zone-h
unrestricted information

About Zone-H

zone-h unrestricted information

zone-h unrestricted information

Home News Archive Archive ★ Onhold Notify

FBI Jobs site gets hacked

10/09/2009 Written by Marcelo Almeida (Vympel)

"The FBI (Federal Bureau of Investigation) is seeking a senior security consultant for a permanent position." This is probably the next job offer that will appear on the FBI job site (fbijobs.gov) as they got defaced yesterday.

A turkish crew, known as turkguvenligi.info, managed to exploit a SQL injection flaw and insert a record that redirected the "events" page to an image with their site name.

One sided hacktivism (updated)

22/06/2009 Written by Roberto Preatoni

Since Zone-H started its mirroring activity of defacements, it always witnessed any sort of hacktivism. Sure, most of the times defacers are/were/will be just defacing *just for the pleasure of it* but when it comes the time of big protests related to world's events, we are used to see both regular defacers or improvized cyber protesters taking a stand and spell out their disappointments by posting something using the defacement media.

Because... yes.... defacement is a media, it has been proven in several occasion that by defacing just one well targeted website, defacers were capable to attract the attention of regular medias which were reporting his message to the world.

zone-h in numbers

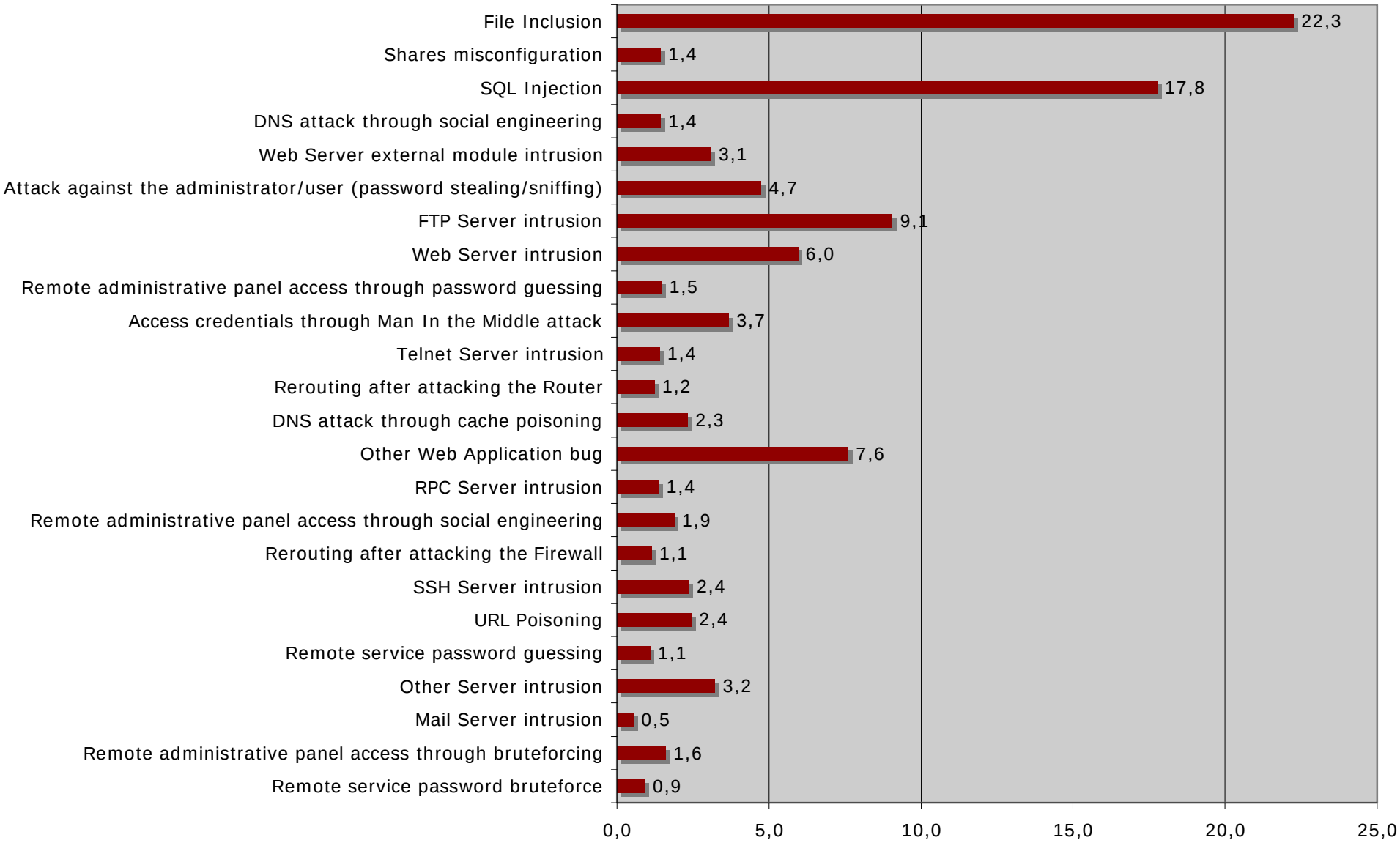
News: **4713**
Editors: **1**
Super Administrators: **2**
Operators:
Registered Users:
Downloadable Files:
Digital Attacks: **3447944**
Attacks On Hold: **1327**
Online Users:

