE' SUFFICENTE UN SOLA PORTA APERTA).

**Nessus** – LA PIU' FAMOSA APPLICAZIONE PER IL VULNERABILITY ASSESSMENT.

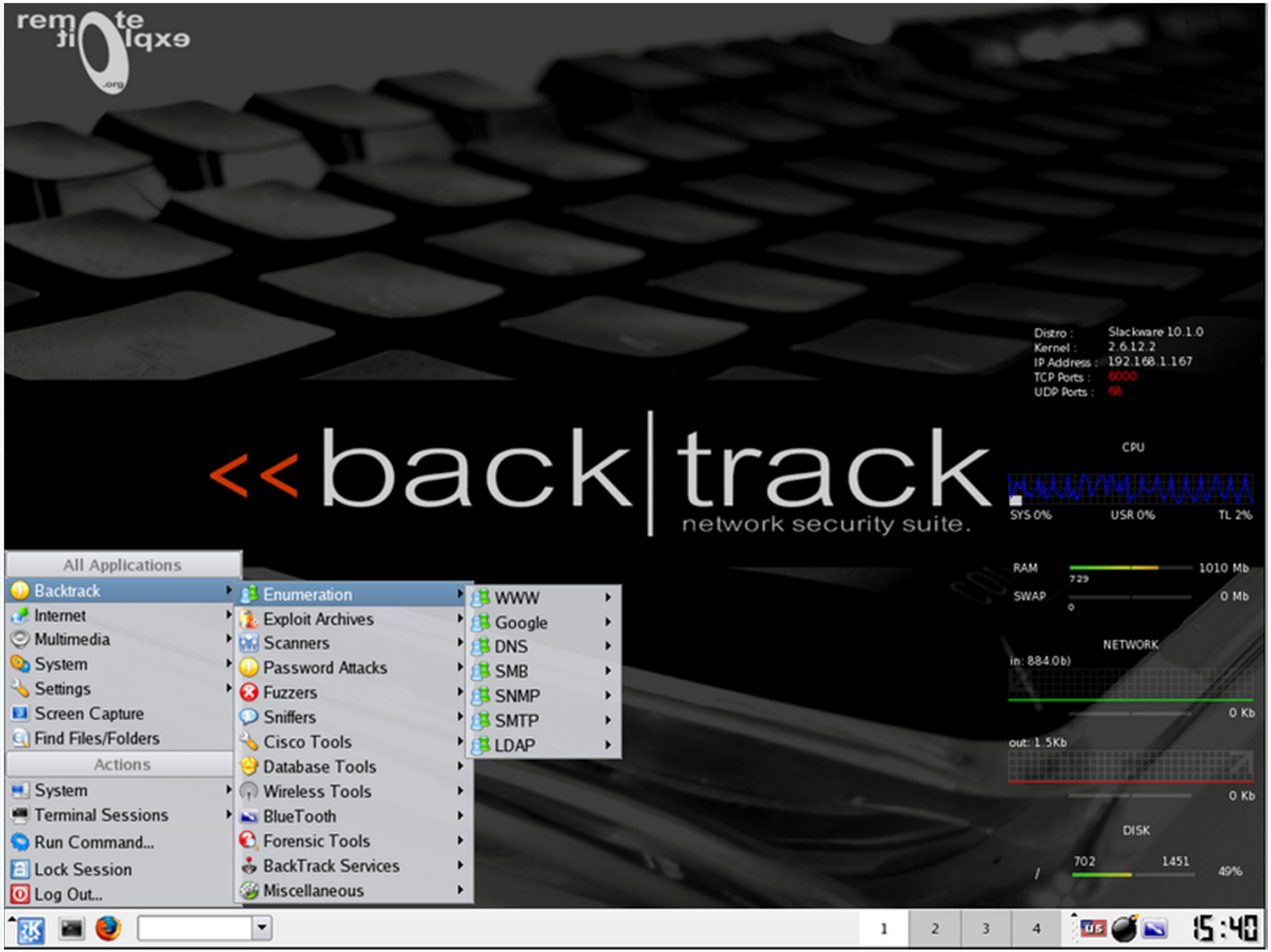
**Saint5** – ANALIZZATORE NON "INVASIVO" PER RETI E SISTEMI OPERATIVI. RICHIEDE UNA BUONA CONOSCENZA DI BASE

