Vol III Issue VIII Feb 2014

Impact Factor : 2.2052(UIF)

ISSN No :2231-5063

International Multidisciplinary Research Journal

Golden Research Thoughts

Chief Editor
Dr.Tukaram Narayan Shinde

Publisher
Mrs.Laxmi Ashok Yakkaldevi

Associate Editor
Dr.Rajani Dalvi

Honorary
Mr.Ashok Yakkaldevi

IMPACT FACTOR : 2.2052(UIF)

Welcome to GRT

RNI MAHMUL/2011/38595 **ISSN No.2231-5063**

Golden Research Thoughts Journal is a multidisciplinary research journal, published monthly in English, Hindi & Marathi Language. All research papers submitted to the journal will be double - blind peer reviewed referred by members of the editorial board.Readers will include investigator in universities, research institutes government and industry with research interest in the general subjects.

Address:-Ashok Yakkaldevi 258/34, Raviwar Peth, Solapur - 413 005 Maharashtra, India
Cell : 9595 359 435, Ph No: 02172372010 Email: ayisrj@yahoo.in Website: www.aygrt.isrj.net

Golden Research Thoughts
ISSN 2231-5063
Impact Factor : 2.2052(UIF)
Volume-3 | Issue-8 | Feb-2014
DOI : 10.9780/2231-5063/382014
Available online at www.aygrt.isrj.net

PENTEST - DOUBLE BLIND AND VULNERABILITY

Watila Ramos Grachet and Fabrício Moraes de Almeida

Postgraduate in methodology and didactics of higher education (FIAR). Graduated in Pedagogy (UNITINS) and Technologist Systems Analysis (UNITINS).
PhD in Physics (UFC), with post-doctorate in Scientific Development Regional (DCR/CNPq).
Researcher of the Doctoral Program and a Masters Degree in Regional Development and Environment (PGDRA - UNIR).

Abstract:-This article deals with information security, essential for proper operation of any computer system criteria, such as confidentiality, security and availability must be prioritized in any IT system. And it has a literature approach to information security, and then is treated on the types of pentest, some methods footprint and fingerprint. Then we present the techniques used primarily for intrusion servers. Therefore, it is necessary to perform tests to diagnose possible vulnerabilities and fix them before someone malicious explore it. The gathering of information, knowledge of the environment and familiarity with the techniques used in pentest are paramount, because from then, the chances of success are higher. The tools (software) for pentest will be the basis for the test to be applied in a practical and results in success. The Pentest is done to find a vulnerability or gap in the system and find out as much as possible vulnerability to invasion and other types of attacks such as session hijacking, buffer overflow, pichamento and so on. Therefore, the research is important, since the topic provides reflections on the prevention of simulations of the possibilities of performing virtual crimes.

Keywords: Pentest. Vulnerability. Virtual crime. Forensic analysis.

1. INTRODUCTION

From the development of technology in recent years, the man has become increasingly dependent on it for common activities such as: buy, sell, pay bills etc.. And using the internet as the media often presents virtual crimes occur, which, unlike crimes of material scenario, the virtual environment in the evidence are not palpable, as they do not always stay in place so they can be analyzed. They can be erased with ease and just with the fact off an outfit some are already erased as Eleuterio and Machado (2010).

Thus, computerized testing environments require that they be not vulnerable to invasions and their systems work more safely. Thus, the Pentest - Double Blind - is a methodology used to test the vulnerability of an IT system.

The test is performed from the hiring company interested to, from then verify the security of your system, and if not discover existing vulnerability or vulnerabilities. This article starts with a literature survey on information security, then are treated on the types of pentest, some methods footprint and fingerprint. Then some techniques used primarily for the intrusion of servers are presented.

2. INFORMATION SECURITY

With the development of computer technology, the use of computers today is very common the use of web systems for Internet shopping, home banking, electronic documentation and others. As Eleuterio and Machado (2010), "Just like any other field of study, technological innovation brings a lot of benefits to people and the wider community. However, with the advantages, it also brings the possibility of realization of new illegal and criminal practices."

As the online Webster's Dictionary (2013) online the security word means," sf Action or effect to hold. / Situation that is safe; removal of all danger: travel safely. / Certainty, confidence, firmness: spoke safely. / Guarantee deposit: a mortgage is a real security, the security personal security. [..] ". This concept should be applied to any service information for both a provider of internet services such as the Home Banking, which a user uses to make a transfer. Therefore, the Information Security aims precisely to protect the information are the main assets of an organization or individual, as Abreu and Fernandes (2012), namely, "The benefits of information security are prevention of financial loss to the organization may have in the event of information security incidents . The organization can also shake your picture lawsuits or suffer the losses that can cause your systems to their customers”.

In addition, the criteria for maintaining the security of the enterprise or service information, to obtain the image of a safe company, should be analyzed according to the requirements of the standard ISO 27001 which defines some criteria for information security, among some of which are described below: Asset: anything that has value to the organization; Availability: the property of being accessible and usable upon demand by an authorized entity; Confidentiality: property that information is not available or disclosed to individuals, entities or unauthorized processes; information Security: preservation of confidentiality, integrity and availability of information; addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved and incident information security, namely a simple or a series of security events of unwanted or unexpected information, which have a high probability of compromising business operations and threatening information security .

The amount of digital crime is rife nowadays as Abreu and Fernandes (2012), “Every day we hear news of digital fraud losses of customer data, network intrusion sensitive information and systems for organizations that translate into losses of millions and millions of real. " And in Brazil the number of banking fraud and invasion of computers have greatly increased in recent years, as Abreu and Fernandes (2012) , or, "According to a study by the Internet Steering Committee in Brazil (see www.cert.br), Brazil is one of the largest emitters of spam and phishing, and fraud of this type have increased significantly. " and based on the above information, is a priority among professional information system implementation mechanism that eliminates the possibilities of implementation of these virtual crimes . Good practices are deployed from an antivirus program that installs itself without much difficulty to a complex firewall and IDS rules - system intrusion detection.

Among the practices used to prevent the Pentest systems - Penetration testing is a process of detailed analysis of the security level: system, network, servers, etc., using the prospect of an offender. Being a realistic test of the level of security of the infrastructure and the information that they hold, these technical and conceptual vulnerabilities of target infrastructure are tested.

As Giaviroto and Santos (2013):

"Defined as Penetration testing, it is a method to test and find vulnerabilities on a network or operating systems. At this stage, are analyzed and explored all the possibilities of vulnerabilities. Pentest inserts methods of safety evaluation in a computer system or network by applying simulations of attacks like a malicious stranger in order to compromise a system. Such Pentest allows you to check the actual structure of the system, which is searched in all areas related to the security structure."

Thus, the main goal is to simulate the Pentest controlled way a real attack that is usually run by criminals. Based on this test it is possible to have full knowledge of what could happen if this attack was executed by a malicious person, thus ensuring the possibility of a prevention strategy.

2.1 – Types Pentest

The types of pentest define how the test will run as Giaviroto and Santos (2013) describe the following types:

(a)Blind: In this procedure, the auditor has no target information system that will attack.
(b)Double Blind: In this procedure, the auditor also has no target information system that will attack. The target system does not know who will be attacked, and the pentest that will be applied by the auditor in the structure of the target system analyzed.
(c)Gray Box: In this procedure, the auditor has a partial knowledge of the target system that you have information that will be attacked, and the tests to be applied by the auditor.
(d)Double Gray Box: In this procedure, the auditor has partial knowledge of the target system, and has information that will be attacked, but was not aware of tests that will be used to scan in order to obtain specific information.
(e)Tandem: in this procedure, the auditor has full knowledge about the target system to be analyzed and is aware that he will be attacked and what procedures to be adopted for achieving these attacks.
(f) Reversal: In this procedure, the auditor has full knowledge about the target system to be analyzed, but he has no conscience to be attacked, as well as the procedures to be adopted while conducting the attacks.

For this work will be used as the base Double Blind method, which is most similar realized with the occurrence of an attack, as the target does not know who will be attacked inhibits the ability of system administrators to apply patches to fix patches Securities and update services, in order to prepare for an attack.

However, the attacker must gather information about the target and does not know when the attack will take place and even what kind will be made. So, how is the model adopted for pentest will be crucial to describe the existing safety level on the target system.

