A penetration test of an Internet service provider
A penetration test of an Internet service provider

Computer Forensics and Information Security
2012 05 14

Author: Petter Svenhard
Author: Amir Radaslic
Supervisor: Olga Torstensson
Examiner: Urban Bilstrup

School of Information Science, Computer and Electrical Engineering
Halmstad University
PO Box 823, SE-301 18 HALMSTAD, Sweden
Preface

This semester has been an incredible learning experience and preparation for our future careers. Therefore we wish to thank all the inspiring people who have made this study what it is today.

We express our gratitude to the generous people at the Internet service provider ABC who granted us the opportunity to perform this test.

To our supervisor Olga Torstensson who provided strong advice and support to our work from the beginning until the end.

To Urban Bilstrup who provided the necessary clarity in structure and content required to produce a successful Bachelor thesis.

To Mattias Wecksten for giving invaluable and sound advice regarding technical concepts.

And to Fredrik Strömberg for helping us seeing the value of our discoveries.
Abstract

Computer security is of ever increasing importance in the modern corporate world due to the risk of disclosing sensitive assets. In a world where technology can be found in most organizations and businesses the importance of ensuring secure assets is not only a good habit but a necessity.

This study concerned an Internet service provider in south western Sweden who saw an interest in ensuring the security of their computer systems. The Internet service provider wished to remain anonymous to protect its name and interests in case sensitive information were to be disclosed.

The approach to test the service provider’s security was to perform an extensive penetration test of the ISP’s relevant network and computer infrastructure. The aims of the penetration test were to map vulnerabilities and assess the risk that a possible flaw would pose if exploited.

The results indicated that the systems of the ISP included several critical flaws that could lead to a denial of service condition and a complete compromise of the service provider’s office intranet. Furthermore the results indicated the possibility that the Internet service provider had in fact already been hacked by an unknown perpetrator.

Finally the study was beneficial for the Internet service provider since they were provided with a deeper understanding of the security flaws in their computer system infrastructure. Moreover they were alerted to the presence of a possible crime scene on their property.
Table of Contents

1 Introduction ............................................................................................................. 1
  1.1 Background ........................................................................................................ 1
  1.2 Objectives .......................................................................................................... 2

2 Theoretical Background ......................................................................................... 3
  2.1 OWASP Top 10 ................................................................................................. 4
  2.2 Memory Corruption ......................................................................................... 6
  2.3 Denial Of Service Flaws .................................................................................. 6
  2.4 Human Factor ................................................................................................... 8
  2.5 Wi-Fi Security .................................................................................................. 8

3 Method ................................................................................................................... 9
  3.1 Reconnaissance ............................................................................................... 10
  3.2 Vulnerability Research .................................................................................... 11
  3.3 Exploitation ..................................................................................................... 12

4 Application ........................................................................................................... 15
  4.1 Network Reconnaissance ................................................................................ 15
  4.2 Website Reconnaissance ................................................................................. 20
  4.3 Wi-Fi Reconnaissance ...................................................................................... 23
  4.4 Network Vulnerability Analysis .................................................................... 23
  4.5 Website Vulnerability Analysis ..................................................................... 26
  4.6 Wi-Fi Vulnerability Analysis ......................................................................... 26
  4.7 Exploitation ..................................................................................................... 27
    4.7.1 Attacking authentication ............................................................................ 27
    4.7.2 Denial of Service ....................................................................................... 28
    4.7.3 Attacking Wi-Fi ......................................................................................... 29

5 Analysis ................................................................................................................ 31

6 Conclusion ............................................................................................................ 37

7 References ............................................................................................................ 39
1 Introduction

The modern technological society in which businesses and governments operate is plagued by the risk of attacks against their assets [1]. Crime syndicates, activists and terrorist organizations frequently utilize technology in attempts to subvert, control and sabotage key points in organizations, corporations and infrastructure. Even Governments are believed to employ such tactics in their quest to stay a step ahead in the international political arena. The Stuxnet worm [2] targeting Iranian nuclear facilities discovered in 2010 is a valid example of such a case. Stuxnet was considered far too complex to have been created by nothing but a nation dedicating considerate resources to produce it.

A key area in the industrial world is business intelligence which is of significant importance to maintain a lead in the worlds ever changing markets. As a result of the importance to stay ahead corporate espionage [3] is reported to be a persistent threat to businesses worldwide.

In between the businesses competing for a head start there are organized crime syndicates [4] working to penetrate and steal assets from individuals, governments and businesses alike. Cybercrime has evolved to constitute a considerate threat and tools are for sale on the Internet underground which can be utilized to steal confidential bank information with relative ease. An example of such a toolkit is the ZeuS trojan [5] which has been largely prevalent in causing widespread infection during recent years.

Yet another phenomenon on the rise is political cyber activism or cyber terrorism where organizations such as Anonymous [6] perform various attacks against corporate organizations and governments. A company which has experienced a considerately rough time with the activist network Anonymous is Sony [7], whom repetitively have had their security breached by various injections.

The above incidents and countless more indicate an increasing importance in securing government and corporate assets to ensure information security.

1.1 Background

To conduct this study an agreement with a local ISP was made wherein their systems would be put to the test. The ISP in question desires to remain anonymous due to the potential of sensitive information disclosure, therefore the ISP will be referred to as ABC and any IP addresses and domain names will be altered. The scope of the test incorporates a comprehensive penetration test of ABC’s system infrastructure. Furthermore any actions or methods which would result in network downtime in the form of a denial of service were prohibited by the client. The actual tests began in
January 2012 and elapsed until deadline in May 2012. Furthermore the tests were
performed with the full awareness of ABC’s Executive Director and employees.

Here on follows a concise summary of the content organized into distinct sections in this
paper. After introducing the subject area the paper begins to explain the theoretical
background of the relevant subjects. After the theoretical background the paper goes
into detail regarding the methodology. Within the method various software including
such as Nmap, Nessus, Nexpose, Metasploit, and w3af are discussed. During the method
the outline of the actual penetration test is also presented. When the method has been
described the application of the methods are described step by step according to the
previously described outline. After the application section the results are analysed in a
section labelled analysis and lastly possible conclusions are made in the section
conclusions.

1.2 Objectives

The primary objectives of this study were to conduct a comprehensive penetration test
to discover how firmly ABC’s system infrastructure stands against a technological attack.
The study aims to achieve the following.

- Identify vulnerability issues in the ISP’s systems
- Attempt to test the exploitability of a discovered vulnerability
- Determine the severity of a potential vulnerability

The purpose of the penetration test was to map vulnerabilities of the hosts in the
network and if possible exploit these vulnerabilities. Additionally a second aim of the
penetration test was to possibly aid in advancing ABC’s network and system security.
Furthermore the results of the test serve to demonstrate the significance of maintaining
secure systems.

The problems which this study faces are complex and multi-faceted in nature. The act of
proof-testing a computer system for vulnerabilities poses a series of problems both for
the client and the testers. The testers face the requirement to deeply understand the
underlying theoretical concepts of security whilst at the same time the need to be able to
practically assess these principles. Specifically there is a risk that the testers may not
identify all relevant vulnerabilities due to lack of experience with a specific technology.
The client on the other hand faces not only the problems of direct vulnerabilities but
also the risk of a problem occurring during the actual testing of the systems.

The methods utilized by the penetration testers can actually in many cases aim to make
systems behave in abnormal ways to express exploit vectors. The very nature of creating
these abnormal circumstances may cause the systems to malfunction or crash causing
problems for the client company at hand. Naturally this type of behaviour should be
controlled to the fullest extent possible.
2 Theoretical Background

A Penetration test [8] is a significant part of a complete risk analysis of an organization and it is used to probe a system and/or network for security vulnerabilities. The significant difference of a penetration test compared to other risk analysis methods is that it is performed in the manner as a probable attacker would approach the company with an interest in compromising it. The test is an efficient reality check because instead of relying on solely on antivirus and intrusion detection to maintain security the organization is actually exposed to an attack in a controlled manner [9].

A penetration test can be performed in different ways depending on the predefined goals of the organization [10]. A white box test is a form of testing wherein the company’s entire technological infrastructure is exposed to the testers. The testers can then practically scan and diagnose everything for vulnerabilities with full knowledge of the entire system and network map of the organization thus reducing testing time.

On the other hand the testers can be ordered to perform a “black box” test where no information what so ever about the organizations structure is given and the testers must on their own explore relevant vulnerabilities and attack methods to compromise the system. To effectively comprehend what this specific test will be looking for in the target ISP this section will provide a theoretical background to past and present computer vulnerabilities.

