Helsinki Metropolia University of Applied Sciences
Degree Program in Information Technology

Abdul Hameed Tutakhail

Implementation of Penetration Testing

Bachelor’s Thesis. 28, April, 2010
Supervisor: Erik Pätynen , Senior Lecturer
Language Advisor: Taru Sotavalta, Senior Lecturer

Helsinki Metropolia University of Applied Sciences Abstract

Author Title Number of Pages Date	Abdul Hameed Tutakhail Implementation of Penetration Testing 53 28 April 2010
Degree Programme	Information Technology
Degree	Bachelor of Engineering
Supervisor	Erik Pätynen, Senior Lecturer

With growing reliance on the Internet, E-commerce and network-based services organizations, companies and governments are facing increasing challenges to safeguard their network infrastructure against electronic security threats. New threats are emerging on a daily basis and networks need to adapt to face these challenges.

Penetration Testing is a proactive security practice which helps organizations and companies better understand vulnerabilities in their data networks and apply security measures to mitigate the chances of security incidents.

The objective of this project was to describe and implement Penetration Testing in a methodical manner. During this project Penetration Testing was carried out in ten phases, each phase was accompanied with examples that pointed to various vulnerabilities. These vulnerabilities if left unmitigated can be exploited by hackers.

By revealing vulnerabilities in networks, Penetration Testing proves to be an effective and proactive method in securing network infrastructure against electronic attacks. Businesses and organizations can be benefit immensely by conducting Penetration Testing on frequent basis thus avoiding any future attacks.

Keywords	Penetration Testing, Ethical hacking, Vulnerability testing, Pen tester, CEH

Contents

1 Introduction..8

2 Background to Security Threats..9
2.1 Types of Security Threats..9
2.2. Hacker Attacks..10
2.3. Evolving Security Threats...11

3 Penetration Testing...12
3.1 Overview...12
3.2 Types of Penetration Testing..12
3.3 Penetration Testers..13

4 Conducting Penetration Testing..14
4.1 Overview... .14
4.2 Information Gathering.. .16
4.3 FootPrinting...20
4.4 Network reconnaissance...21
4.5 Packet Sniffing.. 24
4.6 Ports Scanning...26
4.7 Vulnerability Scanning...28
4.8 Vulnerability Exploits / Metasploit...30
4.9 Wireless Hack.. 32
4.10 Password Cracking...35
4.11 Denial of Service...39
4.12 Mitigation and Countermeasures...42

5 Conclusion 44

References..45

Appendices...48
Appendix 1: Tools used in this Project……………………………………………48
Appendix 2: Penetration Testing Report..49

Abbreviations and Terms

Adware: A Program which contains advertisements and is displayed without the permission of the user. Some adware can be harmless while others can be considered as spyware.

Botnet: Networks of computers which are compromised by attackers and then used as remote control to attack other systems.

Brute force: A type of attack where systems are being attacked by trying all possibilities. Many of the current passwords cracking tools contain a brute force attack where every possible value is tried in order to break a password.

Buffer overflow: A Type of attack whereby the systems are being forced to crash by forcing too much data into storage areas which they were not originally meant to hold.

Dictionary attack: Refers to a type of brute force attack where an attempt is made to break into a system by attempting all the possible keys.

DMZ: Demilitarised Zone, a segment in the network usually partitioned by a firewall which houses services such as web servers or mails servers. The security level on the DMZ is lesser than that of the inside segment but higher than the outside segment. Services hosted in the DMZ are usually publicly accessible services.

DNS: Domain Name System, a protocol which translates DNS names into IP addresses and vice versa. Since remembering IP addresses is hard, DNS helps people use normal names.

DOS: Denial of Service, a form of attack whereby the system or network is overwhelmed by a large amount of bogus or irrelevant requests.

E-Commerce: Electronic Commerce is doing business electronically i.e. via email or websites.

Exploit: A malware code which tries to take advantage of the vulnerabilities in the system. Attackers write exploits as soon as vulnerability is found, it is a cat and mouse game between the attacker and the developer.

Firewall: A network device which controls and restricts access to the network segment inbound/outbound, based on the rules or algorithm in place. Today firewalls provide more than just controlling access, such as intrusion detection or spam filtering.

Hash value: A value returned by a one way hash function, which is one way mathematical function that converts large data into small variable integers.

IDS: Intrusion Detection System, a hardware device or an application which triggers an alarm when an attack is detected. Usually the IDS uses a set of rules known as signatures which contains a pattern of an attack to detect possible intrusion.

ISMS: Information Security Management System, a set of polices and practices concerned with information security.

Key logger: Application or hardware which is usually installed without the knowledge of the user and records all activities.

Man in the middle: A type of attack whereby victims communicating with each other believe that they are talking to each other without a third party eavesdropping. In this type of attack the attack usually receives a copy of the communication or the request is relied through the attack to the original parties.

OS fingerprinting: An attempt to identify the Operating System of the target system by attempting various requests and then analysing the responses of each request to identify the OS. Different OSs usually respond to a request somewhat differently.

OSSTMM: Open Source Security Testing Methodology Manual. A methodology for Penetration Testing that identifies what, when and where to test.

Script kiddie: A form of attacker who has minimal technical know-how and uses tools developed by others to attack and penetrate systems.

Session Hijacking: Attacks where an already established legitimate connection is either broken or taken over. Inherit weaknesses in the protocol make it easier for attackers to take over established connections.

Spam attacks: A form of attack where networks are being bombarded by spam emails generated by compromised sources.

SQL: Structured Query language is a computer language that is used to manage data in database systems.

SQL injection: Attacks where by the attacker penetrates database systems by carrying out unauthorised SQL commands. Applications with big backend databases are usually the primary target.

SSID: Service Set Identifier, a mechanism in wireless LANs where clients can associate to with a specific WLAN.

Topology Diagram: A document which details the physical and logical diagram of network infrastructure and how they are being interconnected. Topology diagrams help network engineers immensely in understanding the network and assisting in troubleshooting if any issue arises.

TTL: Time to Live, a segment in the IP header which determines the amount of time a packet can traverse the network. This helps in eliminating an endless loop of packets moving around the network.

VLAN: Virtual Local Area Network, a logical segmentation of different segments. The idea behind the VLAN is that although stations can share the physical medium, they will not be able to talk to each other unless they are part of the same VLAN. This type of segmentation helps traffic remain local to the VLAN

VPN: Virtual Private Network, a mechanism to transport traffic in a secure manner. VPNs usually help remote users connect to the central office over an insecure channel such as the Internet and still be able to communicate safely.

WEP: Wired Equivalent Privacy, a protocol used to ensure secure communication within a wireless network

1 Introduction

With the extensive increase in security related incidents, today’s network managers and engineers are facing a daunting task of safeguarding their infrastructure against such attacks.

The objective of this project is to describe and implement Penetration Testing which is a security practice that helps organizations and companies better understand vulnerabilities in their data networks and apply security measures to mitigate the chances of security incidents in their networks.

Although the main theme of the project is to discuss and implement penetration testing, the project will start by describing the background of security threats and how security threats evolved over the last decade, as then no extensive technical knowledge was needed to carry out such attacks.

In addition, to provide the reader a deeper insight the project will briefly describe the major types of hacker attacks and types of security threats. It aims to describe Penetration Testing and implementing in a manner that a real hacker would do, so to reveal vulnerabilities in systems and networks.

This project aims to provide a sample report discussing the contents of Penetration Testing Reports, for instance details of all the vulnerabilities, the severity of each case and the tactical and strategic recommendations for them.

2 Background to Security Threats

With massive increase of information exchange through electronic means business and organizations are facing extensive range of electronic threats. These threats are increasing both in sophistication and numbers. Information security professionals need to understand the dynamics behind these threats in order to safeguards their infrastructure.

2.1 Types of Security Threats

Below are four general categories of security threats to the network [1].

- Structured threats
- Unstructured threats
- External threats
- Internal threats

Threats posed by a well planned and organized effort to penetrate and attack systems are called **structured threats**. Usually systems and network-specific attacks are carried out by a single individual or individuals belonging to an organised group in order to penetrate the system. The attackers have a high level of intelligence on the target.

Unlike structured threats, **unstructured threats** are usually carried out at random, for example automated scanning programs are used to scan a range of stations and those who reply are then further targeted. In others words, the efforts are not organized but systems and networks are targeted at random.

Some of the threats that today’s multinational companies and organisations face are the security threats posed internally within their trusted network, which are employees and staff. Unlike external threats where one has a clear boundary of separation between the trusted and untrusted network. **Internal threats** pose a bigger challenge to today’s data networks.

Threats posed to systems and network infrastructures that emerge outside the trusted boundary of the network are considered **external threats**.

2.2. Hacker Attacks

Hackers are attacking systems in networks in increasing numbers. The relative sophistication and methods vary depending on the target the hackers are trying to breach. Generally attacks carried out by hackers can be categorised into three types [1].

- Configuration Attack
- Application Attack
- Operating System

One important aspect of security that professionals in the security community forget is the importance of proper configuration of the solution. No matter how secure a particular solution is if it is not properly configured according to the best practices it will be prone to attacks. Usually these types of attacks are known as **configuration attacks**. Network devices such as Routers, Switches, Firewalls, Intrusion Detections systems can be attacked or used as platform to attack other infrastructure if vital configuration parameters are missing.

The particular type of attacks that are carried out against systems that are running operating systems which have inherit weaknesses or bugs are termed as **Operating System attacks.** For example if vital updates are missing on a Windows machine, it will be prone to various exploits.

Furthermore the type of attack carried out against vulnerabilities found in the application layer i.e. vulnerabilities found in applications are considered the **Application attacks.** A few examples of such attacks are Buffer overflow, Spam attacks and SQL injection.

2.3. Evolving Security Threats

Electronic security threats have increased extensively over the last decade [1]. As shown in Figure 1, the level and the number of security threats have both increased in number and sophistication, but on the other hand, the knowledge needed to carry out such attacks has decreased. Unlike before, today's network managers and engineers are facing a daunting task of safeguarding their infrastructure against attacks that are emerging on daily basis. Whenever there is a vulnerability that shows up in a particular solution, the next day or week an exploit emerges which then hackers can use to target vulnerable systems.

Furthermore it is no longer mandatory to have advanced knowledge of programming or networking to conduct such attacks as there are a number of tools available in the public domain for anyone to download and carry out attacks. Most of the attacks carried out today are done by Script Kiddies [2] who use these publicly available tools to penetrate and attack networks.

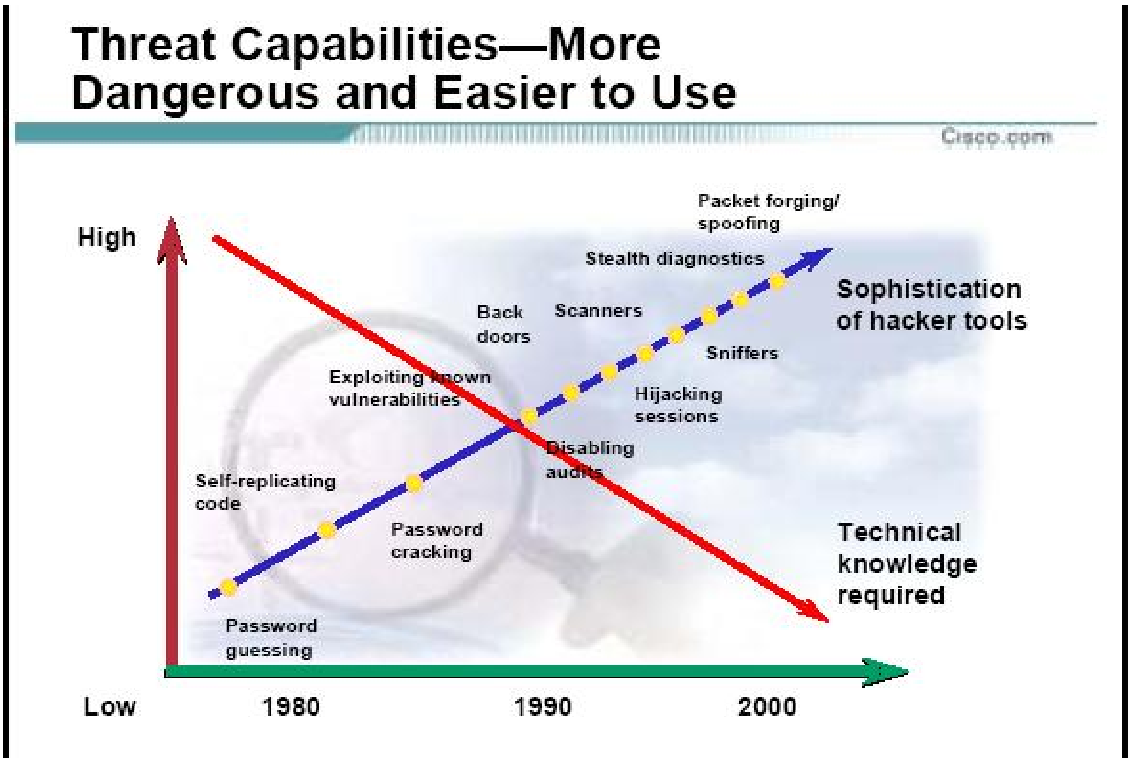


Figure 1: ICT Threats [1]

3 Penetration Testing

3.1 Overview

The need for companies and organizations to communicate and internetwork with partners, collaborators, customers has brought upon new complexities and challenges to securing networks and systems. Earlier only certain groups had access to network resources, now for companies to survive they need to communicate and internetwork with others. Therefore as a security manager your security management paradigm should reflect and face these new challenges.

One such measure is Penetration Testing which must be a part of a company's Information Security Management System (ISMS) [31] Penetration Testing is a security practice which helps organizations and companies reveal vulnerabilities, in their systems and data networks and apply security measures to mitigate the chances of security incidents. It fits into the Check-Act phases of the ISMS model.

Unlike vulnerability assessment that simply identifies and reports noted vulnerabilities, Penetration Testing attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible [24]

3.2 Types of Penetration Testing

Penetration Testing is divided into two categories [3]: Black Box and White Box.
A black box tester has no or very little knowledge of the target and it is his or her duty to find it all and try to penetrate the target. On the other hand a White Box tester has prior knowledge of the target such as IP addresses range or diagrams.

In Black Box Penetration Test(ing)

- The Penetration tester has little or no knowledge of the client's network.
- Usually the client's name is provided and it is then up to the Penetration tester to find out the rest using Penetration Testing.
- The advantage of this method of Penetration Testing as it simulates real world attacks.

In White Box Penetration Test(ing)

- The Penetration tester is given all the information about the client's network.
- The information provided is for example Topology Diagrams, Physical Diagrams, IP addressing scheme.
- The type of equipment used such as Firewalls, Intrusion Detection Systems or core routers.
- The advantage of this type of Penetration Testing is that it simulates an attacker which is the company insider or assistance provided to him/her by someone from the company.

As stated above vulnerability assessment simply identifies and reports the noted vulnerabilities, whereas a Penetration Test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration Testing should [23] include network and application layer testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

3.3 Penetration Testers

It is common practice to outsource the Penetration Testing to security companies who specialise in Penetration Testing. Once the contract is signed the Security Company will implement the Penetration test and provide a detailed report in the end with counter measures explained. It is also possible to implement Penetration Testing with the company's own individual resources, should relevant expertise exist. However one important thing to keep in mind is that the individuals performing Penetration Testing should be organizationally separate from the management of the environment being tested. For example, the firewall administrator should not perform the firewall-Penetration Testing [23].

Furthermore there are well-known certifications such Certified Ethical Hacker [15] which teaches methods and techniques in order to conduct Penetration Testing.

The scope of Penetration Testing depends on the contract being signed by the stakeholders. Of course it is advisable to implement Penetration Testing following the OSSTMM manual. Refer to the Penetration examples later below targeting various systems and networks.

Penetration Testing should be carried out on frequent basis to test, penetrate network and systems to see if the security measures in place are good enough. In addition to that if there are new changes or installations being done then it is also a good idea to perform Penetration Testing to make sure that they are not introducing vulnerabilities. [23]

4 Conducting Penetration Testing

4.1 Overview

There are several methodologies that can be used for Penetration Testing. OSSTMM [24] manual shows a range and different aspects of the networks or systems that needs to be tested.

It is very important to note that the type of Penetration Testing either Black Box or White Box depends on the clients requirements. Selecting either will change how the penetration is being conducted. If White Box Penetration Testing method is selected then the tester should be provided with all the relevant information on the target systems or networks.

In this project I will implement Penetration Testing by following the steps below. Figure 2 shows a step by step approach to Penetration Testing, each step explained in the figure. By following the steps below in a methodical manner systems and networks can be identified, targeted and remedied for vulnerabilities and weaknesses.