2.2 Survey information about the target to be tested (Footprint)

The first phase of intrusion test is part of the collection of the information of the target to be attacked, according Giaviroto and Santos (2013), "At this stage, nothing can be ruled out. We apply 90% of our work. The more information related to our goal, the greater likelihood of access to our audited system. "

To Giaviroto and Santos (2013) the footprint is:

"recognition (or footprinting) is the methodology used to obtain information about a given subject or company. The recognition technique comes from military tactics in which the land is strategically studied before it is attacked by recognizing the attacker can equip of important information related to the target and thus minimize doubts."

To achieve the proposed objective is necessary, in most cases, use of all available resources and, in the case of gathering information, it is important to describe some of the techniques and methodologies used for more footprint.

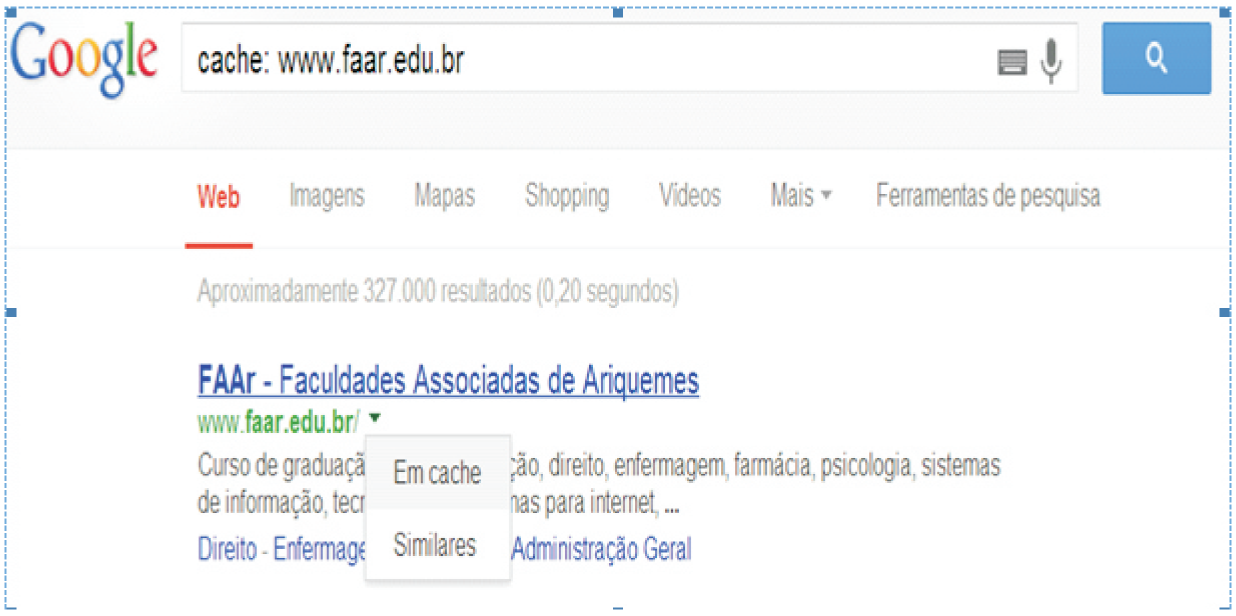
2.3 Google Hacking

In research it is evident that one of the tools most used by Internet search site is the "Google", both the speed of response and quantity of results. According to Carmona (2004), Google is a powerful search engine on the Internet that provides fast and easy access to any type of information available in Large Network in any corner of the world.

Being easy to use and rewarding giving research results are not difficult to imagine that the same tool could be used by people interested in acquiring information for invasion or strokes and so on. And also for administrators and TI professionals. The second Google Carmona (2004) is essentially a search engine for words and links all over the Internet, using various filtering capabilities and cataloging results. The most common term found in the document when it comes to using this to hack something is "Google hacking" which according to Wikipedia Google Hacking is the activity of using the site search capabilities, aiming to attack or better protect information of a company as this information is available on the web servers of the company will probably be in the databases of Google.

Google has several possible being used for a pentest and exactly why it is considered the best tool for hackers resources, as it allows access to all kinds of information one wants. Using as an example, the use of "cache" Google, where it stores older versions of every site that was once indexed by their robots, and possible future research as an image below showing a simple survey of the FAAR the site, which is fetched pages cached, conforms presented in Figure 01.

Figure 01 - Results of the query cache.



cache: www.faar.edu.br

Aproximadamente 327.000 resultados (0,20 segundos)

FAAr - Faculdades Associadas de Ariquemes

www.faar.edu.br/

Curso de graduaçã ção, direito, enfermagem, farmácia, psicologia, sistemas de informação, tecr nas para internet, ...

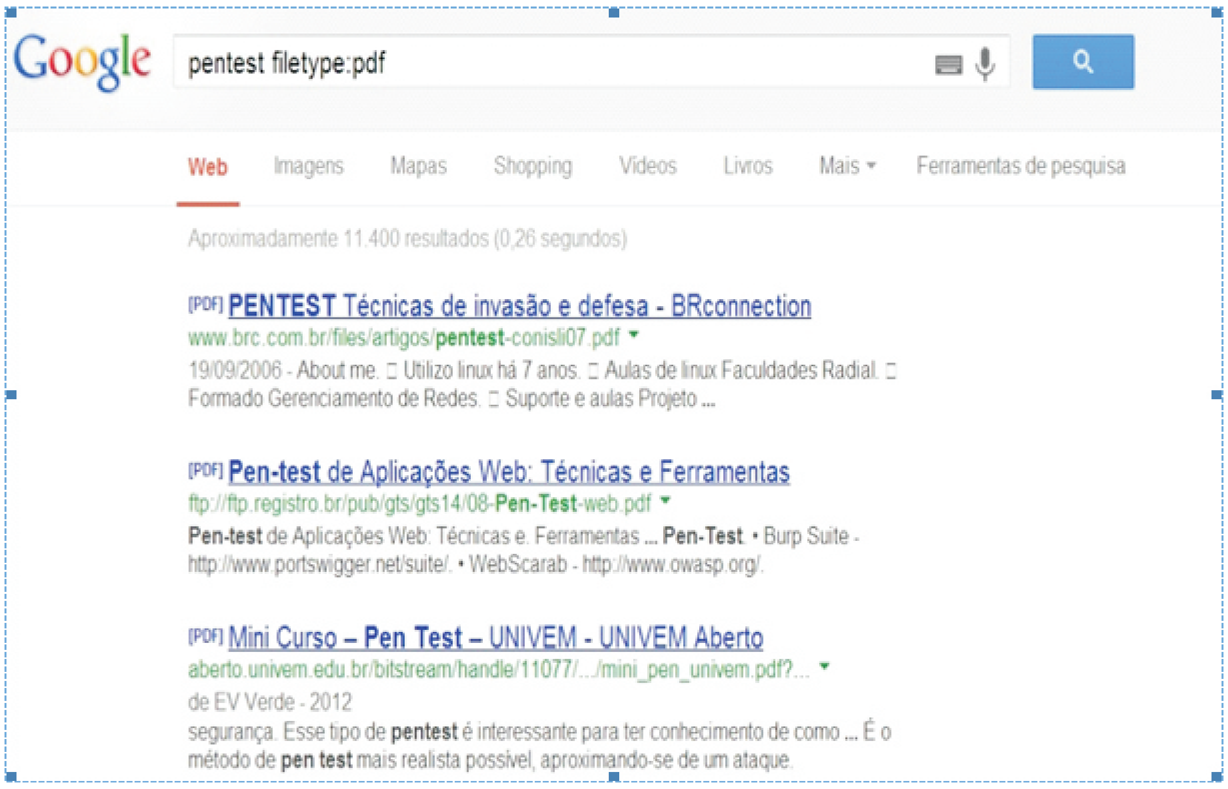
Direito - Enfermage Administração Geral

Source by: Grachet (2013).

As shown in Figure 01 , this feature allows access to pages that have already been taken from the air, provided that the database Google . Imagine that at some point in the history of an organization's site, a more sensitive information was available on the web. After a while, the programmer having been alerted that information removed from the site. However, if the page on the site has already been indexed by Google, it is possible that it has been altered or removed, can still access it using the feature "cache" Google.