The SANS institute has released a report [11] covering gathered data from march 2009 to august of 2009 exposing the most common cyber security threats which have been discovered in the corporate world. The test was made possible partly from data gathered from the TriggerPoint intrusion prevention systems installed in roughly 6000 organizations at that time. The report [11] listed four points of most common infection. The primary point of infection found was through client-side vulnerabilities in software such as adobe flash, Microsoft office and QuickTime. Various phishing attacks tricking clients into accessing infected content enables hackers to utilize this vector.

The second threat [11] described relates to the first problem and refers to vulnerable websites facing the Internet. SQL injections and Cross Site Scripting are the most prevalent forms of attacks targeting websites. The third step states that there has been a decline in OS related vulnerabilities being found exploited by worms such as conficker. However this may recently change with the discovery of the serious flaw in the Microsoft remote desktop service. The final most common cyber security threat is the prevalence of 0-day attacks being discovered.

Cyber threats remains to this date a significant threat against information security and therefore it is essential that governments and organizations employ security measures to prevent incidents.
2.1 OWASP Top 10

OWASP is an abbreviation for the Open Web Application Security Project [12] and is a community dedicated to the development of a higher security within the web application arena.

The organization is non-profit and allows individuals to help improve existing technologies and software released by OWASP in the quest for heightened application security. The organization provides research, tools, papers and conferences within the context of application security. One such project is the OWASP Top 10 [12] which has been published in various versions since 2004 and most recently in 2010. The purpose of the document is to provide awareness of the top ten critical web application risks at that time.

The OWASP Top 10 is structured according to the risk of occurrence rather than the frequency of occurrence. The first flaw[13] in the Top 10 list is various Injection attacks ranging from SQL injections to OS injections. An SQL injection occurs when a server accepts input that has not been sanitized. An example [14] would be a web server with a login form that performs the following sql query, “SELECT * FROM users WHERE username = ‘marcus’ and password = ‘secret’”. In a regular circumstance the statement would create a query to the database asking every row within the table called users for a username that matches the one provided by input. The same test is performed in the password column with the inputted password value. However if all input here is not sanitized and removes certain sql significant characters such as " " then a malicious user can submit the username “admin’-- “ and thereby bypass the login mechanism by making the query login admin without a password check.

The second [15] most common flaw on the OWASP top 10 is Cross Site Scripting abbreviated XSS which similarly to injection flaws is made possible when a web server does not perform suitable input validation and sanitization. There are generally three types of cross site scripting flaws stored, reflected and DOM-based. A reflected XSS vulnerability could be a website application that uses a dynamic page for displaying error messages to users. The website could use various URL parameters to display a certain error message. In this context a malicious user could manipulate the parameters to inject a script which could make any ordinary users run the arbitrary code. In this manner a malicious user can gain control of a web server.

An XSS [15] vulnerability can be referred to as stored when the content being manipulated is stored onto the server and not generated dynamically. A DOM based vulnerability differs from the other flaws in the following ways. The arbitrary code is not stored in any way on the server and is supplied directly to an ordinary user and the executed server response does not include the attacking script in any form.

The third flaw [17] in the OWASP Top 10 is Broken Authentication and Session Management. This flaw relates to the fact that many applications have misconfigured functions in relation to authentication such as stored credentials that are unencrypted or unhashed. Session management could be vulnerable if session variables such as cookies can be rewritten in the URL. A few examples of the broken session management
would be an authenticated user of a sales site wanted to show his friends a specific product and in some manner sends his specific URL to his friends and in so provides them with an authenticated session on the website. Moreover if this is the case that a website only employs a specific URL value or parameter setting to define "authenticated" a malicious user may craft a script that brute forces various variables to find authenticated sessions.

The fourth flaw [18] in the OWASP top ten is Insecure Direct Object References. This flaw describes situations wherein restricted resources and content on a website is provided to unauthenticated users. One such example would be a password or configuration file that should only be available to administrators on the local network when in fact a misconfiguration in the web applications code makes the file available to any user on the local or public network.

The fifth flaw [19] in the OWASP top ten is called Cross-Site Request Forgery and makes a logged on client to a website to send a forget HTTP request to a vulnerable web application. In this request the user’s session cookie and other authentication information is provided. In this situation a malicious user could force the victim user’s browser to make requests to the vulnerable web application. An example of such a vulnerability would be an attacker providing a user with a request, that makes a transfer from a account to the malicious users account by using a malicious web server that the attacker owns. The web server then authorizes the request if the victim is still authenticated at the vulnerable server.

The sixth flaw [20] in the OWASP top ten is called Security Misconfiguration. This is a broad topic consisting of several different hardening aspects. The misconfiguration flaw may exist if software is not kept up to date, unnecessary ports and services are running on the server, no default passwords used, no error handling and properly configured security settings on the used framework.

The seventh flaw [21] in the OWASP top ten refers to Insecure Cryptographic Storage. This flaw can occur if cryptographic keys and passwords are not encrypted in every location in which they are stored. It can also occur if access to the keys and passwords is not protected by efficient authorization and session controls. Furthermore if the cryptographic algorithm is considered weak or out of date this may also pose a cryptographic storage problem.

The eighth flaw [22] in the OWASP top ten refers to the failure of the web server to Restrict URL access. This flaw may contribute to the possibility of other flaws but essentially URL access problems may occur if authentication is mismanaged.

The ninth flaw [23] in the OWASP top ten is called Insufficient Transport Layer Protection. This flaw refers to the problem if any user would be able to monitor local network traffic and intercept sensitive data. This can occur if SSL is not used to authenticate and to protect assets. Furthermore if weak algorithms are used and session cookies are insecure then network traffic may also be intercepted and disclosed.

The tenth flaw [24] in the OWASP top ten is called Unvalidated Redirects and Forwards and could be possible if the target or source URLs are included in any redirect or forward parameter values.
2.2 Memory Corruption

Aside from the web based vulnerabilities there have been widespread exploits against system and client software relating to memory corruption [25]. In fact most program exploits are possible because of various memory corruptions.

Buffer Overflows [25] is one of the most commonly occurring memory corruptions that have been exploited by malware authors. Buffer overflows occur in several programming languages but most notably in languages such as C. The problem lies within the strength of C which is that the programmer is given strong control over many aspects of the computer being programmed. One such aspect is the principle of allocating and manipulating physical memory in the computer. Similarly to the OWASP top ten issues if proper error and bounds checking is not utilized memory may be corrupted [26].

For example if a programmer allocates sixteen bytes to a variable and then attempts to store 20 bytes of memory into the allocated space the buffer will with high probability cause the program to crash. If the data is not controlled the extra bytes are flooded into the next piece of memory following the allocated variable.

This process is exactly what malware authors are trying to control when creating exploits for Buffer Overflow vulnerabilities. Instead of letting the program crash the malware authors may for example insert additional code which provides a remote shell on the computer where the vulnerable program is run [26]. A recent example of a published buffer overflow came from Microsoft in their MS12-027 [27] security bulletin.

The MS12-027 vulnerability is found in a component of Windows called the Windows Common Controls [28]. Windows common controls are a component of the graphical interface which interacts with other components of the windows operating system.

The vulnerability occurs if a user is tricked into visiting a website that includes special content which triggers the buffer overflow. There is at this moment a Metasploit module called MS12-027 MSOMCTL ActiveX Buffer Overflow [29] which exploits this very vulnerability.

2.3 Denial of Service Flaws

Buffer overflows if unhandled causes an application to crash and the concept of being able to make a program or service crash is in itself a serious vulnerability. The subject of crashing programs correlates with another vulnerability that has seen recent heavy use from various activist networks such as anonymous [30].

This vulnerability is commonly called Denial of Service (DOS) or Distributed Denial of Service (DDOS). The difference between a DOS and DDOS is that a DOS attack comes from a single host whilst a DDOS is utilizing a large quantity of computers. The purpose of a
Denial of Service attack is simply to crash a server or website and in so doing deny the normal traffic and usage of the server.

Generally Denial of Service attacks can be separated into two distinct versions [31]. One version is similar to the exploits corrupting memory described previously, while the other denial of service version utilizes large amounts of traffic of various kinds to attempt to flood a network.

A buffer overflow which does not result in a remote code execution may simply just crash a service instead of throwing a remote shell back at the attacker. However this may be exactly what the attacker aimed to do. A software based denial of service [32] is made possible depending on the type and version of the operating system running the server. One such vulnerability that has recently been discovered is the MS12-020 [33] vulnerability published by Microsoft.

