

Intrusion Defence

by Paul Anthony Gooch

FILE	17641_PAUL_ANTHONY_GOOCH_INTRUSION_DEFENCE_78196_43797 220.DOC (4.66M)		
TIME SUBMITTED	21-APR-2016 09:37 AM	WORD COUNT	13287
SUBMISSION ID	56176721	CHARACTER COUNT	74651



PRIFYSGOL CYMRU

Y Drindod Dewi Sant

UNIVERSITY OF WALES

Trinity Saint David

SWANSEA - ABERTAWE

Intrusion Defence, How it works and why it's needed

By

Paul Gooch

P130137

Supervisor Dr Carlene Campbell

Second Marker Dr Kapilan Radhakrishnan

Project submitted as part of the requirements for the award of BSc
(Hons) Computer Networks

Declaration of Originality

I, Paul Gooch declare that I am the sole author of this Project; that all references cited have been consulted; that I have conducted all work of which this is a record, and that the finished work lies within the prescribed word limits.

This work has not previously been accepted as part of any other degree submission.

Signed : P.Gooch

Date : 12/04/2016

FORM OF CONSENT

I Paul Gooch hereby consent that my Project, submitted in candidature for the B.Sc.(Hons) Computer Networks degree, if successful, may be made available for inter-library loan or photocopying (subject to the law of copyright), and that the title and abstract may be made available to outside organisations.

Signed : P.Gooch

Date : 12/04/2016

Copyright Acknowledgement

I acknowledge that the copyright of this project report, and any product developed as part of the project, belong to University of Wales Trinity Saint David, Swansea.

ABSTRACT/SYNOPSIS

Network intrusion is becoming more common by the day from unwanted spyware/malware to the more serious of attacks like DOS and MITM (Man in the Middle) attacks. There are many different intrusion methods in the world today and although all usually are upgraded versions of ways created years ago, there are yet no trends to follow to try and foresee any future technology and to get one step ahead. Intrusion detectors and other relative security features are doing a great job at keeping networks secure but there is always a risk or threat from outside groups of so called hackers, to the less obvious employee with malicious intent at the forefront of their mind. This has called for Cybersecurity over the years to greatly enhance its presence. Pen testing (Penetration Testing) is a proactive and authorized attempt to evaluate the security of an IT infrastructure by safely attempting to exploit system vulnerabilities, including OS, service and application flaws, improper configurations, and even risky end-user behaviour

A project has been completed to show the need for network security with the above being the focal point of attention, network intrusion methods, ways to counteract them, and the importance of regular penetration testing to be carried out on the given network.

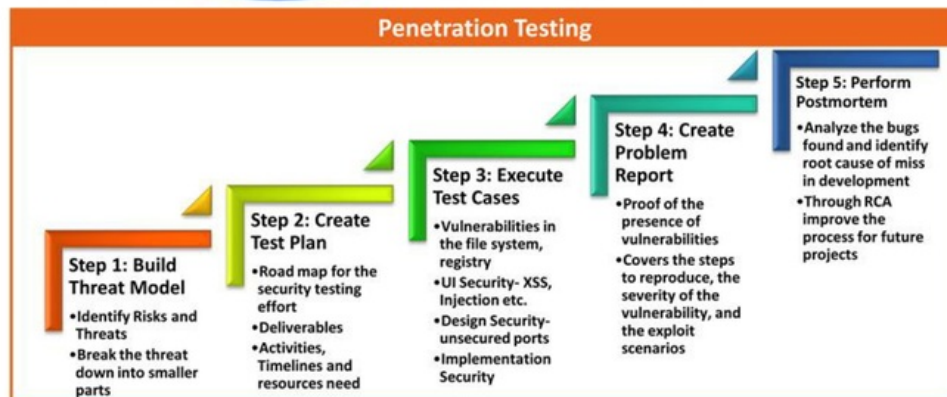
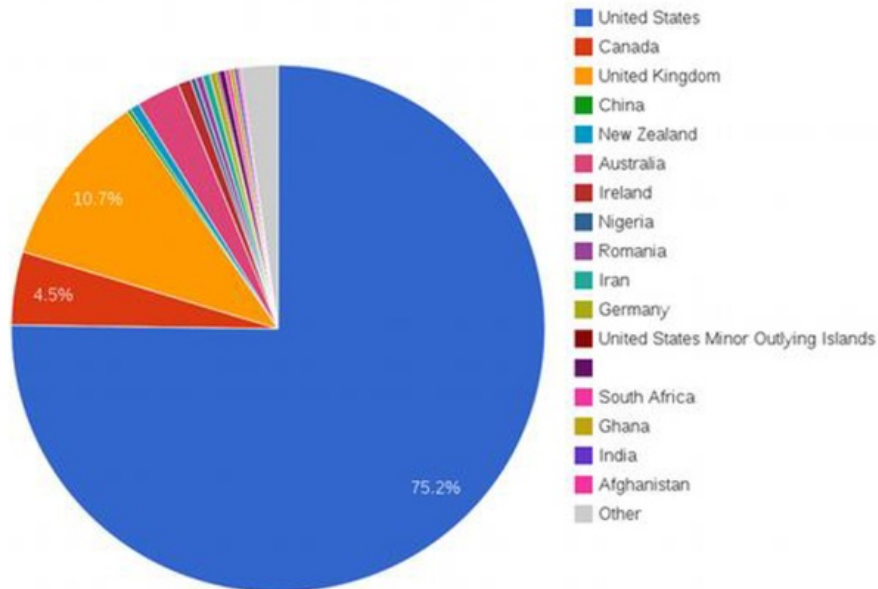
TABLE OF CONTENT

Contents

Copyright Acknowledgement.....	ii
CHAPTER 1 10	
1.1 Introduction.....	10
1.2 Objectives.....	11
1.3 Structure Of The Project.....	12
CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE.....	14
2.1 Introduction.....	14
2.2 Methodology	21
CHAPTER 3 - DESIGN & IMPLEMENTATION	25
3.1 Introduction	25
3.2 problem formulation	25
3.3 Design	28
3.4 Implementation and Difficulties.....	28
CHAPTER 4 – TESTING AND EVALUATION.....	31
TEST 1 31	
4.1 DHCP exhaustion/Dos Attack.....	31
TEST 2 36	
4.2 Brute Force	36
TEST 3 38	
4.3 Browser Attacks.....	38
CHAPTER 5 – RECOMMENDATIONS.....	41
5.1 Recommendation for security concepts	41
5.2 Conclusion.....	45
5.3 Recomendations FOR FURTHER Research.....	45
CHAPTER 6 – REFLECTIONS.....	47
6.1 Main Aim of project	47
6.2 Difficulties and aims that couldn't be met.....	47
CHAPTER 7 REFERENCES.....	49

CHAPTER 8 APPENDIX..... 53

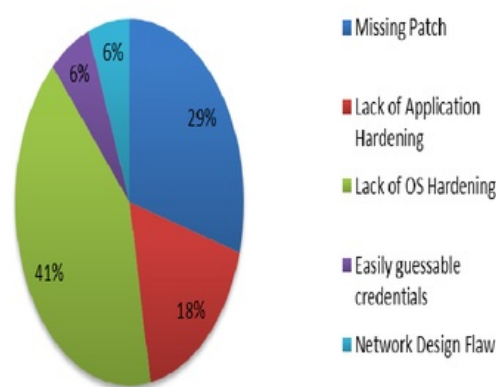
- 53
-



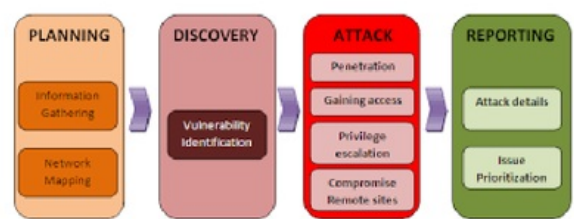
53

- 53
- 53
- 54
- 54

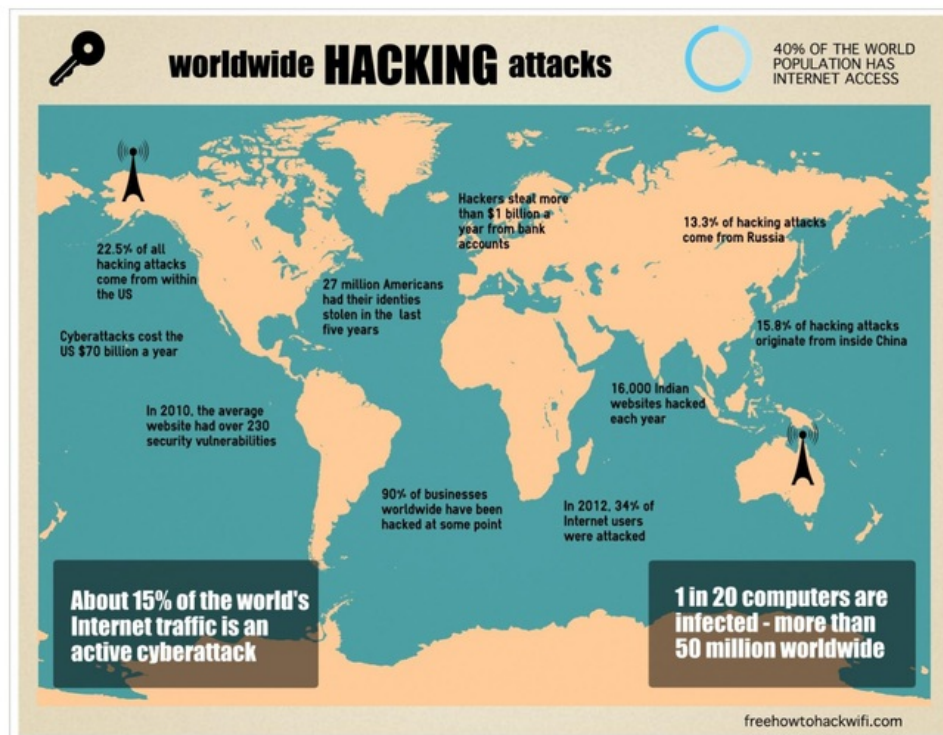
Security Risk Origin/Category



54



54



55

- 55
- 55
- 30 Helpful Nmap Commands For Pentester or System Admins 55
 - Attachments 56
- A brief history of computer networking 56
 - Attachments 56
- Forecast: The Internet of Things, Worldwide, 2013 56
 - Attachments 56
- How a 'denial of service' attack works 56
- How to avoid attacks that exploit a Web browser vulnerability 56
 - Attachments 57
- Kali Linux Tutorial: Hack A Web Browser Using BeEF 57
 - Attachments 57
- News Release | Infoblox 57
 - Attachments 57

• Next big thing: Preparing for the Internet of Things in the enterprise	
Information Age	58
• Attachments	58
• provos.pdf.....	58
• security - Why is it bad to have open ports? - Super User.....	58
• Attachments	58
• The Internet of Things and its impact on enterprise networks	
Information Age	58
• Attachments	59
• Top 7 Network Attack Types in 2015.....	59
• Attachments	59
• What every business must know about the Internet of Things	
Information Age	59
• Attachments	59
• What is brute force cracking? - Definition from WhatIs.com	59
• Attachments	60
• What is configuration management (CM)? - Definition from WhatIs.com ..	60
• Attachments	60
• What is network management system? - Definition from WhatIs.com	60
• Attachments	60
• What is Penetration Testing and Why is It Important?	61
• Attachments	61
• What is Penetration Testing and Why is It Important?	61
• Attachments	61
• Wireless Network Management.....	61
• Attachments	61
• ZoneAlarm by Check Point - Award winning PC Protection, Antivirus,	
Firewall, Anti-Spyware, Identity Protection, and much more.....	62
• Attachments	62
• Attachments	62
• Attachments	62

ACKNOWLEDGEMENTS

I wish to thank Dr Carlene Campbell for the overall supervision of this report and the advice and guidance that has been given.