search... Go

latest defacements

www.sonymusic.co.kr
balkanlarplastik.com
www.reseauenscene.fr
www.dominos.com.tw
www.notleyhigh.com
reg.hcu.ac.th
www.advancedscientifichealth.
www.pddd.pudong-edu.sh.cn
www.nvbar.org
www.trenton.k12.nj.us

Attacks techniques (%)



Hackers and such …

Whitehat Hackers

Good technical skills, good programmers, enjoy the intellectual challenge but no damages on systems. Knowledge is free for everyone.

Blackhat Hackers

Good technical skills and programmers but used to steal information, cause damages, and control the attacked system. Knowledge is for a small elite.

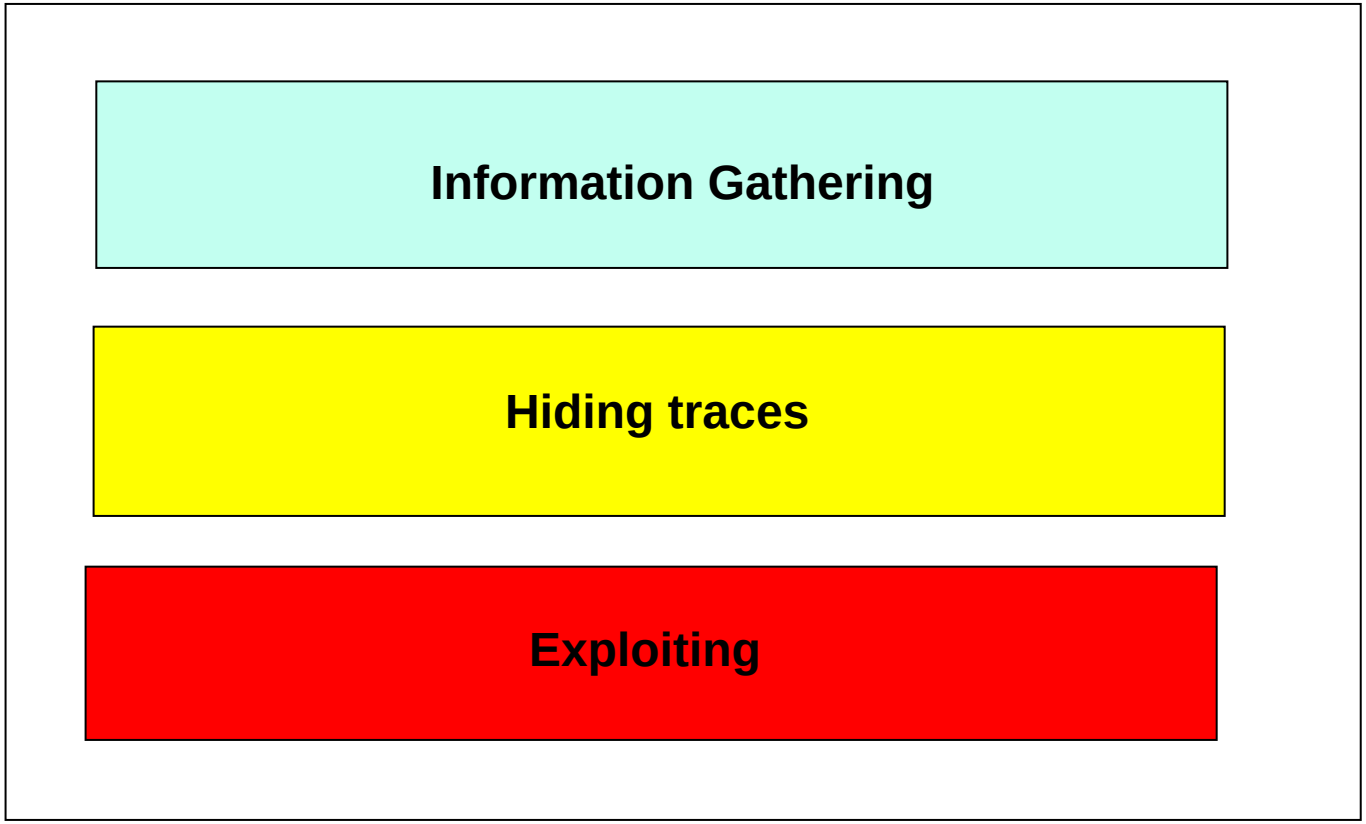