This security bulletin published two vulnerabilities in the windows remote desktop service that could be exploited either to gain a remote shell or to cause a denial of service condition. Furthermore this vulnerability is according to Microsoft also vulnerable to a remote shell exploit. However at the present time none have been created that can be successfully implemented.

At this moment the denial of service exploit is commonly available in a Metasploit module whilst the remote shell exploit is being created by malware authors and security engineers worldwide [34]. The denial of service condition caused by this vulnerability is extremely serious and causes the target operating system to blue screen in a predictable manner every time the exploit is executed.

On the other hand the network based denial of service exploits are mostly dependent on the amount of bandwidth that the attackers can charge a victim with and the amount of bandwidth the victim’s servers can handle. SYN Flooding [35] is a network based denial of service condition wherein the attacker aims to fatigue the TCP/IP stack. The TCP/IP stack aims to maintain reliable connections to effectively organize the inbound and outbound traffic.

To do so TCP/IP utilizes a control mechanism [36] consisting of a challenge and a reply. The challenge to initiate a communication with the server is called a SYN and the response is an SYN/ACK. In a SYN flood the attacker spoofs various source IP addresses and relentlessly throws immense amounts of SYN packets towards a target server aiming to fill the TCP/IP queue. The victim server will try to respond to each address with a SYN/ACK packet to complete the connection. However the attacker will not respond to any SYN/ACK packets and will simply continue to send SYN packets and thus no other hosts will be able to create normal TCP/IP connections to server.
2.4 Human Factor

Yet another vulnerability in the computer security arena has little to do with the actual technology and everything to do with the employees using the technology. There is an entire aspect of penetration testing dedicated to manipulating humans into revealing sensitive information or performing seemingly innocent actions which prove to compromise security. The area is commonly referred to as Social Engineering [37] and includes everything from website spoofing to phishing and phone calls.

2.5 Wi-Fi Security

Various forms of wireless networks are commonly used today and the technology has experienced several critical problems related to the security. Arguably most forms of issues at the present time concerning wireless networks arise due to insufficient knowledge or effort from the people configuring and maintaining the Wi-Fi equipment. It is still possible to set up a wireless router with no password authentication at all and clearly this is a serious threat to any business that uses a wireless network to handle assets. Furthermore there exist various forms of encryption to use when configuring a wireless router wherein the most common are WEP and WPA/WPA2 [38].

WEP is considered extremely unsecure by today’s standards since the encryption contains flaws which enable attackers to relatively swiftly acquire login credentials to the router. WPA/WPA2 is considered secure unless the router was configured using weak credentials such as username “admin” and password “pass123”. If a password consisting of random letters, characters and numbers of a greater length than 10 is used then cracking [39] WPA/WPA2 can be difficult and extremely time consuming.

However there exists another relatively recent vulnerability which bypasses a router configured to use WPA/WPA2 and a strong password. Wi-Fi Protected Setup (WPS) is a functionality added to modern routers which enables easier access to a wireless router by pressing a button on the router to initiate communication. However the problem [40] with this is that this functionality allows a client to connect using a PIN code consisting of 8 characters. Moreover the last of these is a checksum and the remaining characters are divided into two separate PIN codes which can be individually confirmed to be either correct or faulty. This results in 11 000 uniquely required brute force attempts which is breakable within hours.
3 Method

A variety of different tools were studied and implemented to effectively perform the penetration test. The penetration testing arena consists of a vast area of diverse topics where relevant information can be found across many facets of society. There are no guidelines set in stone explaining how to properly perform a penetration test. However several organizations try to structure and provide a clearer view of the topic to aid those who venture within this business. One such organization is the Institute for security and open methodologies (ISECOM) whom have created the OSSTMM manual. The OSSTMM [41] manual aims to cover most of the methods available when performing a penetration test for diverse types of systems ranging from Internet applications to wireless systems.

Another organization which has released a study analysing and outlining appropriate methods regarding penetration tests is the German Federal Office for Information Security. In this study a model consisting of five distinct steps is formulated to describe the various sections of a penetration test.

The first step [42] is a preparatory step consisting of various formal agreements between the testers and target company to ensure that all parts are satisfied. The second step is where the actual testing begins as the testers start using various technique’s to map the target. The third step consists of analyzing the gathered data and recognizing any risks and potential vulnerabilities. The fourth step is the actual exploitation of the risks and is regarded as the most dangerous for the targets assets and should therefore be conducted with great care. The final step can be described as a debrief wherein any potential security holes are disclosed to the target organization.

The majority of the tools studied and used during the test were found on the Linux distribution Backtrack5 R1. Furthermore the methodology of the test can be separated into three distinct areas which can be referred to as Network testing, Web application testing and Wi-Fi testing. The act of deciding which tools to utilize in this study was straightforward since a significant amount of commonly used tools for penetration testing exist. Therefore this study generally uses these common tools when performing this penetration test [43]. An example is the Nmap, W3af and Metasploit tools which will be explained in the upcoming sections. Rapid7 the creators of Metasploit and w3af have also created tools such as Nexpose and even if this tool may not come preinstalled on the Backtrack distribution the tool is in this study considered to be trustable with regard to rapid7’s reputation [44]. For the purpose of testing the ISP ABC the testing methodology was created based roughly upon methods described in the book Metasploit- A penetration tester’s guide and the method formulated by the German Federal Office for Information Security. The basic outline of the test was structured according to the following sections.

- Reconnaissance
- Vulnerability Research
- Exploitation
3.1 Reconnaissance

The reconnaissance phase [45] of a penetration test is used to build a complete picture of the target at hand. Every single device and service should optimally be discovered and placed into a context of operation in regard to the target organization. If the penetration test is a black box test the reconnaissance phase should be conducted without revealing the attackers presence to the organization and likewise if the test is a white box test stealth is not of that high importance. The aim of performing this phase is to discover the best point of entry of entry so that a minimal amount of trial and error time will be wasted during the remaining phases. Therefore it is highly important to conduct a thorough reconnaissance phase to ensure that fine details are not missed which could greatly aid in exploiting the target.

Initially this study will contain research which aims to discover the most basic information regarding an organization and it achieves this with minimal noise to the target. Often passive gathering utilises open sources of information such as the targets publicly available website information.

Another method that will be utilized in this study is a tool named whois which queries the host for organization relevant information. A query to whois [46] with the target website name can reveal information such as the domains, domain owners and email addresses. Yet another tool resides on the website www.robtex.com [47] which can be used to identify any subnet ranges and owned by the company. Furthermore the website can match hosts with their DNS hostnames.

When publicly available information has been gathered using online websites such as www.robtex.com and tools such as whois the study aims to start identifying which hosts are actually alive using ping and ping sweeps. Once hosts have been identified as being live this study will aim to identify running services on the various hosts and this is will be conducted using a port scanner [48]. The port scanner of choice in this test was Nmap [48] and was chosen mainly due to previous experience with the tool and the public popularity of the tool.

Nmap can perform a wide array of actions and comes with a large amount of options to configure custom scans against a target. Some simple features of nmap include identifying live hosts on a network, scanning for open ports on one or several targets at once, detecting services and operating systems and various scripts. Furthermore nmap can be used in variety of different ways [49] depending on what the goal of the scan is.

If the scan simply is a security audit scan the tester can specify nmap to be extremely thorough [50] and scan through a whole subnet of IP addresses and do so in a noisy but efficient manner. However if the scan must be performed with stealth the tester can specify that nmap should insert pauses between packets to reduce network overhead though sacrificing the speed of the scan.

Furthermore nmap can specify several different scan methods where the most common are TCP SYN scan and TCP connect scan [50]. They difference is that the SYN scan performs only half the TCP handshake by sending a SYN packet, waits for the SYN/ACK
response and then determines the state of the port without ever responding. The TCP connect scan on the other hand performs the whole TCP handshake resulting in greater chance of detection than the SYN scan.

Another purpose of nmap is host discovery wherein nmap can perform a ping sweep [50] of a specified subnet and identify live hosts. This is a significant part of the active reconnaissance phase because this reveals hosts that an organization may think are unnoticeable. To perform a ping sweep or as it is called in nmap a list scan specify nmap with the -SL flag and start the scan.

If stealth is significant nmap can perform a scan called “idle scan” [50], wherein nmap uses another host as a ”zombie“ to perform the port scan resulting in that no packets are sent to the target from the tester’s real IP address. The method utilizes the predictable IP ID sequence generation on the zombie host in an attempt to gather information regarding open ports of the target and if successful conceals the identity of the true attacker.