Steps by step Penetration Testing

- Information gathering
- Footprinting
- Network reconnaissance and Sniffing
- Ports scanning
- Vulnerability scanning
- Exploiting vulnerabilities
- Password cracking
- Wireless hack
- Denial of services
- Mitigation and counter measures

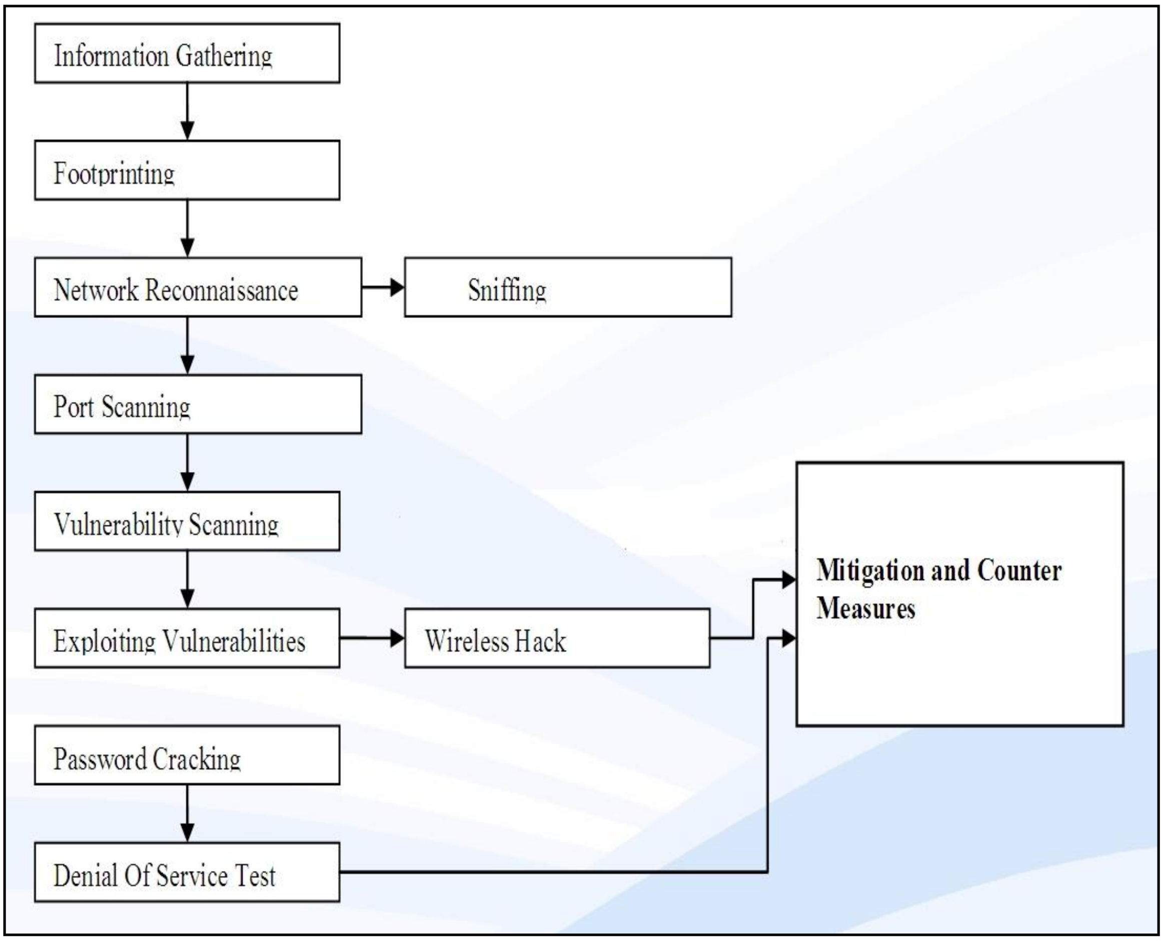


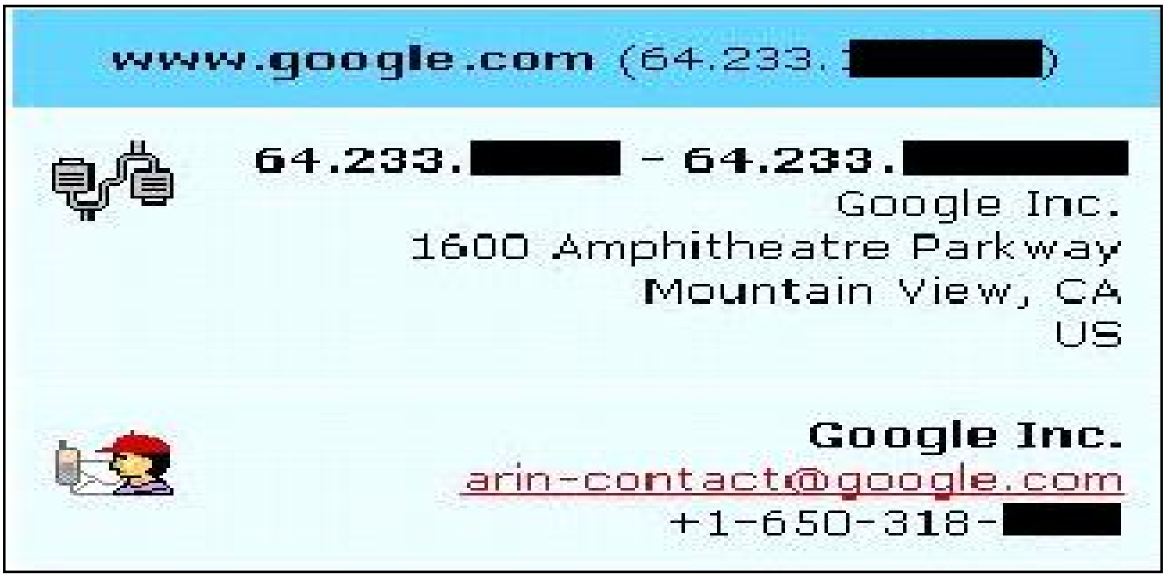
Figure 2: Penetration Testing Flow

Below is a brief description of each individual phase of Penetration Testing followed by examples of each phase either by showing an individual tool in action or an attack carried out by using a combination of tools.

4.2 Information Gathering

One of the first phases in Penetration Testing, where the tester attempts to collect as much information as much as possible on the target system or network. Information collected ranges from domain registration details and telephone numbers, to physical address and email address.

Figure 3 shows a simple WHOIS [4] search carried out using freely available tools providing lots of information on the potential victim. The lookup return provides range of information such as the Web address, the IP address of the site, the range of IP allocation, the physical address, telephone number or email address. This information is essential for the later stages of the attack.



www.google.com (64.233.[redacted])

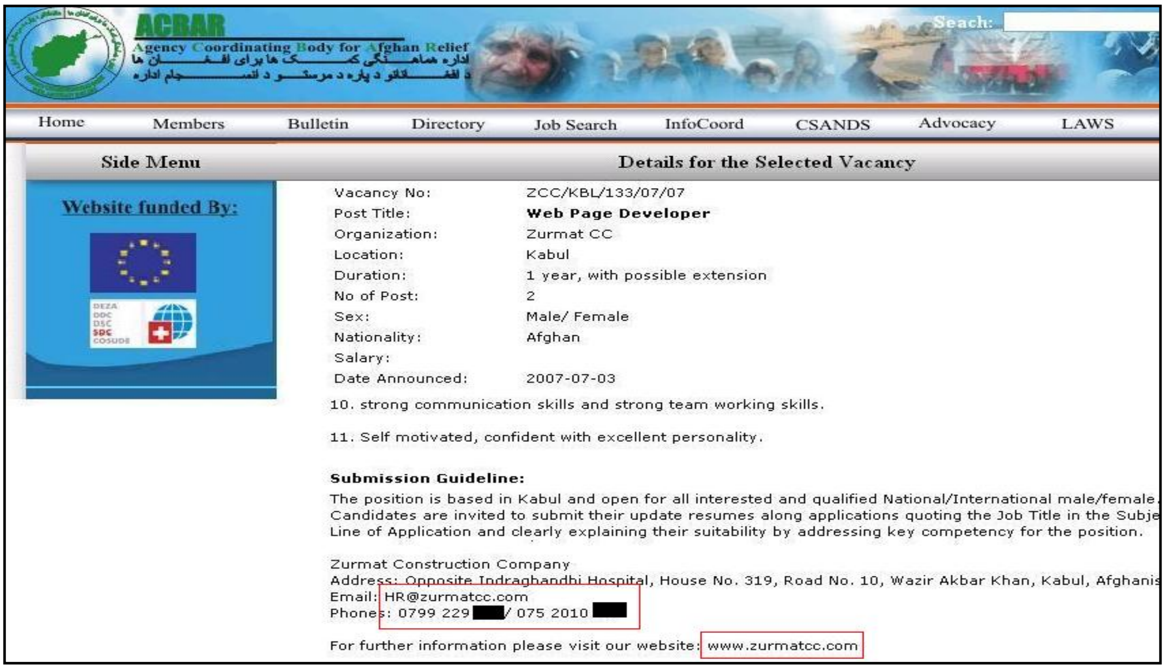
64.233.[redacted] - 64.233.[redacted]

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA
US

Google Inc.
arin-contact@google.com
+1-650-318-[redacted]

Figure 3: WHOIS lookup [4]

Online sites as such as forums, job portals, phone books or yellow pages can be used to gather information on the victim. As simple query can reveal lots of information on the victim such as telephone numbers, email address, postal address or web addresses as in Figure 4. This information is helpful as it will be used in the latter stages of the attacks.



Details for the Selected Vacancy

Vacancy No:	ZCC/KBL/133/07/07
Post Title:	**Web Page Developer**
Organization:	Zurmat CC
Location:	Kabul
Duration:	1 year, with possible extension
No of Post:	2
Sex:	Male/ Female
Nationality:	Afghan
Salary:	
Date Announced:	2007-07-03

10. strong communication skills and strong team working skills.

11. Self motivated, confident with excellent personality.

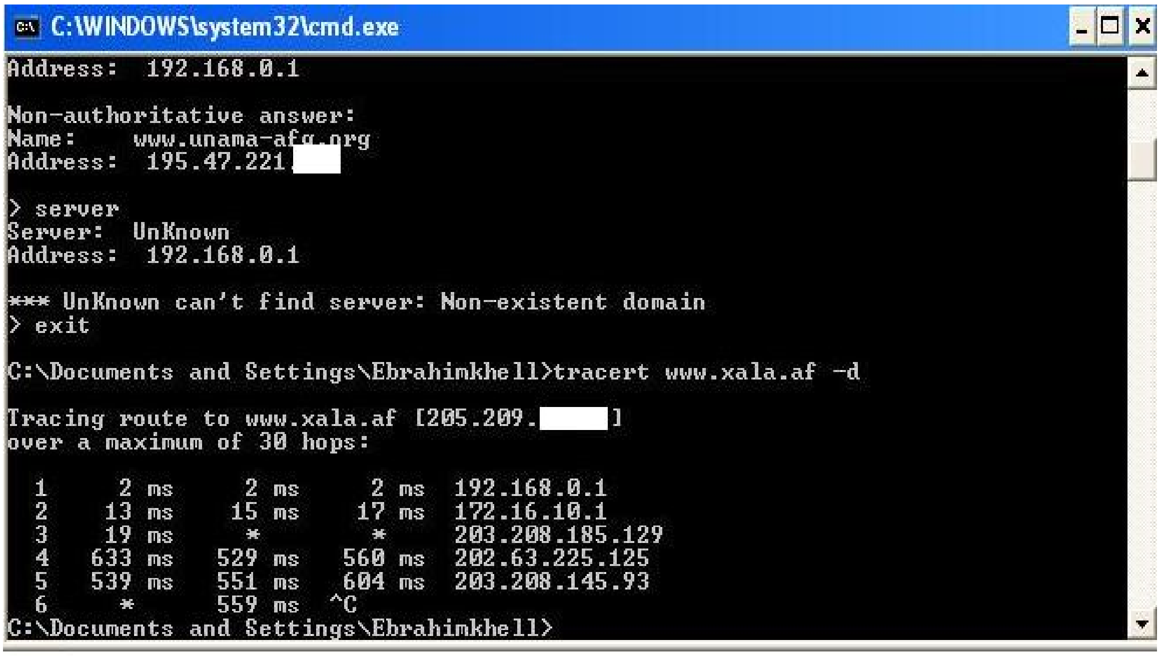
Submission Guideline:
The position is based in Kabul and open for all interested and qualified National/International male/female. Candidates are invited to submit their update resumes along applications quoting the Job Title in the Subje Line of Application and clearly explaining their suitability by addressing key competency for the position.

Zurmat Construction Company
Address: Opposite Indraghandhi Hospital, House No. 319, Road No. 10, Wazir Akbar Khan, Kabul, Afghanis
Email: HR@zurmatcc.com
Phones: 0799 229[redacted]/ 075 2010[redacted]

For further information please visit our website: www.zurmatcc.com

Figure 4: Job Portal lookup [32]

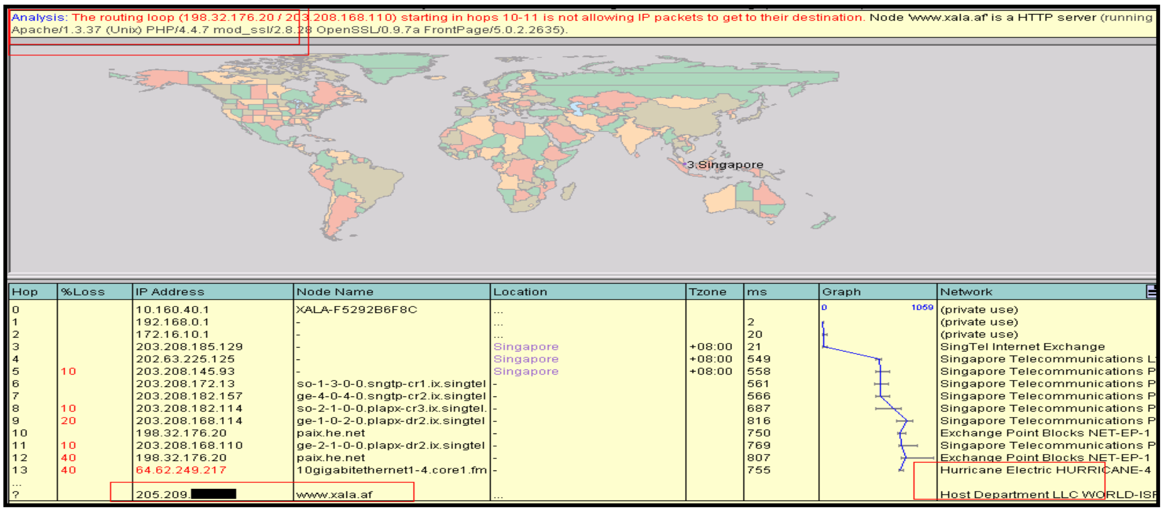
Domain Name System resolution provides one with the IP address of the target system. Similarly a simple Ping or Traceroute will provide information on the reachability of the targets and how packets traverse the network in order to reach the target see Figure 5. By carrying out simple ICMP Ping and Trace, one can get an idea if there are any filtering devices such as Firewalls on the way to the targets.



```
Address:  192.168.0.1

Non-authoritative answer:
Name:     www.unama-afg.org
Address:  195.47.221.[redacted]

> server
Server:  UnKnown
Address:  192.168.0.1

*** UnKnown can't find server: Non-existent domain
> exit

C:\Documents and Settings\Ebrahimkhell>tracert www.xala.af -d

Tracing route to www.xala.af [205.209.[redacted]]
over a maximum of 30 hops:

  1     2 ms     2 ms     2 ms  192.168.0.1
  2    13 ms    15 ms    17 ms  172.16.10.1
  3    19 ms     *        *     203.208.185.129
  4   633 ms   529 ms   560 ms  202.63.225.125
  5   539 ms   551 ms   604 ms  203.208.145.93
  6     *      559 ms   ^C
C:\Documents and Settings\Ebrahimkhell>
```

Figure 5: DNS lookup, Traceroute [5]

A simple route lookup using the Visual Route [5] application shows the IP route and global map to the target. Figure 6 shows how a system is being targeted with Visual route giving detailed data.



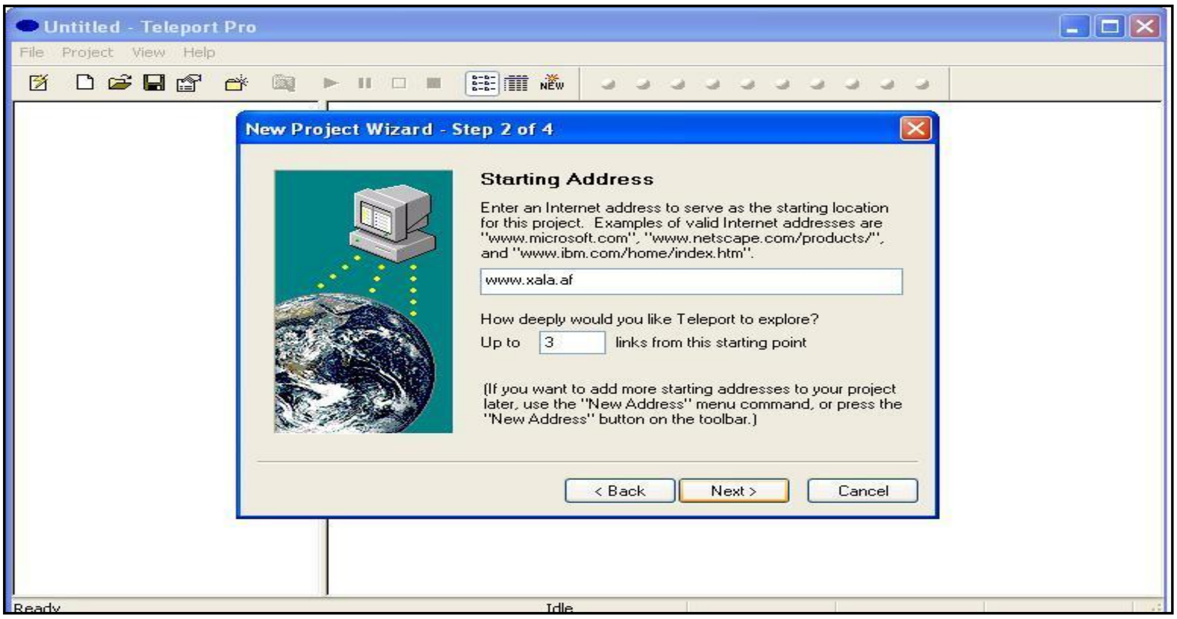
Analysis: The routing loop (198.32.176.20 / 203.208.168.110) starting in hops 10-11 is not allowing IP packets to get to their destination. Node 'www.xala.af' is a HTTP server (running Apache/1.3.37 (Unix) PHP/4.4.7 mod_ssl/2.8.28 OpenSSL/0.9.7a FrontPage/5.0.2.2635).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		10.160.40.1	XALA-F5292B6F8C	...			0 1059	(private use)
1		192.168.0.1	-	...		2		(private use)
2		172.16.10.1	-	...		20		(private use)
3		203.208.185.129	-	Singapore	+08:00	21		SingTel Internet Exchange
4		202.63.225.125	-	Singapore	+08:00	549		Singapore Telecommunications L
5	10	203.208.145.93	-	Singapore	+08:00	558		Singapore Telecommunications P
6		203.208.172.13	so-1-3-0-0.sngtp-cr1.ix.singtel	-		561		Singapore Telecommunications P
7		203.208.182.157	ge-4-0-4-0.sngtp-cr2.ix.singtel	-		566		Singapore Telecommunications P
8	10	203.208.182.114	so-2-1-0-0.plapx-cr3.ix.singtel.	-		687		Singapore Telecommunications P
9	20	203.208.168.114	ge-1-0-2-0.plapx-dr2.ix.singtel	-		816		Singapore Telecommunications P
10		198.32.176.20	paix.he.net	-		750		Exchange Point Blocks NET-EP-1
11	10	203.208.168.110	ge-2-1-0-0.plapx-dr2.ix.singtel	-		769		Singapore Telecommunications P
12	40	198.32.176.20	paix.he.net	-		807		Exchange Point Blocks NET-EP-1
13	40	64.62.249.217	10gigabitethernet1-4.core1.fm	-		755		Hurricane Electric HURRICANE-4
...								
?		205.209.[redacted]	www.xala.af	...				Host Department LLC WORLD-ISF

‘

Figure 6: Visual route lookup [5]

Furthermore Teleport which is a useful tool for downloading files from the Web sites can be used to find and download all types of files from the target site. As seen in Figure 7 , a site is being targeted for a teleport download.