This is just a simple Google feature that can be very useful when it comes to information gathering, but still have many more that can be more important than others see this sample code to the search filter: (a) Filetype: type (type is the type of file can be avi, doc, xls, mdb, jpg and etc.), eg pentest filetype: pdf, the search will be performed in order to find pdf files;

Figure 02 - Results of query using the site Google Hacking.



pentest filetype:pdf

Aproximadamente 11.400 resultados (0,26 segundos)

[PDF] PENTEST Técnicas de invasão e defesa - BRconnection
www.brc.com.br/files/artigos/pentest-conisli07.pdf ▾
19/09/2006 - About me. □ Utilizo linux há 7 anos. □ Aulas de linux Faculdades Radial. □ Formado Gerenciamento de Redes. □ Suporte e aulas Projeto ...

[PDF] Pen-test de Aplicações Web: Técnicas e Ferramentas
ftp://ftp.registro.br/pub/gts/gts14/08-Pen-Test-web.pdf ▾
Pen-test de Aplicações Web: Técnicas e. Ferramentas ... Pen-Test. • Burp Suite - http://www.portswigger.net/suite/. • WebScarab - http://www.owasp.org/.

[PDF] Mini Curso – Pen Test – UNIVEM - UNIVEM Aberto
aberto.univem.edu.br/bitstream/handle/11077/.../mini_pen_univem.pdf?... ▾
de EV Verde - 2012
segurança. Esse tipo de pentest é interessante para ter conhecimento de como ... É o método de pen test mais realista possível, aproximando-se de um ataque.

Source by: Grachet (2013).

resume+socialsecurity+id+name –> we already have a lot of information of this person; (c) site:gov.br ext:sql -> search for a specific server; (d) inurl:e-mail filetype:mdb ; (Search search files in email format. mdb); (e) inurl:intranet + intext:"phone number"; (This research seeks phones available in intranet found by Google); (f) inurl:8080 -intext:8080 Encontrando VNC - (Detecting systems using port 8080); (g) intitle:VNC inurl:5800 intitle: - (VNC finding VNC); (h) intitle:"VNC Viewer for Java"; (i) "Active Webcam Page" inurl:8080 -(Finding Webcam on); (j) intitle:"toshiba network camera - User Login" - (Finding Webcam da Toshiba) e (l) "Apache/1.3.20 server at" - (Finding Apache 1.3.20:)

2.4 Possible flaws in web applications:

allinurl:".php?do="
allinurl:".php?content="
allinurl:".php?meio="
allinurl:".php?produto="
allinurl:".php?cat="; intitle: login; return all pages with login in the page title, according to Carmona (2004, P. 71):

"Another of the intitle command that makes the joy of crackers: everyone who works with networks know that the Telnet service (TCP port 23), FTP side (TCP port 21) is one of the most insecure of the history of network services. In turn, Microsoft has a remote administration service, Terminal Server, which uses a lot of Telnet and is used to administer Windows 2000 machines in areas of local networks, but also to manage remote hosts (on other networks, or connected directly to the Internet). A cracker looking for specific servers running Windows 2000 Server, you can do a Google search using the following parameter intitle: Terminal Server Connection Webs."

The amount of possibilities to test is vast, enabling interested panning what interests you most and provided this knowledge to run a data collection via the web, locating a huge range of information, which are personal, business both as a platform particular system or site was developed. However in the example of the above quote is very difficult to make an invasion via browser, but we know that is a vulnerability that can be exploited.

2.5 Social Engineering

Currently, much quoted when it comes to information security, the term social engineering became known in 1990, by Kevin Mitnick. This is used to practices carried out in order to obtain confidential or sensitive information of companies, people and information systems. Where the practitioner explores people's trust to cheat them.

You can also define social engineering as the art of manipulating people in order to bypass security devices or building methods and strategies to lure people using information transferred by them in order to gain their trust for information. (SILVA, 2008).

Among the various meanings and interpretations given to the term "Social Engineering", cannot fail to mention that:

“Social engineering is the science that studies how knowledge of human behavior can be used to induce a person to act according to his wishes. It is not hypnosis or mind control, social engineering techniques are widely used by detectives (for information) and magistrates (to see if a deponent speaks the truth). It is also used to achieve all types of fraud, including invasion of electronic systems. (Konsultex 2004 apud PEIXOTO, 2006, p. 4)”.

When it comes to social engineering, then a question arises, what is the relationship between information security and social engineering, since the systems are full of IDS, Antivirus, Firewall and so on.? To respond is important to describe what Kevin Mitnick describes in your book "The Art of cheating”:

“A company may have purchased the best security technologies that money can buy, can have its staff trained so well that they lock all the secrets before going away and may have hired guards to the building on best security company that exists. Yet the company still vulnerable. Individuals can follow each of the best practices recommended by security experts, can install every recommended security product very well and watching proper system configuration and implementation of security patches. These individuals are still completely vulnerable. (MITNICK; SIMON, 2003, p 3).”

So it's not just technology that an institution must have to perform information security but also privacy and local officials, as the survey information of an institution can be easy if the person who has access to equipment and information not watch the confidentiality of these probably put all security at risk.

In intrusion test social engineering should be implemented (depending on the case), since in everyday life no hacker or malicious person would take advantage of this feature for whatever common sense, and above all because it is a vulnerability found in the institution.