I would like to thank Kapilan Radhakrishnan for the support giving over the years as my tutor.

Advice given by John Rees on network security has been a great help.

I would like to show appreciation to Daniel Turner for his expertise in the Cyber security industry and his help with statistics.

CHAPTER 1

1.1 INTRODUCTION

This report expects to deliver an understanding into intrusion defence (network intrusion), what types of intrusion are out there and lastly to explain the defence and how it works to counteract these attacks.

The development of new technology that addresses the issues faced by network owners has enhanced greatly over the years, the different methods used to help deal with the threats will be looked into closely, along with the technological advancements that were founded over the years. A look at restrictions to the current technology of the time is also a key factor, mainly being due to the advancements not being made at that moment in time.

Network intrusion is becoming more common by the day from unwanted spyware/malware to the more serious of attacks like DOS and MITM (Man in the Middle) attacks. This has called for Cybersecurity over the years to greatly enhance its presence.

The project will be carried out using Virtual machines to identify and counter the different types of attack, whilst gradually implementing different security features.

A network will be created with two clients in Virtual Box, using Windows10 as the operating system, the security that will be implemented from start to finish will range from firewalls with exceptions to patch management and encryption services, a home server using Windows Server 2012 r2 also represented within Virtual Box with Ethernet as the LAN solution. A client will be created outside of the network to initiate and replicate attacks that may be carried out from an external threat, this client will be running Kali Linux as the preferred operating system due to the large amount of tools ready to be used and are used by security professionals in the IT sector mainly penetration testers every day.

There are difficulties and benefits that have to be considered when using Virtual Machines to run these tests, the difficulties being that even though there is network connectivity, this virtual network has no ability to be controlled other than that of a Virtual NIC (Network Interface Card) which gives the Virtual Machine the ability to receive and transmit data, thus being the reason certain tests cannot be carried out.

One major downside to this is the lack of ability to sniff data packets and steal information as it is being passed over the network itself, this is one major concern at the moment within IT Security, if further thought is to be put in this report after the completion then there are possibilities that a “live” network could be used for a weekend to run attacks, or at the very lowest option the ability to create a network at home using multiple devices to be able to implement the wider range of security threats.

The threats that will be carried out will be documented with its own sub heading and the results from that particular test will be discussed along with the final collection of information gained, that will be used to give recommendations on the security methods to be used to counter the attacks carried out.

1.2 OBJECTIVES

The overall aim is to be able to evaluate different methods in the success of preventing intrusion and data manipulation. And to show that using multiple methods is a more secure strategy when it comes to implementing security on a network, however this does not mean that this is the only field of study. A look at arguments for and against using multiple methods will be evaluated, and will also explore the individual more common security hardware and or software that have been used over the years, a look into how the development of certain security

methods came into play and lastly how security has coped in general with attacks over the years.

Multiple objectives will be set for example:

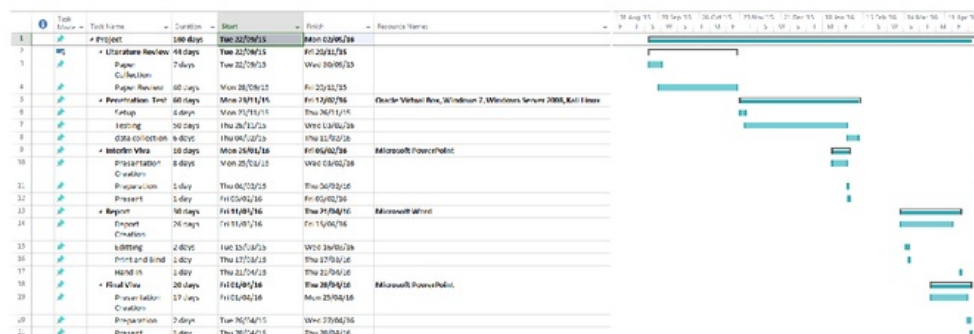
- Testing of the network with security features off
- Evaluation of how this works
- Testing with certain features in place i.e. firewall
- Evaluation of the differences
- Final testing with all security features available
- Final evaluation of methods used.

The results from these tests will all be collaborated into a much larger report which will be the final deliverable report on the findings and evaluation along with any recommendations.

The hope is to find a common ground between attack and defence, and to be able to get a much clearer warning on when these attacks may happen, at the very least the ability to implement security that will stop these attacks will be desired.

1.3 STRUCTURE OF THE PROJECT

The following Gantt chart has been created to oversee the overall project:



This will be available to see in the appendix for a much more detailed view on the Steps that will be taken. The project creation is the simplest part, the creation of the network and the peripherals used herein will take a small

amount of time, when compared to the vast amount of data and intelligence that needs to be obtained. Also numerous problems that were encountered along the way to the creation of the project and how the timescale changed.

CHAPTER 2 - RESEARCH & REVIEW OF LITERATURE

2.1 INTRODUCTION

The overall aim of this project is to be able to evaluate different methods in the success of preventing intrusion and data manipulation. The key to this is consistency and regularity, this project is not going to be the first in this field and neither will it be the last, but it will be current and up to date on the ways currently being used. The goal of this project isn't to actually prevent all security intrusions as this would be impossible but to at least make it harder or be able to detect when it may be about to happen. This is where Penetration Testing comes into play, pen testing is the act of a network security consultant trying to gain access to your network and/or probing it for weakness, thus giving the network owner the ability to correct these problems before and user with malicious intent in mind can take advantage of, this report will help to show the need for penetration testing as an ongoing security advantage, a student at Linkopings University Sweden, Michele Fiocca[3] written in 2009 has some valid points that will help with this statement, and it will be key to see if any similarities arise being this paper is 6 years in the future. As mentioned the main flaws with this paper will be that the software used would be dated and could potentially miss new and up to date intrusion methods. Michele also explains about a new platform created by three computer scientist students called SolarSword, this is particularly interesting as there doesn't seem to have been any advancement in this, or not a relatively open one as it hasn't been well documented, so it will be interesting to see what happened with this and find out any problems that they faced, so that they could be introduced in this projects testing to see if any more advancements could be made. One issue that has been found with this platform from a quick glance is that a lot of the testing that was carried out was restricted by time they state:

- 1) Test should be performed in a more automatic way.
- 2) Test should start from many different positions, therefore a quick deployment is needed.
- 3) The platform needs to be immune to attacks and likely not controlled by external attackers [4]. A statement made by Dr Daniel Geer [5] 'Successful

penetrations can be characterized as the illegitimate acquisition of legitimate authority.' This is taken from his duet of a journal written and collaborated with John Harthorne. This paper takes a closer look at the evolution of a Penetration Tester and will be very interesting to carry this on further than the year 2002 as when it was created, it will be more of an honour to carry on findings from then to now as it is a 13 year gap in technological advancements.

Another journal that will be looked into is "Google Hacking for Penetration Testers" written by Johnny Long [6], the book is written in a more industrial way i.e. for engineers by engineers, as the wording of the journal doesn't necessarily suggest the words in an academic way, however, the hands on approach taken by the author suggests experience in the field and boasts a wide range of other members that help compiled the journal. The paper takes a look at advanced operators and being able to understand them. This will help with the SQL injection methods that will be used as it describes flaws in the code.

One last paper written by Professor Matt Bishop of the University of California will be studied closely as it takes close looks at key areas regarding the topic which include, what is a penetration test?, what do the attackers know?, and what resources do the attackers have? [7]. This all falls in line with the project being carried out as it helps to think like an attacker, which will be of great use when it comes to the physical stages of actual intrusion or "hacking" of the network being created for this project.

Many journals and books have been used to differentiate between the research that has been carried out to complete this project, all work will be referenced within this section and any work that has been used but not directly will be illustrated within the appendix.

This project is not the first in its field, and due to the steady rise in Cybercrime it most certainly won't be the last, in best hopes it is a stepping stone to continue on the ever changing journey of intrusion defence which over the years has grown rapidly.

Network security in the broad sense is any activities designed and implemented to protect your network [8]. It is all to do with the integrity reliability and safety of said network, and the data which travels along its paths.

Although the threats to network security have grown rapidly, the most commonly known threats include:

- Viruses, worms, and Trojan horses
- Spyware and adware
- Zero-day attacks, also called zero-hour attacks
- Hacker attacks
- Denial of service attacks
- Data interception and theft
- Identity theft [9]

In order to understand these attacks many people took to becoming a penetration tester, which is someone who attacks your networks using the methods used by hackers, to gain entry or check for weaknesses within the security of all aspects of the network. Penetration Testing is a good way to keep your network up to date from attacks due to the trained Penetration testers always adapting their skills to new technology.

In 2009 a student at Linkopings University, Michele Fiocca[10], undertook a literature study of penetration testing which falls in line with certain aspects of what this report is trying to explain.

One question she asks and identifies clearly is what is a penetration test and why is it useful to perform it? [11].

This helps identify the attack aspect of the report and raise awareness to the rise of attacks which outlines the need for more studies to be carried out in this field.

The key factor to this question as stated is "Because the list of potential insecurities is unknowable and hence innumerable, a penetration testing alone cannot prove security of the system, just as no doctor can prove that you are

without occult disease; thus, it can just prove that the system is vulnerable [12]". This suggests that with the current technology the world of networks will need more than penetration alone to stop anyone wishing to gain unlawful access to your network. It also states that it is possible to find the vulnerability before the attacker does, which benefits security greatly. In section 2.2 of her report the need for testing is shown as a benefit to enhance security as an ongoing procedure, this report will give evidence on how this is measured and to show how penetration testing is not considered a physical defence, and to also show that without the testing being carried out networks would be more susceptible to attack.

Another book that backs this argument up is Penetration Testing: Assessing Your Overall Security before Attackers Do. On page 5 of this report there is a great deal of information on why we must perform pen-testing, to put into the simplest form the need is outlined here "In a sense, think of a Penetration Test as an annual medical physical. Even if you believe you are healthy, your Physician will run a series of tests (some old and some new) to detect dangers that have not yet developed symptoms [13].

Penetration tests are also helpful at getting the support of management, many networks will have a known vulnerable exploit that the internal network team know about, but find it difficult to get the support. A penetration tester can be used to leverage this support in the same way administrators go about getting a budget increase for new technology, third parties will seem to hold more reasoning with management and can underline the need more efficiently, and unfortunately management will often respect this opinion more than their own internal staff.

As mentioned earlier in this report, penetration testing alone does not give networks security, there has to be physical hardware and software in place to help detect and block certain information or access requests, for example a form attack that is commonly used is a MITM (Man In The Middle) attack, this is achieved by the use of a rogue DHCP server, the server is made to imitate that of the current legal DHCP server but As clients connect to the network, both the rogue and legal DHCP server will offer them IP addresses as well as default gateway, DNS

servers, WINS servers, among others. If the information provided by the rogue DHCP differs from the real one, clients accepting IP addresses from it may experience network access problems, including speed issues as well as inability to reach other hosts because of incorrect IP network or gateway. [14]

These are things that cannot be detected with penetration testing, but there are IDS (intrusion detection systems) and IPS (intrusion prevention systems) that are used to combat this. There are argument made for the use of either of these singularly or in conjunction with each other, even though the technology that you use to detect is very similar to the technology you use to prevent they are considered completely different tools and used in a variation of ways.