For the purpose of performing reconnaissance on the ISP’s websites the OWASP tool DirBuster [51] was used to identify any folders or files not immediately found during browsing. The tool lets the user specify host, methods of brute force (either pure brute force or wordlist based), and furthermore specific the files to search for on the website. Enumerating a website in this manner may reveal subdirectories and services which can be of importance for the network testing as well.

To identify wireless networks Airodump-ng [52] will be used to discover SSID and the MAC address of any routers being used in the physical office of the Internet service provider. Moreover the type encryption will be documented using Airodump-ng and the type of encryption will also determine how the analysis will proceed.

### 3.2 Vulnerability Research

The next phase of this penetration test can be referred to as vulnerability research. In this phase the testers assemble the picture of the organization and started looking for vulnerabilities that are applicable to the target. Vulnerability research can consist of several different tools to thoroughly identify security holes. One of the simplest methods of performing a vulnerability scan is using a tool called Netcat. Netcat is often referred to as the “Swiss army knife of network tools” simply because its applications are so diverse.

Netcat can be used as a port scanner, to send and receive files, connect to services over the network, and Netcat can be used to perform banner grabbing on a host. Banner grabbing [53] is the action of connecting to a remote host and analyzing the information the host sends back to the client connecting with Netcat. From there conclusions regarding the services on the host could possibly be drawn.

A common but noisy practice is to use a vulnerability scanner such as Nessus which is an automated program that tests various vectors into a system and analyses the responses it receives. Nessus can employ a wide array of methods to perform both initial
information gathering such as port scans and NetBIOS queries as well as actual vulnerability testing. Nessus [54] can be configured to perform either a network or a web application test of a specified target and comes preconfigured with a massive amount of plugins which probe for vulnerabilities.

A program that is similar in function to Nessus is Rapid7’s Nexpose [55] which is utilized in the same manner as Nessus through a graphical browser interface. Nexpose can utilize several different manners to scan a target from vulnerabilities ranging from penetration test to exhaustive full system scans.

When probing a website for vulnerabilities there is another scanner called W3af [56] created by Rapid7 which will be utilized in this study. W3af can be configured to perform a wide variety of tasks ranging from web crawling to brute forcing, sql injections and cross-site scripting. The tool comes with both a command-line interface and a graphical interface to make testing efficient. A useful feature is that once a vulnerability has been found which could possibly spawn a shell w3af can launch the shell and exploit the security hole automatically.

To identify if a wireless router has Wi-Fi Protected Setup activated the program wash that comes with the tool Reaver will be used.

Furthermore simply analysing the data from the information gathering phase and using a search engine such as google.com is arguably quite an efficient method of discovering a vulnerability. The information which Nessus and w3af provides regarding vulnerabilities and methods to subvert different services may not always be enough to be able to find exploit vectors in a target. In this case google.com [57] is excellent to retrieve that little missing fact of essential information which was not described or perhaps overlooked by an automated scanner.

### 3.3 Exploitation

Once a detailed vulnerability research has been performed and if possible attack vectors have been recognized exploitation may begin. To perform exploitation several tools were tested and the exploitation phase will for clarity’s sake be divided into several subsections.

- Attacking vulnerable services
- Attacking authentication
- Denial of service
- Website Exploitation
- Wi-Fi exploitation

The process of attacking vulnerable services will be performed using the Metasploit framework. The Metasploit framework [58] is an open source exploitation framework which comes with both graphical and command line interfaces for launching attacks.
The framework contains a large database of existing vulnerabilities that gets updated almost daily with aid from the open source hacking community.

For the purpose of this test the command line interface will be used exclusively. The framework is structured around exploits, denial of service modules, scanners and various auxiliary methods to audit a target. For most services and program based exploitation the Metasploit framework can effectively be utilized if a module exists.

To attack authentication this study plans to use hydra. Hydra [59] is a general purpose password cracking tool which comes with both a graphical and command line interface. It can be used to perform dictionary based cracking against several different services such as ftp, telnet, rdp and http. Furthermore the tool Brutus AE2 [60] will be used to perform brute forcing and wordlist cracking against various hosts. The tool can be utilized with a simple graphical interface.

To perform denial of service several different methods can be utilized however for the purpose of this study Metasploit was deemed to be sufficient. Metasploit includes a vast amount of available denial of service modules which can be executed against a considerate amount of protocols and servers. The Metasploit Framework [61] includes modules ranging from FTP, HTTP, Apache, IIS, and recently the Microsoft RDP service.

To perform website exploitation the w3af [56] website scanner created by Rapid7 was planned to be utilized. This tool can be configured to launch a wide array of website attacks ranging from misconfigurations which could allow an attacker to upload a file and get a shell on the server to performing exploits against a vulnerable unpatched service.

To exploit any Wi-Fi related vulnerabilities the Aircrack-ng-suite [39] will be used to attempt to brute force a captured authentication hash. Furthermore Reaver [40] will be used to brute force the PIN code on the router if Wi-Fi Protected Setup was identified during the vulnerability research phase.
4 Application

4.1 Network Reconnaissance

The reconnaissance phase began with a thorough research of the ISPs topology and with identifying relevant IP addresses owned by the ISP. The website www.whois.com provided IP addresses and returned basic data concerning the ISP. The service gave data such as the owners of the domain, their contact information, the physical address of the company, and email addresses.

A DNS lookup using nslookup was performed on the ISP websites to identify their respective IP addresses. The results of the lookup were successful and provided two IP addresses ***.***.128.10 and ***.***.144.2 which showed that the ISP most probably had their systems divided over two subnets. Further Google searches revealed additional information regarding the ISPs system infrastructure. A website called www.robtex.com was efficiently used to identify all IP address ranges owned by the target organization. Furthermore the website revealed that the ISP ABC did in fact not own two IP subnets but 32 class C-Networks. IP addresses ranging from ***.***.128-***.168.159 were identified.

After a brief discussion with the client ISP a mutual agreement was made that the subnets of highest interest were ***.***.128, ***.***.133 and ***.***.144. Therefore we decided to limit our scope and research to these three ranges. Thereafter the three subnet ranges were queried using robtex.com. Table 4.1 shows the hosts with matching IP address that were discovered on subnet ***.***.128.

<table>
<thead>
<tr>
<th>HOST</th>
<th>IP ADDRESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns1.abc.net</td>
<td><em><strong>.</strong></em>.128.1</td>
</tr>
<tr>
<td>smtp1.abc.net</td>
<td><em><strong>.</strong></em>.128.2</td>
</tr>
<tr>
<td>netcontrol.abc.net</td>
<td><em><strong>.</strong></em>.128.3</td>
</tr>
<tr>
<td>mail.abc.com</td>
<td><em><strong>.</strong></em>.128.9</td>
</tr>
<tr>
<td>web9.abc.net</td>
<td><em><strong>.</strong></em>.128.10</td>
</tr>
<tr>
<td>Isp10.abc.net</td>
<td><em><strong>.</strong></em>.128.11</td>
</tr>
</tbody>
</table>

Additionally using an Nmap list scan an immense amount of previously unfound hosts were discovered, however for the sake of brevity only these two are worth
mentioning. The command used was “\texttt{nmap \textasciitilde -sL 128.0/24}” and provided the following previously unidentified IP address 128.14. Robtex.com was used to query the network 128.133 as well and returned the following result. This subnet consisted mostly of hosts owned by clients of the ISP and there is only one host worth mentioning and that was 133.204. When querying the network 144, robtex.com provided the two interesting hosts dns2.abc.net (144.1) and smtp2.abc.net (144.2).

When the relevant hosts within the scope of interest were identified nmap was used to identify running services and open ports on the various hosts. Nmap was configured to run a SYN scan against the remote host with the following command "\texttt{nmap -A -p [hostname]} The ",A" flag to check services and operating system and the ",p" flag to scan through the entire port range 0-65535. The command was run against all the previously identified hosts and the results of the scans are displayed in table 4.2.