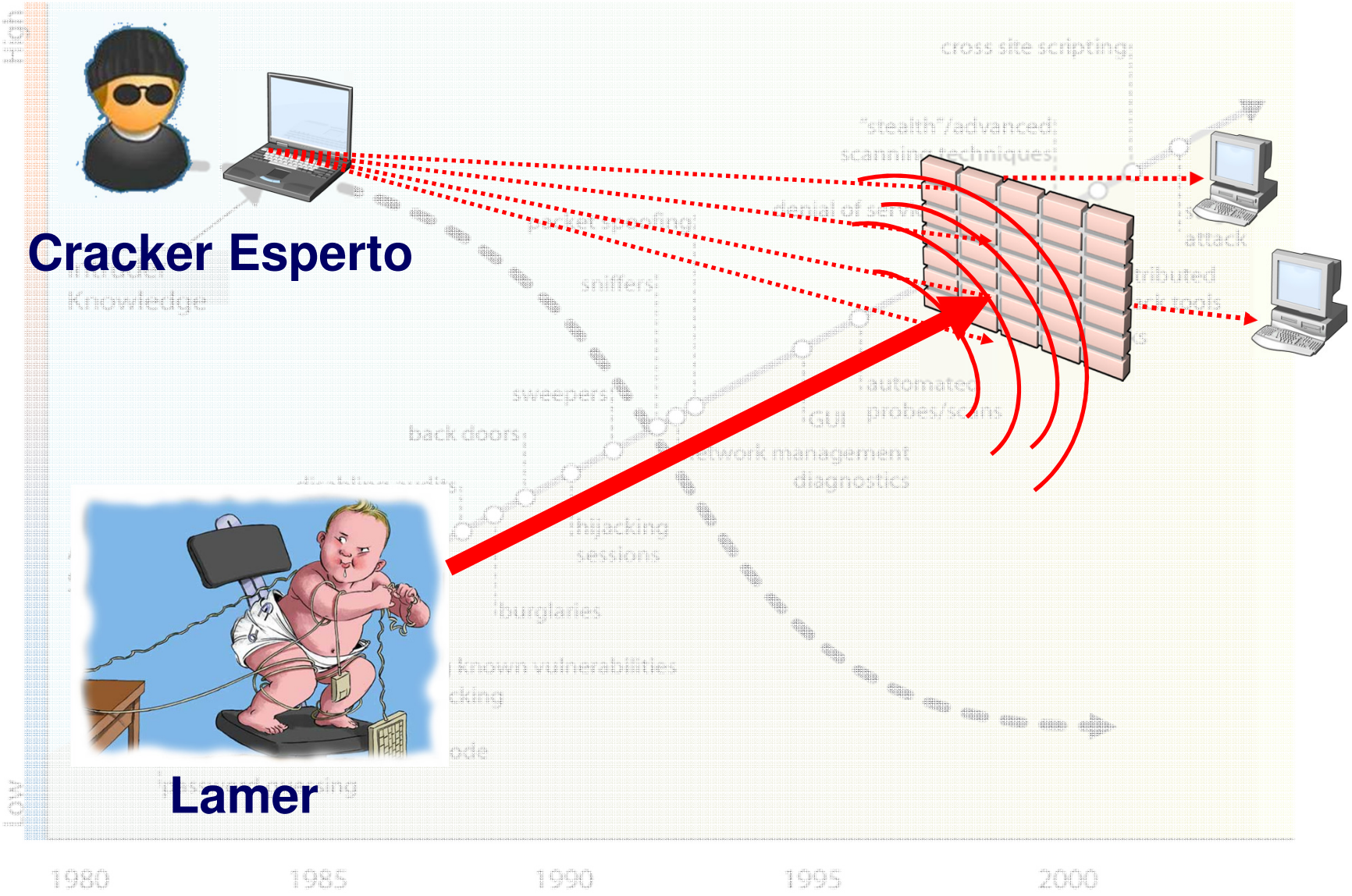
**Retina** – VULNERABILITY ASSESSMENT.