An IPS and IDS described here by Joel Snyder [15] can be placed into two categories *'If an IPS is a control tool, then an IDS is a visibility tool.'* This helps to distinguish whether to use one or the other is to understand what it is that is needed, if visibility of the network is needed i.e. network forensics and analysis capabilities then the IDS should be used if not then use IPS, although after some research most IPS vendors, because of the IDS heritage can sell their products to combine these functions. They have the powerful malware and attack recognition engine needed to identify and block attacks, but they also have additional rules and tools designed to enhance network visibility, so both will be used on the network to show the difference and to hopefully achieve total control.

Firewalls play a big part in securing a network as a Firewall can be configured in hardware or software or both, they allow network managers to implement filters for the network traffic and helps to block unwanted or unauthorized access to the network, this is done by analysing the packets sent to and from the internet and match them against the criteria set by the network administrator, if they do not meet the criteria they are simply dropped if they do meet the criteria needed they are allowed access.

The only downside to a firewall is that at some point it will fail, a company called Camber, who specialise in Firewall Failure plans state 'Sooner or later, you're going to have a problem with your firewall. It doesn't matter whether it's a

hardware or software firewall. It's electronic and a terrific target for experienced hackers, at some point it will fail. What you do to prepare for that failure and those actions you take following that failure will make a big difference to your company.' [16]. This agrees with the overall aim of this project, the use of multiple methods is a great benefit to network security, and this statement suggests that firewalls are not as great a security feature on their own, but with the addition of the IDS and IPS a lot more can be achieved with the network.

A project similar to this was undertaken by the SANS institute, in a paper titled designing a secure local area network, this paper shows that the point of this project is true due to the fact that they use many devices and different methods.

The basic network diagram that was used can be seen here:

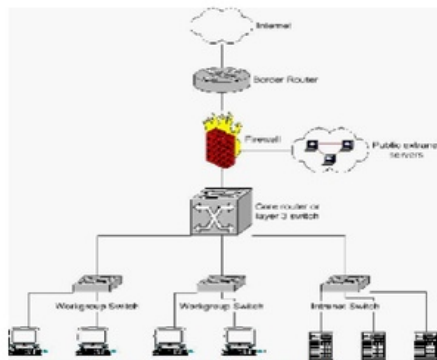


Figure 1: Basic Network Design

As noted this is a basic network design, but can be used as a fully functioning network which is deemed to be secure due to the fact that the firewall is in place and the relevant devices are being used.

However the paper goes on to describe the different methods adapted to this network to make it become more secure. One major point that coincides with this report is the use of an IDS or IPS, the benefit to security these create cannot be measured, but can be understood.

In this diagram the use of IDS systems is shown:

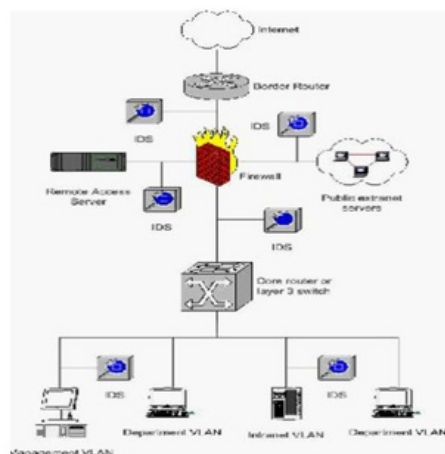


Figure 3: Location of IDS Sensors

Now it must be noted that the security taken on by the SANS institute talks about layering and hardening switches as well as the use of IDS, IPS and Firewalls. In relation to Figure 1, the use of separate security zones enables the network admin to create a security policy that will be easier to roll out with the way that the network is created, although in Figure one there is a lack of infrastructure for managing the network, a few tftp servers and maybe a syslog server could be added.

To achieve maximum security, the SANS institute has implemented layer 3 and layer 2 security methods, and although the software used is dated the methods are still the same, for example they are running Windows Server 2000 which this project will be running Windows Server 2010, this is not a hindrance as this will help strengthen this project in showing the next steps taken in the modern era, and to show how the evolution of methods has been achieved which could lead to trends being set and the understanding of how some attacks may be worked.

One key point that will be looked at closely is some of the methods used in the late 2000's like VLAN hopping, this is where an attacker could jump from one VLAN to another and gain access to more sensitive VLANs, which could lead to a misconfiguration giving undesired access to and intruder [17]. These vulnerabilities were found by David Taylor [18], David took on a VLAN security test report and found that it was possible to jump across VLANs on a Cisco switch by injecting specially crafted frames in a default configuration [19], there are many arguments put forth that discuss the use of multiple VLANs on one switch and the

risks vs benefits to security. The network architect would need to decide between these two factors as there is insufficient information to state either way is more effective than the other. This will be looked at within this project when setting up the security on the devices themselves, if it is found that singular or multiple use is best for security then a separate report should be conducted to show the facts and help alleviate any uncertainty in the future.

In this chapter you compare literature and critically review them. Compare books and journals as these attract higher marks as they are mostly peer reviewed. You can use *some* website as sources but I recommend books and journals. You can also put in items like a competitor analysis in this chapter. For example, a part of your literature review may look at design of a website. You could compare what several different authors say about how a website should be designed and then use this later on to justify why you have designed/developed your website in such a way. Also another thing you should think about putting in your literature review is a feasibility study and a competitor analysis. You may also compare different tools that you may use to develop your system.

Each chapter should have its own introduction and conclusion so as to retain a formal report structure. It is not always advisable to use Literature Review as a chapter heading. Think of a sensible title for each chapter which reflects its content.

2.2 METHODOLOGY

When creating a major project like this then it is necessary to incorporate the numerous research methods that are used in current papers, these can come under Qualitative and Quantitative research methodologies [20]. For the purpose of this project the quantitative methods will be used as this paper will be looking at data and measuring variable, will also be verifying and questioning existing theories around the subject, both these methods can be used together however, qualitative methods are more to understand meanings, look at, describe and understand experience, ideas, beliefs and values, intangibles such as these [21].

The research philosophy and approach to this project is aided by Positivism due to the fact that Positivism adheres to the view that only "factual" knowledge gained through observation (the senses), including measurement, is trustworthy [10], whereas phenomenology is more based on occurrences, happenings with a certain disregard for the external or physical reality [22]. This project needs factual data that is ascertained using tests on a vulnerable and non-vulnerable network not possibilities as this would be hard to gather relative evidence, even greater difficulty to get conclusive results.

There would be certain risks to this project if it were to be carried out in a real world scenario, ethical and legal practices would have to be called upon to restrain certain methods being used, which will hinder this report as total coverage is needed. As the project is being carried out on Virtual machines created by the tester then these matters do not exist, the only real risk is that of the software that this is being implemented on, as technology moves in such a rapid way that if for example, the machines being tested upon were running Windows 95 then the considerations from any OS further than that point would be obsolete, due to the aged security features being more vulnerable.

There may be some limitations to what tests can be carried out due to the fact that this project is only using Kali Linux, which is a Pen testing favourite. However there are other suites out there like, Parrot Security OS or Backbox for instance [25] that carries their tests out in different ways and with different methods so some data may not relate, overall though the results should not differ too greatly.

The research strategy being used for this project is experimental and document review, as tests are going to be carried out on a network to ascertain data that is hopefully going to help with the defence against intrusion, the environment used is for experimental purposes and to help network engineers understand the issues faced of an unsecure network, and in turn helps to combat them [26].

Also as mentioned in the Literature review there will be at least 4 papers reviewed which comes under document review, to see if their methods which mainly are dated, help to understand the evolution of hacking. This will help to understand the ways and means used to overcome intrusion or data manipulation which will enable a better testing environment as the data will be 100% identifiable. For example if the tests were to be carried out using just the outdated methods then

results would be inconclusive as methods have taken advancements over the years, and older methods of stopping or sensing attacks have become redundant and are no longer in use.

Ethical and Legal Issues

As this project is going to be carried out in a virtual environment, the ethical and legal issues of a "live" project cannot be considered due to the fact that it is all virtual, in a "live" (currently used) network then there would be major issues to be taken into consideration due to the fact that the whole security of the "virtual" environment needs to be compromised to the full to see relative results. If the "live" network had its firewalls turned off for a moment then not only would the tester be able to intrude [27], but also that of attackers from all over the world would have access and leave the network in a very vulnerable state.

The results that will be collected from this project will be analysed by using older methods vs current methods, that way a comparison can be made and the differences could show any evolutionary techniques or simple methods that have been used to get around the security of the time. the stages of data collection will be time framed and will be clearly marked as to what era they are from, for example as mentioned above, some older intrusion methods are still in use today and as security patches or fixes are released regularly [28], it will be key to see how an intrusion was successful or not and to see how the updated security features have contested the intrusion method and forced evolution of itself to enable a new way around the security.

Resources and Planning

The resources needed for this project are that of, firstly Oracle VMWare (Virtual Box) also (dependant on availability) Windows Server 20010 with Windows 10 clients, a working version of Kali Linux. These will all be needed to create the network and carry out the tests, Kali Linux has all the tools needed to be able to test fully. Access to the library will also be key to obtain further journals for inspirations and for knowledge and understanding.

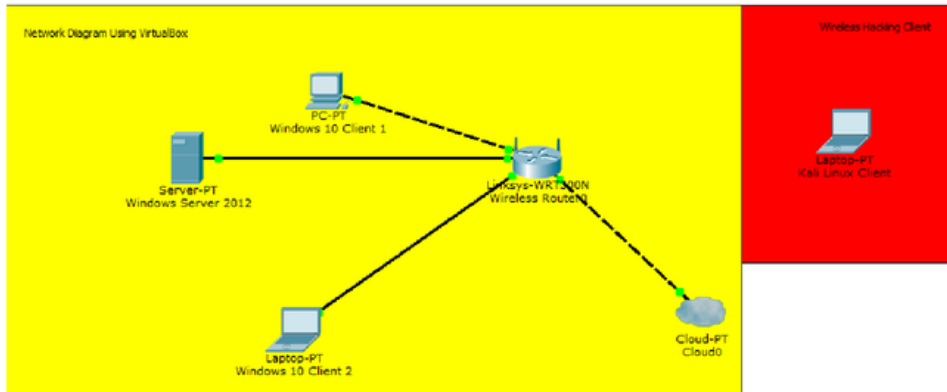
Phenomenology uses an inductive method to build on theory, which is what this project will be doing, building on the tests that have already been carried out to try and find a link or common ground between security methods used.

Data analysis will be taken on by an empirical study as close analysis of how the attacks happen and how the defence works to counteract these attacks, a theoretical approach could have been used but this would lose the applicability of the specific tests carried out, in a more broader sense then theories would be used to see the different stages of execution as they happen but to help with the timescale of this project then empirical study will be used, for feasibility reasons the approach of becoming future proof as such is not realistic, due to the timescale again and the need for more factual data given on a live network.

CHAPTER 3 - DESIGN & IMPLEMENTATION

3.1 INTRODUCTION

The design of the network will be restricted due to the software being used that virtualises the more basic features that are needed to carry out certain attacks, as mentioned the whole project will be done using Virtual Machines within Virtual Box and the network can be seen here (represented within packet tracer):



This diagram of what the Virtual machines will look like show a desktop user, a laptop user using a hotspot and the Server running as a Database/DHCP server. The wireless hacking client (Kali box) is represented outside of the network.

A Domain will be issued to represent a corporate environment and security benefits from creating a domain will be documented in the recommendations section of this report.