\textbf{Table 4.2 Selected results from Nmap scans against all previously identified hosts (Source: 2012 nmap \textasciitilde -A \textasciitilde -p [IP Address])}

<table>
<thead>
<tr>
<th>HOST</th>
<th>PORT</th>
<th>SERVICE</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>128.2</td>
<td>53/tcp open</td>
<td>Domain</td>
<td>Microsoft Windows</td>
</tr>
<tr>
<td>128.3</td>
<td>80/tcp open</td>
<td>http</td>
<td>Linux,Netgear, Cisco</td>
</tr>
<tr>
<td>128.9</td>
<td>110/tcp open</td>
<td>pop3</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td></td>
<td>143/tcp open</td>
<td>imap</td>
<td></td>
</tr>
<tr>
<td></td>
<td>465/tcp open</td>
<td>ssl/smtps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>993/tcp open</td>
<td>ssl/imap</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32000/tcp open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td></td>
<td>32001/tcp open</td>
<td>ssl/http</td>
<td></td>
</tr>
<tr>
<td>128.10</td>
<td>21/tcp open</td>
<td>ftp</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td></td>
<td>80/tcp open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td>128.11</td>
<td>-</td>
<td></td>
<td>Microsoft Windows Server 2008</td>
</tr>
<tr>
<td>128.14</td>
<td>80/tcp open</td>
<td>Tcpwrapped</td>
<td>Microsoft Windows 7</td>
</tr>
<tr>
<td>144.1</td>
<td>53/tcp open</td>
<td>Domain</td>
<td>Linux,Netgear,Cisco</td>
</tr>
<tr>
<td></td>
<td>3389/tcp open</td>
<td>microsoft-rdp</td>
<td></td>
</tr>
<tr>
<td>144.2</td>
<td>21/tcp open</td>
<td>ftp</td>
<td>Linux,Netgear,Cisco</td>
</tr>
<tr>
<td></td>
<td>3389/tcp open</td>
<td>microsoft-rdp</td>
<td></td>
</tr>
<tr>
<td>133.204</td>
<td>21/tcp open</td>
<td>ftp</td>
<td>Microsoft Windows 2003</td>
</tr>
<tr>
<td></td>
<td>80/tcp open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td></td>
<td>1000/tcp open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3000/tcp open</td>
<td>http</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3306/tcp open</td>
<td>mysql</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3389/tcp open</td>
<td>microsoft-rdp</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5621/tcp open</td>
<td>ntlm?</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8081/tcp open</td>
<td>blackice-icecap?</td>
<td></td>
</tr>
</tbody>
</table>
On host ***.***.128.1 nothing of value was identified therefore this host was removed from the list of hosts to be further analysed. Open port 53 was identified on ***.***.128.2 unfortunately this information was still vague and various Google searches were conducted to identify any possible exploit vectors. However no suitable leads to proceed were identified on this host.

Host ***.***.128.3 had an open port 80 which instantly made it eligible for further vulnerability analysis. The remote operating system seemed to be some form of switch or Cisco device rather than a general purpose device.

The scan results showed that host ***.***.128.9 had several interesting ports open, therefore this host was also eligible for further vulnerability analysis. Host ***.***.128.10 had a ftp and http server running on standard ports therefore this host was also considered interesting for further analysis and thus was added to the list of hosts to be scanned for vulnerabilities.

The nmap scan of host ***.***.128.11 did not return any interesting results however the hostname isp10.abc.net proved to be connected to a web server with the hostname abc.tv with an open port 80 which made this host eligible for further vulnerability analysis. Host ***.***.128.14 had an open port 80 which means that this host will be examined deeper during the upcoming vulnerability analysis phase.

The two host’s ***.***.128.35- returned zero results of interest therefore they have been omitted from the results.

The host ***.***.144.1 was running an open domain on port 53 and had the remote desktop protocol port 3389 open towards the Internet. This host was considered exceptionally interesting since it is a core DNS server therefore was added to the list of hosts to be analyzed further. Furthermore host ***.***.144.2 returned almost identical results to ***.***.144.1 with the exception that instead of an open DNS port it had an open ftp port.

Yet another host with an open remote desktop port 3389 and this may also possibly be a high risk since the target is a central SMTP server. Therefore this host is considered highly interesting and will be added to the list of hosts to be searched for vulnerabilities. The host ***.***.133.204 had a large amount of open ports ranging from ftp servers, to web servers to email login prompts. To gather further information banner grabbing was performed using telnet on the two ftp servers. The first ftp server running on standard port 21 proved to return a normal Microsoft FTP service command line terminal however the second ftp on port 8081 returned a different result. Figure 4.3 displays the results which is returned when telnetting to the servers port 8081.
This result hints a rather severe possibility. It would seem that when viewing the result from the telnet session that this host had in fact already been hacked in reality. After a brief discussion with the client ISP ABC it seems this attack was not discovered up until this point. A brief Google search for "DuffXP ftp" enforced this feeling of discontent. The Google query returned several ftp leecher sites that is shown in figure 4.4.
Figure 4.4 The Google query for DuffXP ftp (Source: 2012 www.google.com)

In the first link found using google.com the following ftp is identified “ftp://DuFFxP:frt875HH%25M@130.239.56.69:57894/14” and when performing a nslookup on the IP address identified in the ftp URL it may seem that yet another institution has been hacked. Because the DNS hostname of the IP address 130.239.56.69 translates to pc69.poljus.umu.se. The domain umu.se is owned by Umeå University. The fourth link involves the ftp server “ftp://DuFFxP:L33CHiT@146.115.72.148:25996/005.%20%...” and when using nslookup on this ftp IP
address the results return "146-115-72-148.c3-0.lex-ubr1.sb0-lex.ma.cable.rcn.com".

The domain rcn.com seems to be connected to Washington DC high speed Internet however its source origin is unknown. The extents of this attack can not be fully understood at this point and may possibly be outside the scope of this study. The severity situation and the fact that this host may already be hacked results in that no further testing will be performed on this host.

4.2 Website Reconnaissance

To effectively map the web servers belonging to the ISP the hosts from the network reconnaissance phase were accessed using a web browser on the standard web server ports 80 and 443. Host ***.***.128.3 proved to be running a web server directly prompting for a username and password, and if none was provided the website returned an error message that is displayed in figure 4.5

*Figure 4.5 Unauthorized access attempt on host ***.***.128.3 (Source: 2012 web browser http connect on port 80 at host ***.***.128.3)*

Unauthorized User

*WhatsUp Gold 8.0 Copyright © 1996-2003 Ipswitch, Inc. 2012/05/19 11:20*

This host was also scanned using the OWASP DirBuster 1.0-RC1 for additional undiscovered directories, however none were found. But due to the fact that this host presented a user with a login prompt made it interesting enough to be added to the list of websites to be scanned for vulnerabilities.

The next host to be checked was mail1.abc.net which did not run any standard web servers but did however run a mail client on port 32000 as was previously found
using nmap. DirBuster 1.0-RC1 was run on IP-address on port 32000 and further interesting directories were found such as mail, admin, pda, sms and therefore this host was also added to the list of websites to be scanned for vulnerabilities.

The last of the hosts who had a accessible website was ***.***.128.11 which if browsed directly to the IP address returned the root directory of an apache server. Or if browsed using the DNS name abc.tv returned a costumer login form. This website was also scanned using DirBuster 1.0-RC1 and this returned several interesting directories that are showed in figure 4.6.

**Figure 4.6 Discovered Directories on host ***.***.128.11 (Source: Dirbuster 1.0-RC1 against host ***.***.128.11)**

```
/cgi/bin
/icons/
/assets/
/wiki/
/ajax/
```

The directory cgi-bin proved to be forbidden and most of assets proved to be forbidden as well. However the directories have misconfigured access privileges since an unauthenticated user can access the scripts /frontlogin.js and /login.php. However the most serious directory identified was the /wiki/ wherein an entire internal configuration wiki was fully available across the Internet for unauthenticated users. The discussion on the wiki concerns two servers ISP10 and ISP11 where ISP11 seems to be out of use whilst ISP10 is the server wherein the wiki resides. Linux configuration information such as who are in the sudoers file and what permissions they have is available. The contents of the sudoers file is displayed on figure 4.7.

**Figure 4.7 Sudoers file found in wiki (Source: 2012 browse to port 80 on host ***.***.128.11/wiki)**

```
root     ALL=(ALL)   ALL
johan    ALL=(ALL)   ALL
stefan   ALL=(ALL)   ALL
```
Furthermore MySQL credentials for the out of use host ISP11 is published on the websites wiki directory and is showed below in figure 4.8.

*Figure 4.8 MySQL credentials (Source: 2012 browse to port 80 on host ***.***.128.11/wiki)*

The ISP remains lucky that the host is not still active however the credentials provide information regarding possible password policies. Additionally, login credentials to the Linux box were provided and are displayed in the figure 4.9.

*Figure 4.9 Usernames and passwords (Source: 2012 browse to port 80 on host ***.***.128.11/wiki)*

Yet again the ISP is lucky since these credentials point to the inactive machine ISP11. The website abc.net/wiki was added to the list of possible vulnerable hosts for further analysis.
4.3 Wi-Fi Reconnaissance

The Wi-Fi penetration testing was conducted in the Head Quarter Office owned by the Internet service provider. The testing was performed overtly in the presence of the technical personnel working at that present time. The reconnaissance consisted of discovering any existing Wi-Fi networks using the tool airodump-ng with the command “airodump-ng wlan0”.