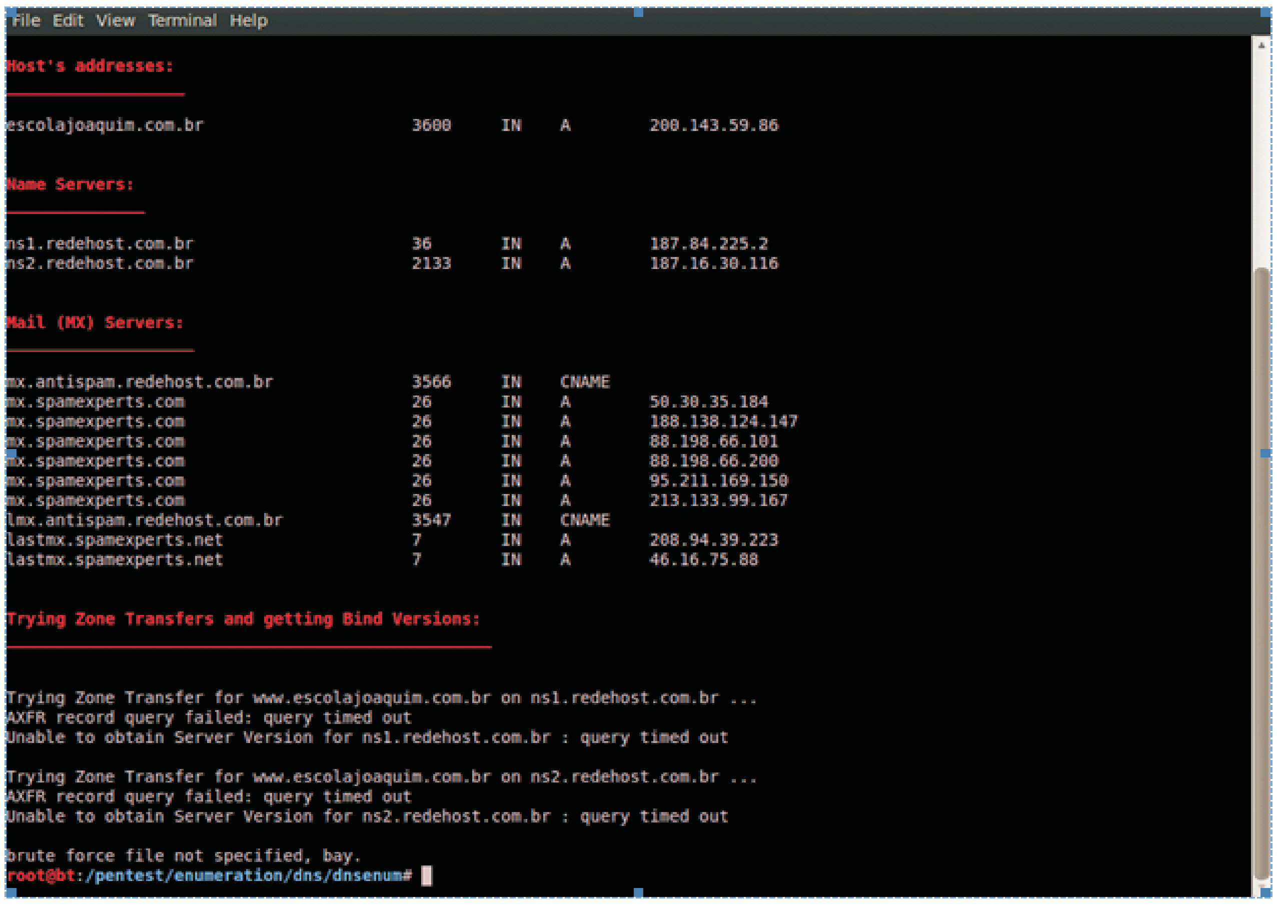
2.6 Domain information

When the intrusion test is done on a website or even a company that has a system on the web, which is extremely important to make a research on the DNS (Domain Name System - Domain Name System) as Giaviroto and Santos (2013), DNS is a database of information used in resolving names, translates IP addresses into domain names, and if this service is configured incorrectly, can provide critical information about a particular organization. The tools that will be used for this research are: NSLOOKUP, DNSENUM and FIERCE. To not extend much the item will be displayed just the photo of the implementation of a tool. The tool to be tested is the NSLOOKUP, user will be tested on a site own responsibility www.escolajoaquim.com.br. The command was executed in BackTrack:

```
root@bt:/pentest/enumeration/dns/dnsenum#
./dnsenum.pl www.escolajoaquim.com.br
```

Below that with this simple command you can find out the address of the site that serves uses, and many other information that apparently does not matter much, however, joined the others, can be of great importance to data collection, and if there some vulnerability can now be discovered at this stage easily.

Figure 03 - Results of a consultation with the software DNSENUM.



```
Host's addresses:
__________________

escolajoaquim.com.br                      3600     IN    A        200.143.59.86


Name Servers:
______________

ns1.redehost.com.br                       36       IN    A        187.84.225.2
ns2.redehost.com.br                       2133     IN    A        187.16.30.116


Mail (MX) Servers:
___________________

mx.antispam.redehost.com.br               3566     IN    CNAME
mx.spamexperts.com                        26       IN    A        50.30.35.184
mx.spamexperts.com                        26       IN    A        188.138.124.147
mx.spamexperts.com                        26       IN    A        88.198.66.101
mx.spamexperts.com                        26       IN    A        88.198.66.200
mx.spamexperts.com                        26       IN    A        95.211.169.150
mx.spamexperts.com                        26       IN    A        213.133.99.167
lmx.antispam.redehost.com.br              3547     IN    CNAME
lastmx.spamexperts.net                    7        IN    A        208.94.39.223
lastmx.spamexperts.net                    7        IN    A        46.16.75.88


Trying Zone Transfers and getting Bind Versions:
_________________________________________________


Trying Zone Transfer for www.escolajoaquim.com.br on ns1.redehost.com.br ...
AXFR record query failed: query timed out
Unable to obtain Server Version for ns1.redehost.com.br : query timed out

Trying Zone Transfer for www.escolajoaquim.com.br on ns2.redehost.com.br ...
AXFR record query failed: query timed out
Unable to obtain Server Version for ns2.redehost.com.br : query timed out

brute force file not specified, bay.
root@bt:/pentest/enumeration/dns/dnsenum#
```

Source by: Grachet (2013).

Other programs used for this test were: DNSENUM and FIERCE both installed by default in BackTrack 5 R3 for Giaviroto and Santos (2013) , that is, " Another interesting and not less interesting than the dnsenum tool is dnsmap with it you can discover subdomains related to the target domain . The dnsmap comes with a wordlist built for research, but for this lab, we will create our own list."

The test should be performed with both the tools for having a particularity, what a tool ignores the other does not. Therefore, it is interesting that the pentest is performed using the mean number of possible tools, each course uses the one that best fits the situation.

A very interesting feature in the existing DNSMAP tool is the possibility to create a list in which words are written as: FTP, MYSQL, panel, admin uploads and she will test these features.

A network administrator must be very careful when setting up a DNS server so there are no vulnerabilities as cash transfers from area to another server. To do so, when testing DNS, should look for vulnerabilities zone transfer. Although, it's kind of hard to let someone that gap, but it is not impossible.

2.7 Fingerprint

The fingerprint is another technique used in the recognition phase pentest as Giaviroto and Santos (2013) in that the attacker tries to find out information about the versions of operating systems (used) by capturing and banners, an attacker can determine the best alternative for successful intrusion. However, not only the operating systems have banners versions, but other services such as SSH, Telnet, Apache, etc. also feature SNMP.

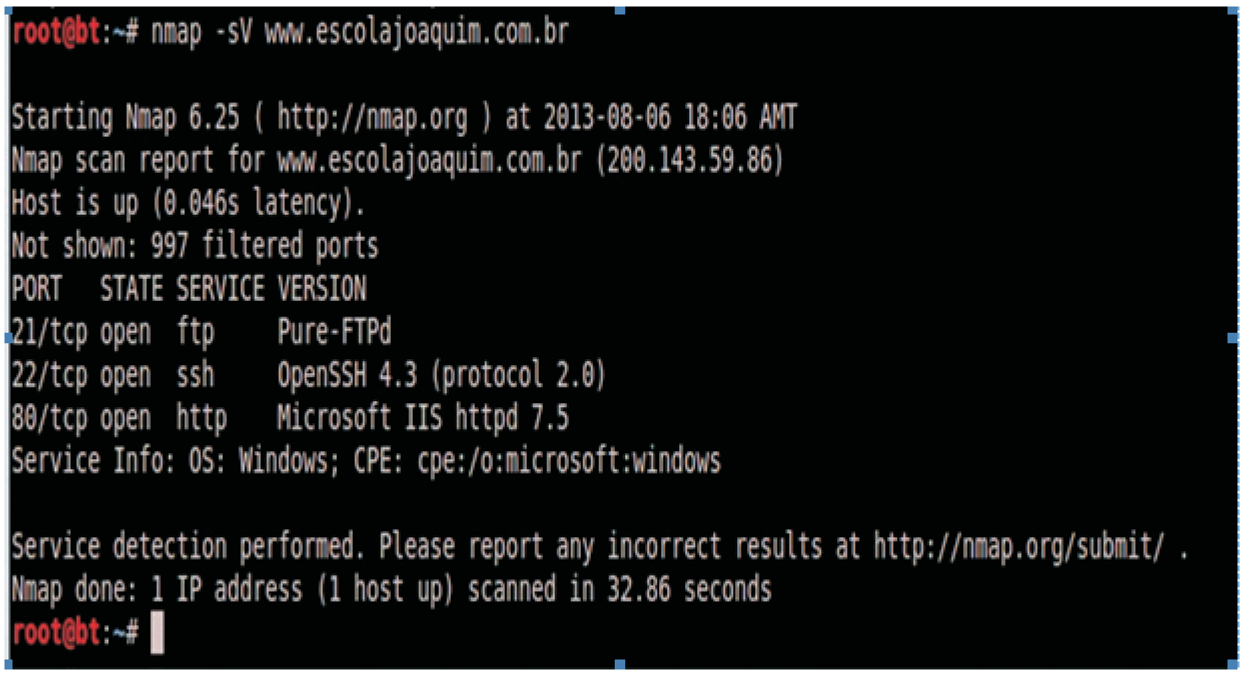
A tool available in BackTrack V5 r3, and versions for Linux and Windows, as well as totally free documentation (available on the website http://nmap.org/), nmap creator Fyodor Lyon Gordon is a powerful tool among its features can describe the following:

Specification of target;
Discovery of Hosts;
Scanning of ports;

Detection Service;
Detection version;
Detection S.O.

Nmap is a tool for simple functionality, when we need to do an inventory and figure out what assets are being used in the network, soon the network administrator can enter a command and get various information from the network operating system, ports that are listening. In a simple with nmap, you can get interesting results, see below.

Figure 04 - Services for open ports with Nmap (Sites).