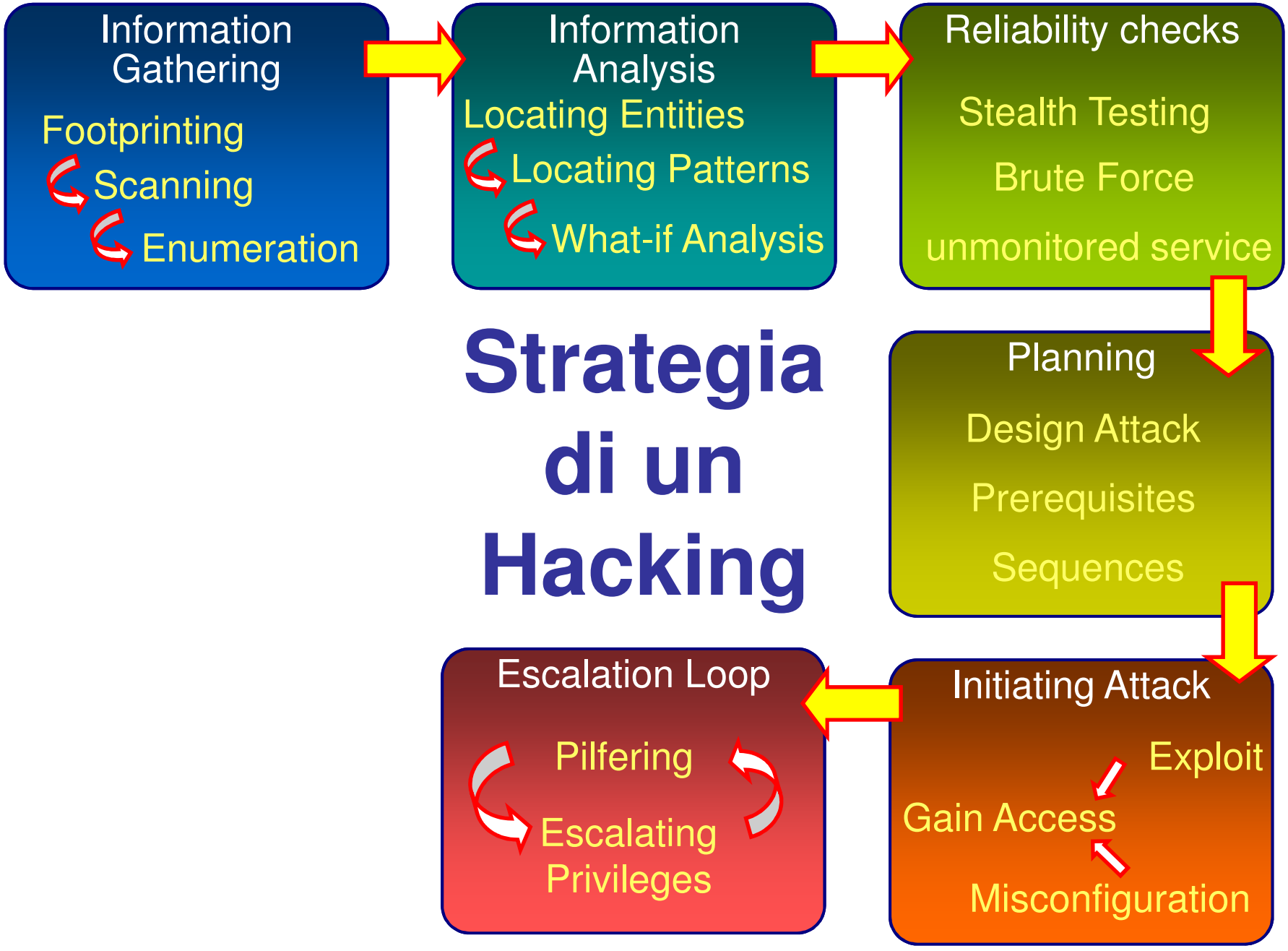
**Scando** – ANALIZZA IL SITO WEB OGGETTO DI ATTACCO E PROPONE PER OGNI PAGINA I POSSIBILI EXPLOIT A CUI POTREBBE ESSERE SOGGETTA (AD ES. SQL INJECTION, COOKIE TAMPERING, ETC.)