Starting Address

Enter an Internet address to serve as the starting location for this project. Examples of valid Internet addresses are "www.microsoft.com", "www.netscape.com/products/", and "www.ibm.com/home/index.htm".

www.xala.af

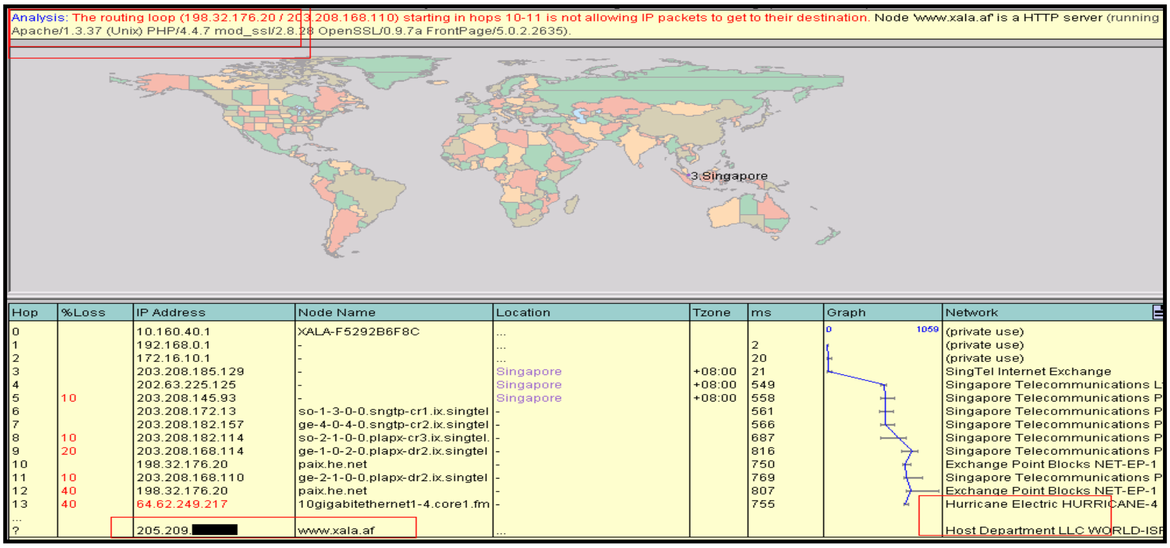
How deeply would you like Teleport to explore?

Up to 3 links from this starting point

(If you want to add more starting addresses to your project later, use the "New Address" menu command, or press the "New Address" button on the toolbar.)

Figure 7: Teleport download [6]

In Figure 8 the Visual route application is used to check connectivity to remote ports, roundtrip delay and Time to Live (TTL).



Analysis: The routing loop (198.32.176.20 / 203.208.168.110) starting in hops 10-11 is not allowing IP packets to get to their destination. Node 'www.xala.af' is a HTTP server (running Apache/1.3.37 (Unix) PHP/4.4.7 mod_ssl/2.8.28 OpenSSL/0.9.7a FrontPage/5.0.2.2635).

Hop	%Loss	IP Address	Node Name	Location	Tzone	ms	Graph	Network
0		10.160.40.1	XALA-F5292B6F8C	...			0 1059	(private use)
1		192.168.0.1	-	...		2		(private use)
2		172.16.10.1	-	...		20		(private use)
3		203.208.185.129	-	Singapore	+08:00	21		SingTel Internet Exchange
4		202.63.225.125	-	Singapore	+08:00	549		Singapore Telecommunications Lt
5	10	203.208.145.93	-	Singapore	+08:00	558		Singapore Telecommunications P
6		203.208.172.13	so-1-3-0-0.sngtp-cr1.ix.singtel	-		561		Singapore Telecommunications P
7		203.208.182.157	ge-4-0-4-0.sngtp-cr2.ix.singtel	-		566		Singapore Telecommunications P
8	10	203.208.182.114	so-2-1-0-0.plapx-cr3.ix.singtel.	-		687		Singapore Telecommunications P
9	20	203.208.168.114	ge-1-0-2-0.plapx-dr2.ix.singtel	-		816		Singapore Telecommunications P
10		198.32.176.20	paix.he.net	-		750		Exchange Point Blocks NET-EP-1
11	10	203.208.168.110	ge-2-1-0-0.plapx-dr2.ix.singtel	-		769		Singapore Telecommunications P
12	40	198.32.176.20	paix.he.net	-		807		Exchange Point Blocks NET-EP-1
13	40	64.62.249.217	10gigabitethernet1-4.core1.fm	-		755		Hurricane Electric HURRICANE-4
...								
?		205.209.[redacted]	www.xala.af	...				Host Department LLC WORLD-ISF

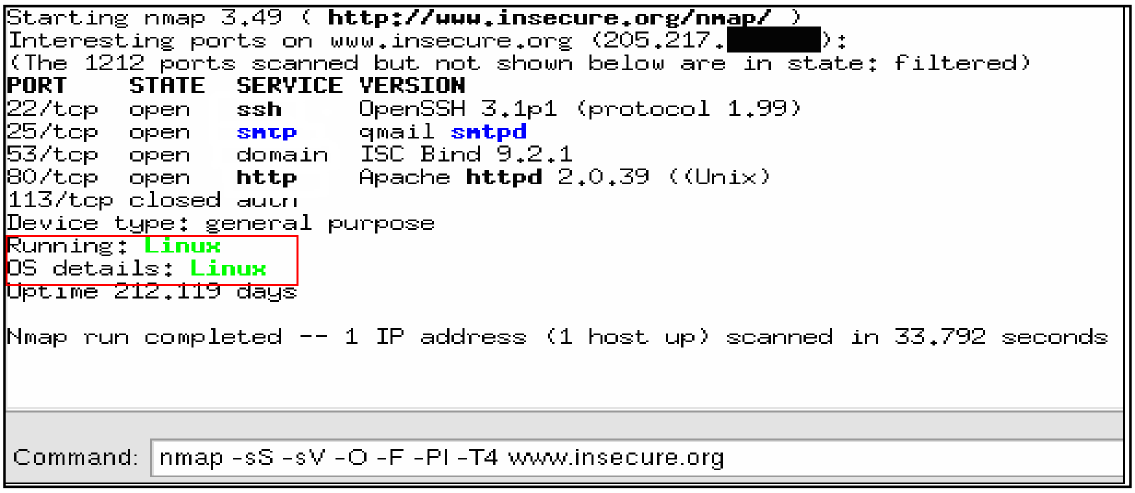
Figure 8: Visual Route Trace [5]

Furthermore even well-known search engines such as Google can be used as tool to harvest information on victims. A technique termed as Google hacking is used profoundly by hackers to passively scan their victims for information.[21]

4.3 FootPrinting

Footprinting is a phase of Penetration Testing where information regarding the type of operating system running, type of web server or range of applications is gathered.
Foot printing generally refers to one of the pre-attack phases, the tasks performed prior to doing the actual attack.

In Figure 9 using NMAP [7,19] the target system reports that it is running Linux. NMAP is an extremely useful scanning to tool for Operating System Fingerprinting. This information is useful for the tester-attacker to narrow down his or her exploits
to the specific OS running on the target system. In this scan we can also see that apart from the OS different open ports on the system are also reported.

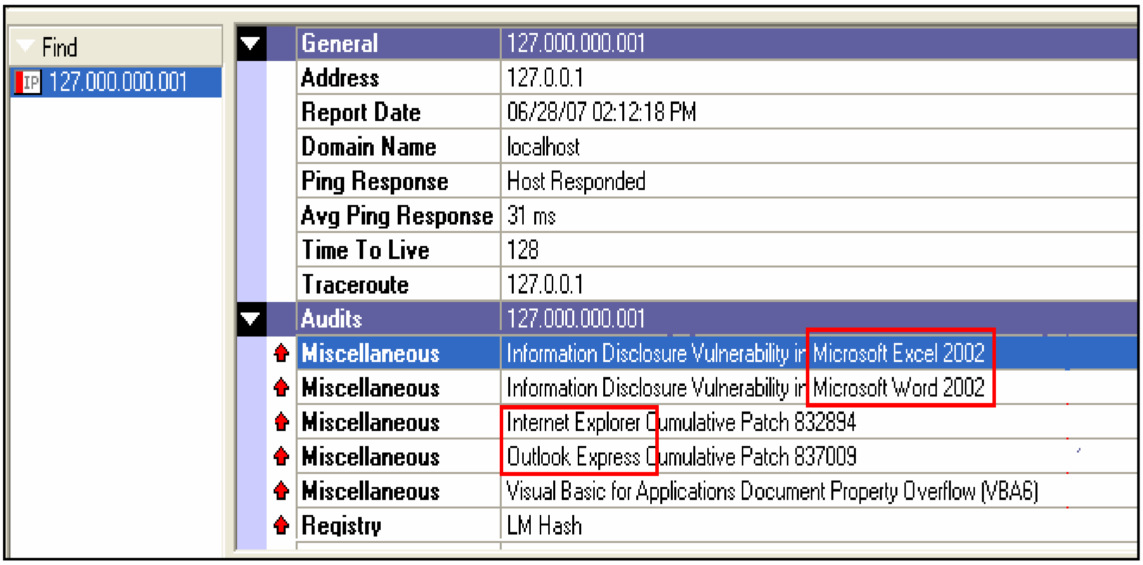


```
Starting nmap 3.49 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.[redacted]):
(The 1212 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp   open   smtp    qmail smtpd
53/tcp   open   domain  ISC Bind 9.2.1
80/tcp   open   http    Apache httpd 2.0.39 ((Unix)
113/tcp  closed auth
Device type: general purpose
Running: Linux
OS details: Linux
Uptime 212.119 days

Nmap run completed -- 1 IP address (1 host up) scanned in 33.792 seconds
```

Command: nmap -sS -sV -O -F -PI -T4 www.insecure.org

Figure 9: Nmap OS Fingprinting, Port scan [7]

In addition to the OS fingerprinting it is also useful to identity the types of applications that are running on the system. Some of the inherit vulnerabilities in different applications can later be exploited. In Figure 10 Eeye's Retina is used to identify the applications running on the target system.



Find

127.000.000.001

General	127.000.000.001
Address	127.0.0.1
Report Date	06/28/07 02:12:18 PM
Domain Name	localhost
Ping Response	Host Responded
Avg Ping Response	31 ms
Time To Live	128
Traceroute	127.0.0.1
Audits	127.000.000.001
Miscellaneous	Information Disclosure Vulnerability in Microsoft Excel 2002
Miscellaneous	Information Disclosure Vulnerability in Microsoft Word 2002
Miscellaneous	Internet Explorer Cumulative Patch 832894
Miscellaneous	Outlook Express Cumulative Patch 837009
Miscellaneous	Visual Basic for Applications Document Property Overflow (VBA6)
Registry	LM Hash

Figure 10: Retina Scan [33]

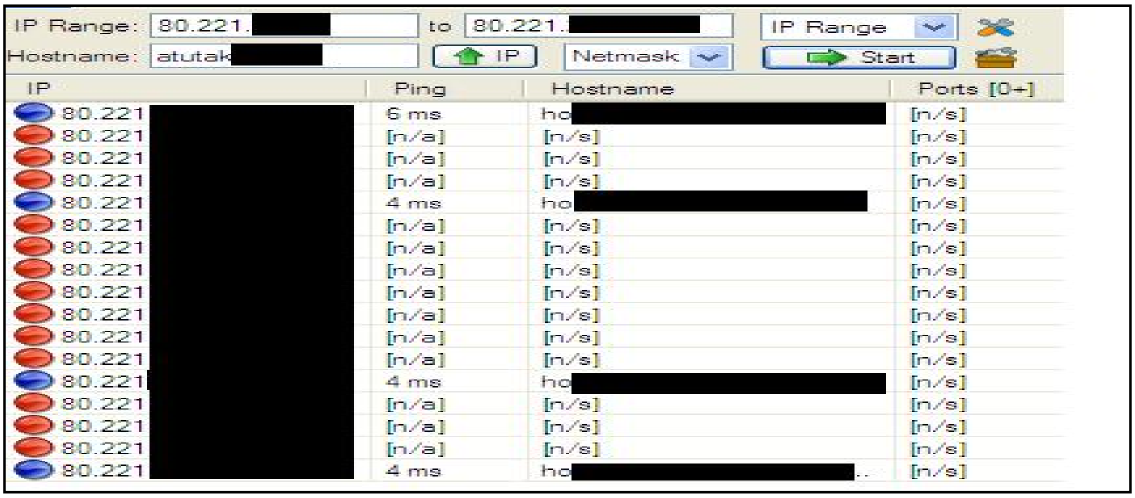
In addition to that the scan also shows the various vulnerabilities the applications are having. In this instance the system is running vulnerable Internet Explorer, Outlook Express, Microsoft Excel and Microsoft Word.

4.4 Network reconnaissance

Network reconnaissance is a process through which target stations are scanned to see if they are up and also analyse the type of service running on them.

Most of the network reconnaissance tools available send ICMP echo requests to a range of stations in the subnet and those without any filtering mechanisms will reply. Usually today's network infrastructures are equipped with filtering devices which restrict the use of ICMP echo. Therefore network reconnaissance applications have evolved and use other sophisticated methods to scan networks such UDP scans.

In Figure 11 the IP Angry Scanner is used to scan a range of target systems in the network. As shown some of the hosts have replied to the scan showing their IP addresses and DNS names [17]. It is also possible that other hosts are up in this network but it is assumed they are running some type of filtering application or firewall which filters ICMP echo or scan attempts.



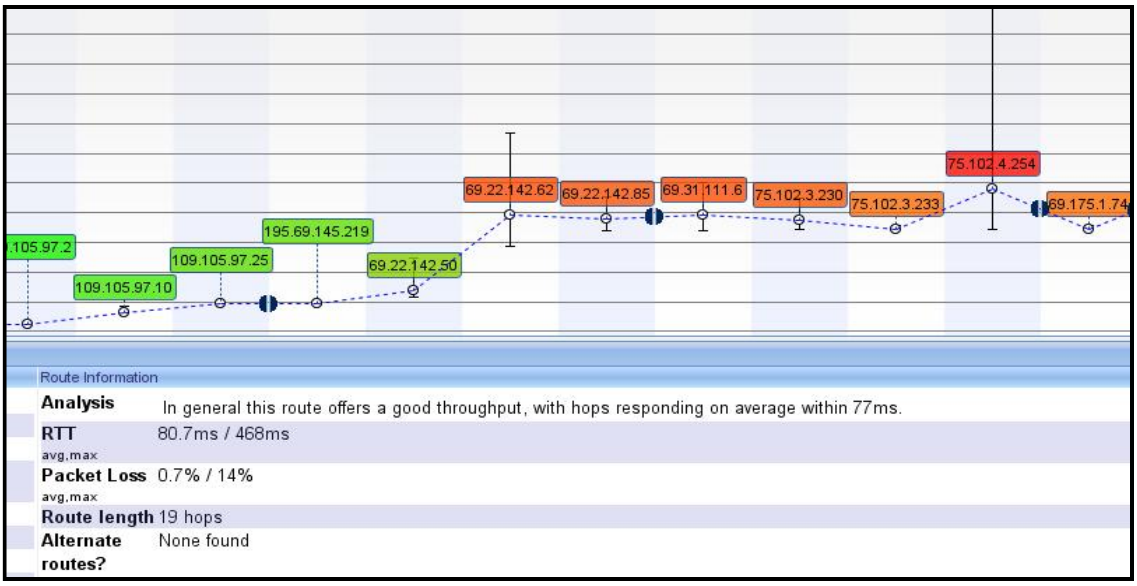
IP Range: 80.221.[redacted] to 80.221.[redacted] IP Range

Hostname: atutak[redacted] IP Netmask Start

IP	Ping	Hostname	Ports [0+]
🔵 80.221[redacted]	6 ms	ho[redacted]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔵 80.221[redacted]	4 ms	ho[redacted]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔵 80.221[redacted]	4 ms	ho[redacted]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔴 80.221[redacted]	[n/a]	[n/s]	[n/s]
🔵 80.221[redacted]	4 ms	ho[redacted]..	[n/s]

Figure 11: IP Angry scan [17]

In Figures 12-13 Visual route application is shown to do a source to destination trace and then present the route map showing source to target route map. This is useful scan as it shows the number of hops it takes to the destination, the IP, DNS names and location of the routers on the path to the target and also the service providers hosting them.



Route Information

Analysis	In general this route offers a good throughput, with hops responding on average within 77ms.
RTT avg,max	80.7ms / 468ms
Packet Loss avg,max	0.7% / 14%
Route length	19 hops
Alternate routes?	None found

Figure 12: Visual route scan [5]

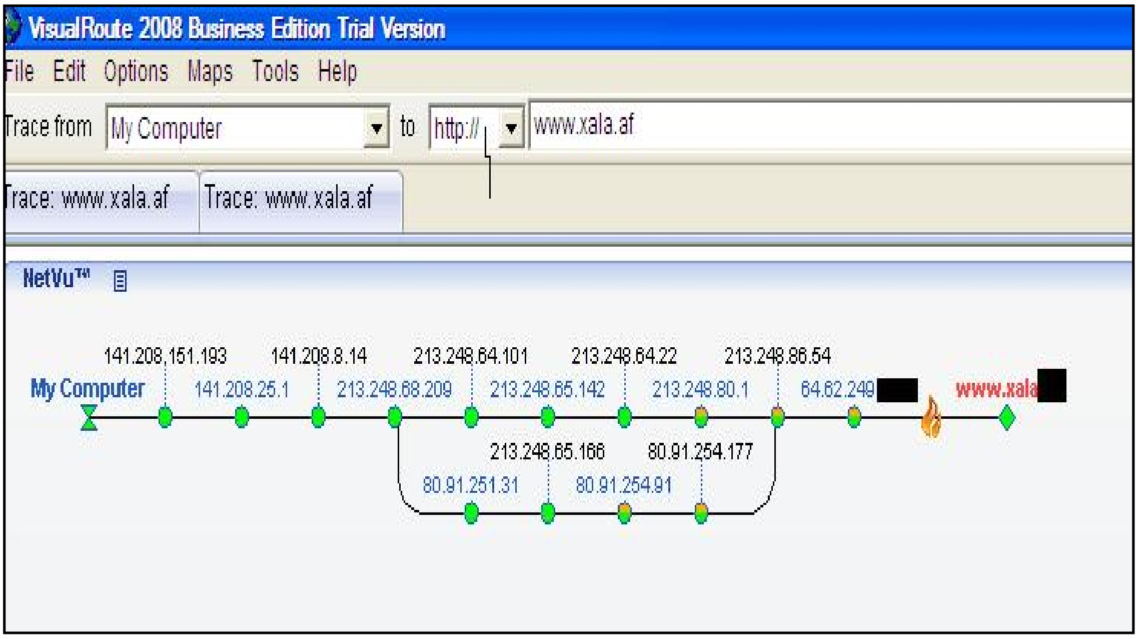
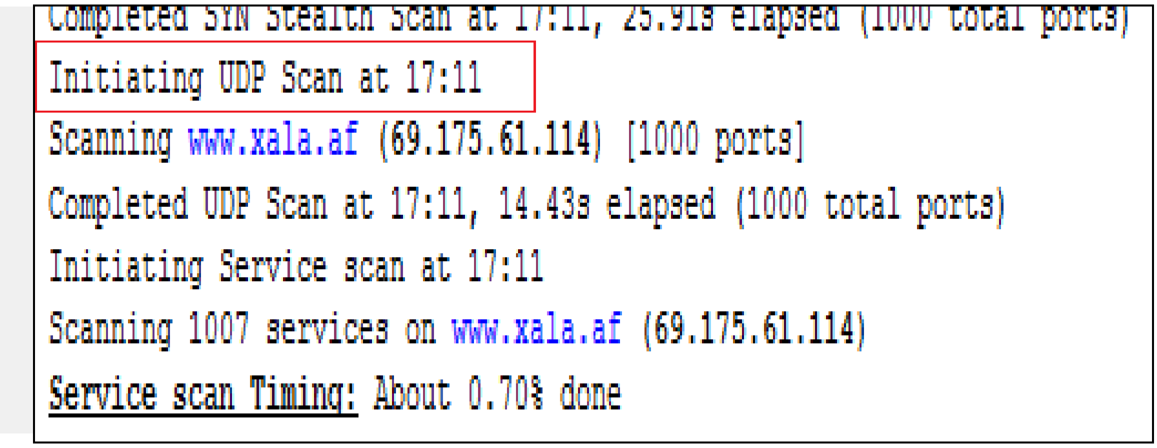