The restrictions will be documented in its own heading towards the end of the design and implementation stage.

3.2 PROBLEM FORMULATION

The main problem with network security be it at home or at work, is the amount of ways to carry out the same kind of security, and the amount of tools that are offered by companies, these may all may work the same but can pose a great

shroud over any network professionals progression of security on the network they are monitoring. The Internet is a large and substantial place where all sorts of information can be found on everyday matters, people look to the Internet as a referencing guide in a social, work or academic environment and is used as a backup tool. This report itself will be using a multitude of information gathered from the internet and from security agents working in the field.

Another reason for Network Security is the Internet itself; it harbours individuals with malicious intent, sometimes known as a "hacker" or "hackers". Hackers are people who use the internet to gain information about individuals or to gain information about a company or even just to stop a company from trading on the internet. The home network and work network although greatly dissimilar are just as much at risk as each other, it holds the valuable information that hackers want, and need to be able to get on with their everyday routines, Which in turn makes it more likely that they will attempt to intrude on these networks.

The kinds of attack that will be identified in this report are mainly at the Ethernet, TCP/IP and application layers, these are the areas at major risk and what security agents are currently plummeting a lot of time into.

An attack at Ethernet layer would be ARP Spoofing.

ARP Spoofing is fundamentally simple but is extremely hard to detect in the beginning, ARP (Address Resolution Protocol) is a protocol used for mapping IP addresses with the physical (MAC) address of a user on the network, ARP spoofing is the ability to send falsified ARP messages over a local area network [29]. This then gives the sender the ability to link their machine with that of the legitimate computer which enables the sender to intercept, modify or even stop data in-transit by receiving the data that was originally intended for the legitimate machine. ARP spoofing attacks then lead to a few different types of attack from DOS attacks to MITM attacks, a DOS (denial of service) attack does exactly what it says on the tin, it overloads a target with traffic that is

intended to go elsewhere where as a MITM (Man in the middle) attack is used to intercept and modify data between the victims.

ARP spoofing as suggested is hard to detect in the beginning due to the fact that the default configuration for most network switches allows ARP spoofing attacks to take place unchecked [30] however there are ways and means of catching these attacks by using a simple yet great piece of software called Wireshark, Wireshark has a function called ARP duplicate address detection and not only that there is another feature called detect ARP request storms function.

An attack at TCP/IP layer would be Port Scan and Banner/Vulnerability identification.

Port Scanning is used in both legitimate network management and also in malicious use, all information sent and received is in and out of computers ports, so port scanning is used to identify open doors [31]. Hackers then exploit these "open doors" as an entry into a system and, without the relevant security some serious damage can be done. Banner/Vulnerability Identification is a similar technique but has the ability to ascertain the software and version from whatever protocol is running on that port. These can both be detected by various detection tools out there to help network managers detect and shutdown these port scan attacks, like Scanlogd.

A common attack at application layer would be SQL Injection.

SQL Injection is used by these aforementioned hackers to steal data from organizations. It is the type of attack that uses brute force when finding an error or improper coding of a web application to "inject" SQL commands into say a login form to allow access to data held within a database [32].

These improper coding errors cause breaks that allow SQL statements to pass through and query a database directly without any authentication.

SQL injection is a very serious matter and is very hard to combat, especially as human error cannot be relied upon not to happen, it's the human error when

creating the html code that causes the breaks for SQL injection to happen. One sure fire way of solving SQL injection attacks is to constrain input. This is just simply put the art of ensuring no human error in code logic and to ensure that all means tested are normal and extreme.

The overall problem is lack of security, or in certain cases the lack of backing for security from management, which is why these tests are being carried out, to show the difference in what happens with or without the security and to compare the loss to the benefits whether it be through tangible or intangible sources.

3.3 DESIGN

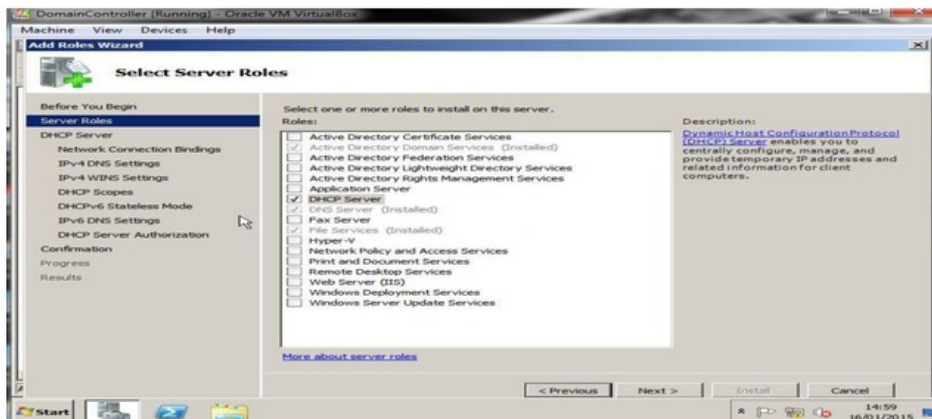
The design has been implemented this way due to restrictions in the software used, as mentioned above if enough interest and study is put into this field then two options are available, the use of a current live network or the collection of end devices to be able to emulate a network environment at home.

There is no ability to run defensive tests on network peripherals, like IP spoofing, packet sniffing etc.

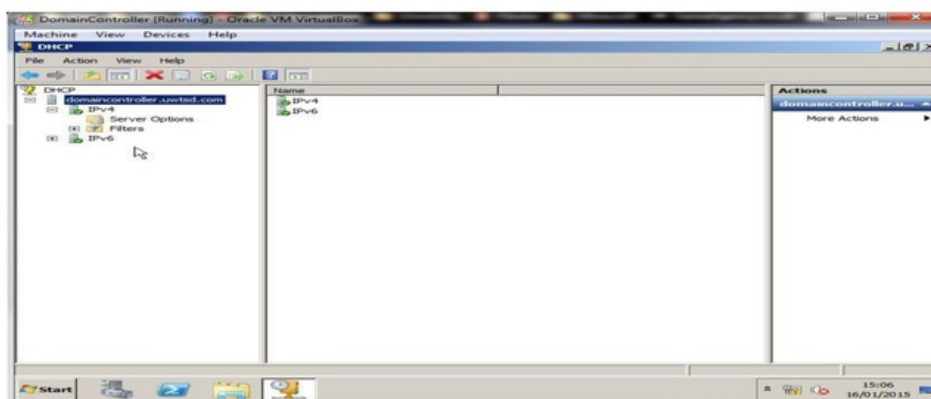
3.4 IMPLEMENTATION AND DIFFICULTIES

The network implementation is relatively simple, create two virtual machines using Windows 10 as the operating system then a Windows Server 2012 install and a Kali Linux install.

The network management will be handled by using the Virtual NICS available on the machines to produce connectivity, the server will run as a DHCP server and all confirmation can be seen here:



And here shows the ability to run IPv4 and IPv6 as per request.



Here shows the user obtaining an IP address via the DHCP server:

```
Ethernet adapter Public-Classroom:

Connection-specific DNS Suffix  . : UWTSD.com
Description . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Physical Address. . . . . : 08-00-27-50-38-42
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::98ed:f788:7534:cd9a%11(Preferred)
IPv4 Address. . . . . : 192.168.1.10(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : 16 January 2015 15:18:46
Lease Expires . . . . . : 24 January 2015 15:18:45
Default Gateway . . . . . :
DHCP Server . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . : 235405351
DHCPv6 Client DUID. . . . . : 00-01-00-01-11-4A-B6-68-08-00-27-50-38

DNS Servers . . . . . : 127.0.0.1
NetBIOS over Tcpip. . . . . : Enabled
```

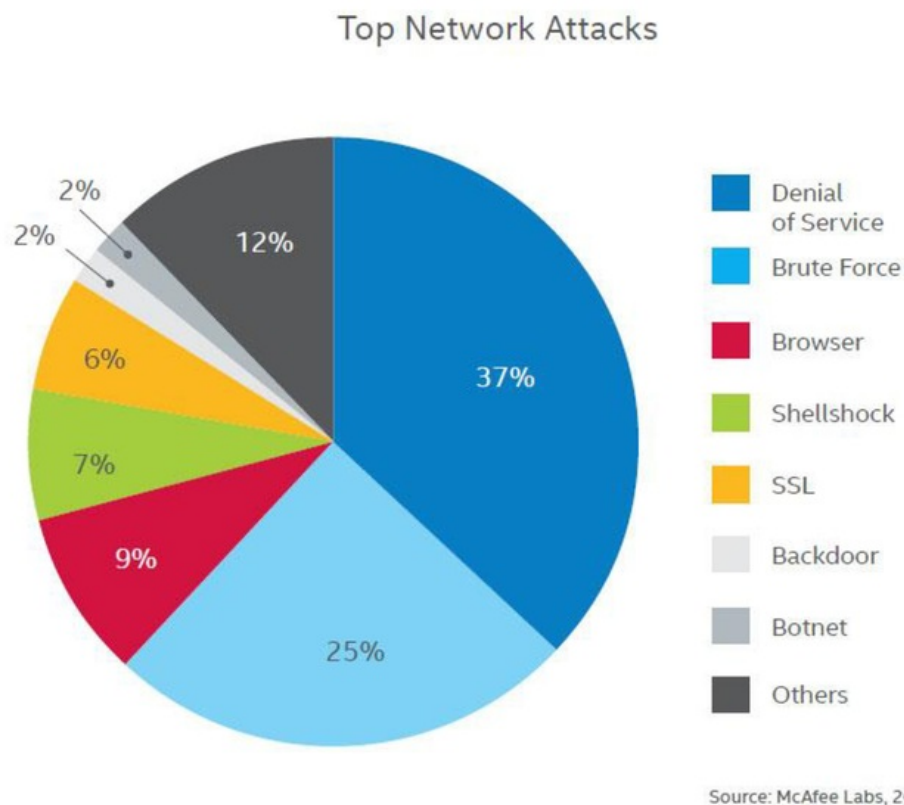
The difficulties encountered involve the software whereas there is no way to represent a wireless router or a standard router and no cabling can be used, the

problems faced with this are overcome by the attacks that have been carried out not needing that particular bit of hardware, but if a more comprehensive testing is needed to be done to carry on this research then, as mentioned the use of a live network would be extremely beneficial to grant total coverage of attacks.

More details on the difficulties encountered can be found in the reflections section of this paper.

CHAPTER 4 – TESTING AND EVALUATION

The testing that will be carried out will be documented in this section and have its own subheading for ease of reading, information gathered will be put into factual data and collaborated to prove the overall aim of this report. A graph created by a company called McAfee Labs shows here the 7 most common network attacks and for the purpose of this report the top three will be demonstrated, countered and documented herein [32]:



TEST 1

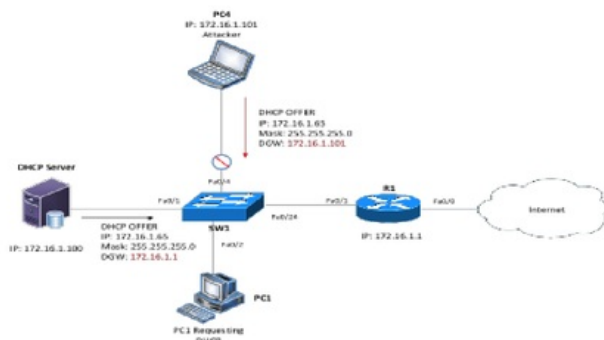
4.1 DHCP EXHAUSTION/DOS ATTACK

The first test to be carried out on the virtual network is that of the DHCP exhaustion attack, this is a DOS attack that exhausts the IP Pool found within the DHCP Server which then will not allow any client on the domain to obtain an IP

address from this server as all address will be exhausted as the attack suggests, then a MITM (Man-in-the-middle) attack can be initiated which could be detrimental to any organisations data. As a MITM attack mitigates any IP lease request from the server to itself obtaining connectivity and the ability to monitor and alter network connectivity and traffic, this is a great risk to the confidentiality of any company and their clients information.