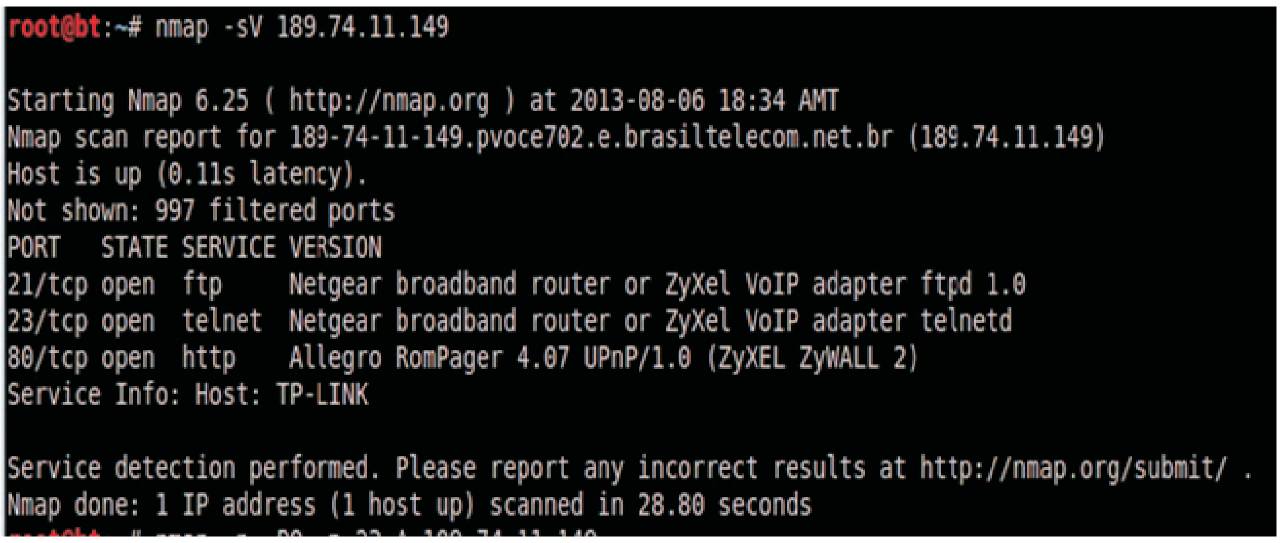


```
root@bt:~# nmap -sV www.escolajoaquim.com.br

Starting Nmap 6.25 ( http://nmap.org ) at 2013-08-06 18:06 AMT
Nmap scan report for www.escolajoaquim.com.br (200.143.59.86)
Host is up (0.046s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Pure-FTPd
22/tcp open  ssh     OpenSSH 4.3 (protocol 2.0)
80/tcp open  http    Microsoft IIS httpd 7.5
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.86 seconds
root@bt:~# 
```

Source by: Grachet (2013).

See you in a simple query displays the server operating system (Windows), the doors of the service FTP and SSH, as well as the version of OpenSSH installed. Under a test done with another server available on the web, check that the server has an active service that should not telnet.

Figure 05 - Services for open ports with Nmap (Web Servers).

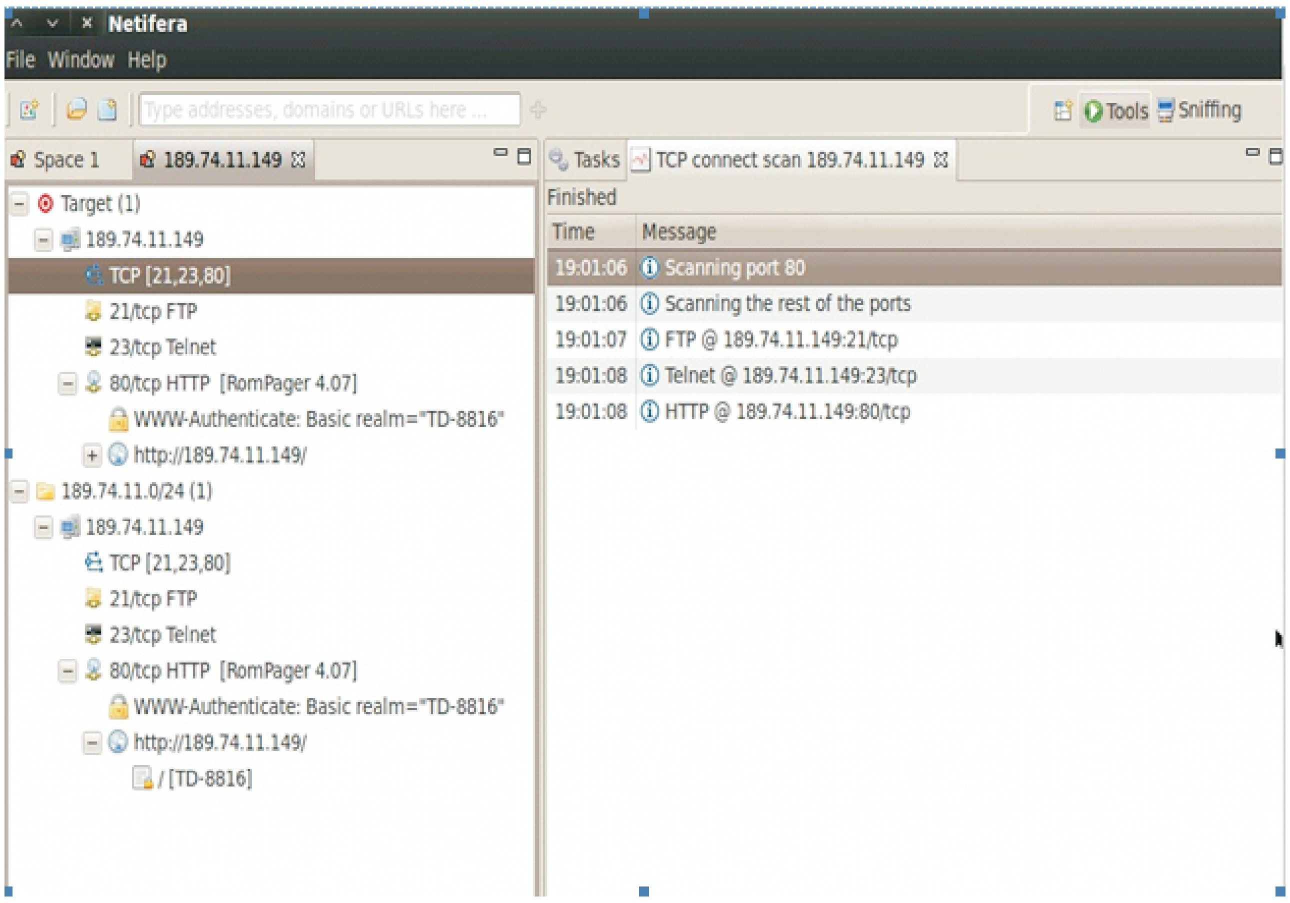


```
root@bt:~# nmap -sV 189.74.11.149

Starting Nmap 6.25 ( http://nmap.org ) at 2013-08-06 18:34 AMT
Nmap scan report for 189-74-11-149.pvoce702.e.brasiltelecom.net.br (189.74.11.149)
Host is up (0.11s latency).
Not shown: 997 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Netgear broadband router or ZyXel VoIP adapter ftpd 1.0
23/tcp open  telnet  Netgear broadband router or ZyXel VoIP adapter telnetd
80/tcp open  http    Allegro RomPager 4.07 UPnP/1.0 (ZyXEL ZyWALL 2)
Service Info: Host: TP-LINK

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.80 seconds
```

Source by: Grachet (2013)

Another very interesting to fingerprint, available at backtrack tool is netifera which has a friendly and simple to use platform. To access the netifera, go to: Gathering information BackTrack Network Analysis Identify Live Hosts Netifera. See the example below of her execution.

Figure 06 - Scanning software with Netifera.


Netifera
File Window Help
Type addresses, domains or URLs here ...
Tools
Sniffing
Space 1
189.74.11.149
Tasks
TCP connect scan 189.74.11.149

```
Target (1)
  189.74.11.149
    TCP [21,23,80]
    21/tcp FTP
    23/tcp Telnet
    80/tcp HTTP  [RomPager 4.07]
      WWW-Authenticate: Basic realm="TD-8816"
      http://189.74.11.149/
189.74.11.0/24 (1)
  189.74.11.149
    TCP [21,23,80]
    21/tcp FTP
    23/tcp Telnet
    80/tcp HTTP  [RomPager 4.07]
      WWW-Authenticate: Basic realm="TD-8816"
      http://189.74.11.149/
        / [TD-8816]
```

```
Finished
Time      Message
19:01:06  Scanning port 80
19:01:06  Scanning the rest of the ports
19:01:07  FTP @ 189.74.11.149:21/tcp
19:01:08  Telnet @ 189.74.11.149:23/tcp
19:01:08  HTTP @ 189.74.11.149:80/tcp
```

Source by: Grachet (2013).