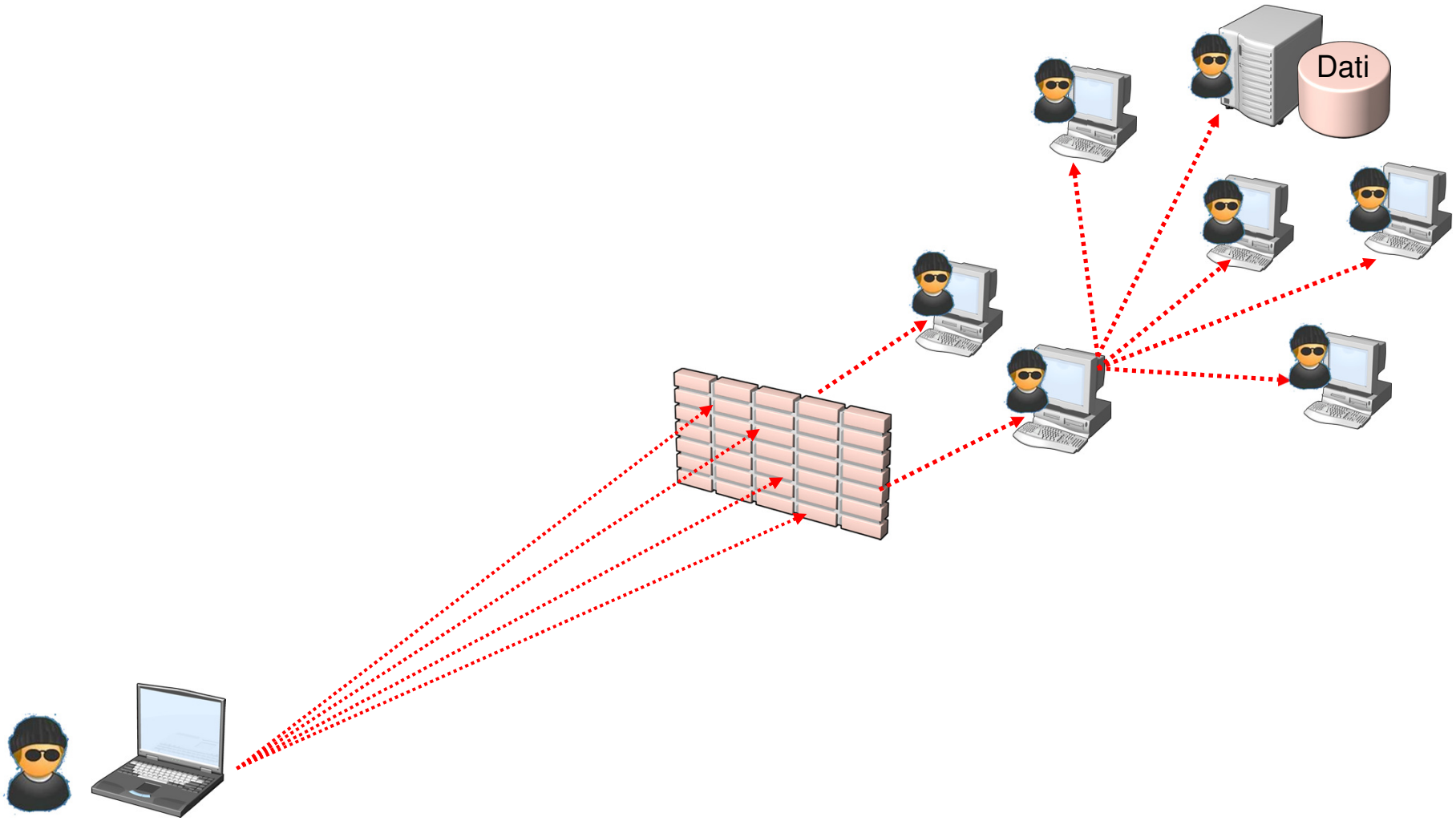
www.remote-exploit.org

## **BACKTRACK**: Distribuzione Linux su CDROM bootable con installati i principali tools per testare la sicurezza di sistemi e reti




Cracker Esperto
Lamer
cross site scripting
"stealth"/advanced
scanning techniques
sniffers
sweepers
back doors
GUI
automated
probes/scans
network management
diagnostics
hijacking
sessions
burglaries
known vulnerabilities
1980
1985
1990
1995
2000