This will be carried out using the DHCPig tool found within Kali Linux. The attack will be carried out and security methods to stop this will be documented at the end of the attack, this is due to the fact that a switch cannot be used in the virtual network. As the exhaustion attack relies on broadcasting DHCP requests with spoofed MAC addresses. The way it does is by finding an open port on a switch and then through that port flooding the DHCP with authentication requests, filling it up. All requests have false return addresses, so the server can't find the user when it tries to send the authentication approval. The server waits, sometimes more than a minute, before closing the connection. When it does close the connection, the attacker sends a new batch of forged requests, and the process begins again--tying up the service indefinitely [33].

The Exhaustion attack carried out on the network gave mixed results, at first the attack was run using DHCPig which caused problems within Virtual Box, unfortunately it seems to be that when running a Dos attack in Virtual Box the original machine that the virtual machines are run on gets involved with the attack, and after 3 unsuccessful attempts due to the original machine getting the Blue screen error and shutting itself down, the test was scrapped on the original machine but run on a backup Linux machine using Backtrack instead of Kali, which does not affect trustworthiness of the test due to the fact that Kali is an extended version of Backtrack. This is mainly due to the reason stated above the lack of switches in the network, research into why these attacks work for some virtual machines and not for others is very vague as the reason varies from one tester to another but the overall consensus is that it's the problem with the virtual rooting of the networks data. An example of a man-in-the-middle attack can be seen here to understand the DHCP offer that is being sent out.



Here shows the attack being carried out on the Virtual Linux machine and the given IP Pool set within the domain of UWTSD:

```

root@bt: /pentest/stressing/dhcpig
File Edit View Terminal Help
Sending DHCPDISCOVER on eth0
timeout waiting on dhcp packet count 3
Sending DHCPDISCOVER on eth0
waiting for DOS
Sending DHCPDISCOVER on eth0
timeout waiting on dhcp packet count 3
waiting for DOS
DHCP exhausted, knock all remaining hosts offline

root@bt: /pentest/stressing/dhcpig
File Edit View Terminal Help
Knocking 192.168.100.124 offline, goodbye
Knocking 192.168.100.125 offline, goodbye
Knocking 192.168.100.126 offline, goodbye
Knocking 192.168.100.127 offline, goodbye
Knocking 192.168.100.128 offline, goodbye
Knocking 192.168.100.129 offline, goodbye
Knocking 192.168.100.130 offline, goodbye
Knocking 192.168.100.131 offline, goodbye
Knocking 192.168.100.132 offline, goodbye
Knocking 192.168.100.133 offline, goodbye
Knocking 192.168.100.134 offline, goodbye
Knocking 192.168.100.135 offline, goodbye
Knocking 192.168.100.136 offline, goodbye
Knocking 192.168.100.137 offline, goodbye
Knocking 192.168.100.138 offline, goodbye
Knocking 192.168.100.139 offline, goodbye
Knocking 192.168.100.140 offline, goodbye
Knocking 192.168.100.141 offline, goodbye
Knocking 192.168.100.142 offline, goodbye
Knocking 192.168.100.143 offline, goodbye
Knocking 192.168.100.144 offline, goodbye
Knocking 192.168.100.145 offline, goodbye
Done with 192.168.100.146 offline, goodbye

```

Even though only three IP addresses are assigned it may be questioned as to why all addresses were exhausted, this is just the way the program runs as it is meant to be a stress load test on a fully functioning network which would generally have more than just the two clients.

And as mentioned the problem encountered on the original machine causing this particular test to be run on a backup machine due to time restriction, there are more clients available on the Linux machine that are actually shown in the network diagram above as this was a setup being used for testing different defence

methods against dos attacks, although it shows the attack on a larger scale it doesn't show the original network being tested.

Host Name	IP Address	MAC Address	Conn. Count	Ratio (1024)
FAIANE55	192.168.100.106	00:0C:29:63:9A:74	1	0%
OT81VYUK	192.168.100.102	00:0C:29:56:A1:89	1	0%
V1L9D4ZY	192.168.100.119	00:0C:29:7A:30:F9	1	0%
DT796BN	192.168.100.108	00:0C:29:83:F6:1C	34	3%
DO-WRT	192.168.100.1	00:0C:29:83:F6:1C	53	5%
IAC5I5JY	192.168.100.117	00:0C:29:3D:28:48	1	0%
91JIQRV2	192.168.100.105	00:0C:29:14:D2:F2	1	0%
DXLQBAJD	192.168.100.100	00:0C:29:52:D5:F8	1	0%
DRVPRN3O	192.168.100.115	00:0C:29:2E:B4:88	1	0%
OTGYDX4Z	192.168.100.116	00:0C:29:6D:98:79	1	0%
UPMSECEL	192.168.100.118	00:0C:29:78:D8:33	1	0%
PYXQLQ75	192.168.100.113	00:0C:29:1A:E2:00	1	0%
69W2XSE2	192.168.100.104	00:0C:29:6E:DD:F0	1	0%
256ZLS7T	192.168.100.111	00:0C:29:62:EF:C1	1	0%
764OLRQ0	192.168.100.114	00:0C:29:27:DE:18	1	0%
M3TTOK3T	192.168.100.109	00:0C:29:17:8F:72	1	0%
FX9FUFJ8	192.168.100.103	00:0C:29:3D:9A:F3	1	0%
JTFMTEGO	192.168.100.112	00:0C:29:50:49:71	0	0%
PSJ9M1DJ	192.168.100.110	00:0C:29:68:C3:0F	1	0%
QIC8PAQH	192.168.100.101	00:0C:29:5C:68:1B	1	0%
D19MW7GH	192.168.100.107	00:0C:29:5D:1D:B8	1	0%

Here you can see that the Comm Count (Communication Count) is set to 1 for all but 3 machines, this is standard to show that they are up and running and communicating effectively. Here is the same screen just after the exhaustion attack has been run.

Host Name	IP Address	MAC Address	Conn. Count	Ratio (1024)
FAIANE55	192.168.100.106	00:0C:29:63:9A:74	0	0%
OT81VYUK	192.168.100.102	00:0C:29:56:A1:89	0	0%
V1L9D4ZY	192.168.100.119	00:0C:29:7A:30:F9	0	0%
DT796BN	192.168.100.108	00:0C:29:83:F6:1C	35	3%
DO-WRT	192.168.100.1	00:0C:29:83:F6:1C	41	4%
IAC5I5JY	192.168.100.117	00:0C:29:3D:28:48	1	0%
91JIQRV2	192.168.100.105	00:0C:29:14:D2:F2	0	0%
DXLQBAJD	192.168.100.100	00:0C:29:52:D5:F8	0	0%
DRVPRN3O	192.168.100.115	00:0C:29:2E:B4:88	0	0%
OTGYDX4Z	192.168.100.116	00:0C:29:6D:98:79	1	0%
UPMSECEL	192.168.100.118	00:0C:29:78:D8:33	1	0%
PYXQLQ75	192.168.100.113	00:0C:29:1A:E2:00	1	0%
69W2XSE2	192.168.100.104	00:0C:29:6E:DD:F0	0	0%
256ZLS7T	192.168.100.111	00:0C:29:62:EF:C1	1	0%
764OLRQ0	192.168.100.114	00:0C:29:27:DE:18	0	0%
M3TTOK3T	192.168.100.109	00:0C:29:17:8F:72	1	0%
FX9FUFJ8	192.168.100.103	00:0C:29:3D:9A:F3	0	0%
JTFMTEGO	192.168.100.112	00:0C:29:50:49:71	0	0%
PSJ9M1DJ	192.168.100.110	00:0C:29:68:C3:0F	0	0%
QIC8PAQH	192.168.100.101	00:0C:29:5C:68:1B	0	0%
D19MW7GH	192.168.100.107	00:0C:29:5D:1D:B8	0	0%

As you can see the majority of clients are now down, the ones that are still up is due to the virtual software not effectively shutting down each client and ignoring the Dos attack all together, this attack was run several times with the exact same

clients going on and off, the only conclusion that can be made to this is as mentioned the problems faced by running these tests on virtual machines.

Prevention

A key note to make here is to not mistake the above DoS attack with a DDoS (Distributed Denial of Service) attack, this kind of attack although similar in method and execution is on a much larger scale, it usually involves something called a botnet[34], which is a distribution of machines that are designed to attack the more larger of organisations and the payload is much more severe due to the scale of resources being used to bombard the switch or DHCP server with requests, this kind of attack is much more complicated to defend against and almost impossible to prevent for a certain amount of time. As a DoS attack is typically a malicious user gaining access to a switch on a single end device then the problem although cannot be prevented as such, can be handled in a more efficient fashion. The use of SNMP Agents/Traps are very advantageous as these can be set to alert agents when an outage is taking place thus alerting the network management team and allowing them to act efficiently and given the ability to get ahead of the attack and maybe shut off the switch that is being bombarded, routing protocols will then take place and find the next best path which should automatically be located in the routing tables for that network. Although one method can greatly help in prevention is the use of Firewalls, and ensuring ports are closed on switches.

Firewalls can be setup so a network administrator can block certain connections and allow others, if only trusted connections are allowed then the DoS attack should not be able to get through, however if the connection that is allowed gets removed but not removed from the firewalls instruction base then the risk would be just the same as without a firewall, as firewalls sometimes tend to leave ports open that it has used for an old trustworthy connection. This is where proper network management and efficiency come into play, if security policies can be written up to ensure all network managers run regular checks then the potential to stop these threats increases significantly depending on the regularity of these checks.

Same with the SNMP Agent/Trap, this is a listening device that can open a port to listen to its communication and then alert the relevant agent if there is any problem or irregularity with the function of the port its listening in on, but as these open ports an attack can be just as easily, a mixture of firewall and SNMP Traps and security policies are the best way to overcome and help deter this sort of attack.

TEST 2

4.2 BRUTE FORCE

The second test that was simulated on the network was the Brute Force attack also known as brute force cracking, this is a method used by hackers and initiated through an application to decode encrypted data such as passwords or even data encryption standard (DES) keys. The application proceeds through all possible combinations of legal characters in sequence. Brute force is considered to be an infallible, although time-consuming, approach [35].

In a traditional brute-force attack, the hacker just tries the combination of letters and numbers to generate password sequentially. However, this traditional technique will take longer when the password is long enough. These attacks can take several minutes to several hours or several years depending on the system used and length of password [36]. There are other ways that this can be used, for example an attacker can use this algorithm to find secret back end webpages or PHP pages but the test carried out on the UWTSN domain only focuses on password cracking.