Figure 13: Visual route scan [5]

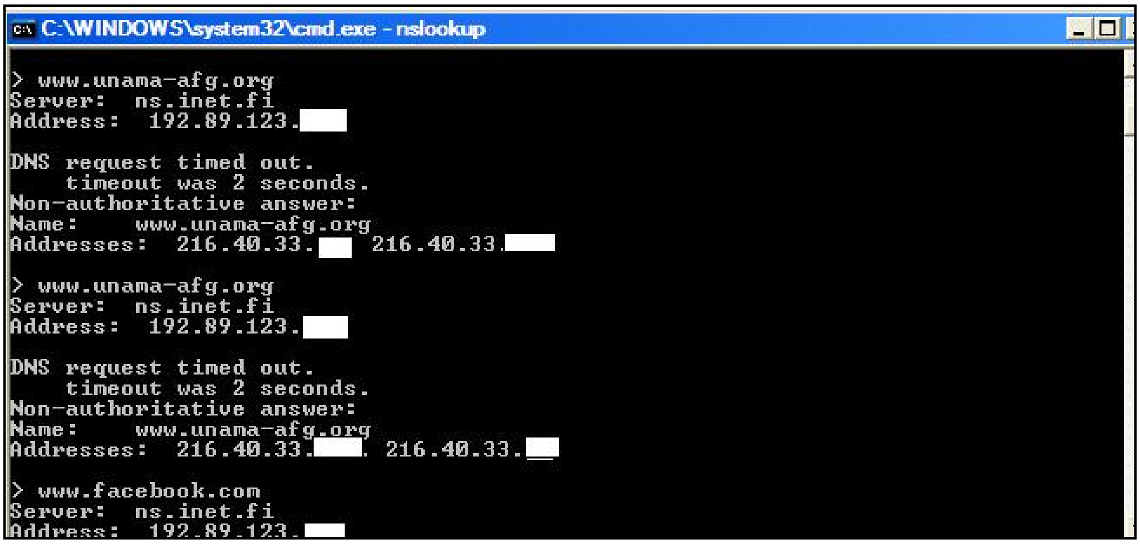
As indicated in the first IP angry scan that some of the target stations did not reply to the traditional ICMP Ping scan which is usually due to filtering applications such as firewall but other techniques are devised to scan systems for instance UDP- ping to see if the systems are up and running as shown in Figure 14.



```
Completed SYN Stealth Scan at 17:11, 25.91s elapsed (1000 total ports)
Initiating UDP Scan at 17:11
Scanning www.xala.af (69.175.61.114) [1000 ports]
Completed UDP Scan at 17:11, 14.43s elapsed (1000 total ports)
Initiating Service scan at 17:11
Scanning 1007 services on www.xala.af (69.175.61.114)
Service scan Timing: About 0.70% done
```

Figure 14: UDP scan [7]

Domain Name System (DNS) which translates DNS names to IP address or vice versa can also be used to scan for targets. Figure 15 shows some sites with their respective IP addresses.



```
> www.unama-afg.org
Server:  ns.inet.fi
Address:  192.89.123.[redacted]

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    www.unama-afg.org
Addresses:  216.40.33.[redacted]  216.40.33.[redacted]

> www.unama-afg.org
Server:  ns.inet.fi
Address:  192.89.123.[redacted]

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    www.unama-afg.org
Addresses:  216.40.33.[redacted]. 216.40.33.[redacted]

> www.facebook.com
Server:  ns.inet.fi
Address:  192.89.123.[redacted]
```

Figure 15: Nslookup [5]

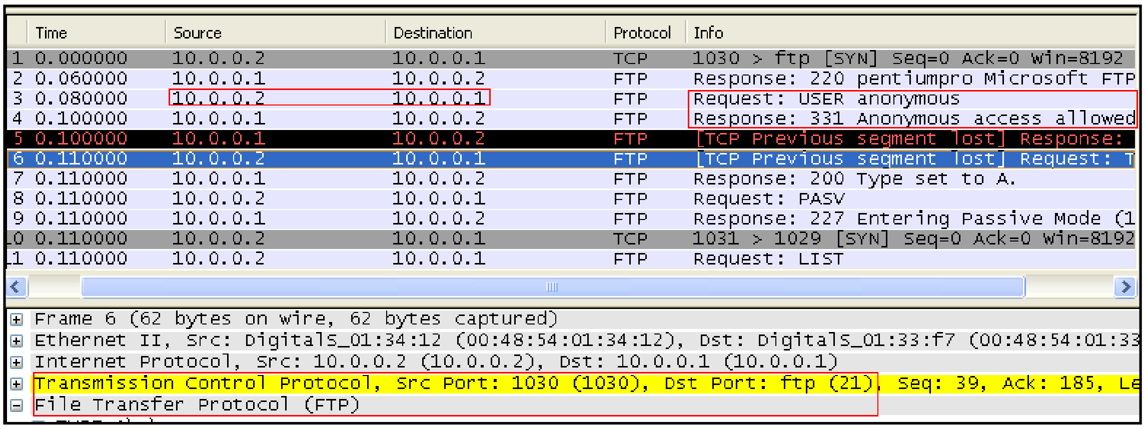
Once the attacker gets the IP addresses of the target system he can use this information to attack them in later stages.

4.5 Packet Sniffing

Sniffing is a practice where network traffic that is traversing the network is analysed and read. Sniffing is used by network engineers to identify issues in the network and troubleshoot accordingly.

Sniffing can be misused as it can be used to capture sensitive data such as passwords or username. Unless data travels within some sort of encrypted channels such as Virtual Private Networks (VPN) where the data is in encrypted form, it will be always prone to sniffing attacks. In addition to VPNs, a secure network design such as the use of VLANS also decreases the chances of sniffing attacks.

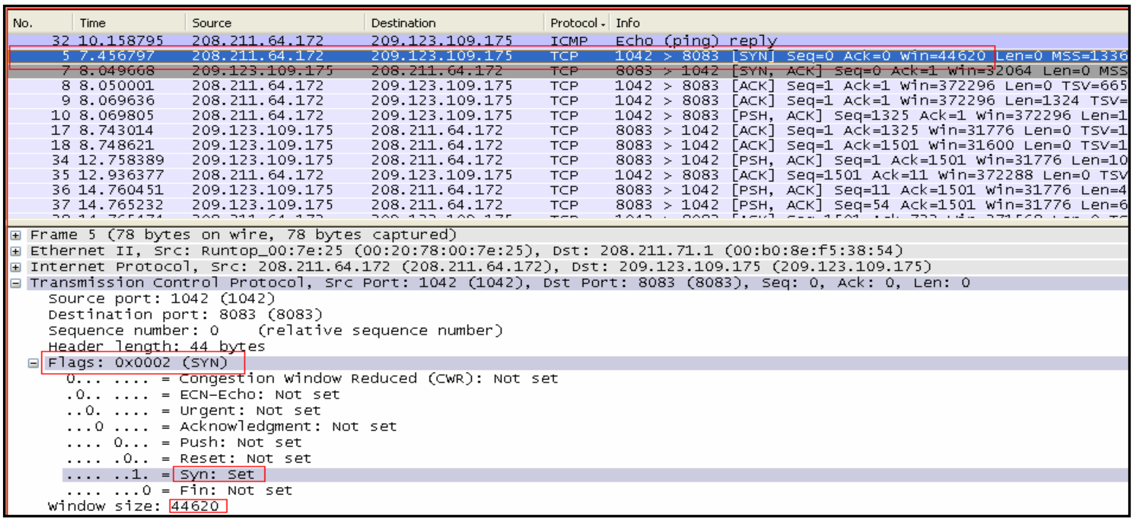
Ethereal LAN sniffer [8] is used to sniff the LAN, as shown in Figure 16. The sniffer was able to catch an FTP session between stations 10.0.0.2 and 10.0.0.1 where the FTP anonymous access is allowed. The penetration tester armed with this information can access the FTP server and upload or download data accordingly



```
   Time       Source          Destination     Protocol  Info
1  0.000000   10.0.0.2        10.0.0.1        TCP       1030 > ftp [SYN] Seq=0 Ack=0 Win=8192
2  0.060000   10.0.0.1        10.0.0.2        FTP       Response: 220 pentiumpro Microsoft FTP
3  0.080000   10.0.0.2        10.0.0.1        FTP       Request: USER anonymous
4  0.100000   10.0.0.1        10.0.0.2        FTP       Response: 331 Anonymous access allowed
5  0.100000   10.0.0.1        10.0.0.2        FTP       [TCP Previous segment lost] Response:
6  0.110000   10.0.0.2        10.0.0.1        FTP       [TCP Previous segment lost] Request: T
7  0.110000   10.0.0.1        10.0.0.2        FTP       Response: 200 Type set to A.
8  0.110000   10.0.0.2        10.0.0.1        FTP       Request: PASV
9  0.110000   10.0.0.1        10.0.0.2        FTP       Response: 227 Entering Passive Mode (1
10 0.110000   10.0.0.2        10.0.0.1        TCP       1031 > 1029 [SYN] Seq=0 Ack=0 Win=8192
11 0.110000   10.0.0.2        10.0.0.1        FTP       Request: LIST

⊞ Frame 6 (62 bytes on wire, 62 bytes captured)
⊞ Ethernet II, Src: Digitals_01:34:12 (00:48:54:01:34:12), Dst: Digitals_01:33:f7 (00:48:54:01:33
⊞ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 10.0.0.1 (10.0.0.1)
⊞ Transmission Control Protocol, Src Port: 1030 (1030), Dst Port: ftp (21), Seq: 39, Ack: 185, Le
⊟ File Transfer Protocol (FTP)
```

Figure 16: Ethereal FTP sniffing [8]

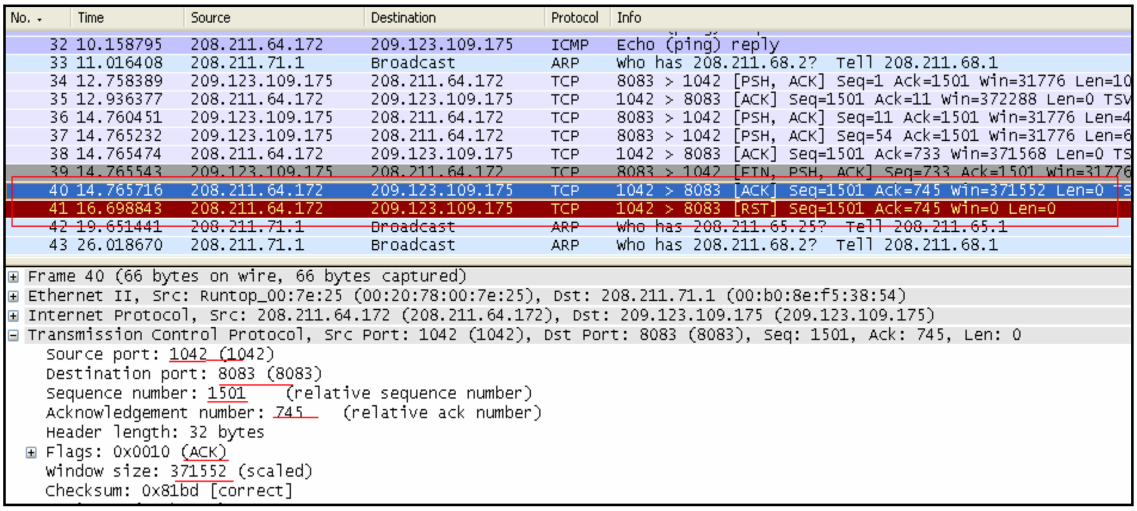
Ethereal LAN sniffer [8] has captured a simple conversation between certain stations. This capture includes the valuable layer 2 to layer 4 information. As shown in Figure 17, the information includes layer 2 MAC address, Source-Destination IP address, Source-Destination Ports. Armed with this valuable information target system can be narrowed down.



```
No.   Time        Source           Destination      Protocol  Info
   32 10.158795   208.211.64.172   209.123.109.175  ICMP      Echo (ping) reply
    5 7.456797    208.211.64.172   209.123.109.175  TCP       1042 > 8083 [SYN] Seq=0 Ack=0 Win=44620 Len=0 MSS=1336
    7 8.049668    209.123.109.175  208.211.64.172   TCP       8083 > 1042 [SYN, ACK] Seq=0 Ack=1 Win=32064 Len=0 MSS
    8 8.050001    208.211.64.172   209.123.109.175  TCP       1042 > 8083 [ACK] Seq=1 Ack=1 Win=372296 Len=0 TSV=665
    9 8.069636    208.211.64.172   209.123.109.175  TCP       1042 > 8083 [ACK] Seq=1 Ack=1 Win=372296 Len=1324 TSV=
   10 8.069805    208.211.64.172   209.123.109.175  TCP       1042 > 8083 [PSH, ACK] Seq=1325 Ack=1 Win=372296 Len=1
   17 8.743014    209.123.109.175  208.211.64.172   TCP       8083 > 1042 [ACK] Seq=1 Ack=1325 Win=31776 Len=0 TSV=1
   18 8.748621    209.123.109.175  208.211.64.172   TCP       8083 > 1042 [ACK] Seq=1 Ack=1501 Win=31600 Len=0 TSV=1
   34 12.758389   209.123.109.175  208.211.64.172   TCP       8083 > 1042 [PSH, ACK] Seq=1 Ack=1501 Win=31776 Len=10
   35 12.936377   208.211.64.172   209.123.109.175  TCP       1042 > 8083 [ACK] Seq=1501 Ack=11 Win=372288 Len=0 TSV
   36 14.760451   209.123.109.175  208.211.64.172   TCP       8083 > 1042 [PSH, ACK] Seq=11 Ack=1501 Win=31776 Len=4
   37 14.765232   209.123.109.175  208.211.64.172   TCP       8083 > 1042 [PSH, ACK] Seq=54 Ack=1501 Win=31776 Len=6

⊞ Frame 5 (78 bytes on wire, 78 bytes captured)
⊞ Ethernet II, Src: Runtop_00:7e:25 (00:20:78:00:7e:25), Dst: 208.211.71.1 (00:b0:8e:f5:38:54)
⊞ Internet Protocol, Src: 208.211.64.172 (208.211.64.172), Dst: 209.123.109.175 (209.123.109.175)
⊟ Transmission Control Protocol, Src Port: 1042 (1042), Dst Port: 8083 (8083), Seq: 0, Ack: 0, Len: 0
    Source port: 1042 (1042)
    Destination port: 8083 (8083)
    Sequence number: 0    (relative sequence number)
    Header length: 44 bytes
  ⊟ Flags: 0x0002 (SYN)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 44620
```

Figure 17: Ethereal Sniffer Layer2-Layer4 [8]

In Figure 18 layer 4 segment the information can be seen which includes normal TCP flags, window size, source and destination ports. This information is helpful in carrying out various attacks such session hijacking, man-in-the-middle or synchronisation.



```
No. -   Time        Source            Destination       Protocol  Info
     32 10.158795   208.211.64.172    209.123.109.175   ICMP      Echo (ping) reply
     33 11.016408   208.211.71.1      Broadcast         ARP       Who has 208.211.68.2?  Tell 208.211.68.1
     34 12.758389   209.123.109.175   208.211.64.172    TCP       8083 > 1042 [PSH, ACK] Seq=1 Ack=1501 Win=31776 Len=10
     35 12.936377   208.211.64.172    209.123.109.175   TCP       1042 > 8083 [ACK] Seq=1501 Ack=11 Win=372288 Len=0 TSV
     36 14.760451   209.123.109.175   208.211.64.172    TCP       8083 > 1042 [PSH, ACK] Seq=11 Ack=1501 Win=31776 Len=4
     37 14.765232   209.123.109.175   208.211.64.172    TCP       8083 > 1042 [PSH, ACK] Seq=54 Ack=1501 Win=31776 Len=6
     38 14.765474   208.211.64.172    209.123.109.175   TCP       1042 > 8083 [ACK] Seq=1501 Ack=733 Win=371568 Len=0 TS
     39 14.765543   209.123.109.175   208.211.64.172    TCP       8083 > 1042 [FIN, PSH, ACK] Seq=733 Ack=1501 Win=31776
     40 14.765716   208.211.64.172    209.123.109.175   TCP       1042 > 8083 [ACK] Seq=1501 Ack=745 Win=371552 Len=0 TS
     41 16.698843   208.211.64.172    209.123.109.175   TCP       1042 > 8083 [RST] Seq=1501 Ack=745 Win=0 Len=0
     42 19.651441   208.211.71.1      Broadcast         ARP       Who has 208.211.65.25?  Tell 208.211.65.1
     43 26.018670   208.211.71.1      Broadcast         ARP       Who has 208.211.68.2?  Tell 208.211.68.1

⊞ Frame 40 (66 bytes on wire, 66 bytes captured)
⊞ Ethernet II, Src: Runtop_00:7e:25 (00:20:78:00:7e:25), Dst: 208.211.71.1 (00:b0:8e:f5:38:54)
⊞ Internet Protocol, Src: 208.211.64.172 (208.211.64.172), Dst: 209.123.109.175 (209.123.109.175)
⊟ Transmission Control Protocol, Src Port: 1042 (1042), Dst Port: 8083 (8083), Seq: 1501, Ack: 745, Len: 0
    Source port: 1042 (1042)
    Destination port: 8083 (8083)
    Sequence number: 1501    (relative sequence number)
    Acknowledgement number: 745    (relative ack number)
    Header length: 32 bytes
  ⊞ Flags: 0x0010 (ACK)
    Window size: 371552 (scaled)
    Checksum: 0x81bd [correct]
```

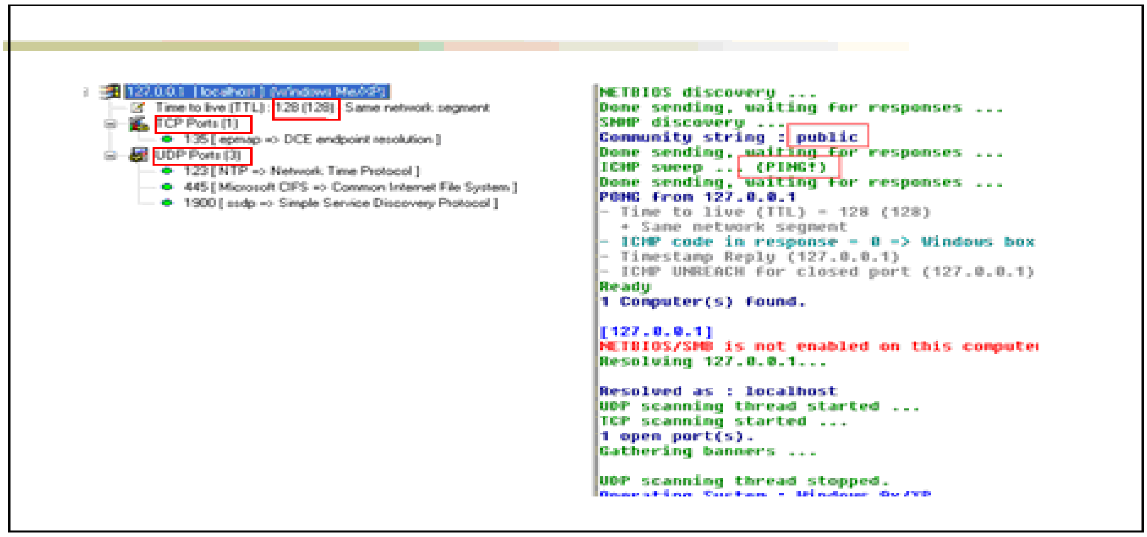
Figure 18: Ethereal Sniffer TCP flags [8]

Furthermore Sniffing attacks have been gaining ground as more and more people use wireless or flat networks to access network resources and even some of the security mechanisms in place are vulnerable to attacks.