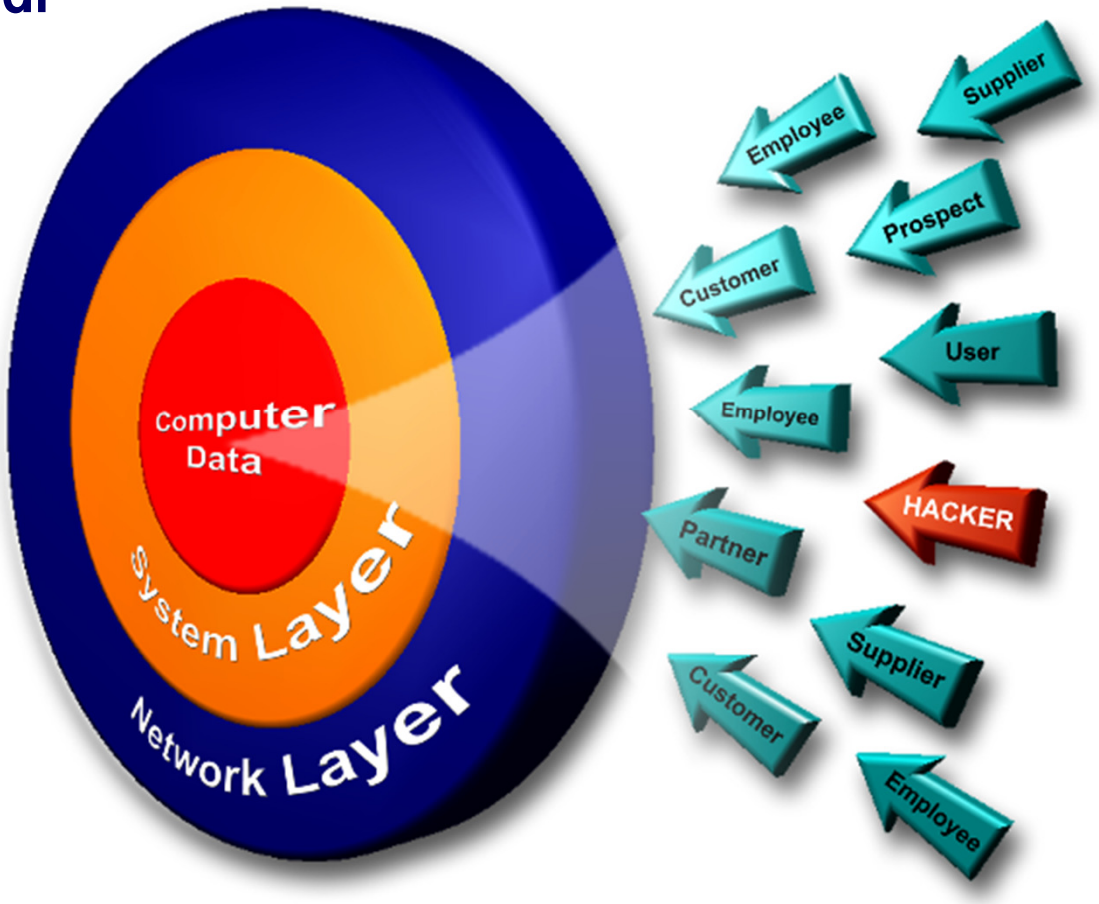

Information Gathering
Footprinting
Scanning
Enumeration
Information Analysis
Locating Entities
Locating Patterns
What-if Analysis
Reliability checks
Stealth Testing
Brute Force
unmonitored service
Strategia di un Hacking
Planning
Design Attack
Prerequisites
Sequences
Initiating Attack
Exploit
Gain Access
Misconfiguration
Escalation Loop
Pilfering
Escalating Privileges




# Cracker Esperto

**IL 70 % degli attacchi ai siti web ed alle applicazioni web delle aziende avviene a livello applicativo e non a livello di sistema o di rete**