Among the features of netifera, we can highlight the following: discover TCP services, UDP search service, zone transfers, Brute Force on FTP, DNS information, and more. As Giaviroto and Santos (2013) the Netifera, open source DNS Lookup allows searches and discoveries of TCP and UDP services tool. Being in a graphical environment is very simple to use. Another tool is the fingerprint xprobe2 as Giaviroto and Santos (2013): The xprobe2 is an active tool fingerprint, but you need root privileges to run the tool, its use is very simple just by typing the following command:

```
# # pentest/scanners/xprobe2 ./xprobe2 ip_alvo;
```

I can make fingerprint on an open door:

```
# Xprobe2 - p tcp : 80 : ip_alvo open;
```

Thus, the higher the fingerprint information is lifted up have greater options for intrusion test as well as the more information the better editing tool will use.

2.7 Scanning networks

The scanning of networks is important because with it we discover how many computers are active and which ports are being used on the network. As Giaviroto and Santos (2013):

"There are three types of scanning: port, and network vulnerability. In port scanner, the active ports and services are checked, the vulnerability scanner is detected the weaknesses and vulnerabilities in the system and, finally, the network scanner are identified active hosts."

The (Internet Protocol), IP protocol has the characteristic of always looking for the best path to a particular network or host. The IP has as part of the ICMP (Internet Control Messages Protocol) and, according to the RFC792:

"ICMP messages are sent in several situations: for example, when a datagram can not reach its destination, when the gateway does not have the storage capacity to forward a datagram, and when the gateway can direct the host to send traffic to a shortest route."

Tools like ping and traceroute use the ICMP protocol control to determine if a host is alive on the network and to map routers to a destination. Armed with this particularity, we can use a simple tool called fping BackTrack, which can easily detect all active hosts on the network, provided that they meet icmp.

```
# fping-c 1-g ip_alvo/24 2> / dev / null> / tmp / ips.txt
```

The fping tool is not the only contrary has several other such as when using the NMAP Ping scan (-sP), and own Ping command available on Linux and Windows and other operating systems.

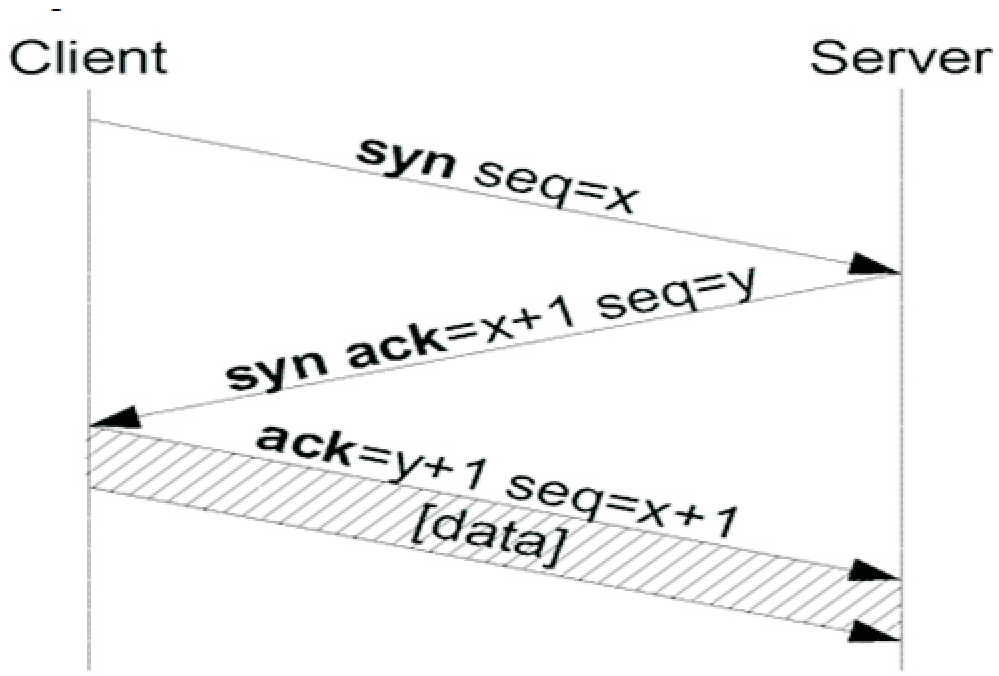
2.8 TCP's Scanning

If ICMP scans tell the amount of active hosts on the network, TCP inform us the number of open ports on a given computer. To find out if a door is open or closed, the program handles a feature of the TCP protocol, called Three Way Handshake, described in RFC 793, which as Giaviroto and Santos (2013 p. 64):

"The client sends a SYN (connection type, with initial number of numbering sequence of bytes in the client server x direction), the server acknowledges the connection request by sending a SYN segment with type acknowledge bit ACK (The same is connected with an initial number sequence numbering established in client server x direction. fate sends a type ACK segment acknowledging the SYN server (data exchange occurs resulting effectively in data transfer and connection termination that can be initiated either by the client or server. Accordingly, the source sends a FIN segment type and destination sends an acknowledgment ACK type, after a while the target sends FIN featuring signaling the end of the connection and finally the source sends another acknowledgment."

Figure 7 shows as "Three Way Handshake functions".

Figure 7 - TCP-handshake.



Source by: Commons Wikimedia (2013).

To perform the test, is simple, if the attacker sends a SYN and SYN ACK reply with targeted, means that it is available, and for this test hping3 tool, also available in Bactrack can be used, following the example of a command below testing port 80 (www): # hping3 - syn-c 1-p 80 ip_alvo, for this type of test can also be done with NMAP software.

2.8 Assembling a toolkit to Pentest

For an IT professional is critical that software has to perform activities that would take days or even plan could not, so below is a list of programs and their characteristics, however, for textbooks and other readers of this article should refer to website makes it available to the addendum that all of these tools have free version .

AutoScan: Performs scan the network and informs active hosts, open ports and services running on time. Use graphical interface.

Hping: we walked with a command line inspired by the ping Unix command interface, but it is not only able to send ICMP echo requests, but also supports TCP, UDP, ICMP and RAW - IP, has a trace route mode.

Lanmap: Searching across the network and capture packets, creating along your running an image file (PNG format.) With the network map, graphically informing the list of machines found.

Maltego: Scans of networks, protocols, services, domains and several other options, stating graphically the relationship enters active hosts.

Nessus: Uses specific to sweep a target, stating the vulnerabilities found and displays the link where you can find more information about specific vulnerability and its exploit plugins.

Nmap: A powerful tool that performs network scan, looking for active hosts, open ports and services running in real time.

Xprobe2: Analyzes banners of operating systems compared to your database, compare and informs the OS used and the version of it.

Evident that the user can customize a version of software for pentest and it install programs that are more interactive, but in this article I describe these as were used in the same, however, that the BackTrack5 r3 operating system was conducted, and it has all these and many other tools installed.

2.9 Attacking the target

Part of the attack will be the moment when the professional contractor attempt to carry invasion or even another type of attack, obviously a contract previously signed and all the legal issue was agreed. If not, this type of activity configures a crime, according to the Law n. 12,737, of November 30, 2012.

After performing the entire process of information gathering, target knowledge and discovery of vulnerabilities, there then it's time to start exploring the flaws or vulnerabilities for the invasion. Evidently, in this case this factor is excluded that the attacker may have got the password of a given system on the Internet or intranet. In this case no longer need anything, so our case is further treat the situation where there is only information or vulnerabilities and attacks to invade.