Crackers/Defacers/Script Kiddies

People with low technical and programming skills, usually teenagers, that use tools written by other people to cause damages and for self amusement.

Phreakers

Active on hacking telephone lines, originally mostly oriented to hardware hacking but nowadays turning to the digital side (VoIP).

Cyber Attack



Collecting information on our target

The most critical phases revolve around the accessibility of various online resources such as:

Internet Service Registration:
Registration and maintenance of IP addresses information

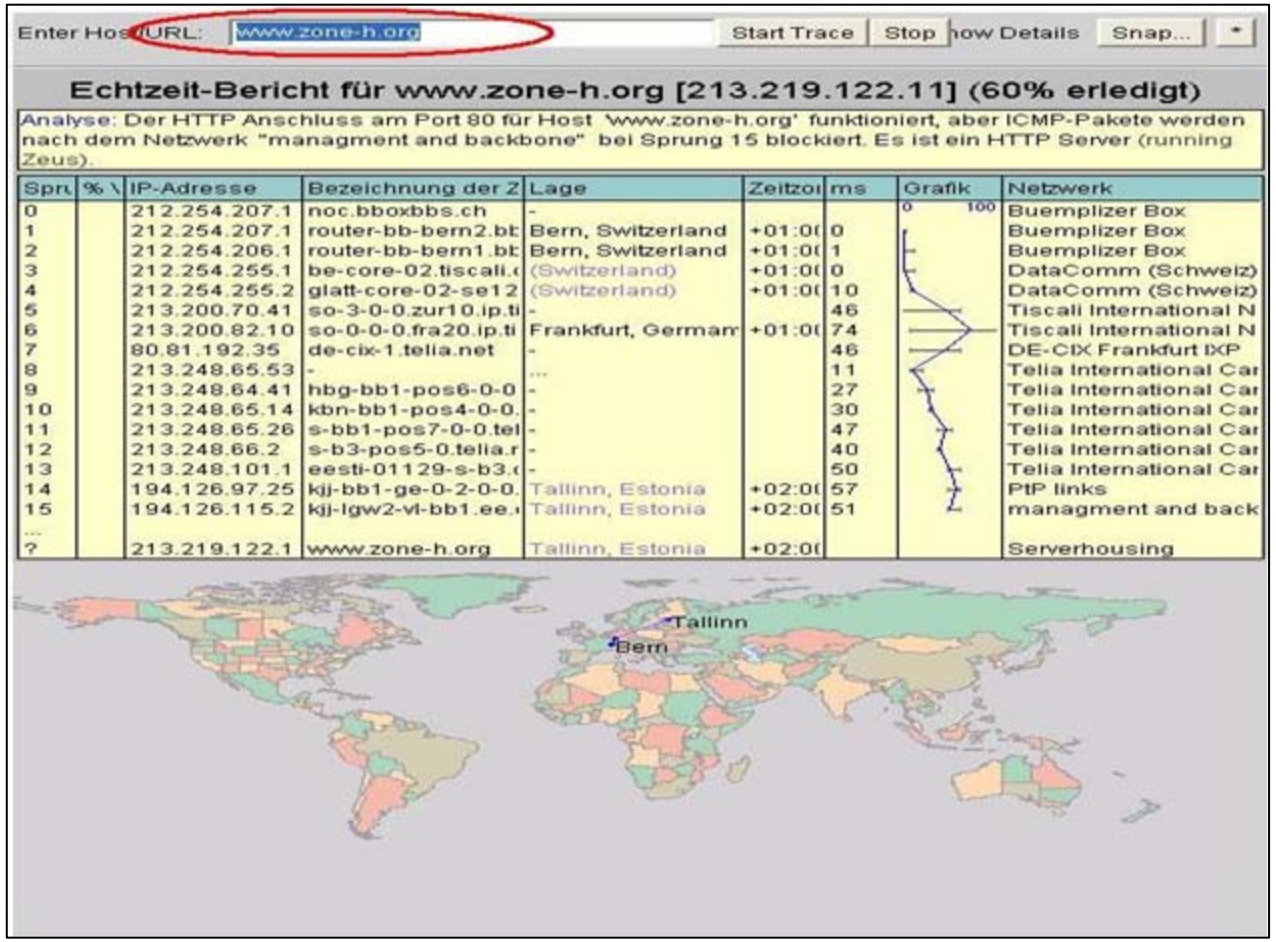
Domain Name System:
Registration and maintenance of host naming