**- Gartner Group**



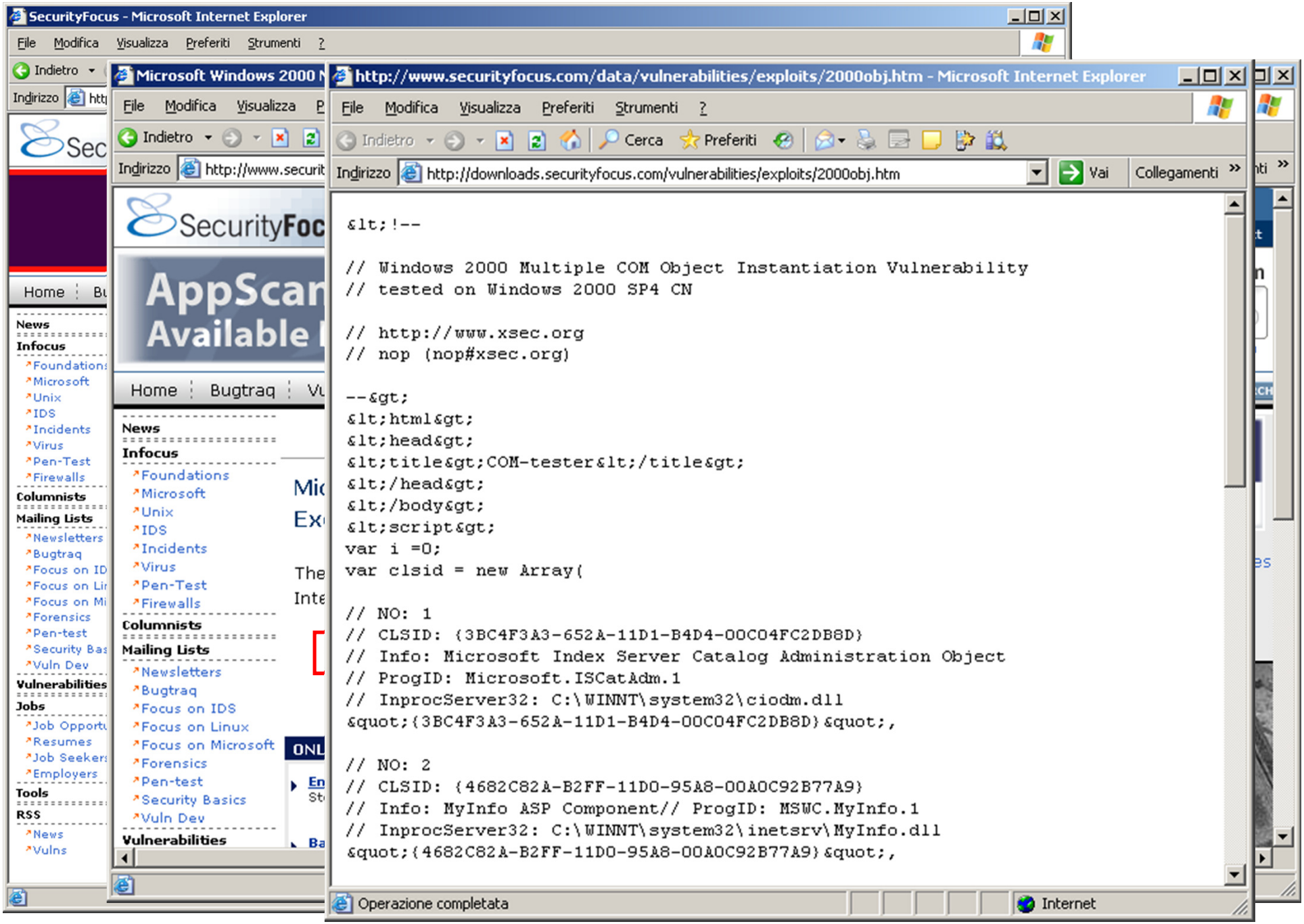

# Perché ?

- **Controlli di accesso deboli**
- **Configurazioni di default**
- **Le vulnerabilità sono facili da trovare**