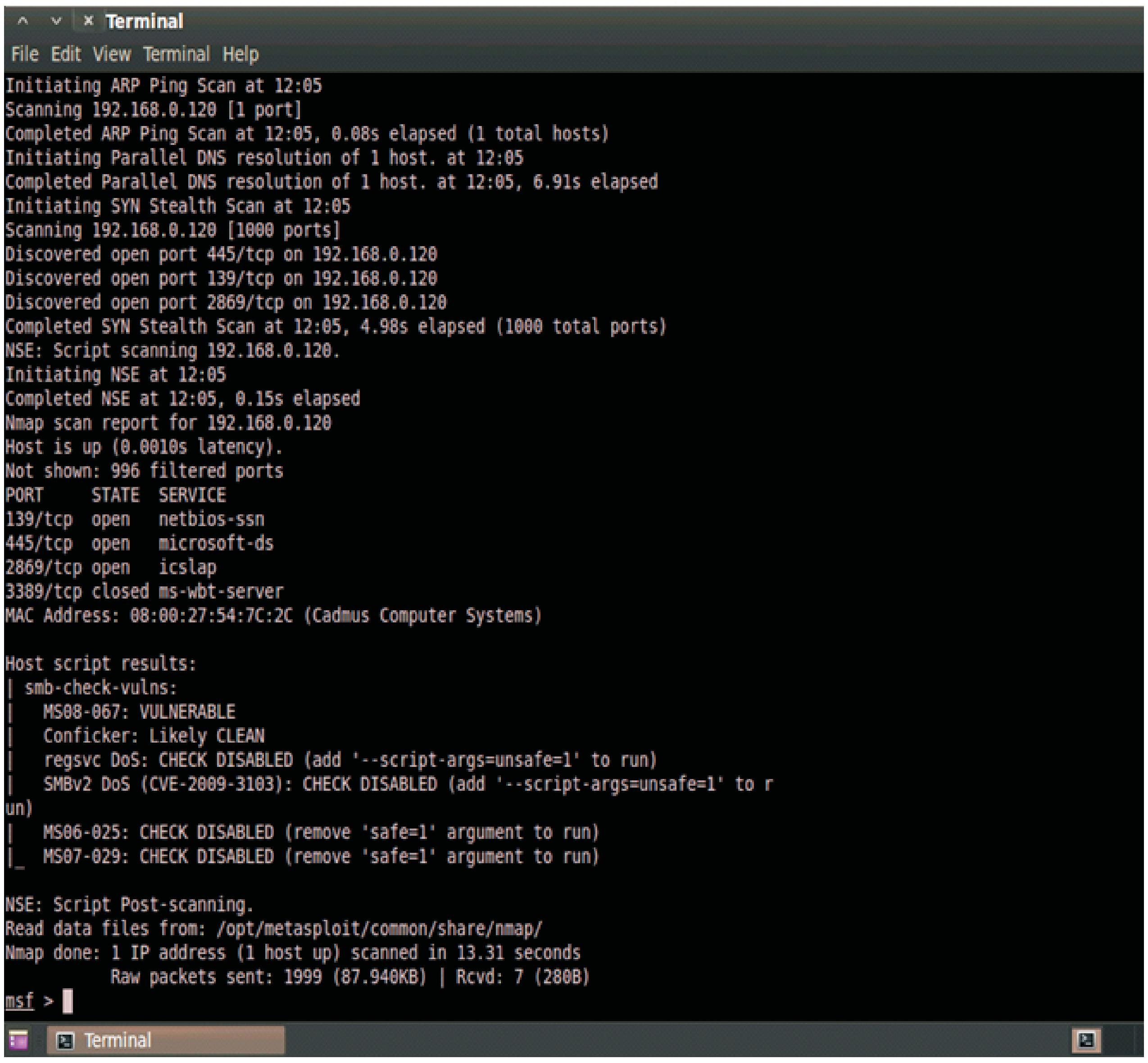
When it comes to invasion privilege escalation or even attacks, there are a multitude of tools as well as various forms and methods to accomplish. However, in this case we will focus only on the use of Metasploit Framework tool existing in BackTrack 5 v3 and we focus on system penetration and denial of services. So is a few others without being cited, but the survey information serves as a principle for all attacks, it will be very improbable that any attacker will already widespread fire on something unknown.

The Metasploit is a tool used extensively by security researchers as Giaviroto and Santos (2013) at the time, the framework is in version 4 and is still one of the most popular options when it comes to gaining access to systems.

As Metasploit Giaviroto and Santos (2013 p. 127) uses Exploit which is a program code written in order to exploit vulnerabilities and Payload load which is applied to the target code system, it is possible through opening communication between the attacker and the target. Already Shellcode codes are written, aimed injecting code to exploit vulnerabilities in the target system, because the so-called buffer overflow.

For the completion of this work will be done a test with a virtual machine using Windows XP sp3, which will be exploited the vulnerability of it. Step by nmap to see himself who also works on the Metasploit frame a command was executed to test if the machine had Windows vulnerability. This same test and much more could be done with full nessus, nmap because the case was tested a vulnerability in particular.

Figure 08 - Testing vulnerability in Windows XP with Metasploit software.



```
Initiating ARP Ping Scan at 12:05
Scanning 192.168.0.120 [1 port]
Completed ARP Ping Scan at 12:05, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:05
Completed Parallel DNS resolution of 1 host. at 12:05, 6.91s elapsed
Initiating SYN Stealth Scan at 12:05
Scanning 192.168.0.120 [1000 ports]
Discovered open port 445/tcp on 192.168.0.120
Discovered open port 139/tcp on 192.168.0.120
Discovered open port 2869/tcp on 192.168.0.120
Completed SYN Stealth Scan at 12:05, 4.98s elapsed (1000 total ports)
NSE: Script scanning 192.168.0.120.
Initiating NSE at 12:05
Completed NSE at 12:05, 0.15s elapsed
Nmap scan report for 192.168.0.120
Host is up (0.0010s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE
139/tcp  open   netbios-ssn
445/tcp  open   microsoft-ds
2869/tcp open   icslap
3389/tcp closed ms-wbt-server
MAC Address: 08:00:27:54:7C:2C (Cadmus Computer Systems)

Host script results:
| smb-check-vulns:
|   MS08-067: VULNERABLE
|   Conficker: Likely CLEAN
|   regsvc DoS: CHECK DISABLED (add '--script-args=unsafe=1' to run)
|   SMBv2 DoS (CVE-2009-3103): CHECK DISABLED (add '--script-args=unsafe=1' to r
un)
|   MS06-025: CHECK DISABLED (remove 'safe=1' argument to run)
|_  MS07-029: CHECK DISABLED (remove 'safe=1' argument to run)

NSE: Script Post-scanning.
Read data files from: /opt/metasploit/common/share/nmap/
Nmap done: 1 IP address (1 host up) scanned in 13.31 seconds
           Raw packets sent: 1999 (87.940KB) | Rcvd: 7 (280B)
msf >
```

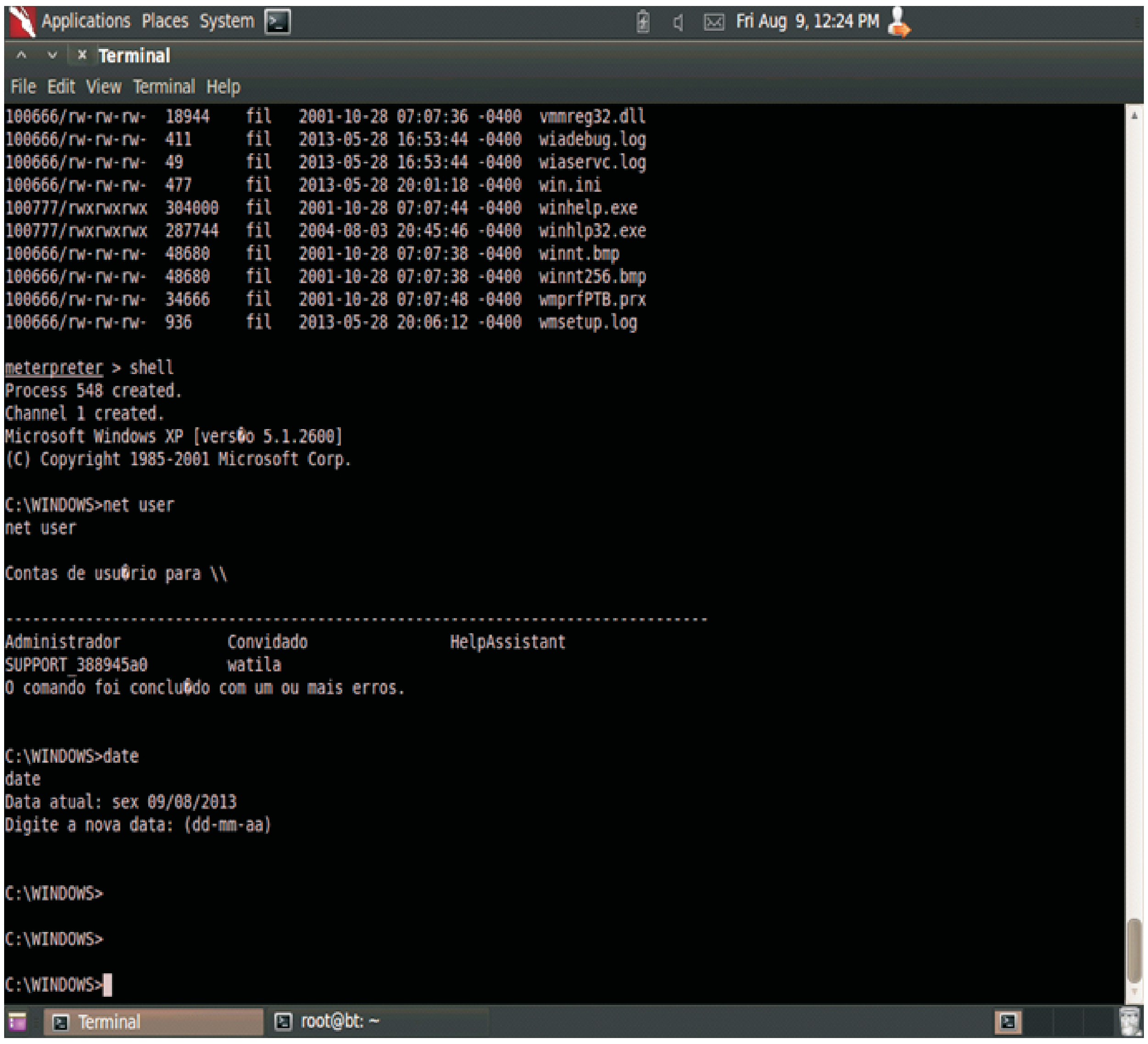
Source by: Grachet (2013).