Naming Conventions:
How an organization encodes or categorizes the name of machines or services

Email Systems:
Info contained inside email headers

Website Analysis:
Public information that may pose a risk to security

VisualRoute/TraceRoute



www.visualroute.ch

visualroute.visualware.com

Naming convention

It is important to analyze the names used to define each service.The naming convention used provides valuable insights into the use and position of hosts within an organization. Common naming convention includes:

Functional information (e.g. FW.acme.com for firewall, OWA.acme.com for exchange Web-mail interface, webdev.acme.com for developer webserver, etc.)

Network location information (fwDMZ.acme.com)

Physical location information or common location shorthand (e.g. NY - New York, LA - Los Angeles, etc.)

Operations system information (e.g. the Microsoft Windows 2003 as w2k3)

Hardware/model information (Cisco2611.acme.com)

Common sequences to identify servers (jupiter.acme.com, moon.acme.com)

Users name like (pc-bob.acme.com, smith-pc.acme.com)

Email info gathering

A lot of information about an organization can be gathered through analysis of its e-mail system.

Email headers provide insight into internal server naming, IP addresses, possible content filtering or anti-virus solutions, smtp server type, patch levels and even the version of the client's mail client.

How can we get this info ?

Through search engines or by sending an email to non-existent email addresses… And why?

…because returned error notification e-mails contain headers!