4.6 Ports Scanning

Port scanning is a process by which systems are scanned for open ports. Part of the reconnaissance phase where the attacker tries to identify open, closed or filtered posts in the target system and some of these vulnerable ports are then further exploited. Port scan gives the attacker a good idea of the type of services running on the target system, such as Shares, Web services or FTP.

LAN guard scanner is used to port scan the target system [9]. Although well-known as vulnerability scanner it can also help in port scanning system. As shown in Figure 19 the target system is checked for open ports and services. This system has four ports open in total i.e. TCP 125 while port UDP 445, 1900,123.

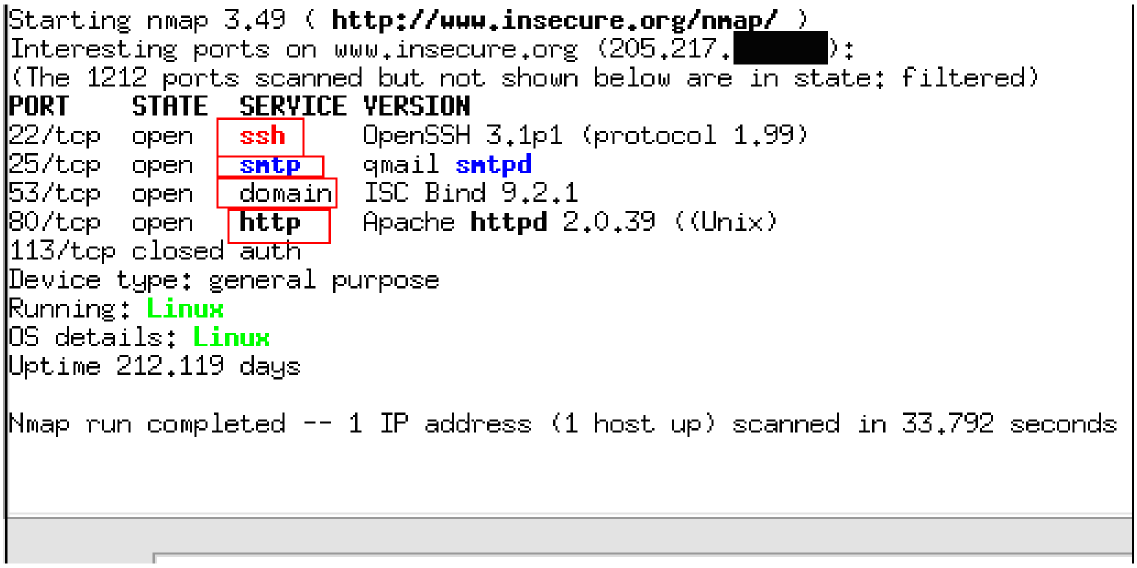


```
127.0.0.1 [ localhost ] (Windows Me/XP)
    Time to live (TTL) : 128 (128) Same network segment
    TCP Ports (1)
        135 [ epmap => DCE endpoint resolution ]
    UDP Ports (3)
        123 [ NTP => Network Time Protocol ]
        445 [ Microsoft CIFS => Common Internet File System ]
        1900 [ ssdp => Simple Service Discovery Protocol ]
```

```
NETBIOS discovery ...
Done sending, waiting for responses ...
SNMP discovery ...
Community string : public
Done sending, waiting for responses ...
ICMP sweep ... (PING!)
Done sending, waiting for responses ...
PONG from 127.0.0.1
- Time to live (TTL) = 128 (128)
  + Same network segment
- ICMP code in response = 0 => Windows box
- Timestamp Reply (127.0.0.1)
- ICMP UNREACH for closed port (127.0.0.1)
Ready
1 Computer(s) found.

[127.0.0.1]
NETBIOS/SMB is not enabled on this compute
Resolving 127.0.0.1...

Resolved as : localhost
UDP scanning thread started ...
TCP scanning started ...
1 open port(s).
Gathering banners ...

UDP scanning thread stopped.
Operating System : Windows 9x/XP
```

Figure 19: LAN Guard Port Scan [9]

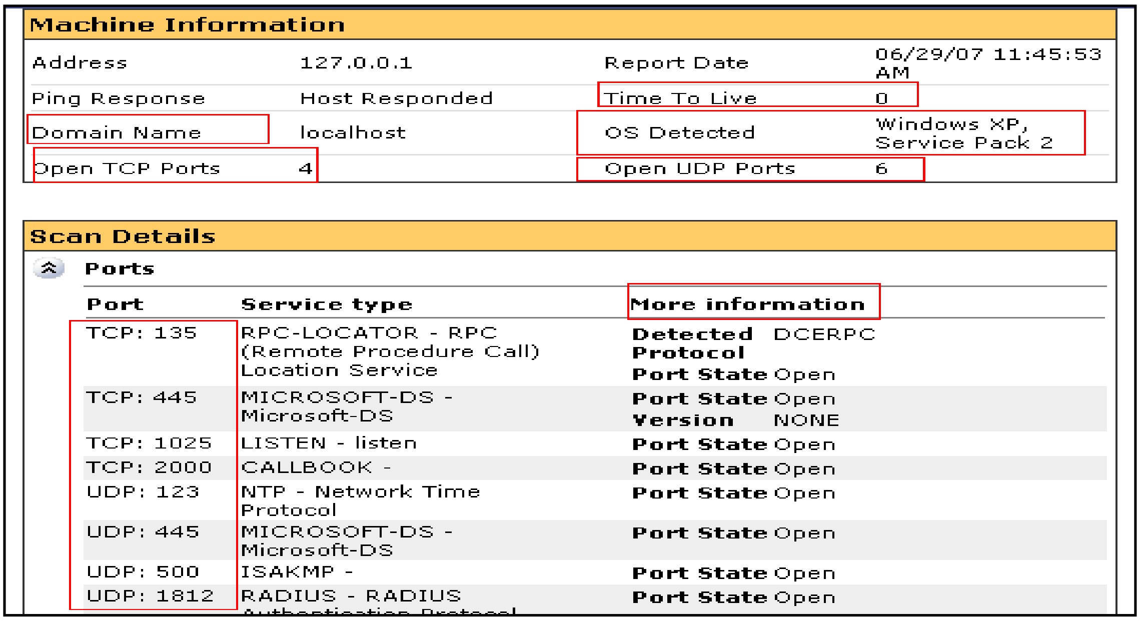
Although LAN guard scanner [9] does an excellent job in scanning target systems if the systems accept ICMP echo requests however as majority of the systems now a days are by default denying ICMP ping, therefore in those situations NMAP works much better. It comes with intelligent techniques to port scan system and bypass basic filtering. Figure 20 shows a system being targeted by NMAP.



```
Starting nmap 3.49 ( http://www.insecure.org/nmap/ )
Interesting ports on www.insecure.org (205.217.[redacted]):
(The 1212 ports scanned but not shown below are in state: filtered)
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 3.1p1 (protocol 1.99)
25/tcp   open   smtp    qmail smtpd
53/tcp   open   domain  ISC Bind 9.2.1
80/tcp   open   http    Apache httpd 2.0.39 ((Unix)
113/tcp closed auth
Device type: general purpose
Running: Linux
OS details: Linux
Uptime 212.119 days

Nmap run completed -- 1 IP address (1 host up) scanned in 33.792 seconds
```

Figure 20: NMAP Port Scan, OS Fingerprint [7]

Furthermore in Figure 21 Eye's security scanner [33] is used to port scan a target system for open ports. The result from the scan shows that system has four TCP and six UDP ports.



Machine Information

Address	127.0.0.1	Report Date	06/29/07 11:45:53 AM
Ping Response	Host Responded	Time To Live	0
Domain Name	localhost	OS Detected	Windows XP, Service Pack 2
Open TCP Ports	4	Open UDP Ports	6

Scan Details

Ports

Port	Service type	More information
TCP: 135	RPC-LOCATOR - RPC (Remote Procedure Call) Location Service	**Detected Protocol** DCERPC **Port State** Open
TCP: 445	MICROSOFT-DS - Microsoft-DS	**Port State** Open **Version** NONE
TCP: 1025	LISTEN - listen	**Port State** Open
TCP: 2000	CALLBOOK -	**Port State** Open
UDP: 123	NTP - Network Time Protocol	**Port State** Open
UDP: 445	MICROSOFT-DS - Microsoft-DS	**Port State** Open
UDP: 500	ISAKMP -	**Port State** Open
UDP: 1812	RADIUS - RADIUS Authentication Protocol	**Port State** Open

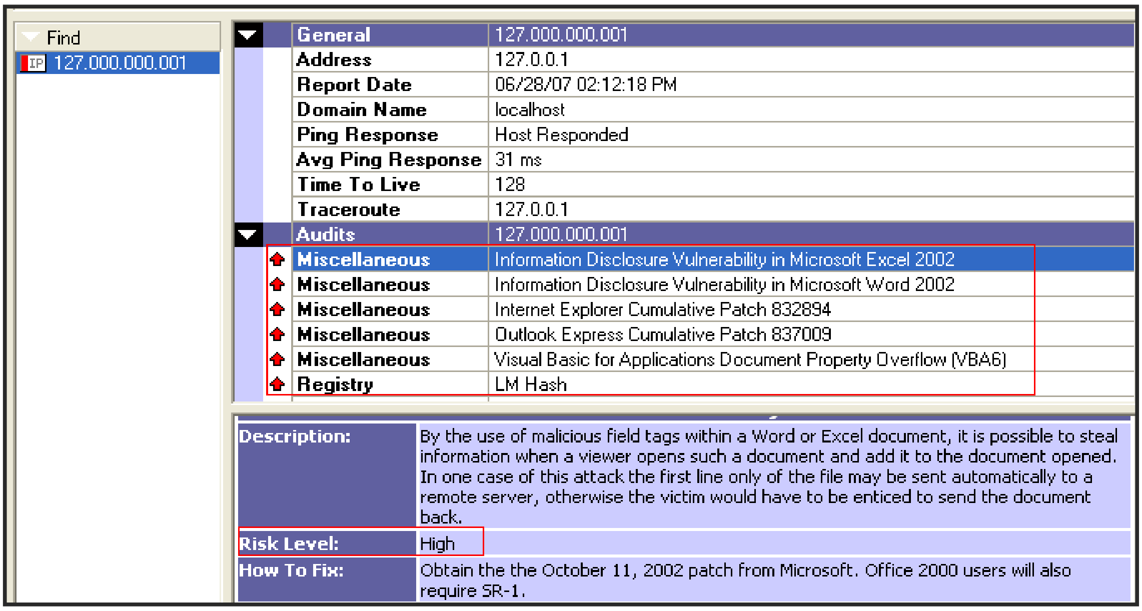
Figure 21: Port Scan Cont [33]

These open ports can then used as a way to target systems for further attacks. The more vulnerable ports open in the system the more it is prone to attacks.

4.7 Vulnerability Scanning

Vulnerability scanning tools such as LAN guard, Retina and Nessus are used to find weak points in target systems and provide mitigations measure for them. But on the flip side the same tools can be exploited to assist in penetrating target systems

In Figure 22 Retina shows a target system with various vulnerabilities. It is [33] actually meant for system administrators to patch vulnerable system, but the same listed vulnerabilities can be exploited by deploying various publically available exploits to penetrate target systems.



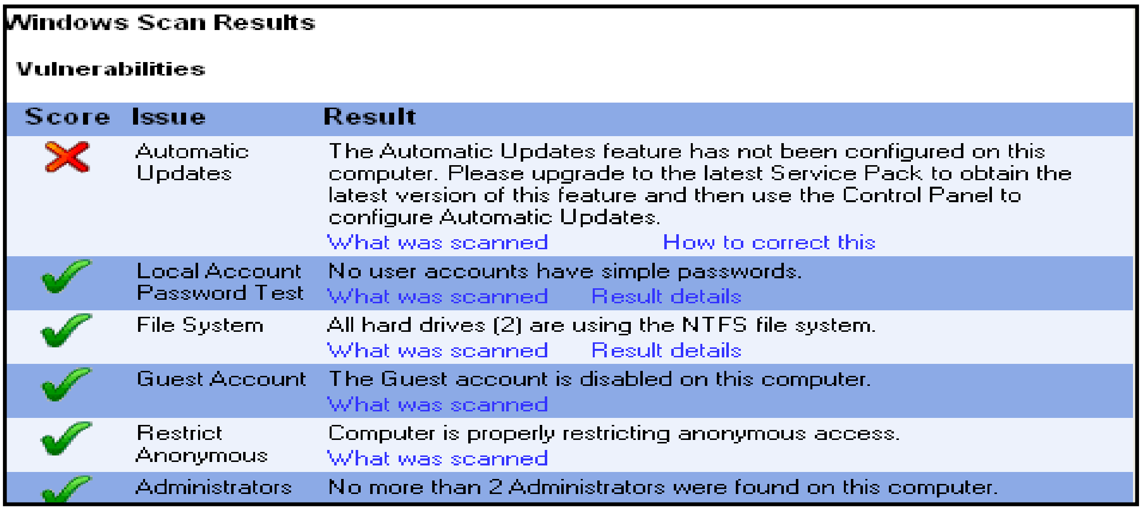
Find
127.000.000.001

	General	127.000.000.001
	Address	127.0.0.1
	Report Date	06/28/07 02:12:18 PM
	Domain Name	localhost
	Ping Response	Host Responded
	Avg Ping Response	31 ms
	Time To Live	128
	Traceroute	127.0.0.1
	Audits	127.000.000.001
⬆	Miscellaneous	Information Disclosure Vulnerability in Microsoft Excel 2002
⬆	Miscellaneous	Information Disclosure Vulnerability in Microsoft Word 2002
⬆	Miscellaneous	Internet Explorer Cumulative Patch 832894
⬆	Miscellaneous	Outlook Express Cumulative Patch 837009
⬆	Miscellaneous	Visual Basic for Applications Document Property Overflow (VBA6)
⬆	Registry	LM Hash

Description:	By the use of malicious field tags within a Word or Excel document, it is possible to steal information when a viewer opens such a document and add it to the document opened. In one case of this attack the first line only of the file may be sent automatically to a remote server, otherwise the victim would have to be enticed to send the document back.
Risk Level:	High
How To Fix:	Obtain the the October 11, 2002 patch from Microsoft. Office 2000 users will also require SR-1.

Figure 22: Retina Vulnerability Scan [33]

Microsoft Baseline Security Analyzer (MBSA) [18] does the same vulnerability scan with various vulnerabilities listed on the level of risk. Figure 23 shows an example of MBSA.



Windows Scan Results

Vulnerabilities

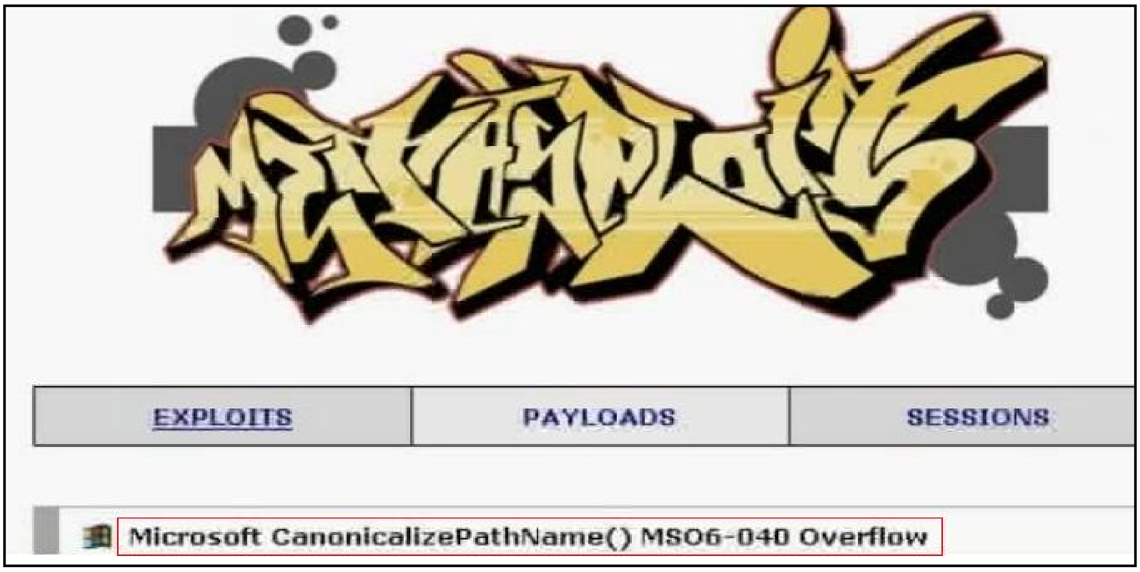
Score	Issue	Result
✗	Automatic Updates	The Automatic Updates feature has not been configured on this computer. Please upgrade to the latest Service Pack to obtain the latest version of this feature and then use the Control Panel to configure Automatic Updates. What was scanned How to correct this
✓	Local Account Password Test	No user accounts have simple passwords. What was scanned Result details
✓	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
✓	Guest Account	The Guest account is disabled on this computer. What was scanned
✓	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
✓	Administrators	No more than 2 Administrators were found on this computer.

Figure 23: MBSA Vulnerability Scan [18]

4.8 Vulnerability Exploits / Metasploit

Once the target systems have been tested for vulnerabilities and weaknesses, these vulnerabilities can be exploited by either writing one’s own exploits or using publicly available exploits. There are well-known automated tools that use a large pool of exploits to attack systems. One of the most well known is Metasploit. [10]

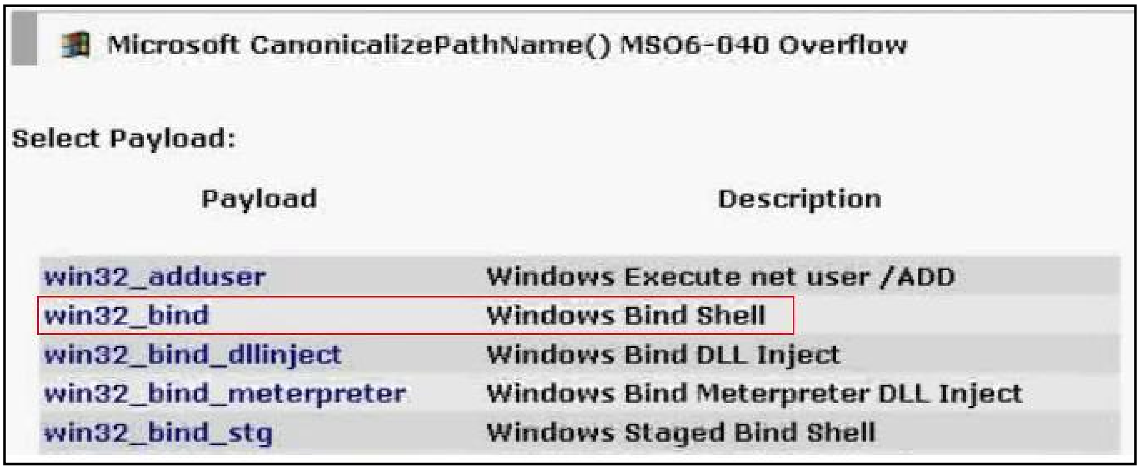
Metasploit is used to attack an unpatched vulnerable system. The specific exploit is selected from a list of exploits available to the attacker, see Figures 24-25. In this particular exploit the attacker penetrates the target system and acquires administrative privileges.