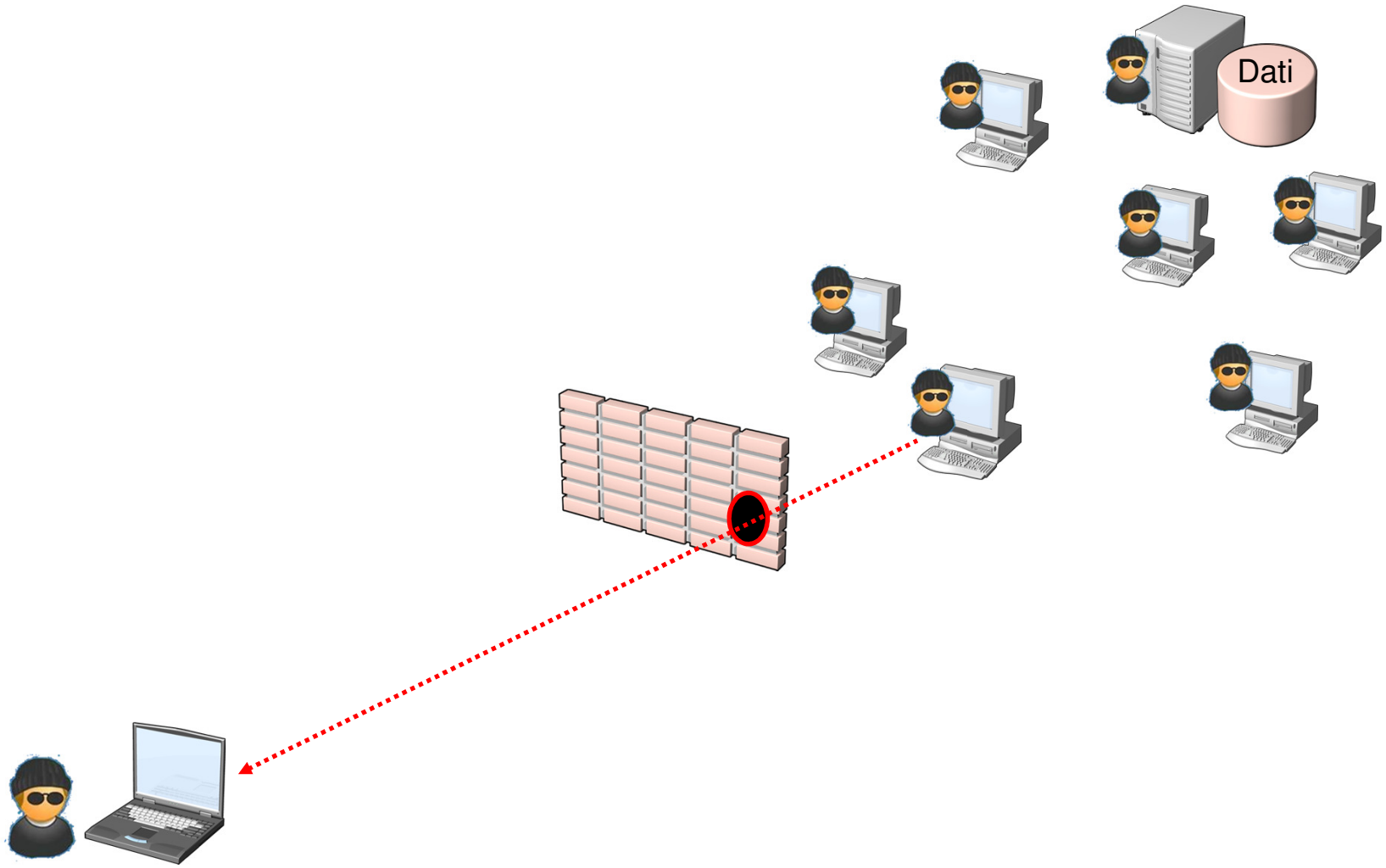
# Explotation

**Accesso alle informazioni necessarie per effettuare un exploit :**

- **BugTraq**
- **Hacker/Security websites**
- **www.securityinnovation.com**
- **www.securityfocus.com**
- **www.packetstormsecurity.com**
- **Vari PoC Code**
- **Vari Exploit Tools**