Hiding your traces

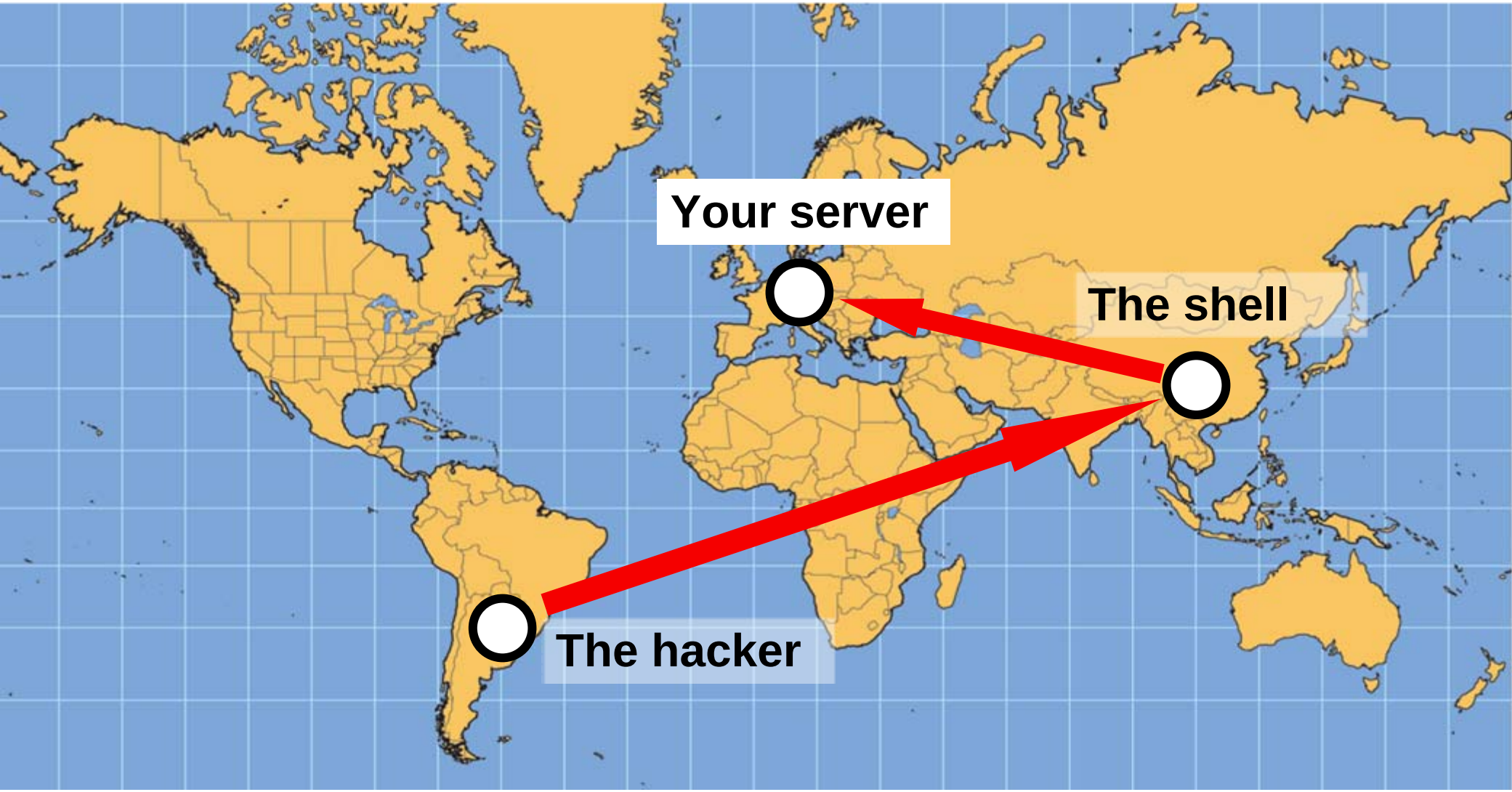
It is mandatory, for an attacker, to cover as much as possible his traces during all the phases of the attacking process, including the simple web based information gathering. In order to do so, several methods are available.

Proxies

Strategic shell bouncing

TOR

Strategic shell bouncing



Scanners

There are various categories of scanners, some available for free and some upon payment.

There are scanners just to test the network and the TCP/UDP layer, scanners to test generic vulnerabilities on systems (services) and scanners for specific daemons (like databases) or web applications.

IP/Port Scanners

IP scanners are designed to scan for active hosts or active services on a network. Port Scanners instead, are designed to search a network host for open ports. They are often used by administrators to check the security of their networks and by hackers to compromise it.