Microsoft CanonicalizePathName() MS06-040 Overflow

Figure 24: Metasploit Vulnerability exploit [10]

‘



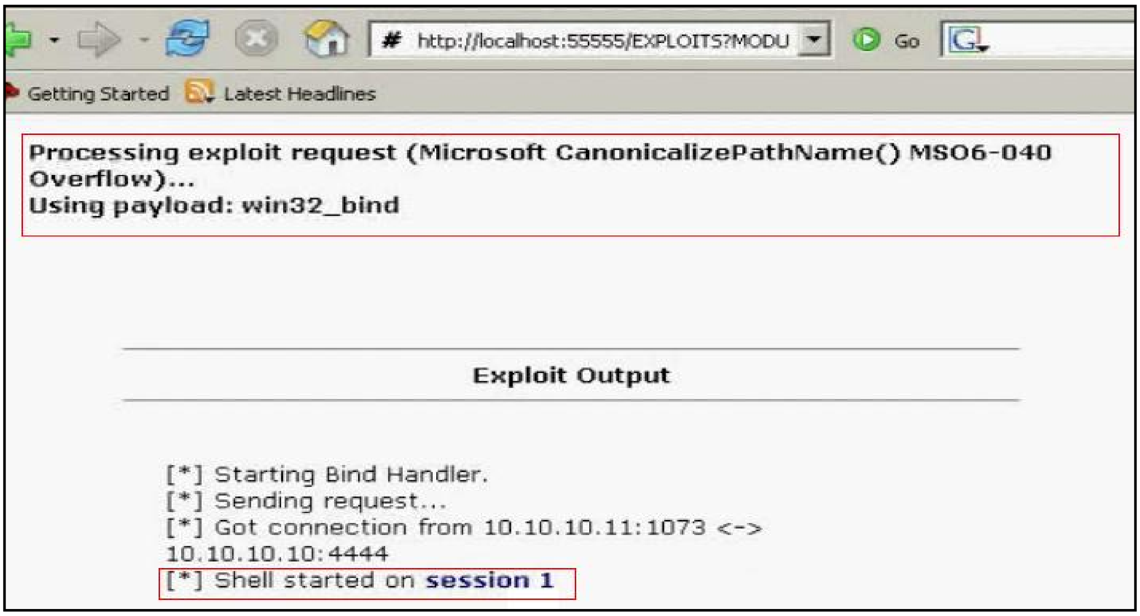
Microsoft CanonicalizePathName() MS06-040 Overflow

Select Payload:

Payload	Description
win32_adduser	Windows Execute net user /ADD
win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject
win32_bind_stg	Windows Staged Bind Shell

Figure 25: Metasploit Vulnerability exploit [10]

Once the exploit is deployed, the attacker gains a shell connection the target system as shown in Figure 26, there he has a complete control over the system.



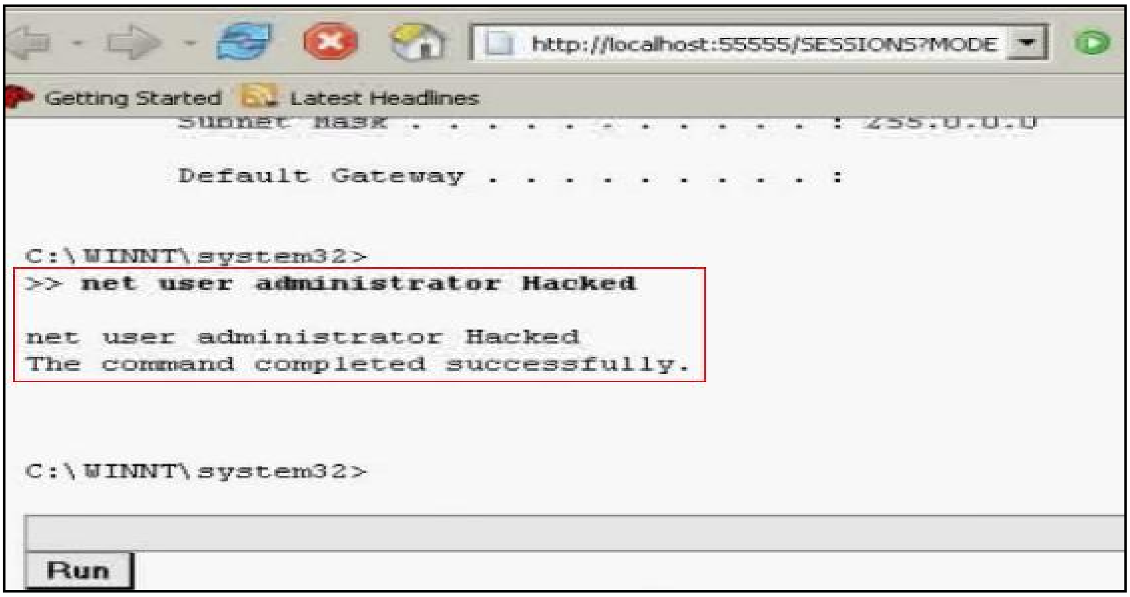
```
Processing exploit request (Microsoft CanonicalizePathName() MS06-040
Overflow)...
Using payload: win32_bind
```

Exploit Output

```
[*] Starting Bind Handler.
[*] Sending request...
[*] Got connection from 10.10.10.11:1073 <->
10.10.10.10:4444
[*] Shell started on session 1
```

Figure 26: Metasploit connected [10]

In this instance the attacker gains shell access to the target system via vulnerability in the OS and changes the administrator password, See Figure 27.



```
        Subnet Mask . . . . . . . . . . . : 255.0.0.0

        Default Gateway . . . . . . . . . :


C:\WINNT\system32>
>> net user administrator Hacked

net user administrator Hacked
The command completed successfully.



C:\WINNT\system32>
```

Figure 27: Metasploit password changed [10]

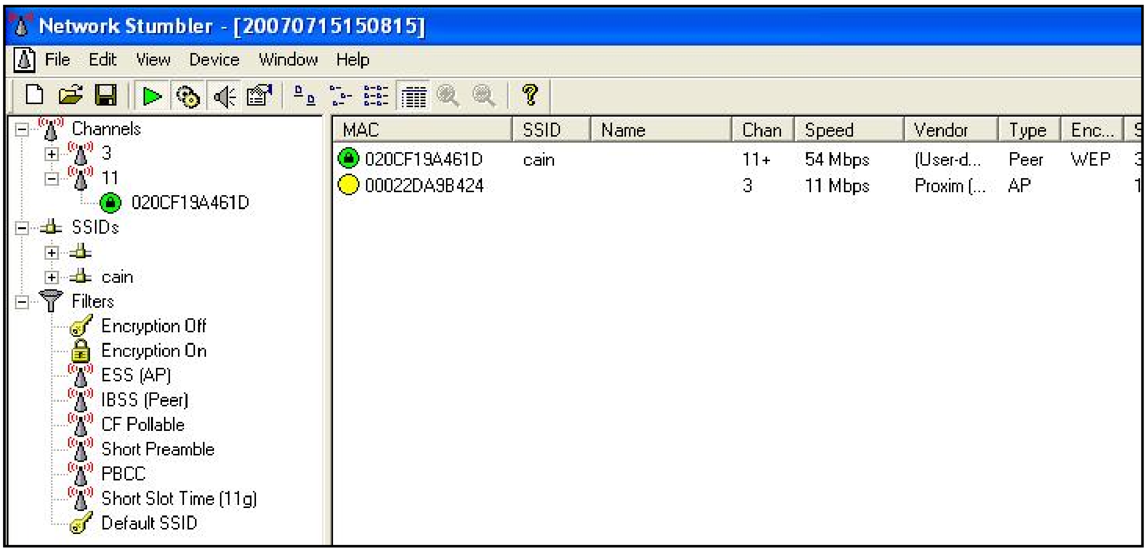
In addition to Metasploit there are other commercial tools such as Immunity's CANVAS or Core Security Technologies Core Impact which can also conduct vulnerability testing but the flip side is that they are more expensive.

4.9 Wireless Hack

Users are increasingly using the wireless technology to communicate. Such use of the so called Wi-Fi has increased the chances of attacks. Although wireless technologies do come with security feature to securely transfer data over encrypted means, still these security measures are prone to attacks. One of the mostly widely used wireless security mechanism is the WEP [11]. In this project it will show how WEP can be broken and compromised using publicly available cracking tools.

NetStumbler [30] has been used extensively by network engineers to site survey and troubleshoot WLANs but on the flip side the same tool is used by attackers to identify and seek out wireless networks in the area, see Figure 28.

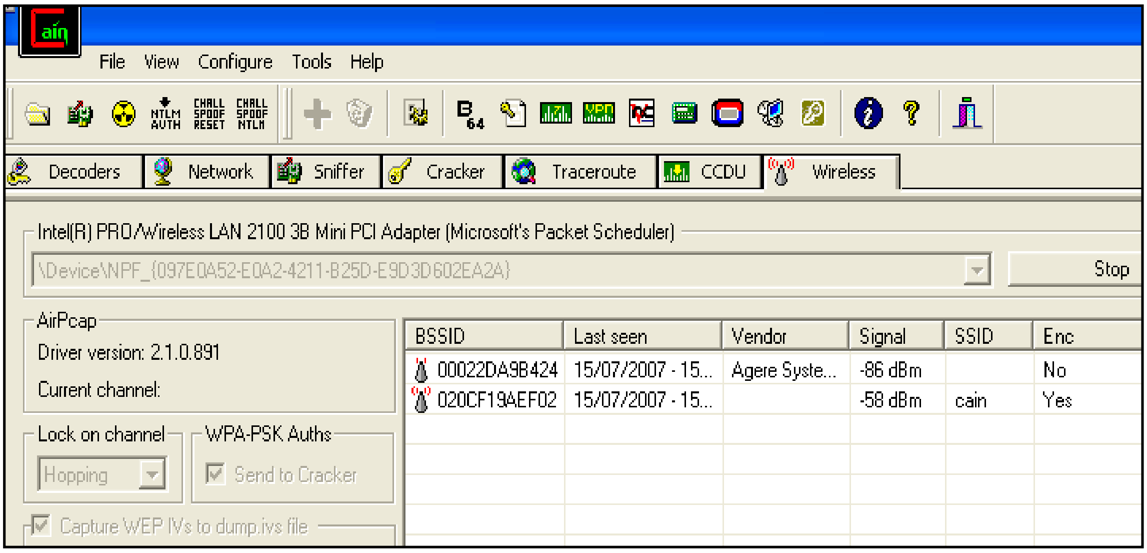
NetStumbler shows the MAC address, SSID, the respective radio channel and security mechanism in place like WEP. Usually the attacker uses a high gain antenna to seek out as much wireless networks as possible.



MAC	SSID	Name	Chan	Speed	Vendor	Type	Enc...	S
● 020CF19A461D	cain		11+	54 Mbps	(User-d...	Peer	WEP	3
○ 00022DA9B424			3	11 Mbps	Proxim (...	AP		1

Figure 28: NetStumbler WLAN Reconnaissance [30]

Cain [12] one of the most well known testing tool is also used to identify WLAN. Cain also shows the signal strength of each WLAN Figure 29.



Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter (Microsoft's Packet Scheduler)

\Device\NPF_{097E0A52-E0A2-4211-B25D-E9D3D602EA2A}

AirPcap

Driver version: 2.1.0.891

Current channel:

Lock on channel: Hopping

WPA-PSK Auths: ☑ Send to Cracker

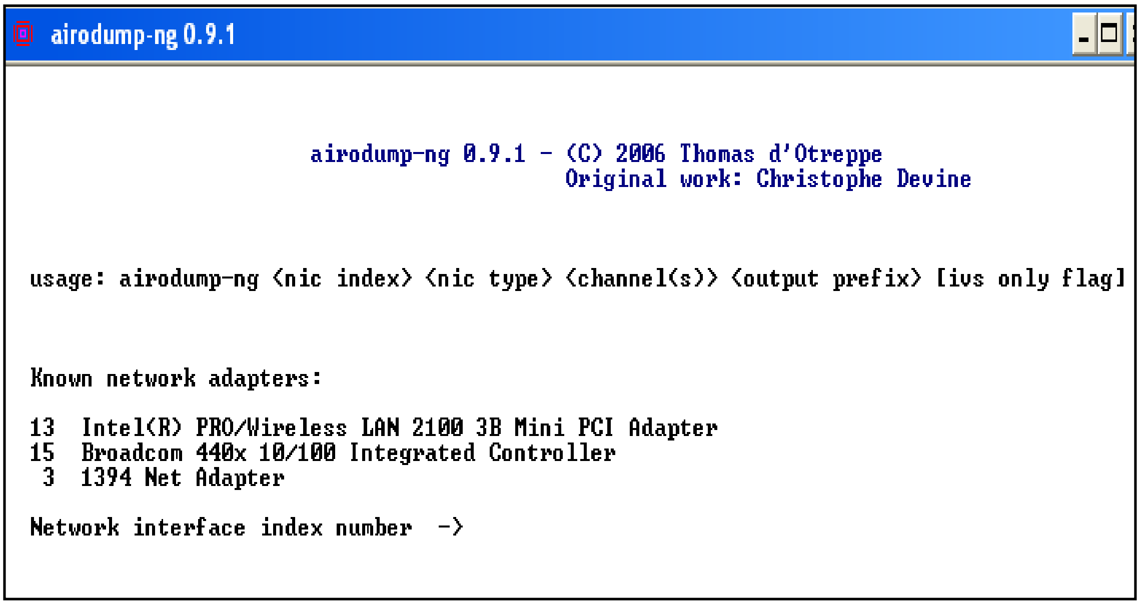
☑ Capture WEP IVs to dump.ivs file

BSSID	Last seen	Vendor	Signal	SSID	Enc
00022DA9B424	15/07/2007 - 15...	Agere Syste...	-86 dBm		No
020CF19AEF02	15/07/2007 - 15...		-58 dBm	cain	Yes

Figure 29: Cain WLAN Reconnaissance [12]

Once the WLAN is identified and known to be running WEP, the next step is to use tools such as Airodump [28] to capture as much encrypted traffic as possible. Each encrypted packet contains a 3-byte Initialization Vector (IV) which is later used to crack WEP.

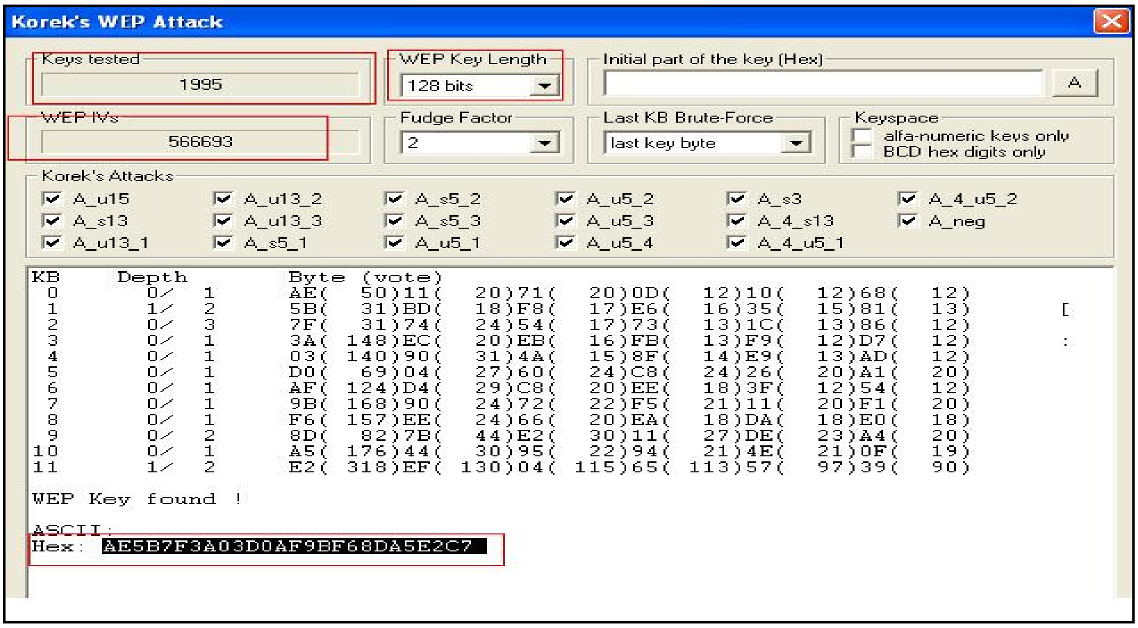
As shown in Figure 30, Airodump is used to capture traffic by selecting the appropriate network interface card.



```
                      airodump-ng 0.9.1 - (C) 2006 Thomas d'Otreppe
                                          Original work: Christophe Devine


usage: airodump-ng <nic index> <nic type> <channel(s)> <output prefix> [ivs only flag]


Known network adapters:

13  Intel(R) PRO/Wireless LAN 2100 3B Mini PCI Adapter
15  Broadcom 440x 10/100 Integrated Controller
 3  1394 Net Adapter

Network interface index number  ->
```

Figure 30: Airodump Traffic Capture [28]

After sufficient WEP IVs have been collected by Airodump, the WEP crack utility is used to crack WEP keys as shown in Figure 31. WEP crack is an impressive utility to crack the WEP security mechanism if sufficient IVs are available [29]



Korek's WEP Attack

Keys tested: 1995

WEP Key Length: 128 bits

Initial part of the key (Hex):