The problem faced with password cracking as mentioned above is length over complexity, here is a chart created by John the Ripper a tool found within Kali linux that was used to force the passwords on the network:

	A	B	C
1	Characters	Seconds	In other words:
2	1	0.005102041	5 milliseconds
3	2	0.071428571	10th of a second
4	3	1	1 second
5	4	14	14 seconds
6	5	196	3 minutes
7	6	2744	45 minutes
8	7	38416	11 hours
9	8	537824	6 days
10	9	7529536	90 days
11	10	105413504	3.5 years
12	11	1475789056	50 years
13	12	20661046784	700 years

the initial test run on the Windows 10 client was deemed as good news for security but not particularly good for testing purposes as Windows 10 security features have been enhanced beyond the simple security of that of a Windows 95 or NT machine, and the overall testing of this feature could be deemed as a failure however, enough insight can be given to recommend and show the need for security to be in place

This proves that length certainly beats complexity as a password with a character length of 12 would take 700 years to crack, which is enough of a deterrent to ensure hackers cannot gain access to a user's password, a situation that proved difficult was the ability to get hold of password databases, these password databases or hashes are loaded into the relevant tool being used and then the algorithm is run with these in mind here is the test file being successfully ready in Kali:

```

root@kali: ~
File Edit View Search Terminal Help
OPT
some service modules support additional input (-U for module help)

Supported services: asterisk afp cisco cisco-enable cvs firebird ftp ftps http[s]
]-(head|get) http[s]-(get|post)-form http-proxy http-proxy-urlenum icq imap[s] i
rc ldap2[s] ldap3[-(cram|digest|md5)[s] mssql mysql ncp nntp oracle-listener ora
cle-sid pcanywhere pcnfs pop3[s] postgres rdp rexec rlogin rsh s7-398 sip smb sm
tp[s] smtp-enum snmp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra
These services were not compiled in: sapr3 oracle.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY - and if needed HYDRA_PROXY_AUTH - environme
nt for a proxy Setup.
E.g.: % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or socks4:// or connect://)
% export HYDRA_PROXY_HTTP=http://proxy:8080
% export HYDRA_PROXY_AUTH=user:pass

Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/TLS:DIGEST-MD5
root@kali:~#

```

This was using the hydra system as currently there are not a lot of applications that are compatible with Windows 10. It is relatively easy to set up your own password hash but the complications and time restrictions with this for the purpose of this test is unnecessary, restrictions being the time used to create the password hash file and the complications that the password is already known so a buyist view can be taken when entering these passwords and the time it takes to crack may not relate to a trustworthy test.

The restrictions imposed by using Windows 10 as the device being attacked for the purpose of Brute force attack is deemed as a failure, there is insufficient information available to be able to gather enough data to run secure and accurate tests, and due to certain time restrictions faced by this project then work must continue on to the last attack, the testing itself is very vague as the lack of resources prove that security is getting tighter as Operating Systems grow.

Security concerns can still be drawn up and implemented from the insight gained by the research completed on this section of the attacks, enough information is there to understand the attacks at a comprehensive level and to help grant more security in the future, the problem faced is with the applications themselves and with hindsight maybe windows 7 systems would be more vulnerable and would grant ease of access, as in all sections the overall security methods to combat these attacks will be documented in the recommendations section.

TEST 3

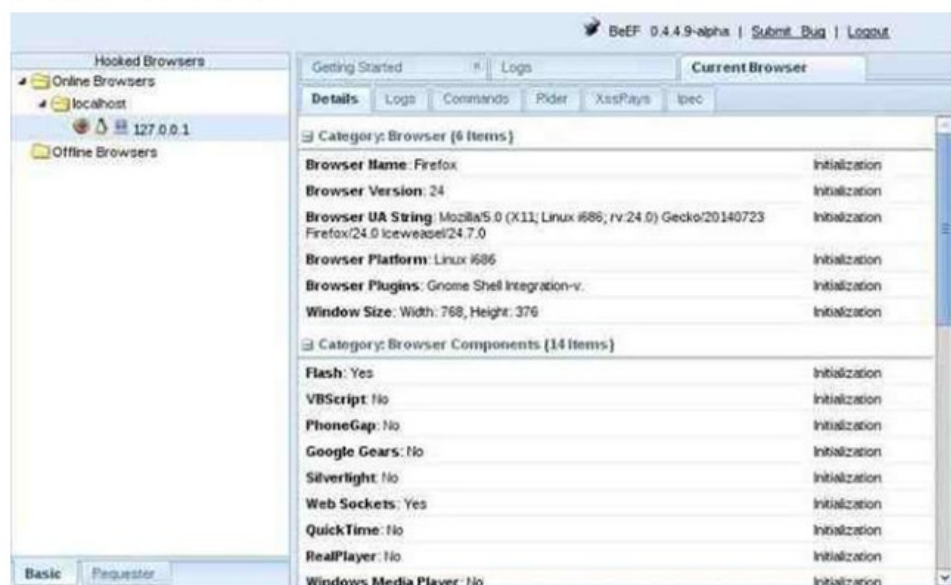
4.3 BROWSER ATTACKS

Browser-based attacks target end users who are browsing the internet. The attacks may encourage them to unwittingly download malware disguised as a fake software update or application.

Malicious and compromised websites can also force malware onto visitors' systems. They often do this by exploiting a weakness in a visitor's browser or related software, typically caused by the software being out of date [37]. The need for more security into browser attacks is highlighted by a study undertaken by

Google [] who say 1 in 10 sites are now booby-trapped as such with malware infections silently installing viruses and spyware or tricking you into revealing your confidential information [38].

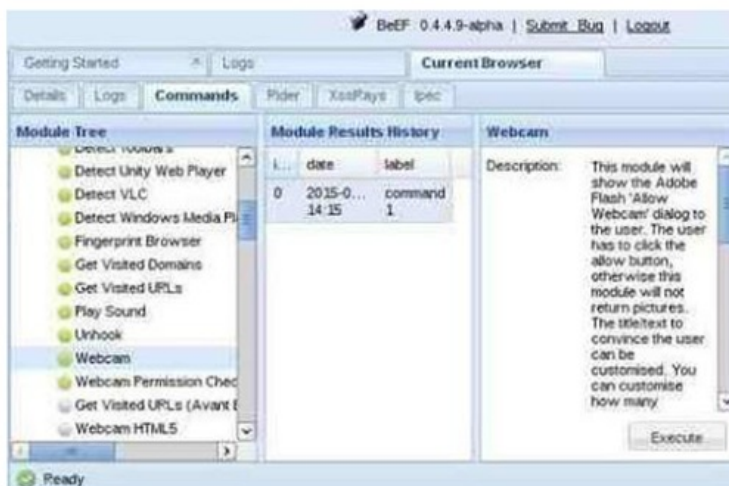
The application used for this attack is called BeEF, it is started as a service and accessed via the web browser on the hacking client here is the client screen once the service has been run:



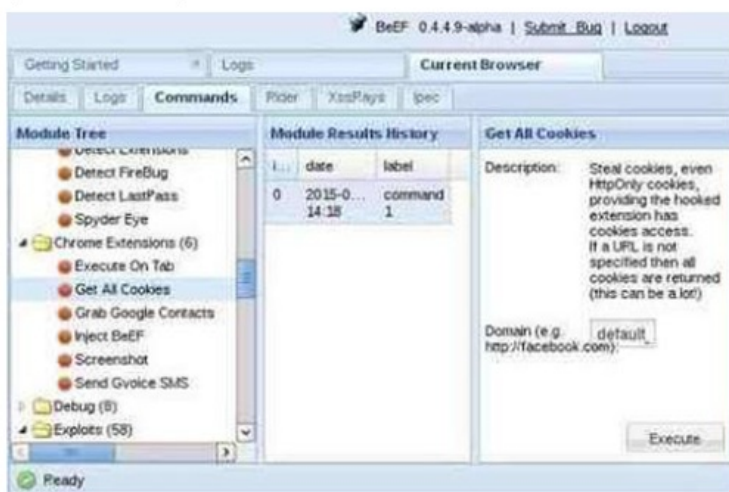
It shows the browser info and any related information for the user currently logged in, the way this system works is to hook a browser, this is getting a user to visit a vulnerable web app that is linked to BeEf server. Within BeEF there is a JavaScript called hook.js, this is the script that runs once a user access the vulnerable web app.

The client within the domain is running Internet explorer and has been hooked for the purpose of this test. From here the infected user can then be manipulated and BeEF's built in commands can be executed from the victims browser, there are many possible options here to execute like getting the visited domains information, accessing the webcam of the user, grabbing google contacts and the ability to take screenshots but to mention a few.

This is the screen that shows what happens when you try to access the Webcam:



In the rightmost box the ease of this application can be seen as it fully states what it is doing and what will happen like this example here of stealing the cookies (internet cache) from the infected user:



These are just a few examples of the attacks that can be run within Kali Linux and although used within a controlled environment the risks are still real, they also show the need for intrusion defence to be at the most important agenda of any network management meeting.

CHAPTER 5 – RECOMMENDATIONS

5.1 RECOMMENDATION FOR SECURITY CONCEPTS

With the attacks that have been carried out above then a security recommendation can be drawn up to help any new or existing network reach a shielded environment from network intrusion, with a few steps followed any organisation can have a secure network and although it may not be completely hack proof as such, the resources can be put in place to help deal with these in a timely and efficient manor to ensure an organisations stability and downtimes do not falter.

The first recommendation is to have proper security audits in place, a security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria [39], and are essential to a company's security. They can be a review of policies, configurations, and code review all these security audits, policies and procedures and security measures are needed as hackers get intelligent and learn new ways to obtain information, so too security engineers have to understand these new methods and work out a way to stop them, as proven in the attacks above, for example if a company decided to avoid creating a password policy and allow free reign of password creation then a serious security flaw would come to light with the findings of the speed to brute force passwords on a length basis, whereas security is the main focus of this paper, unfortunately it is not at the forefront of every employees mind, more like ease of workload and the ability to shorten tasks like creating a simple password to remember like 12345 rather than 123456789101112, this alone would deter any hacker from getting access to the network this way and surely secures the company in questions data.

Policies can be easily created and distributed between the work-force, an example of a policy would look like this:

Dear User,

To enable us to get you onto the system, the first time you log on please enter your password as "Password" , which you will then be required to change before you log on to the system.

All passwords must be at least 9 characters in length have a combination of lower and upper case letters and must contain at least one number and one symbol, a-z,A-Z,0-9,@-\$ example Monday@1.

This can also be controlled by using the software of the system being logged onto, to ensure the least human error a bit of coding could be applied to the text box for entering the password to show the parameters that must be met and if they were not met then the password creation would not be allowed.

This is a guide to new users entering onto the system, and using this procedure enables basic password security to be met from the ground up, ideally everyone should have a random hex password generator or some kind of remote log on device but for basic security the above is enough.

Secondly to help with the unwanted and heavy handed DoS attacks then regular testing of the network needs to take place, whether it be through pen testing or the relevant network manager using one of the following tools, everything can help towards being totally secure.

In today's modern network any network professional needs an array of network analysers, security tools and gadgets to do their jobs, There are numerous tools that can be used in a typical ethical hacking suite for example nmap, metasploit and sqlmap

Nmap as the name implies is a network mapping utility [40], if you were to give nmap the detail of a TCP/IP address scheme then nmap would identify any open doors or ports that might be available. It is currently used by thousands everyday to keep systems secure and being as its source code has been ported to many operating systems, it can be used on most OS's (operating systems) like Linux, windows and mac's. Nmap runs from the command line of any operating system, which does turn certain users away when they are used to using a graphical utility,

but being able to understand command line functions and syntax is essential as things like batch files and redirected text have a more advanced functionality.

Metasploit is another open source penetration tool used in the development and execution of exploit code against a target remote machine. Metasploit can be used to test the Vulnerability of computer systems in order to protect them and on the other hand it can also be used to break into remote systems [41]. Metasploit can be used by simply selecting the right exploit (code which allows a hacker to take advantage of a vulnerable system) and setting a target, verify all the exploit options to determine vulnerability then select the payload (actual code that will run on system after exploitation) and execute the exploit.