WINDOWS

Superscan - www.foundstone.com

Nmap - www.insecure.org

LINUX

Nmap - www.insecure.org

Hping - www.hping.org

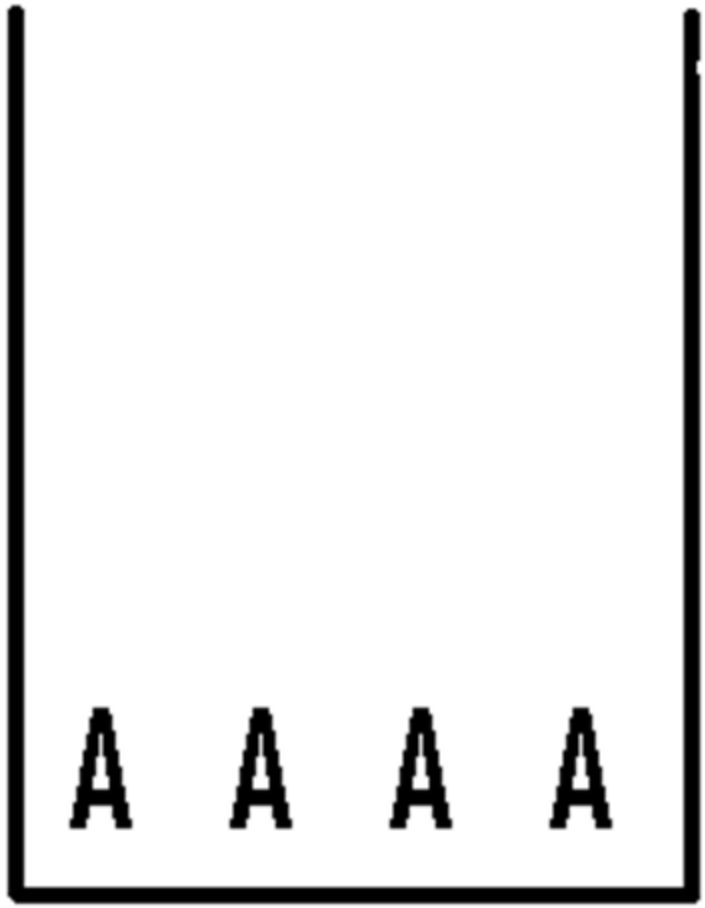
What is an exploit?

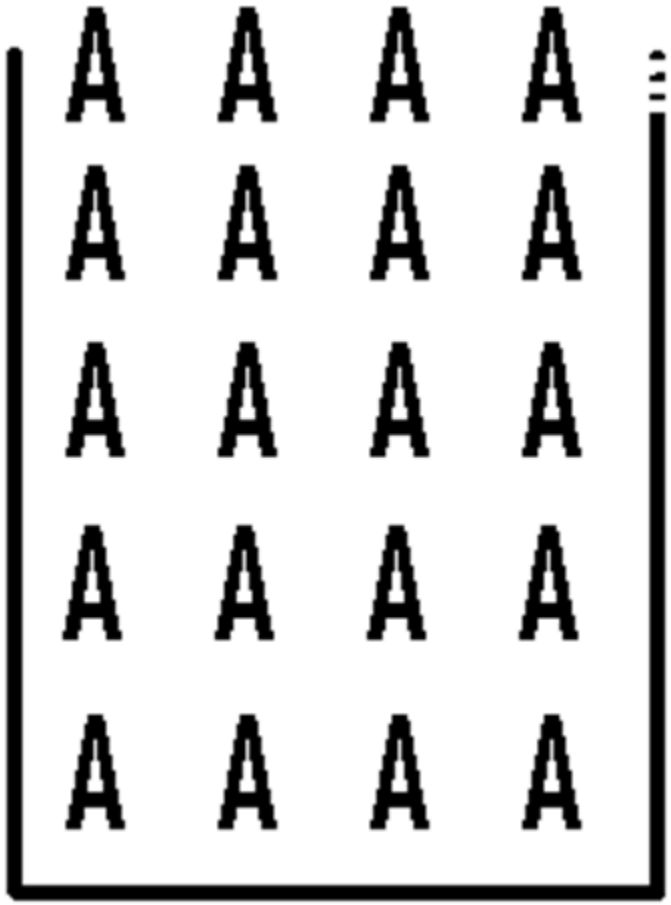
An exploit is a piece of software, a chunk of data, or sequence of commands that take advantage of a bug or vulnerability in order to get unintended or unanticipated behavior out of computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Example of vulnerable code