The scan revealed two Wi-Fi networks “secretsecret” and “ispisp”. Secretsecret had WPA2/PSK enabled as authentication encryption while ispisp had WPA enabled. This information was deemed interesting enough to attempt further vulnerability analysis on the Wi-Fi access points.

4.4 Network Vulnerability Analysis

After the reconnaissance phase has been successfully completed the hosts displayed in figure 4.9.1 were eligible for network vulnerability analysis.

*Figure 4.9.1 Hosts to scan for vulnerabilities (Source: 2012 Reconnaissance phase)*

| ***.***128.3 |
| ***.***128.9 |
| ***.***128.10 |
| ***.***128.11 |
| ***.***128.14 |
| ***.***144.1 |
| ***.***144.2 |

Host ***.***128.3 was scanned with Nessus and Nexpose and no significant vulnerabilities were discovered. On machine ***.***128.9 no critical vulnerabilities
were identified however according to Nexpose some "severe" vulnerabilities were found. The server was identified as supporting weak TLS/SSL cipher algorithms and using invalid or expired X.509 Server Certificates. Furthermore within the TLS/SSL server the host uses MD5-based signatures which are at this point in time deemed insecure. This encryption configuration flaw stands in direct relation to the ninth most common vulnerability in the OWASP TOP 10.

Additionally the host utilizes Self-Signed TLS/SSL certificates. Other than these vulnerabilities none significant were found using Nexpose. Using Nessus no other flaws on host ***.***.128.9 than those already found by Nexpose were identified.

Using Nessus and Nexpose Host ***.***.128.10 did not return any serious vulnerabilities except that the FTP server handled credentials between server and clients in clear text. The fact that the ftp sends credentials in clear text makes this a local vulnerability which would be quite serious if attackers had access to the internal network.

However on host ***.***.128.11 there were critical vulnerabilities identified. Nessus identified that the host was using an outdated Unix operating system Debian 5.0 which is not supported any more. This could pose to be a serious threat if vulnerabilities were discovered in the operating system since no further patches would be released by the creators of this obsolete version.

Using Nexpose the apache 2.2.9 server proved to be vulnerable to a overflow vulnerability that could possibly cause a denial of service condition. The vulnerability was called Apache httpd APR apr_paloc heap overflow (CVE-2009-2412). Another apache 2.2.9 denial of service vulnerability was identified on this remote host.

A fault in the manner in which the apache HTTP server handled the Range HTTP headers could provide a remote attacker with the ability to cause the httpd service to use excessive amounts of memory and CPU through HTTP requests with a malformed range header. The vulnerability was called Apache httpd Range header remote DoS (CVE-2011-3192). In addition to these two denial of service vulnerabilities several more denial of service vulnerabilities were identified on host ***.***.128.11 and they are displayed in figure 4.9.2.
Figure 4.9.2 Denial of service vulnerabilities on host ***.***.128.11 (Source: Nexpose comprehensive scan of host ***.***.128.11)

<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP Integer overflow in sh mop_read (php-cve-2011-1092)</td>
</tr>
<tr>
<td>PHP use-after-free in substr_replace() (php-cve-2011-1148)</td>
</tr>
<tr>
<td>PHP format-string vulnerability on Phar (php-cve-2011-1153)</td>
</tr>
<tr>
<td>Apache httpd mod_deflate DoS (CVE-2009-1891)</td>
</tr>
<tr>
<td>Apache httpd mod_proxy reverse proxy DoS (CVE-2009-1890)</td>
</tr>
</tbody>
</table>

Furthermore a buffer overflow vulnerability was found which could possibly be utilized by a specially crafted exploit. The buffer overflow vulnerability was referenced as PHP Fixed stack buffer overflow in socket_connect().

On the host ***.***.128.14 there was only one vulnerability of interest and this vulnerability was called TCP Sequence Number Approximation Vulnerability (tcp-seq-num-approximation). Nexpose explains this to be a flaw in TCP which enables remote attackers to guess sequence numbers and possibly cause a denial of service condition by injecting TCP reset packets.

A Nexpose scan of host ***.***.144.1 returned no vulnerabilities however Nessus provided results that could possibly be serious for the ISP. The host was running an open remote desktop port 3389 and was missing the vital patch for the ms12-020 patch and therefore making it vulnerable to a remote denial of service attack in the form of a remote blue screen.

According to Nexpose the machine ***.***.144.2 does not implement ftp credential encryption and therefore would potentially be vulnerable to a sniffing attack on a local network. However a Nessus scan shows that this host shares the vulnerability in the remote desktop protocol that ***.***.144.1 was found vulnerable to. Therefore this host may possibly be blue screened remotely as well.
4.5 Website Vulnerability Analysis

Website vulnerability analysis was conducted using rapid7’s W3af configured to use the option intensive scan. The scans were conducted against the hosts show in figure 4.9.3 which had previously identified web servers.

Figure 4.9.3 Hosts with identified web servers (Source: 2012 Reconnaissance phase)

| ***.***.128.3 |
| ***.***.128.9 |
| ***.***.128.10 |
| ***.***.128.11 |

The scans returned a wealth of information but nothing substantial. The scans helped to restate information already discovered during the reconnaissance phase. Moreover no website based vulnerabilities such as SQL injection or cookie poisoning were identified were identified using these scans with W3af.

4.6 Wi-Fi Vulnerability Analysis

The purpose of this part of the penetration test was to identify if any of the two identified Wi-Fi networks had Wi-Fi Protected Setup enabled. To test if the routers had WPS enabled the tool wash was using the following command, “wash -I wlan0”.

Using this tool it was discovered that the access point “secretsecret” was configured with WPS enabled whilst “ispisp” did not have WPS enabled. Therefore this access point was documented to be exploited using Reaver during upcoming the exploitation phase.
4.7 Exploitation

When the vulnerability analysis phase was completed a complete picture of existing
attack vectors was apparent. No vulnerabilities on any service was identified that
could result in a remote administrative shell except the hosts suffering from the
MS12-020 flaw. However as described previously there is to present date no
publically available exploit written for this vulnerability and therefore this vector
becomes irrelevant.

Furthermore no vectors to exploit any of the websites were identified using W3af
therefore this option was not pursued any further. The flaws that were identified
and were deemed eligible for exploitation were vulnerabilities pertaining to
authentication, denial of service and Wi-Fi perimeter attacks.

4.7.1 Attacking authentication

The following hosts presented authentication mechanisms and were therefore
tested using the hydra and Brutus AET2. In both cases a username and password list
was utilized that had been custom made by combining online wordlists with phrases
relevant for the ISP in question. The hosts that were tested are displayed in the
figure 4.9.4.

*Figure 4.9.4 Hosts which were tested for weak credentials (Source: 2012
Reconnaissance phase)*

<table>
<thead>
<tr>
<th>****.128.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>****.128.9</td>
</tr>
<tr>
<td>****.128.10</td>
</tr>
<tr>
<td>...****.128.11</td>
</tr>
<tr>
<td>****.144.2</td>
</tr>
<tr>
<td>****.144.1</td>
</tr>
</tbody>
</table>
Host ***.***.128.3 was attacked with the tool Brutus AET2. The graphical interface was configured to perform a dictionary attack against the hosts HTTP basic authentication. The dictionary attack was successful and recognized a valid username and password combination username “guest” and password “test”.

Host ***.***.128.9 at port 32000 was scanned in the same way as the previous host but returned no valid combinations. Host ***.***.128.10 was scanned using hydra with the following command, "hydra -s 21 - U /home/Desktop/crack/users.usr -P /home/Desktop/crack/pass.pwd -t 16 ***.***.128.10 ftp”.

The -s command specifies the type port to be scanned and in this case it is port 21. The -U and -P flags specify the same username and password list that was utilized previously. the -t flag specifies that hydra should limit the number of tasks to sixteen. The final flag specifies that the type of service to be attacked is an ftp server. This dictionary attack did not find any valid combinations. Brutus AET2 was used against the host ***.***.128.11 with the same configuration as the previous Brutus dictionary attacks and again no valid combinations were identified.

Host ***.***.144.1 was exposed to a dictionary attack using hydra against the remote desktop server on port 3389 using the following command, ”hydra -s 3389 - U /home/Desktop/crack/users.usr -P /home/Desktop/crack/pass.pwd -t 16 ***.***.144.1 rdp”.