Sqlmap could be one of the most popular form of sql injection automation tool out there [42]. And also one of the more problematic to an organisation as it has the ability to take over database servers by detecting and exploiting sql injection flaws. These flaws are in the database layer of an application or can even be run from the URL. Even password entry features into sights can have issues with injected code, the login form in this case would be used as an entry point to manipulate data, for example where the form says username a simple command could be run like <input> (the actual code would be a lot more in detail). These tools used in conjunction with the security audits will help any network manager that is trying to secure his or her network.

Lastly to be able to deal with threats from web browser attacks then for the initial recommendation, virtual machines should be used like the ones created for this project, the ability to host multiple images of a desktop on a remote secure server that only grants the access that has been setup on that virtual machine is such a benefit to any company, for example not only is it easier to set up a domain for the users to sit on it also grants the ability to restrict access to certain things, so if the organisation was to be under attack continually from web browser attacks, and constantly having to take machines off the network to perform quarantine of the malware and spyware due to human error, then web access can be restricted when the virtual machines are created. This will stop any user accessing the internet and being able to fall for the ingenious yet simple exploits.

Of course not every company can restrict internet access as a lot of users need this access to be able to perform their roles within the organisation, so other security methods can be used. There is no overall cure-all for any security of a network, security works best with layers be it technical or procedural, simple fixes can include ensuring the most major recent major release of your browser of choice. This will help ensure you have all available security features beyond what are available in incremental patches. The use of phishing filters can also improve security by reducing the chances that one of your users will visit a malicious clone of a legitimate site [43]. In addition to this plugins can be used like Ghostery or ad-blocker for example, but these can also cause security problems as vulnerabilities can come from wrongfully updated plugins that get associated with a .pdf or flash viewer update (most of the common attacks come from these). These can be secured by not giving all end users administrative access, or running application in administrative mode as this would give the vulnerability the access needed to change things and make it difficult to stop the spreading of the application.

An introduction of an host-based IDS (Intrusion Detection System) is a really good way of gaining control, as these systems monitor web traffic to identify and possibly stop the malicious actions, this along with antivirus software helps in all aspects of containing and removing the unwanted malware.

All these security tools focus on the host itself which is caused by human error, albeit not checking proper authenticity of a sites certificates etc., the use of a proxy server can help to combat this as the proxy will inspect the traffic and prevent attacks from reaching the requesting end user. These protective measures could be as "simple" as a URL blacklist, to block access to known bad websites, or as complex as signatures, which may detect JavaScript attacks and other unwanted surprises [44].

The above security methods to help against the attacks carried out in testing can all be access easily and should be brought to light in any network management meeting, that being said without penetration testing to compliment these securities then security satisfaction and reliability would give mixed results, Penetration

testing (otherwise known as pen-testing, or the more general security testing) is the process of testing your applications for vulnerabilities, and answering a simple question: "What could a hacker do to harm my application, or organisation, out in the real world?" [45]. They give security personnel a real experience in handling intrusion methods and without informing the security personnel of the test then the policies and audits mentioned above get a thorough testing also.

Not only at a personnel level do these tests help they can also help to train the developers of applications and such to be more mindful and make fewer mistakes by studying the reports given by the test, one important thing to note, do not ever give a pen tester source code of your organisation, although most official pen testers that offer their service will not use this to their advantage there are the few that would, and if they were to get their hand on this then every method mentioned above could become obsolete. The literature review in this report suggest penetration testing to be used as an ongoing method and this is proved by the need for penetration testing rising over the years, more and more companies now turn to a penetration test when creating a new network, making changes to an existing one or just simply when a security meeting has been called and an organisation requires its security measures to be tightened.

5.2 CONCLUSION

The research carried out in this paper and the testing that has completed was all done to aide and understand a lot more fully the need for security methods to be in place, the risk of these security methods not being in place and to discuss the multiple methods that are currently being used and how to implement them correctly within an organisation

5.3 RECOMENDATIONS FOR FURTHER RESEARCH

The research that has been conducted has many possibilities for further research, as mentioned in the above difficulties section, there are problems to be considered

when attempting these attacks on virtual machines, problems that cannot be foreseen issues with time frame structure once the problems have arisen and the overall lack of quantity to perform a much more thorough attack strategy i.e. a penetration test.

The report although proves the security methods mentioned are needed in the world today there is a lack of evidence as some methods could not be incorporated within the attack of the virtual network, the further research of this paper could carry security into a much more clear understanding if it were to be carried out on a working live network, and if guidelines were properly instructed in the first instance then this would of opened up doors to many opportunity's and security of organisations in the future could look much more prospect full, and more ways and understanding could be incorporated, for example the 3 attacks carried out on the network were attacks that were in a top 7 study created by google, for the purpose of time only the top 3 were used and tested, this doesn't suggest that they were the 3 best suited to use, they were just the 3 more commonly used, the risk factor from anyone of these could have been higher than the 3 that were used, to digress the usage of a live network incorporated by a fully functioning analytical attack of the network would of generated much more results to be deciphered through and much more recommendations could be in place.

CHAPTER 6 – REFLECTIONS

6.1 MAIN AIM OF PROJECT

The aim of this research was to outline the need for proper security methods and to stress the need for penetration testing, along with the possibility of finding a common theme between attacks. 66 percent of these aims were completed satisfactory, the need for security methods is clearly outlined and whether it be down to a simple lack of understanding to the more dire lack of funding from management, with the security methods shown above then it can be achieved, the need for penetration testing has been outlined in many sections of this report and although a penetration test was not actually carried out as such the formalities of a penetration test were there, just unofficial. Along with this the recommendation for further research into this field of penetration testing is also outlined.

6.2 DIFFICULTIES AND AIMS THAT COULDN'T BE MET

The aims that were not met do not discredit this report in anyway, thus being mainly due to the fact that no common ground over the years for methods of attack have been found, each year an analytical company like google sense for one will create the top 7-10 most used attacks of that year, and over the years not one has stood out as the most common for a particularly long time, even though they are all relatively the same list just put in different order, attackers like to mix it up, which coincides perfectly with the recommendations of this report as overall there is no cure-all, the different layers of security protect against different things so the ability to mix it up is a must to stay ahead of users with malicious intent at the forefront of their mind.

Another difficulty faced was that of the operating system, the reasoning behind using the latest software was to ensure that methods be kept up to date, but with hindsight as was proved in the testing part of this report, there were more hindrances created than benefits, a full recommendation for the possibility of a retest will be documented after all conclusions have been drawn up. The main reason for this is down to lack of research into the operating system, and the lack

of resources being there carry out the task given mainly being due to the software/operating system being too new and although could be potentially more vulnerable, not enough organisations use this software which stops certain attacks being carried out on the network.

CHAPTER 7 REFERENCES

- [1] Johnathon Gershater. (2011). What is Penetration Testing. Available: <http://searchsoftwarequality.techtarget.com/definition/penetration-testing>. Last accessed 27th April 2015.
- [2] .. (2013). What is Network Security. Available: http://www.cisco.com/cisco/web/solutions/small_business/resource_center/articles/secure_my_business/what_is_network_security/index.html. Last accessed 27th April 2015.
- [3] Michele Fiocca. (2008). Project Report for Information Security Course . Literature Study of Penetration Testing. . (1), ..
- [4] Dr Daniel Geer, John Harthorne. (2002). Penetration Testing: A Duet .Available: <http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1176290>. Last accessed 27th April 2015.
- [5] Johnny Long. (2011). Google Hacking for Penetration Testers.Available: https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf. Last accessed 29th April 2015.
- [6] Matt Bishop. (2010). About Penetration Testing. Available: <ftp://213.176.96.142/ieee2c0a5c2f-1b40-20140622023107.pdf>. Last accessed 29th April 2015.
- [7] J.D Meier. (2006). Improving Web Application Security: Threats and Countermeasures. Available: <https://msdn.microsoft.com/en-us/library/ff648641.aspx>. Last accessed 1st May 2015.
- [8] .. (2013). What is quantitative research?. Available: <http://www.marketingdonut.co.uk/marketing/market-research/what-is-quantitative-research->. Last accessed 1st May 2015.
- [9] .. (2013). What is qualitative research?. Available: <http://www.marketingdonut.co.uk/marketing/market-research/what-is-qualitative-research->. Last accessed 1st May 2015.
- [10] .. (2011). Positivism. Available: <http://research-methodology.net/research-philosophy/positivism/>. Last accessed 4th May 2015.

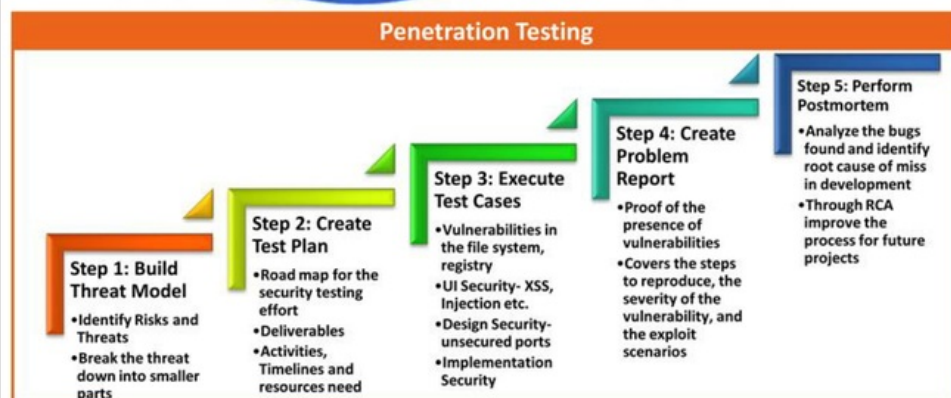
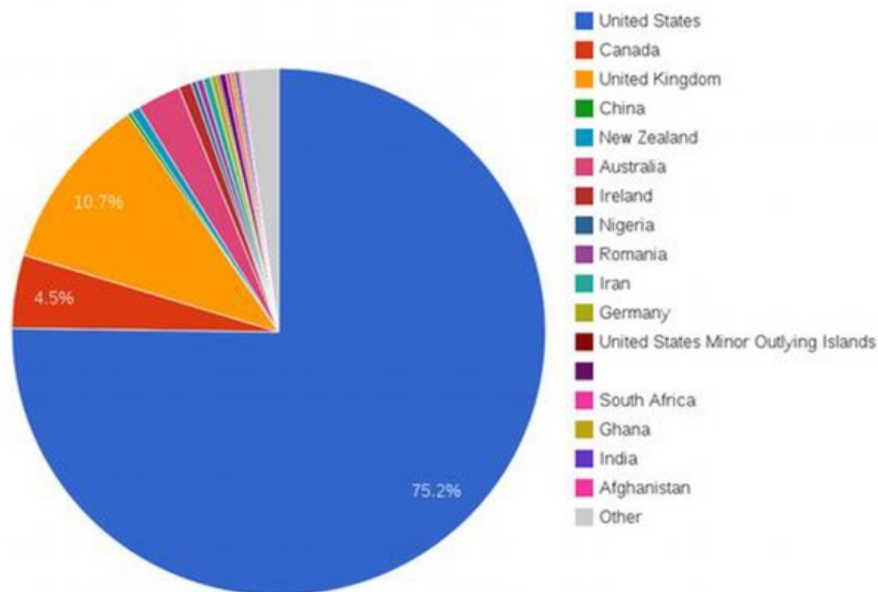
- [11] .. (2011). Phenomenology. Available: <http://research-methodology.net/research-philosophy/phenomenology/>. Last accessed 4th May 2015.
- [12] Jon Espenschied. (2008). Pen Testing Tools. Available: <http://www.computerworld.com/article/2536045/endpoint-security/five-free-pen-testing-tools.html>. Last accessed 5th May 2015.
- [13] Lund Research. (2012). Research Strategy and Ethics. Available: <http://dissertation.laerd.com/research-strategy-and-research-ethics.php>. Last accessed 5th May 2015.
- [14] Kanona, M Rusul. (2011). Legal and Ethical Issues in Computer Security. Available: <http://khabib.staff.ugm.ac.id/downloads/lecture/ITAudit/legal-ethic.pdf>. Last accessed 5th May 2015.
- [15] Microsoft. (2013). Security Bulletin. Available: <https://technet.microsoft.com/en-us/security/bulletin/dn602597.aspx>. Last accessed 7th May 2015.
- [16] Glynn Fergal. (2011). ARP Spoofing. Available: <http://www.veracode.com/security/arp-spoofing>. Last accessed 1st May 2015.
- [17] Keith Barker. (2012). How to use Wireshark to detect and prevent ARP spoofing. Available: <http://searchsecurity.techtarget.com/video/How-to-use-Wireshark-to-detect-and-prevent-ARP-spoofing>. Last accessed 1st May 2015.
- [18] Webopedia. (2013). Port Scanning. Available: http://www.webopedia.com/TERM/P/port_scanning.html. Last accessed 1st May 2015.
- [19] .. (2011). SQL Injection: What Is It?. Available: <https://www.acunetix.com/websitesecurity/sql-injection/>. Last accessed 1st May 2015.
- [20] Chris Anderson. (2005). What is the Difference Between Policies and Procedures. Available: <http://www.bizmanualz.com/blog/whats-the-difference-between-policies-and-procedures.html>. Last accessed 3rd May 2015.
- [21] Brent Jensen. (2013). 5 Myths of Password Security. Available: <https://stormpath.com/blog/5-myths-password-security/>. Last accessed 3rd May 2015.