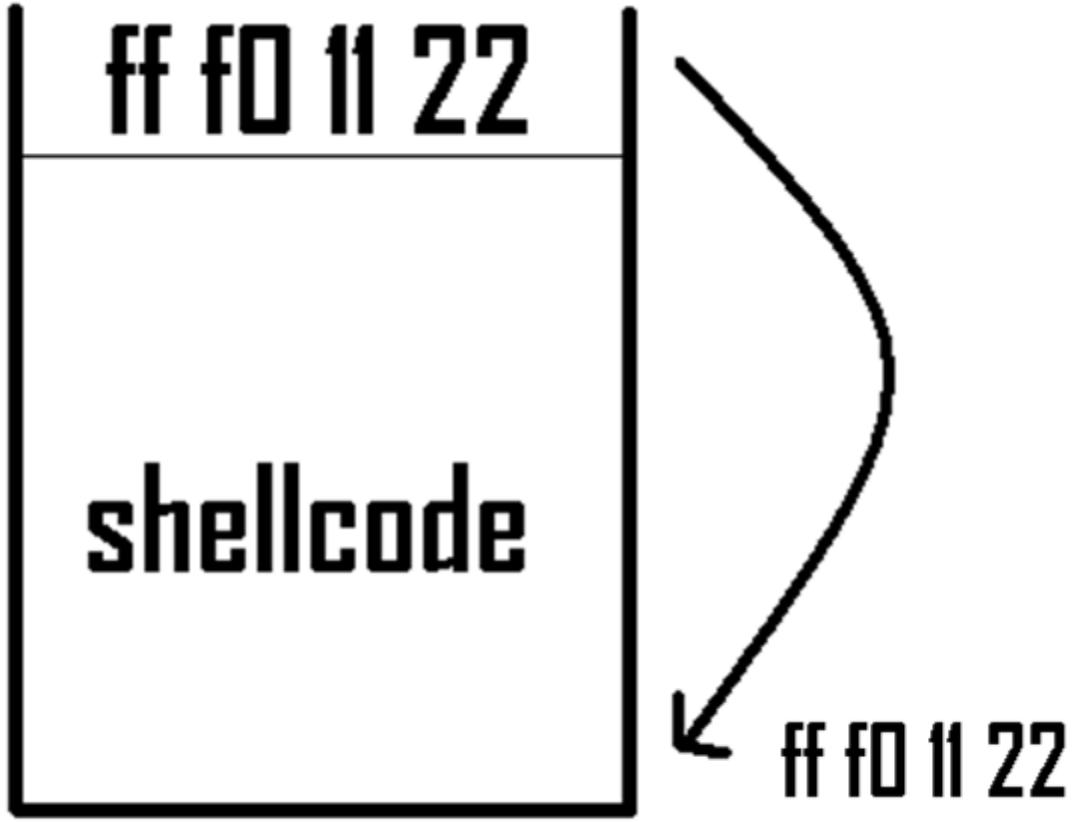

```
#include <stdio.h>
#include <string.h>

int main(int argc, char *argv[])
{
  char buffer[60];
  if (argc < 2)
  {
    fprintf(stderr, "USAGE: %s string\n", argv[0]);
    return 1;
  }
  strcpy(buffer, argv[1]);
  printf("Your text %s\n", buffer);
  return 0;
}
```


A A A A



0x61616161


ff f0 11 22
shellcode
ff f0 11 22

Buffer Overflows

A buffer overflow is a programming error which may result in a memory access exception and program termination, or in the event of the user being malicious, a breach of system security.

In details, it is an anomalous condition where a process attempts to store data beyond the boundaries of a fixed length buffer. The result is that the extra data overwrites adjacent memory locations. The overwritten data may include other buffers, variables and program flow data.

www.phrack.org/archives/49/P49-14