This attempt did not return any accepted login combinations either. Furthermore the ftp on address ***.***.144.2 was attacked using hydra with the following command, ”hydra -s 21 - U /home/Desktop/crack/users.usr -P /home/Desktop/crack/pass.pwd -t 16 ***.***.128.10 ftp”. The above password attack returned no valid login credentials and the testing proceeded by attacking the rdp service on the same host. Similarly to the attack against the hosts ftp service the second attempt failed to provide valid login credentials.

4.7.2 Denial of Service

Several Denial of Service vulnerabilities were identified however the ISP ABC has not permitted the execution of any DoS exploits and therefore none were attempted. However due to the fact that the hosts ***.***.144.1 and ***.***.144.2 were vulnerable to the ms12-020 DoS vulnerability certain conclusions regarding the possibility of the success of the exploit can be drawn.

When using the ms12_020_maxchannelids on multiple versions of windows (windows XP, windows server 2003, windows server 2008, windows 7) in a virtual and physical laboratory environment the following assumptions can be made. All attempts to crash the target host succeeded in every attempt. The test was attempted twice towards each of the unpatched windows boxes. Furthermore
Microsoft states in their vulnerability disclosure that all unpatched versions of windows are vulnerable to the ms12-020 DoS condition. [33]

Therefore a consensus was reached between the testers and the employees of the ISP that a dedicated attack using this exploit would crash the core DNS and SMTP servers of subnet ***.***.144. Furthermore the host ***.***.128.14 had an identified vulnerability which could pose a denial of service condition and therefore a similar agreement as with the hosts on subnet ***.***.144 was performed.

4.7.3 Attacking Wi-Fi

To attack the identified Wi-Fi routers Aircrack-ng and Reaver were used. Aircrack-ng was used to conduct a dictionary attack using the same username and password list used with Hydra. The following command was used in this context “aircrack-ng -w custompass.lst -b [MAC ADDRESS] file.cap”. The flag –w custompass.lst specifies that the wordlist custompass.lst is to be used in the cracking process. Furthermore the flag –b sets the target MAC address of the target whilst the file.cap specifies the capture file containing the WPA2 handshake.

To help with the capturing of the WPA2 handshake aireplay-ng was used with the following command, “aireplay-ng --deauth 10 -a [AP MAC] -c [Client MAC] wlan0”. The AP mac flag is the MAC address of the Internet service providers Wi-Fi router, the flag –deauth 10 specifies how many authentication packets to send and the Client MAC specifies the MAC address of the client that aireplay-ng aims to authenticate.

A valid MAC address of an Office PC was identified during the stay in the service provider’s office and therefore made the process quick. However the password attack using aircrack-ng and the supplied password list file was unsuccessful and returned no valid login credentials.

A brute force authentication attack against the access point secretsecret was conducted using the tool Reaver with the following command, “reaver -i wlan0 –b [MAC ADDRESS] –vv. The flag –i specifies the interface on the penetration testers PC to use, the flag –b specifies the MAC address of the access point, and lastly the –vv flag enables a verbose output to provide a wealth of information. After roughly six hours the PIN code of the access point was identified to be “12345678”. This compromise enabled full access to the Head Quarter Office of the Internet service provider ABC.
5 Analysis

This study aimed to identify any significant security risks or vulnerabilities in the systems of the ISP ABC. By conducting an exhaustive penetration test the ISP’s systems were mapped, scanned, analyzed and evaluated. In the beginning of the study two distinct problem areas were identified which highlighted the complex nature of the study to be performed. The first problem pertained to the actual risk of performing the penetration test on the systems of the Internet service provider and luckily no harm or significant downtime was experienced by the ISP.

However the second problem area was the fact that since this test was performed less like a white box test and more closely resembled a black box test several complications must be taken into account. To effectively perform a black box test and thoroughly identify all relevant vulnerabilities and exploit vectors to a system an immense amount of skill in a wide array of areas is required. It is therefore possible that if this test had been performed by more than two individuals with a greater experience in the penetration testing arena then the results may have been different. This factor must be taken into account when analysing the results of the penetration test.

After all the phases of the application were completed the results were analysed to determine the general threat and risk which the ISP ABC may face. The systems of the ISP were generally well secured but proved to show a series of vulnerabilities which could possibly prove to become critical risks. The first phase of the penetration test where information was gathered about the host almost immediately identified vulnerabilities on host ***.***.128.11 where an entire configuration wiki was publically available across the Internet. This could prove to be a high security risk if discovered by malicious users because the information could provide intelligence of how to structure and craft a custom attack against the host.

The employees of the ISP stated that the host abc.tv was in fact partially administered by an exterior consultant company. The administrative employees of the Internet service provider were completely unaware of the fact that this wiki was publically available. This situation points to another layer of security issues which organizations face in the modern world. This potential issue lies within the process of outsourcing tasks and involving exterior parties in sensitive administration. There are several good reasons for a company to outsource e.g. lowering cost, increasing growth speed and the ability to focus on the organizations core competencies.

However in order to efficiently and safely make use of outsourcing any organization should perform a suitable security assessment of the risks involved. For example care should be taken to examine if the introduction of new outsourced components would create instability or security vulnerabilities which may have been previously
secure. [62] SANS identifies several critical security related guidelines which should be followed to ensure that a secure implementation is made.

For example the organisation should enforce that all interior and outsourced employees be aware of the secure usage of the systems. Furthermore there should be clearly defined security clearances and guidelines on how to handle sensitive information. Moreover SANS pushes that the outsourced personnel should adhere to any existent security policies created by the organisation [63]. In addition an organization could set out to follow a certain standard such as the ISO27000 [64] to enforce the proper security principles. The act of following such a standard would provide a clear set of guidelines to ensure that a good security policy is maintained and followed.

In the context of the wiki breach on abc.tv care should be taken to fully investigate the extent of risk which the vulnerability could pose. Luckily in this specific case the usernames and passwords found on abc.tv/wiki were inactive however the fact that the wiki was publicly accessible and the fact that the concerned ISP were not aware of this situation points to a potential problem in this outsource relationship. Furthermore the host abc.tv was vulnerable to several denial of service vulnerabilities and was running an obsolete Linux operating system.

Host ***.***.128.11 is a web portal for clients of a TV network provided by the ISP and a denial of service attack towards this machine could cause loss of availability. There is a possibility that the buffer overflow vulnerabilities could not only crash the host but break something and result in a longer down time and therefore also cause financial loss. Host ***.***.128.14 was identified as a device running an embedded juniper software and therefore is most likely a router, switch, or firewall.

This host proved to also be vulnerable to a denial of service attack which possibly could cause widespread downtime in the ISP’s network if the host resides in a critical position. The ISP ABC stated that the hosts in subnet ***.***.128 were all considered to be of critical importance. Therefore it is plausible that a denial of service condition on this specific host could result in widespread problems in communications on the ISP’s network.

The host ***.***.144.1 was identified as a core DNS server for the ***.***.144 subnet and proved to harbour a critical vulnerability. The host was vulnerable to the ms12-020 denial of service vulnerability and this could with a high probability be exceptionally problematic for this network. The result of a successful denial of service attack using this exploit creates a blue screen condition on the victim host and the results of blue screening a core DNS server handling an entire standard subnet could be severe.

The purpose of the DNS server is to assign relevant DNS hostnames to IP addresses and without this functionality this process could experience difficulties. Many commonly used applications utilize DNS such as the World Wide Web, email and applications such as instant messaging. The full extent of such an attack may be
difficult to determine however the risk is too high to let pass unnoticed and the host should be patched instantly.

The second analysed host on the network ***.***.144.2 proved to face the same critical vulnerability as host ***.***.144.1. This host was not a DNS server however the results of this vulnerability could prove to be as severe as in the previous case. The host was identified as a core SMTP server for the entire subnet and possibly handles high loads of SMTP traffic. Therefore a blue screen condition on this host could prove to be absolutely critical to the ability to send email through SMTP on this network. As with the host previously analysed host this machine should be updated with the MS12-020 patch immediately.

The two hosts on the ***.***.144 subnet had the two most critical vulnerabilities since they represented a core section of the network. However the severity of these two vulnerabilities fades in the possibility that the ISP may already have been hacked. When connected to the ftp server on host ***.***.133.204 on port 8081 two things are considered abnormal. First the port number is not standard for an ftp server and the service was misdiagnosed by several programs such as Nessus and Nexpose. Only a manual banner grabbing using telnet or Netcat to the specific port revealed this information.

The line "hacked by DuffXP" and the fact the terminal colour changes to green even when the ftp session with the host’s ends makes this service highly suspicious. Considering that the service is an ftp server it is possible that host ***.***.133.204 is being used or has been used to distribute pirated or copy right protected material illegally. The fact that a Google query on the alias in combination with the ftp returns several warez sites takes this possible hack into a new dimension.