WEP IVs: 566693

Fudge Factor: 2

Last KB Brute-Force: last key byte

Keyspace
□ alfa-numeric keys only
□ BCD hex digits only

Korek's Attacks

☑ A_u15 ☑ A_u13_2 ☑ A_s5_2 ☑ A_u5_2 ☑ A_s3 ☑ A_4_u5_2
☑ A_s13 ☑ A_u13_3 ☑ A_s5_3 ☑ A_u5_3 ☑ A_4_s13 ☑ A_neg
☑ A_u13_1 ☑ A_s5_1 ☑ A_u5_1 ☑ A_u5_4 ☑ A_4_u5_1

```
KB     Depth          Byte (vote)
 0       0/  1        AE(  50)11(  20)71(  20)0D(  12)10(  12)68(  12)
 1       1/  2        5B(  31)BD(  18)F8(  17)E6(  16)35(  15)81(  13)      [
 2       0/  3        7F(  31)74(  24)54(  17)73(  13)1C(  13)86(  12)
 3       0/  1        3A( 148)EC(  20)EB(  16)FB(  13)F9(  12)D7(  12)      :
 4       0/  1        03( 140)90(  31)4A(  15)8F(  14)E9(  13)AD(  12)
 5       0/  1        D0(  69)04(  27)60(  24)C8(  24)26(  20)A1(  20)
 6       0/  1        AF( 124)D4(  29)C8(  20)EE(  18)3F(  12)54(  12)
 7       0/  1        9B( 168)90(  24)72(  22)F5(  21)11(  20)F1(  20)
 8       0/  1        F6( 157)EE(  24)66(  20)EA(  18)DA(  18)E0(  18)
 9       0/  2        8D(  82)7B(  44)E2(  30)11(  27)DE(  23)A4(  20)
10       0/  1        A5( 176)44(  30)95(  22)94(  21)4E(  21)0F(  19)
11       1/  2        E2( 318)EF( 130)04( 115)65( 113)57(  97)39(  90)

WEP Key found !

ASCII:
Hex:  AE5B7F3A03D0AF9BF68DA5E2C7
```

Figure 31: WEP Crack [29]

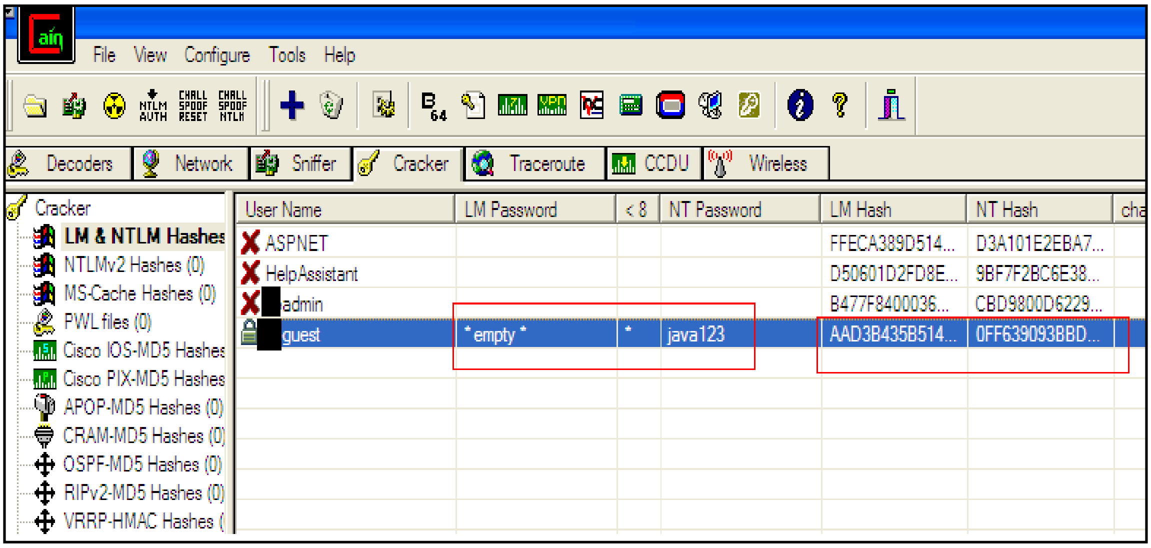
It is estimated that almost 300,000 packets are needed to break 64-bit WEP while 1,000,000 packets are needed for breaking 128-bit WEP

4.10 Password Cracking

Password cracking is the process of revealing or breaking passwords by running automated tools. These password cracks are due to the weakness in the cryptographic algorithms, weak implementation of the algorithm or simply weak passwords. There is lots of password cracking tools in the public domain but the most well-known are Cain and Lopht crack.

Cain is an excellent security testing tool that cracks, war drives and sniffs data networks. Used by network administrators for network auditing purposes, it has a powerful password cracking utility.

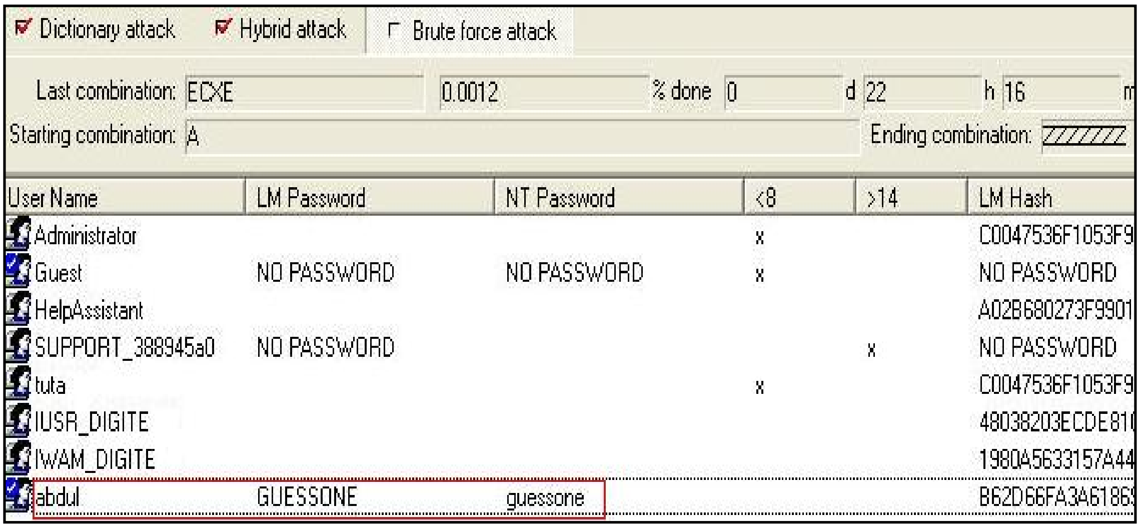
As shown in Figure 32, Cain [12] has successfully cracked the local passwords on the target system, revealing the password and respective hash values. The duration of a typical password crack depends on the type of attack carried out, i.e. Brute force or dictionary and the complexity of the password.



User Name	LM Password	< 8	NT Password	LM Hash	NT Hash	cha
ASPNET				FFECA389D514...	D3A101E2EBA7...	
HelpAssistant				D50601D2FD8E...	9BF7F2BC6E38...	
[redacted]admin				B477F8400036...	CBD9800D6229...	
[redacted]guest	* empty *	*	java123	AAD3B435B514...	0FF639093BBD...	

Figure 32: Cain Password Crack [12]

Lopht Crack [13] is another impressive piece of cracking software that reveals and breaks passwords on Windows and UNIX platforms. It is fast in cracking password as it as a table of millions of passwords. As shown in the Figure 33 LC is used to crack a password on a target windows machine.


☑ Dictionary attack ☑ Hybrid attack □ Brute force attack

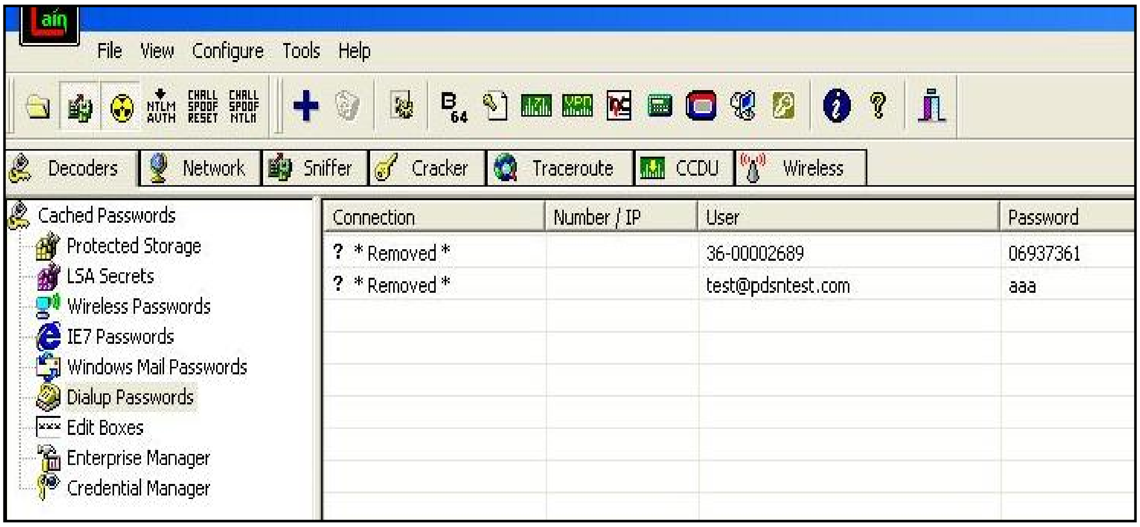
Last combination: ECXE 0.0012 % done 0 d 22 h 16 m

Starting combination: A Ending combination: ZZZZZZZ

User Name	LM Password	NT Password	<8	>14	LM Hash
Administrator			x		C0047536F1053F9
Guest	NO PASSWORD	NO PASSWORD	x		NO PASSWORD
HelpAssistant					A02B680273F9901
SUPPORT_388945a0	NO PASSWORD			x	NO PASSWORD
tuta			x		C0047536F1053F9
IUSR_DIGITE					48038203ECDE81(
IWAM_DIGITE					1980A5633157A44
abdul	GUESSONE	guessone			B62D66FA3A6186

Figure 33: Lopht Crack [13]

In Figure 34 Cain is again used to reveal dial up connection passwords and username on the target stations.

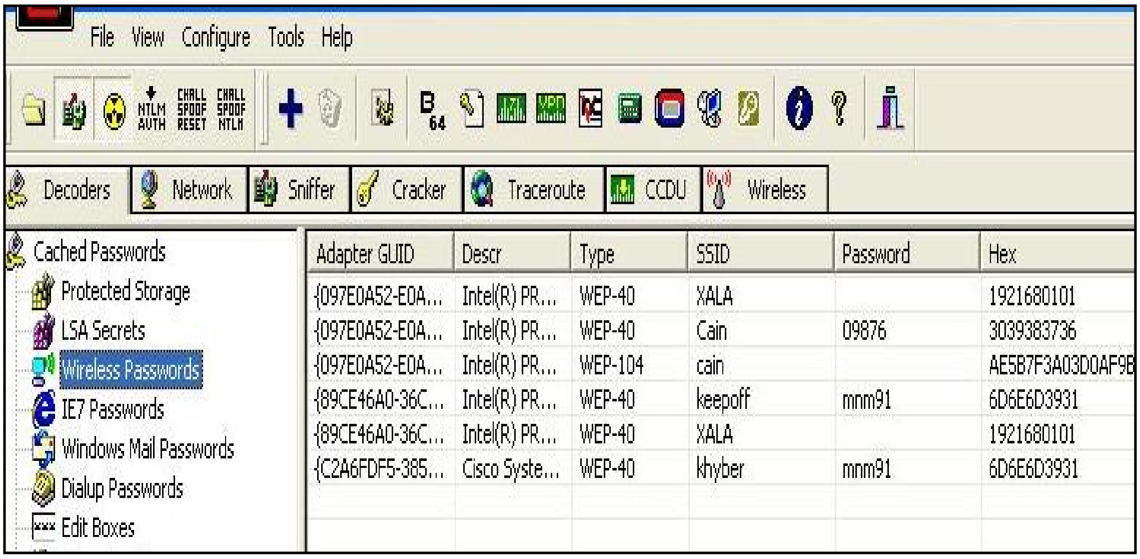


Cached Passwords
- Protected Storage
- LSA Secrets
- Wireless Passwords
- IE7 Passwords
- Windows Mail Passwords
- Dialup Passwords
- Edit Boxes
- Enterprise Manager
- Credential Manager

Connection	Number / IP	User	Password
? * Removed *		36-00002689	06937361
? * Removed *		test@pdsntest.com	aaa

Figure 34: Cain Dialup passwords [12]

In Figure 35 Cain has been used to show the Wireless WLAN SSID, the password or key and also the type of WEP being in place.



Cached Passwords
- Protected Storage
- LSA Secrets
- Wireless Passwords
- IE7 Passwords
- Windows Mail Passwords
- Dialup Passwords
- Edit Boxes

Adapter GUID	Descr	Type	SSID	Password	Hex
{097E0A52-E0A...	Intel(R) PR...	WEP-40	XALA		1921680101
{097E0A52-E0A...	Intel(R) PR...	WEP-40	Cain	09876	3039383736
{097E0A52-E0A...	Intel(R) PR...	WEP-104	cain		AE5B7F3A03D0AF9B
{89CE46A0-36C...	Intel(R) PR...	WEP-40	keepoff	mnm91	6D6E6D3931
{89CE46A0-36C...	Intel(R) PR...	WEP-40	XALA		1921680101
{C2A6FDF5-385...	Cisco Syste...	WEP-40	khyber	mnm91	6D6E6D3931

Figure 35: Cain WLAN SSID [12]

There are other tools in the public domain that reveal and decrypt type 7 passwords used in Cisco Routers and Switches. One of such tools is Solarwinds password decryptor [14]. As shown in Figure 36, Solarwinds tool is used to reveal the Cisco type 7 passwords.

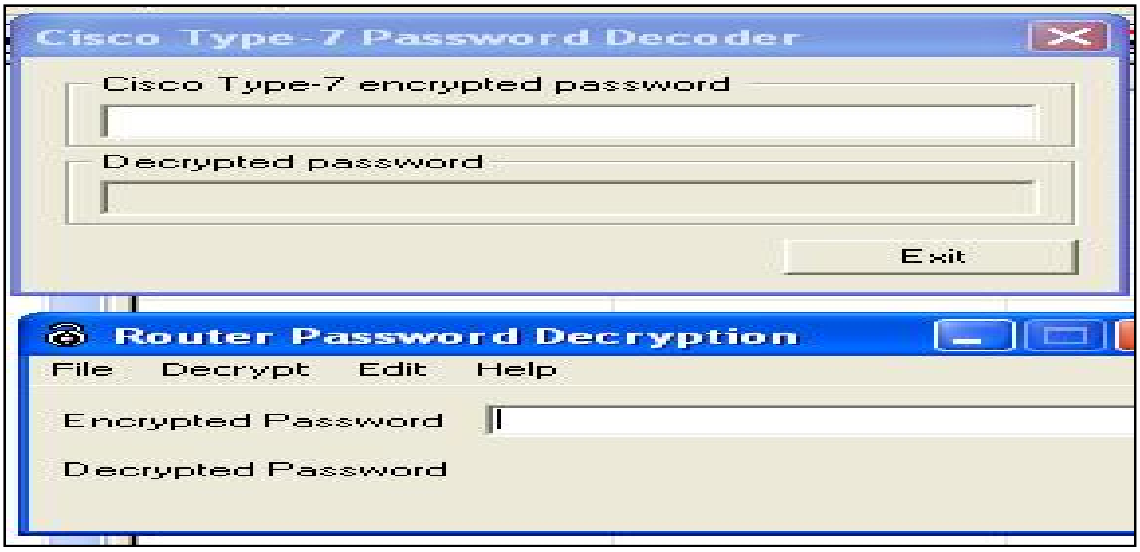
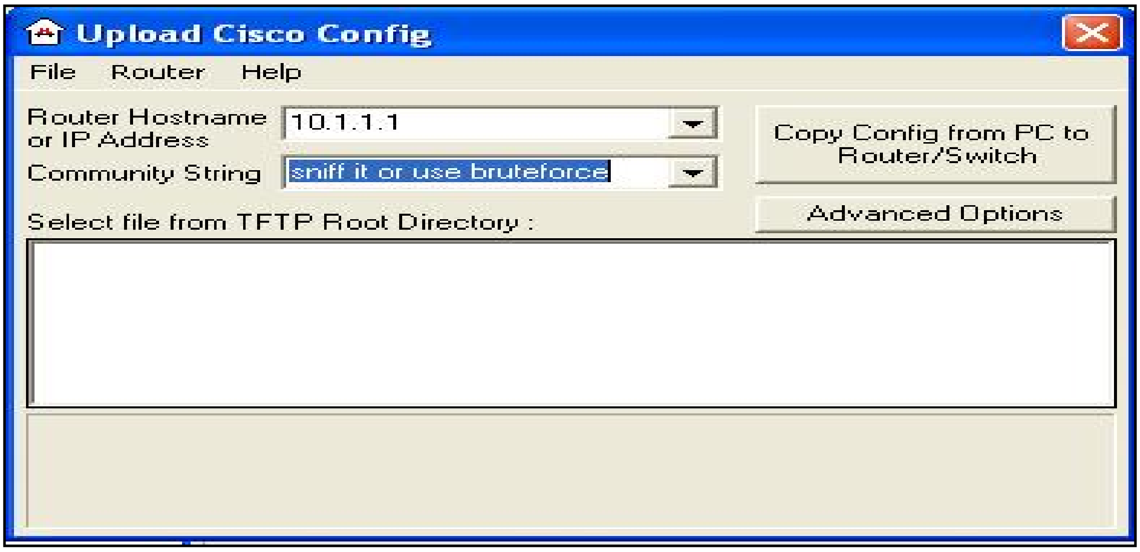

Cisco Type-7 Password Decoder
Cisco Type-7 encrypted password
Decrypted password
Exit
Router Password Decryption
File
Decrypt
Edit
Help
Encrypted Password
Decrypted Password

Figure 36: Solarwinds Type-7 Password Decoder [14]

Usually in the vulnerable versions of SNMP, the community strings are sent in clear text which can be sniffed. Once the SNMP community is sniffed it can be used to upload or download entire configuration of routers or switches. This will result in different forms of attacks including Denial of Service.


Upload Cisco Config
File
Router
Help
Copy Config from PC to Router/Switch
Advanced Options
Select file from TFTP Root Directory :

Router Hostname or IP Address 10.1.1.1

Community String sniff it or use bruteforce

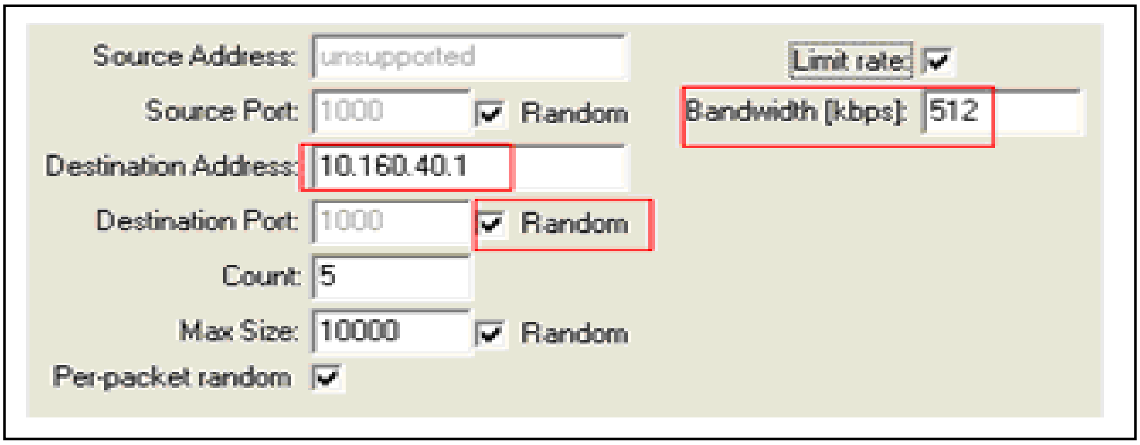
Figure 37: Solarwinds config Uploader [14]

As illustrated in Figure 37 Solarwinds config up loader is used to change the entire configuration of routers or switches by using the SNMP community string to authenticate the connection.