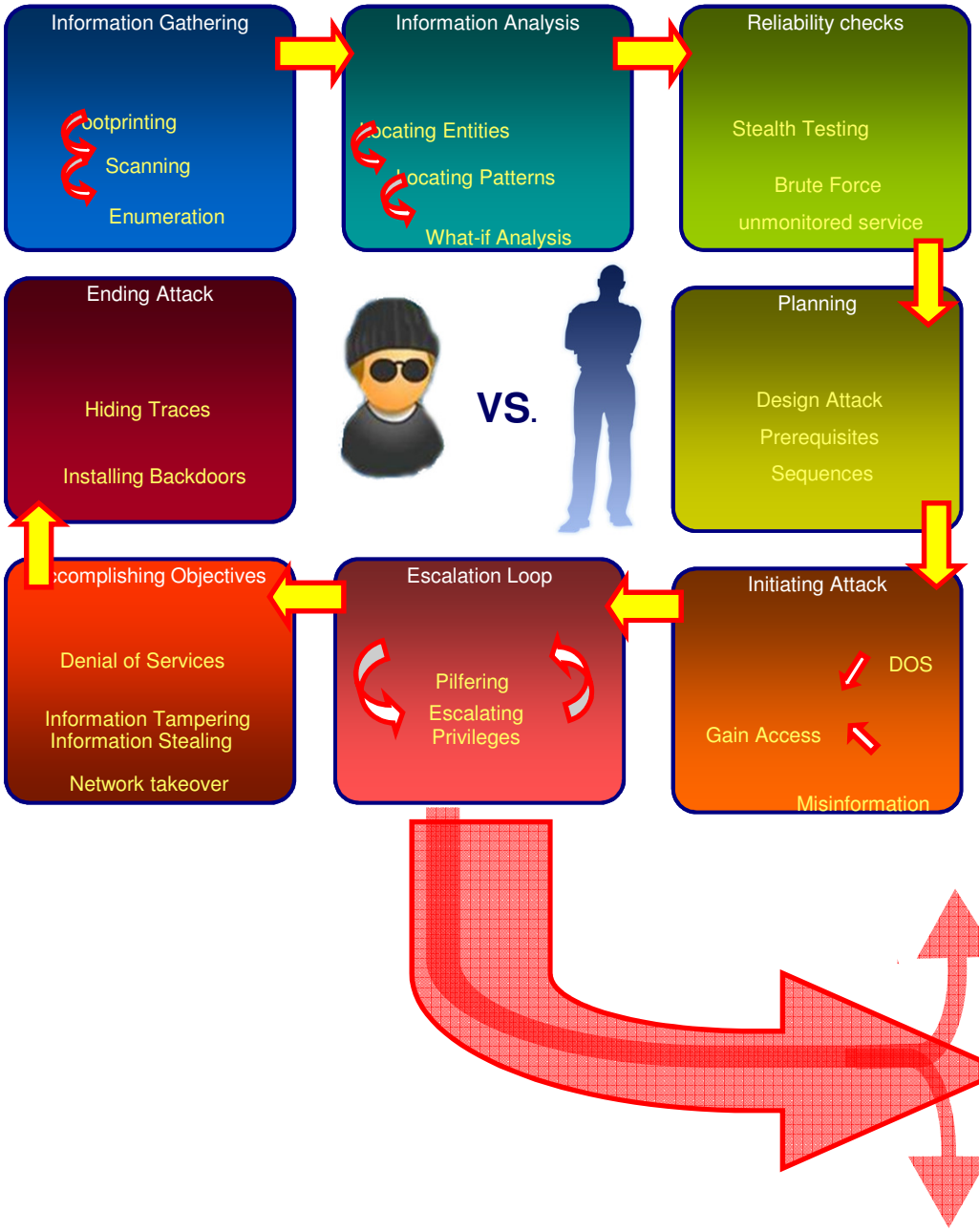

SecurityFocus - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Indietro
Indirizzo http://www.securit
Microsoft Windows 2000
http://www.securityfocus.com/data/vulnerabilities/exploits/2000obj.htm - Microsoft Internet Explorer
File Modifica Visualizza Preferiti Strumenti ?
Cerca Preferiti
Indirizzo http://downloads.securityfocus.com/vulnerabilities/exploits/2000obj.htm
Vai Collegamenti
<!--
// Windows 2000 Multiple COM Object Instantiation Vulnerability
// tested on Windows 2000 SP4 CN
// http://www.xsec.org
// nop (nop#xsec.org)
-->
<html>
<head>
<title>COM-tester</title>
</head>
</body>
<script>
var i =0;
var clsid = new Array(
// NO: 1
// CLSID: {3BC4F3A3-652A-11D1-B4D4-00C04FC2DB8D}
// Info: Microsoft Index Server Catalog Administration Object
// ProgID: Microsoft.ISCatAdm.1
// InprocServer32: C:\WINNT\system32\ciodm.dll
"{3BC4F3A3-652A-11D1-B4D4-00C04FC2DB8D}",
// NO: 2
// CLSID: {4682C82A-B2FF-11D0-95A8-00A0C92B77A9}
// Info: MyInfo ASP Component// ProgID: MSWC.MyInfo.1
// InprocServer32: C:\WINNT\system32\inetsrv\MyInfo.dll
"{4682C82A-B2FF-11D0-95A8-00A0C92B77A9}",
Operazione completata
Internet
Home Bugtraq
News
Infocus
Foundations
Microsoft
Unix
IDS
Incidents
Virus
Pen-Test
Firewalls
Columnists
Mailing Lists
Newsletters
Bugtraq
Focus on IDS
Focus on Linux
Focus on Microsoft
Forensics
Pen-test
Security Basics
Vuln Dev
Vulnerabilities


Information Gathering
Footprinting
Scanning
Enumeration
Information Analysis
Locating Entities
Locating Patterns
What-if Analysis
Reliability checks
Stealth Testing
Brute Force
unmonitored service
Planning
Design Attack
Prerequisites
Sequences
Initiating Attack
DOS
Gain Access
Misinformation
Escalation Loop
Pilfering
Escalating Privileges
Accomplishing Objectives
Denial of Services
Information Tampering
Information Stealing
Network takeover
Ending Attack
Hiding Traces
Installing Backdoors
Strategia di un Hacking




**Cracker Esperto**


Information Gathering
Footprinting
Scanning
Enumeration
Information Analysis
Locating Entities
Locating Patterns
What-if Analysis
Reliability checks
Stealth Testing
Brute Force
unmonitored service
Planning
Design Attack
Prerequisites
Sequences
Initiating Attack
DOS
Gain Access
Misinformation
Escalation Loop
Pilfering
Escalating Privileges
Accomplishing Objectives
Denial of Services
Information Tampering
Information Stealing
Network takeover
Ending Attack
Hiding Traces
Installing Backdoors
Strategia di un Hacking




# Ethical Hacker

# VS.

# Cracker