The piracy scene where copy protected material is distributed on the Internet has seen recent controversy and attention in both the media and from federal authorities [65]. There has been heavy pressure and strong wills from both sides of the matter. The pirates argue in protest that their right to freedom of information is being taken away while the authorities and copyright holders argue that their property is being copied and stolen illegally. Operation site down [65] was a major attempt to shutdown sites serving pirated material and it resulted in several arrests.

If the individual behind the alias DuffXP identified on the host ***.***.133.204 is in fact the same individual serving warez material identified using the Google query brings to mind the eventuality of warez topsites. A warez top site is a high security exclusive file sharing site who distinguishes themselves with secrecy and by having extreme bandwidth speeds at their disposal. These top sites commonly distribute material using high speed ftp servers. Through high speed bandwidth, ftp servers, strategically placed technically competent people the warez scene [66] operates.

Therefore it would seem reasonable that if high bandwidth was required then a probable pirate would attempt to hack someone who possessed a large amount of bandwidth. The Internet service provider ABC certainly possess the ability to
provide high bandwidth since it is in fact an Internet service provider housing nearly 10 000 clients. Therefore it is possible that the host ***.133.204 was in fact hacked with a purpose and may not only have been a hack for fun.

Furthermore the fact that a university domain was found to be connected to the same unique alias on a odd port running an ftp makes the situation considerably disturbing. It would seem strange that a public institution would be serving an ftp server using a nickname connected to leech and warez sites.

The host ***.133.204 resides in the core server room of the ISP and when confronted with the discovery of this host the ISP responded that this host was not still live and was taken down years ago. However the host is still alive and apparently may have been in use to perform malicious activities through their systems. This discovery does not only prove the existence of serious vulnerabilities on the host ***.133.204 it furthermore points to flaws in the organizations security policies. And after a brief discussion with the employees yet again it seems that the outsourced organization which was responsible for the wiki breach on host abc.tv was in fact the people who administered the site ***.133.204.

If the host in fact was not in use then the debate must be taken to analyse who is responsible for not taking down the host when it served no further purpose. A security test like the one performed by this study serves to reveal such flaws in policy that could possibly harm the client company if a malicious hacker would attempt illicit activities. Nevertheless more alarming is the fact that this security test did not only reveal a flaw it revealed a possible crime scene that may not be limited to this one client company. The online nickname DuffXP could be connected to more online leecher ftp sites in at least one more big institution, the University of Umeå.

Furthermore the internal scope of the attack is also unknown and since apparently a leecher possibly runs a clandestine ftp server on a host that resides in the core server room it is possible that more hosts have been secretly compromised. Or perhaps the compromised host ***.133.204 served sensitive content by itself to client business of the ISP who ran servers on the host. There is a risk that confidential information pertaining to the ISP may face the risk of being stolen and published if it has not been stolen already.

Furthermore the fact that the timeframe wherein this host was possibly hacked is unknown it is possible that the usernames and passwords identified on host abc.tv were in fact used by the hackers to compromise parts of the Internet service providers systems. Because the timeframe of attack is unknown it is possible that these credentials were active when this breach occurred. In any case the host abc.tv could be a suitable starting point for investigating a breach.

The occurrence of the possible breach gives rises to several speculations. If a study concerning a local ISP whom may in fact not be one of the largest actors in the technological arena in Sweden has experienced this form of illicit activity. Then the
question arises as to how prevalent these types of incidents are in larger corporations.

Adding to the matter that file sharing and downloading pirated material is an exceedingly common occurrence in our society and therefore is exceedingly prevalent on torrent and warez sites. The matter creates questions regarding how many unknown vulnerabilities occur in small, medium and large sized organizations every week, or even daily. Statistics produced by SANS report [11] that there is a large prevalence of known attacks happening around the world.

Before the hacked server was found there had not been the slightest suspicion about the possibility that the servers would have been exposed to an actual attack. The Internet is full of content which if accessed could pose a security risk to the client accessing the servers.

For example there are numerous phishing sites and files infected with trojans and viruses attempting to infect unsuspecting users. However a directed attack targeting a specific is completely different since it includes an actual attacker with a motive to breach a specific organization. Therefore this discovery was both shocking and intriguing because it showed that directed technological attacks are not limited to the only large actors in the modern world but a local ISP in southern Sweden could become a target.

Moreover the Internet service providers HQ Office access point perimeter security was breached by exploiting the flaws in the enabled Wi-Fi Protected Setup. This resulted in full access to the internal office local area network. Any further testing beyond this point was deemed unnecessary by the authorities of the service provider. This was the case mainly because the ISP ABC had no security what so ever inside the confines of the Office local area network.

The Internet service provider had configured their infrastructure with strong exterior security in the form of expensive Cisco ASA firewalls and considered any activity occurring inside that firewall to be accepted. Clear text ftp services, telnet and open file sharing was used once inside the firewall perimeters. This is an extremely critical security flaw since the Internet service provider use a centralized administration of a large amount assets and customer data providing an attacker located on the LAN with easy access to considerately sensitive data.

Due to the fact that little to no security was deployed within the internal office network and the fact that the access point protecting that LAN was critically vulnerable, the security of the service providers assets can be considered to have been completely compromised.
6 Conclusion

This thesis discussed the vulnerabilities and flaws existent in modern computer systems on both networks and websites and sought to describe the specific security flaws of a Swedish Internet service provider. In today’s technology centred world where an increasing amount of information is being digitalized the importance of protecting that information becomes significant. This necessity to protect information and assets introduces layers of probable attack vectors which could prove to pose a risk for any corporation wishing to utilize technology. With the rise of the digital methods to conduct business there has been an increase in crimes pertaining to technology.

Extensive research is being performed both by security researchers and malicious hackers to develop new methods to exploit systems. Numerous vulnerabilities have been identified in both applications and operating systems with easy to use exploits and often tutorials of compromise a vulnerable component. Moreover there are well developed methods to circumvent security measures protecting servers containing sensitive information. Methods such as SQL injections, cookie injection, cross site scripting and numerous others as described in the OWASP Top 10. Furthermore vulnerabilities pertaining to the control of availability of servers have been identified by hackers and security researchers. Various forms of network based and system based denial of service flaws have been identified across many facets of technological systems.

Therefore it is of utmost importance to test an organizations infrastructure to protect it from ill-minded individuals. A viable part in a complete risk assessment is to perform a penetration test of a company’s network and system infrastructure.

This actual study involved a penetration test of a specific Internet service provider. The aims of the study involved discovering any potential security vulnerabilities in the ISP’s networks and websites. The methods utilized during the study were conducted according to principals from various sources such as SANS, OSSTMM and the Federal office of Information Security.

Furthermore the scope of the test was limited to performing activities that would not cause significant downtime on hosts owned by the ISP. Therefore actually performing methods such as denial of service were prohibited. However the discovery of denial of service flaws and estimation of risk were conducted.

After the tests had been completed several conclusions can be drawn regarding the security and flaws existent in the ISP ABC’s systems. The ISP harboured several critical security vulnerabilities that could result in significant loss of availability, possibly damaged computer systems and full compromise of sensitive assets. There were several hosts who had denial of service vulnerabilities which if exploited could result in serious problematic conditions for various sections of the network.
The study identified several denial of service flaws with high exploitability risk which could result in system downtime in critical systems. Furthermore the study discovered a previously unknown system breach which resulted in an internal investigation to determine the scope of the attack. Lastly the study identified flaws in the service provider’s office perimeter security which could result in a complete compromise of sensitive assets. Therefore this study has been an invaluable contribution to the advancement of the service provider’s security and awareness of system vulnerabilities.

However another valuable contribution of this study concerns not only the Internet service provider but modern society on a greater scale. An important realization is that technological attacks are not limited to the largest organizations in the modern world. Moreover another significant consideration is that economic profit and access to sensitive assets may not be the prime objectives of an attack. The hacking incident discovered in this study connected to the piracy scene brings perspective on a different motive. The underground warez scene [66] utilizes high bandwidth systems to rapidly distribute freshly apprehended content, and organizations such as Internet service providers and universities own the ability to deliver high bandwidth. Therefore these organizations and institutions are at risk of becoming targets of this motive.

Therefore this study ultimately contributes to raising awareness in society of potential alternative motives that could present a critical risk to an organization. Viable motives may not be limited to compromising systems of economic value but individuals may aim to breach systems owning high bandwidth. Conclusively this study provides information of paramount value to the Internet service provider ABC and a small but significant value to modern society.
7 References