See the nmap confirms both the vulnerability and exploit features three to run and try to invade. The command was executed in Metasploit:

use exploit/windows/smb/ms08_067_netapi
(Exploit exploiting the vulnerability.)
# set RHOST 192.168.0.120 - IP of the target machine.
# set PAYLOAD windows / meterpreter / reverse_tcp - This is the payload, but it could be another.
# set LHOST 192.168.0.163 - IP of the attacker machine.
# Exploit - Execution Exploit

And after this step as shown in the picture below was already connected to the target machine.

Figure 09 - Screen Invasion performed with Metasploit software.



```
100666/rw-rw-rw-  18944   fil   2001-10-28 07:07:36 -0400  vmmreg32.dll
100666/rw-rw-rw-  411     fil   2013-05-28 16:53:44 -0400  wiadebug.log
100666/rw-rw-rw-  49      fil   2013-05-28 16:53:44 -0400  wiaservc.log
100666/rw-rw-rw-  477     fil   2013-05-28 20:01:18 -0400  win.ini
100777/rwxrwxrwx  304000  fil   2001-10-28 07:07:44 -0400  winhelp.exe
100777/rwxrwxrwx  287744  fil   2004-08-03 20:45:46 -0400  winhlp32.exe
100666/rw-rw-rw-  48680   fil   2001-10-28 07:07:38 -0400  winnt.bmp
100666/rw-rw-rw-  48680   fil   2001-10-28 07:07:38 -0400  winnt256.bmp
100666/rw-rw-rw-  34666   fil   2001-10-28 07:07:48 -0400  wmprfPTB.prx
100666/rw-rw-rw-  936     fil   2013-05-28 20:06:12 -0400  wmsetup.log

meterpreter > shell
Process 548 created.
Channel 1 created.
Microsoft Windows XP [vers�o 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS>net user
net user

Contas de usu�rio para \\

-------------------------------------------------------------------------------
Administrador            Convidado                HelpAssistant
SUPPORT_388945a0         watila
O comando foi conclu�do com um ou mais erros.


C:\WINDOWS>date
date
Data atual: sex 09/08/2013
Digite a nova data: (dd-mm-aa)


C:\WINDOWS>

C:\WINDOWS>

C:\WINDOWS>
```

Source by: Grachet (2013).

This final part shows just how it's done in a fit case for intrusion test, of course, that in the case of pentest are tested all existing and that the machine which have been tested several vulnerabilities such as open ports possibilities. But for the sake of an article and be limited adhered only to the intrusion test.

The steps are methodical, first make a survey of target information (clearly much more extensive than the one shown), using the tools already mentioned, and then perform all the attacking options in the case of the most popular machine: intrusion, denial of service, session hijacking, and in the case of sites: get them out of the air, puncture and injection codes.

3. FINAL CONSIDERATION

According to the survey the pentest is a practice used to test the safety of a particular IT system, in order to find vulnerabilities and to break into the system, but does not cause the same problems as damage it.

Some information systems are set up by people with little ability to perform a quality job, anyway, are made available for use, usually from people who have no technical knowledge. Of course, that systems are configured to be used by technical professionals in other areas, so they have the knowledge to figure out if it is properly configured and secure. And working with outdated vulnerable software and is not vulnerable to invade or use means to harm the system , sometimes simply to cause damage and to get other information capture , owns a company or even a person.

The Pentest is done to find a vulnerability or gap in a system and find possible vulnerabilities both the invasion as other types of attacks such as session hijacking, buffer overflow. Therefore, completion of the work is important, since the topic provides reflections on the prevention of simulations of the possibilities of conducting cybercrime.

4. REFERENCES

1.____AURÉLIO, DICTIONARY. Available in http://www.dicionariodoaurelio.com/ Seguranca.html. Accessed on 4/23/13.
2._____http :/ / en.wikipedia.org / wiki / Google_hacking. Accessed on June 20, 2013.
Basic Guide for Computational Research for Windows. Overview. Available at: http://technet.microsoft.com/pt-br/library/Dd458998 Accessed on: 02 Sep. 2012.
3.ELEUTERIO Monteiro da Silva, Marcio Pereira Machado, Cracking the Computer Forensics. Sao Paulo: Novatec Editora, 2010.
4.FARMER Dan, VENEMA Wietse, Forensics Applied Computational Theory and Practice. Sao Paulo: Pearson Prentice Hall, 2006.
5.FREITAS, Andrey Rodrigues of Expertise Applied to Forensic Computing: Microsoft Environment. Rio de Janeiro: Brasport, 2006.
6.RAFFAEL GOMES VARGA. PROCESSES AND PATTERNS IN FORENSIC EXPERTISE APLICACADA A COMPUTER. Available at:
http://br.groups.yahoo.com/group/PericiaForense/files/QUALIFICACAO_2006_11_15_FINAL.pdf Accessed on: 03 Sep. 2012.
7.FERNANDES, AGUINALDO ARAGON; ABREU, OF VLADIMIR Ferraz. Deploying IT governance: from strategy to management of processes and services. 3. edition. Brasport 2012.
8.GIAVIROTO, Silvio Cesar Purple. SANTOS, Gerson Raimundo dos. BackTrack Linux - Penetration Testing and Auditing in Computer Networks. Rio de Janeiro: Editora Ltda Modern Science, 2013..
9.Mitnick, Kevin D., SIMON, William L. The art of trick: Hackers Attacks: Controlling Fator
10.Peixoto, Mario C. P. Social Engineering and Information Security in Corporate Management. Rio de Janeiro: Brasport, 2006.
11.WIKIMEDIA, http://commons.wikimedia.org/wiki/File:300px-Tcp-handshake.png. Accessed on: July 10, 2013.

Publish Research Article
International Level Multidisciplinary Research Journal
For All Subjects

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication,you will be pleased to know that our journals are

Associated and Indexed,India

✶ International Scientific Journal Consortium
✶ OPEN J-GATE

Associated and Indexed,USA

- EBSCO
- Index Copernicus
- Publication Index
- Academic Journal Database
- Contemporary Research Index
- Academic Paper Databse
- Digital Journals Database
- Current Index to Scholarly Journals
- Elite Scientific Journal Archive
- Directory Of Academic Resources
- Scholar Journal Index
- Recent Science Index
- Scientific Resources Database
- Directory Of Research Journal Indexing

Golden Research Thoughts
258/34 Raviwar Peth Solapur-413005,Maharashtra
Contact-9595359435
E-Mail-ayisrj@yahoo.in/ayisrj2011@gmail.com
Website : www.aygrt.isrj.net