4.11 Denial of Service

Denial of service is a form attack where normal users are not able to access network resources, for instance users trying to access the Internet, opening their mail boxes or bank accounts. The idea is to overwhelm and choke the network resources to the point that that they are unable to serve the legitimate users.

Figure 38 shows a basic tool used to bombard a particular WAN link with garbage packets to the point that no normal traffic can traverse the link. The tool can define particular destination port, number of counts and also hide the source address or spoof the source address to make it harder for the admins to track the source.



Source Address: unsupported

Source Port: 1000 ☑ Random

Destination Address: 10.160.40.1

Destination Port: 1000 ☑ Random

Count: 5

Max Size: 10000 ☑ Random

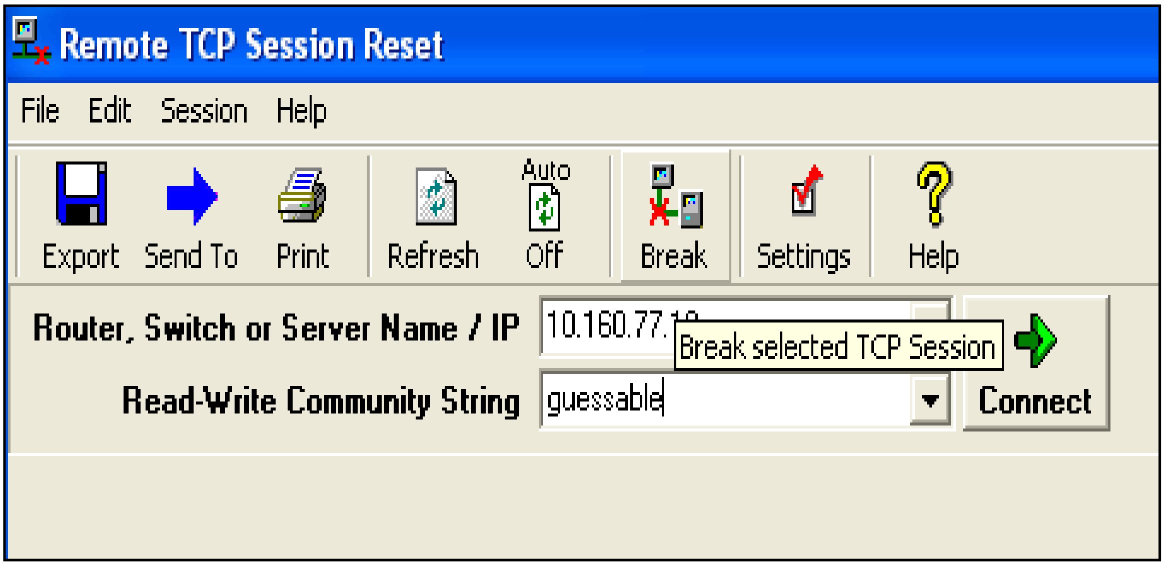
Per-packet random ☑

Limit rate: ☑

Bandwidth [kbps]: 512

Figure 38: UDP Bomber [34]

In certain DOS attacks instead of bombarding the target system and overwhelming it, the legitimate user's active connections are broken. In Figure 39 active connection to a gateway is terminated by Solarwind's Remote TCP Session Reset [27]



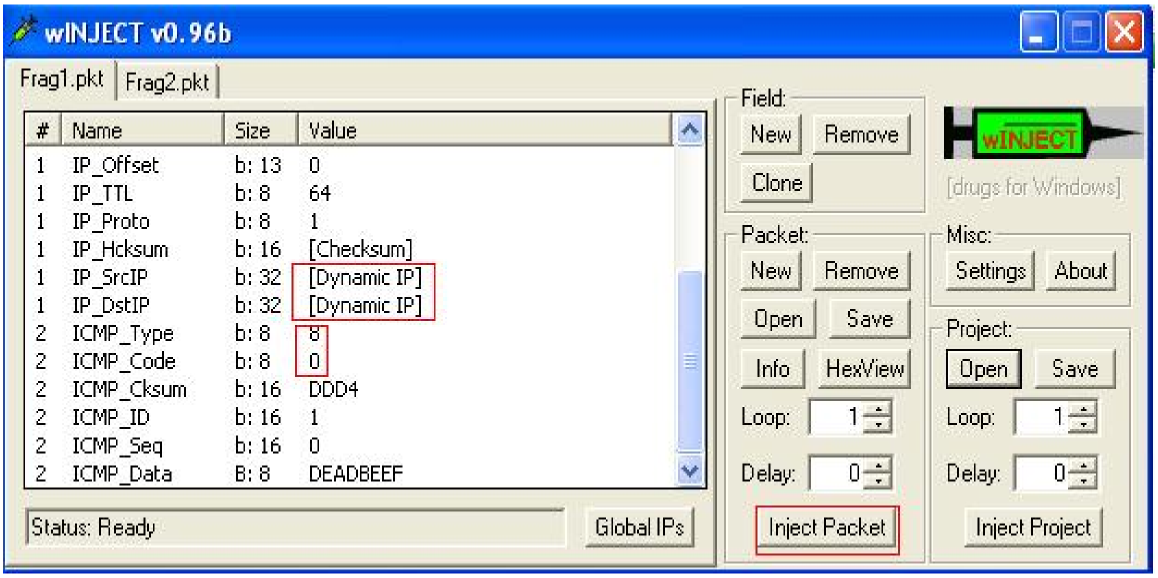
Router, Switch or Server Name / IP: 10.160.77.1

Read-Write Community String: guessable

Break selected TCP Session

Figure 39: TCP Active reset [14]

Furthermore attacking target systems which are vulnerable to certain types of ICMP will result in denial of services. In Figure 40 Winject is used, it is a tool which allows attackers to generate customized packets and target systems that are vulnerable to certain packets [25].



#	Name	Size	Value
1	IP_Offset	b: 13	0
1	IP_TTL	b: 8	64
1	IP_Proto	b: 8	1
1	IP_Hcksum	b: 16	[Checksum]
1	IP_SrcIP	b: 32	[Dynamic IP]
1	IP_DstIP	b: 32	[Dynamic IP]
2	ICMP_Type	b: 8	8
2	ICMP_Code	b: 8	0
2	ICMP_Cksum	b: 16	DDD4
2	ICMP_ID	b: 16	1
2	ICMP_Seq	b: 16	0
2	ICMP_Data	B: 8	DEADBEEF

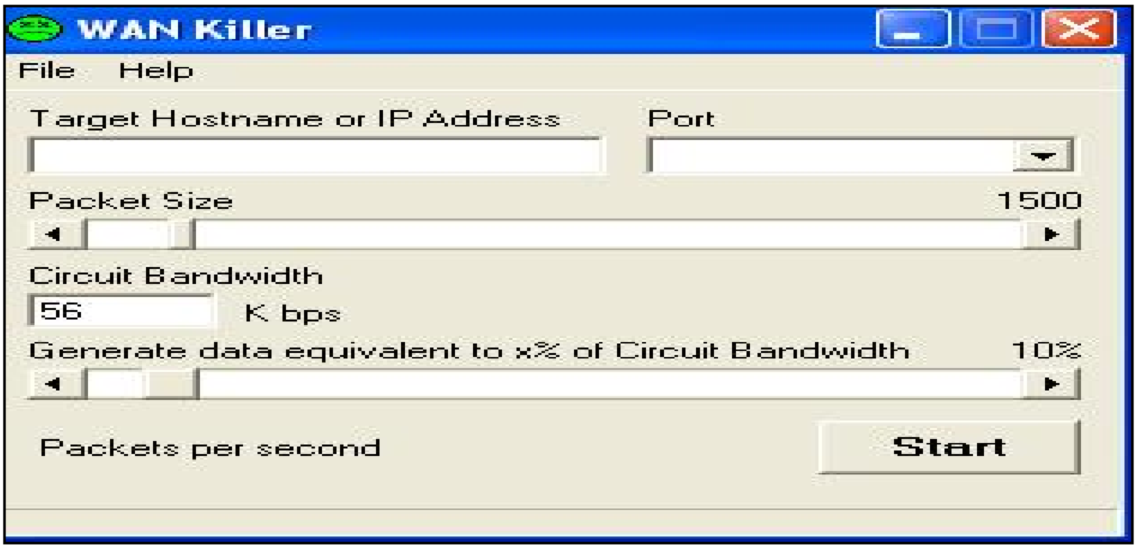
Status: Ready

Packet: Loop: 1 Delay: 0

Project: Loop: 1 Delay: 0

Figure 40: ICMP active injection [25]

On the other hand overwhelming a typical Wide Area Network Circuit using Solarwind’s WAN Killer will prevent normal traffic traversing it, as shown in Figure 41.Solarwind’s WAN killer is used to generate bogus traffic and target limited resources on the WAN link. Once targeted, the link will not be able to handle normal traffic that needs to traverse the WAN segment. [26]



Target Hostname or IP Address

Port

Packet Size 1500

Circuit Bandwidth 56 K bps

Generate data equivalent to x% of Circuit Bandwidth 10%

Packets per second

Figure 41: Solarwinds WAN Killer [26]

Usually in these types of attacks the source address is spoofed making it harder to trace back to the attacker.

4.12 Mitigation and Countermeasures

The final phase in Penetration Testing is to provide the customer with counter measures for rectifying vulnerabilities and weaknesses found during the initial testing. This is the most important phase as far as the customer is concerned as the Penetration Tester will provide the client with a list of specific countermeasures that need to be implemented. For instance if the vulnerability is due to weak and insecure network design the network design will be addressed and all design should adhere to secure multitier design. On the other hand if vulnerability is due to improper system patching or improper device configuration, then the Penetration Tester will advise installation of a proper patch management system and so forth. All of these details are listed in the Penetration Testing Report, see Appendix 2, for a sample Penetration Test report.

It has to be noted that once the countermeasures are in place, the Penetration Tester will carry out a vulnerability scan to see if the countermeasures are mitigating the weaknesses.

In addition since Information Security is a continuing process, organizations and companies will be advised to implement Penetration Testing on a frequent basis to avoid any emerging threats. This can mean that Penetration Testing will become a part of company’s existing ISMS model.

5 Conclusion

The objective of this project was to describe and implement Penetration Testing. It is a proactive method of securing data networks and systems by actively attacking systems and networks in an ethical manner that does not do any harm but reveal vulnerabilities and threats posed by such vulnerabilities.

This project took a practical approach to information security by explaining and implementing Penetration Testing in 10 phases. These phases resembled the same approach a real world hacker would take to attack systems and networks. In each phase concrete examples were provided which pointed to various vulnerabilities, these vulnerabilities if left unmitigated can be exploited by hackers. In each phase of Penetration Testing practical attack was carried on system in a lab or global Internet.

Any attacker armed with the above information can pose a serious threat to the network infrastructure and unless companies and organisations employ counter measures there can be a high risk of incidents leading to extensive disruption and damages. By employing Penetration Testing companies and organisations can pre-empt threats by deploying counter measures.

This project showed that Penetration Testing is a proactive security practice which helps organizations and companies better safeguard their systems and networks against security threats by proactively seeking week points, vulnerabilities and provide recommendations and counter measures for them.

Penetration Testing must be a part of the company's comprehensive Information Security Management System (ISMS) to ensure that systems and networks are routinely tested for vulnerabilities and fixed if needed. This will ensure that future attacks are stopped in their tracks thus preventing huge financial and business continuity losses resulting from these attacks.

References

1 Cisco Systems, Cisco SAFE Implementation (CSI) V2.0. July 2008

2 Script Kiddie [Online]
URL: http://www.iss.net/security_center/advice/Underground/Hacking/Script-Kiddies/default.html . Accessed 28 April 2010

3 Penetration Types [Online]
URL: http://www.secforce.co.uk/blog/2008/11/black-box-penetration-testing-vs-white- box- penetration-testing. Accessed 28 April 2010

4 Whois lookup [Online] All Nettools
URL: http://www.all-nettools.com/toolbox/smart-whois.php . Accessed 28 April 2010

5 Visual route [Online] Visual Ware Co.
URL: http://www.visualroute.com. Accessed 28 April 2010

6 Teleport [Online]Tennyson Maxwell Info Systems
URL: http://www.tenmax.com/teleport/pro/home.htm . Accessed 28 April 2010

7 Nmap Scanner [Online] Nmap Scanner GPL
URL: http://www.nmap.org . Accessed 28 April 2010

8 Ethereal [Online] WireShark
URL: http://www.wireshark.org/download.html. Accessed 28 April 2010

9 LAN Guard [Online] GFI Solutions
URL: http://www.gfi.com/lannetscan . Accessed 28 April 2010

10 Metasploit [Online] Metasploit Framework
URL: http://www.metasploit.com/framework. Accessed 28 April 2010

11 WEP Vulnerability [Online}
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.Accessed 28 April 2010

12 Cain and Abel [Online] Oxid.IT
URL: http://www.oxid.it/cain.html . Accessed 28 April 2010

13 L0phtcrack [Online] Lophtcrack LLC
URL: http://www.l0phtcrack.com/ Accessed 28 April 2010

14 Solarwinds NW tools [Online] Solarwinds Co .
URL: http://www.solarwinds.com/downloads/index.aspx. Accessed 28 April 2010

15 Certified Ethical Hacker [Online] EC Council
URL: http://www.eccouncil.org/ceh.htm . Accessed 28 April 2010

16 Cisco FNS [Online] Cisco Systems
URL: http://www.cisco.com . Accessed 28 April 2010

17 Angry IP Scanner [Online] Angry IP Scanner GPL
URL: http://www.angryziber.com/w/Home . Accessed 28 April 2010

18 Microsoft Baseline Security Analyzer MBSA [Online] Microsoft Corp
URL: http://technet.microsoft.com/en-us/security/cc184923.aspx . Accessed 28 April 2010

19 Security tools [Online]
URL: http://www.insecure.org . Accessed 28 April 2010

20 Net tools [Online] All Nettools Co.
URL: www.all-nettools.com. Accessed 28 April 2010

21 Google Hacking [Online]
URL: http://johnny.ihackstuff.com/. Accessed 28 April 2010

22 Tamo Soft Net tools [Online] Tamo Soft Co.Retina
URL: http://www.tamos.com/download/main/ . Accessed 28 April 2010

23 PCI DSS Requirement 11.3 [Online] PCI Security Standard Council
URL://https://www.pcisecuritystandards.org/security_standards/docs/information_supplement_11.3.pdf . Accessed 28 April 2010

24 Open Source Security Testing Methodology Manual 3.0 [Online]
URL: http://isecom.org/osstmm . Accessed 28 April 2010

25 Winject Customised Packet [Online]
URL: http://www.governmentsecurity.org/forum/index.php?showtopic=2785 . Accessed 28 April 2010

26 Solarwinds WAN Killer [Online] Solarwinds Co .
URL: http://www.solarwinds.com/downloads/index.aspx. Accessed 28 April 2010

27 Solarwinds Remote TCP Session Reset [Online] Solarwinds Co .
URL: http://www.solarwinds.com/downloads/index.aspx. Accessed 28 April 2010

28 Airodump wireless capture [Online]
URL: http://wirelessdefence.org/Contents/Aircrack_airodump.htm Accessed 28 April 2010

29 WEPCrack 801.11 wireless WEP key cracker [Online]
URL: http://wepcrack.sourceforge.net. Accessed 28 April 2010

30 Netsumbler Wireless Scanner [Online]
URL: http://www.netstumbler.com/downloads. Accessed 28 April 2010

31 Information Security Management System [Online]
URL: http://www.maxi-pedia.com/ISMS. Accessed 28 April 2010

32 Acbar Recruiting and Relief Agency [Online]
URL:http://www.acbar.org/index.php?option=com_jsjobs&view=jobseeker&layout=listnewestjobs&Itemid=6. Accessed 28 April 2010

33 Eeye digital security [Online]
URL: http://www.eeye.com/Products/Retina.aspx. Accessed 28 April 2010

34 CERT® Advisory CA-1996-01 UDP Port Denial-of-Service Attack [Online]
URL: http://www.cert.org/advisories/CA-1996-01.html . Accessed28 April 2010

Appendices

Appendix 1: Tools used in this Project

Information gathering

- Netstat
- Tracert
- Visual Route
- Teleport
-
- **Footprinting**
- Nmap
- Eeye Retina
- Visual Route
-

Network reconnaissance

- Angry Scanner
- Solarwinds IP scanner
- Visual Route
-

Sniffing

- Ethereal
-
-

Port scanning

- Nmap
- Retina
- LAN Guard

Vulnerability scan/exploit

- LAN Guard
- Retina
- MBSA
- Metasploit
-

Password cracking

- Cain & Abel
- Lopht crack
- Solarwinds password decryptor
-

Wireless cacking

- Netstumbler
- Cain
- WEP crack
- Airodump
-

Denial of service

- Solardwinds TCP reset
- Wininject
- WAN Killer

Appendix 2: Penetration Testing Report

ABC Inc
Penetration Test Report

Date of test:
xx/xx/xxxx
Conducted by
Team x

Contents

Executive Summary

Some definitions

Approach

Scope

Findings

Recommendations

Appendix

Executive Summary

This section explains the main objectives behind the penetration test and why it was being carried out. It will start by providing a basic background about the customer and its operations and the will move on to the actual date and time of the Penetration Test, the scope of the test. The methodology being followed to carry out the test and so fort

Some definitions

In order for the client to better understand the various terminologies being used in the report this section will therefore provide a brief description and definition of the different terms.

Approach

This section will outline the type of methodology being used to implement the penetration test. Since Penetration Testing is made of the following phases therefore each phase will be shown with their respective results.

Phases of Penetration

- Information Gathering
- Fingerprinting
- Network reconnaissance , Sniffing
- Ports Scanning
- Vulnerability Scanning
- Exploiting Vulnerabilities
- Password Cracking

- Wireless Hack
- Denial of Services (DoS) Testing

Scope

This part of the report usually describes the range of the network or systems being targeted for Penetration Testing. Good example of this would be the range of subnets or range of vlans being pen tested, further more the types of servers being targeted etc.

Findings

This part of the report deals with the range of vulnerabilities or holes being found during the various testing phases. The report will usually highlight the range and severity of each vulnerability.

Recommendations

This is an important phase as far as the customer is concerned since the client will be provided with the list of concrete steps and counters measures that needs to be deployed to fix the vulnerabilities and weakness found during the testing phase.

Recommendations are usually divided between tactical and strategic.

Tactical recommendations deals with urgent and short fixes for the holes found during the penetration test such as patching vulnerable systems or deploying access-lists on certain perimeter routers, but on the other hand strategic recommendations are long term measures that needs to implemented to avoid vulnerabilities now these strategic recommendations can be either the redesign and reconfiguration of the data networks or changes being made to the security policy of the organization.

Appendix

This section usually contains the screenshots of the actual systems and networks that are being compromised during various phases of the test. These pictures can include for instance revealing weak passwords, cracking WEP, conducting network reconnaissance and so fort.