- [22] Null Byte. (2014). Hack Like a Pro. Available: <http://null-byte.wonderhowto.com/how-to/hack-like-pro-crack-passwords-part-1-principles-technologies-0156136/>. Last accessed 9th May 2015.
- [23] Margaret Rouse. (2014). Security Audit. Available: <http://searchcio.techtarget.com/definition/security-audit>. Last accessed 4th May 2015.
- [24] .. (2012). Secrets of Network Cartography. Available: <http://www.networkuptime.com/nmap/page1-1.shtml>. Last accessed 7th May 2015.
- [25] Rafay Baloch. (2012). What is Metasploit. Available: <http://hackyshacky.com/blog/what-is-metasploit/>. Last accessed 7th May 2015.
- [26] .. (2012). Hacking With SQLMap. Available: <https://ctrlaltnarwhal.wordpress.com/2012/10/27/hacking-with-sqlmap-a-beginners-guide/>. Last accessed 9th May 2015.
- [27] Kanona, M Rusul. (2011). Legal and Ethical Issues in Computer Security. Available: <http://khabib.staff.ugm.ac.id/downloads/lecture/ITAudit/legal-ethic.pdf>. Last accessed 5th May 2015.
- [28] Lund Research. (2012). Research Strategy and Ethics. Available: <http://dissertation.laerd.com/research-strategy-and-research-ethics.php>. Last accessed 5th May 2015
- [29] Lund Research. (2012). Research Strategy and Ethics. Available: <http://dissertation.laerd.com/research-strategy-and-research-ethics.php>. Last accessed 5th May 2015
- [30] Helpful Nmap Commands For Pentester or System Admins." *PicaTesHackZ: IT Security | Ethical Hacking | Penetration Testing*. Accessed April 12, 2016. <http://www.picateshackz.com/2016/02/helpful-nmap-commands-for-pentester.html>.
- [31] A Brief History of Computer Networking." *PCR Retail*. Accessed March 16, 2016. <http://www.pcr-online.biz/news/read/a-brief-history-of-computer-networking/037899>.
- [32] Forecast: The Internet of Things, Worldwide, 2013." Accessed March 22, 2016. <https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide->.
- [33] Top 7 Network Attack Types in 2015." Accessed April 12, 2016. <http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/>.

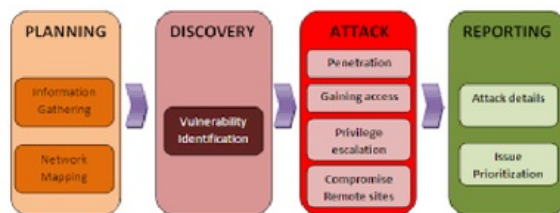
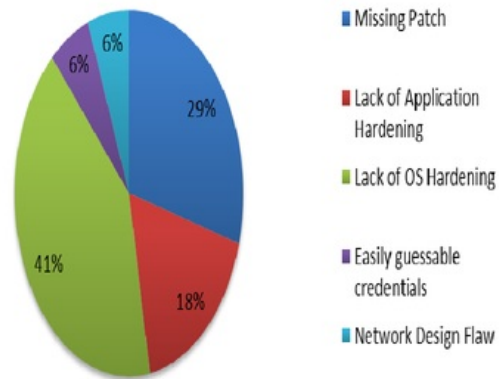
- [34] How to Avoid Attacks That Exploit a Web Browser Vulnerability.” *SearchMidmarketSecurity*. Accessed April 14, 2016. <http://searchmidmarketsecurity.techtarget.com/tip/How-to-avoid-attacks-that-exploit-a-Web-browser-vulnerability>.
- [35] Kali Linux Tutorial: Hack A Web Browser Using BeEF.” *PicaTesHackZ: IT Security | Ethical Hacking | Penetration Testing*. Accessed April 12, 2016. <http://www.picateshackz.com/2015/09/kali-linux-tutorial-hack-web-browser-with-beff.html>.
- [36] News Release | Infoblox.” Accessed March 22, 2016. <http://ir.infoblox.com/phoenix.zhtml?c=251270&p=irol-newsArticle&ID=1943472>.
- [37] Next Big Thing: Preparing for the Internet of Things in the Enterprise | Information Age.” Accessed March 22, 2016. <http://www.information-age.com/technology/mobile-and-networking/123457785/next-big-thing-preparing-internet-things-enterprise>.
- [38] Security - Why Is It Bad to Have Open Ports? - Super User.” Accessed April 11, 2016. <http://superuser.com/questions/82488/why-is-it-bad-to-have-open-ports>.
- [39] The Internet of Things and Its Impact on Enterprise Networks | Information Age.” Accessed March 22, 2016. <http://www.information-age.com/technology/data-centre-and-it-infrastructure/123458408/internet-things-and-its-impact-enterprise-networks>.
- [40] Top 7 Network Attack Types in 2015.” Accessed April 12, 2016. <http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/>.
- [41] What Every Business Must Know about the Internet of Things | Information Age.” Accessed March 22, 2016. <http://www.information-age.com/technology/mobile-and-networking/123458304/what-every-business-must-know-about-internet-things-%E2%80%A8>.
- [42] What Is Brute Force Cracking? - Definition from WhatIs.com.” *SearchSecurity*. Accessed April 12, 2016. <http://searchsecurity.techtarget.com/definition/brute-force-cracking>.
- [43] What Is Configuration Management (CM)? - Definition from WhatIs.com.” *SearchDataCenter*. Accessed March 18, 2016. <http://searchdatacenter.techtarget.com/definition/configuration-management-CM>.
- [44] What Is Network Management System? - Definition from WhatIs.com.” Accessed March 16, 2016. <http://whatis.techtarget.com/definition/network-management-system>.
- [45] Pearson, Alan. “What Is Penetration Testing and Why Is It Important?” Accessed April 14, 2016. <http://www.securityinnovationeurope.com/blog/what-is-penetration-testing-and-why-is-it-important>.
- [] Wireless Network Management.” Accessed March 16, 2016. <https://www.cs.utexas.edu/~lili/projects/wireless-management.htm>.

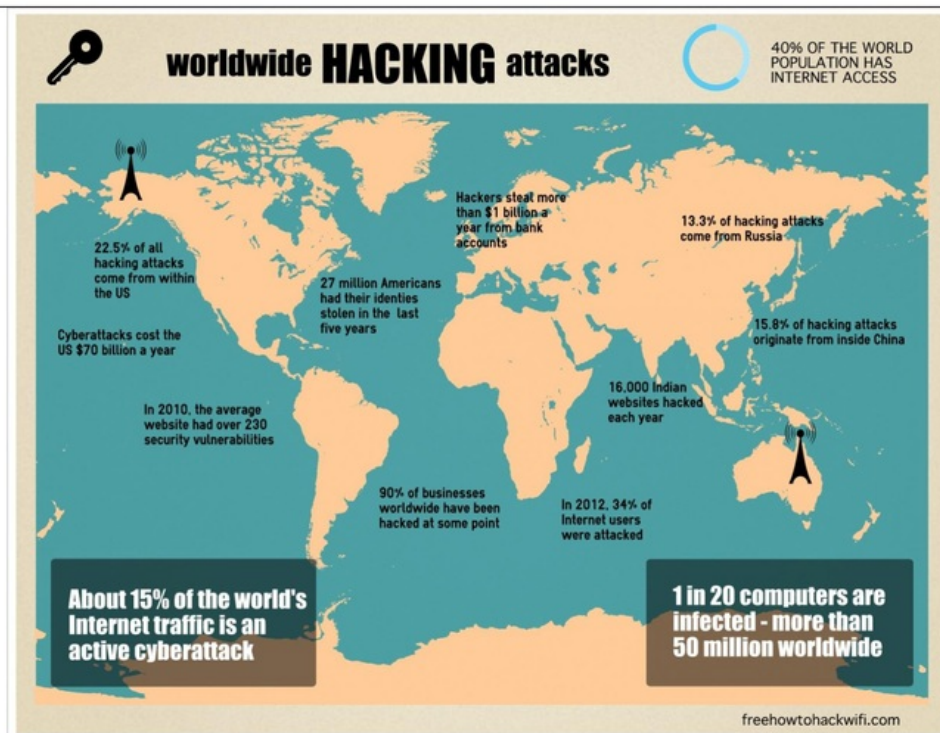
[] ZoneAlarm by Check Point - Award Winning PC Protection, Antivirus, Firewall, Anti-Spyware, Identity Protection, and Much More.” Accessed April 12, 2016.
<http://www.zonealarm.com/security/fr/browser-security/online-threats.htm#>.

CHAPTER 8 APPENDIX



Security Risk Origin/Category





30 HELPFUL NMAP COMMANDS FOR PENTESTER OR SYSTEM ADMIN

Type

Blog Post

URL <http://www.picateshackz.com/2016/02/helpful-nmap-commands-for-pe>

Accessed 12/04/2016 17:20:13

Abstract The purpose of this post is to introduce a user to the nmap command l
vulnerable points in the hosts. You will also learn how to use Nmap for

Blog Title PicaTesHackZ: IT Security | Ethical Hacking | Penetration Testing

Date Added 12/04/2016 17:20:13

Modified 12/04/2016 17:20:13

Attachments

- Snapshot

A BRIEF HISTORY OF COMPUTER NETWORKING

Type Web Page

URL <http://www.pcr-online.biz/news/read/a-brief-history-of-computer-networking>

Accessed 16/03/2016 16:22:15

Abstract We look back on the most important events in networking over the year

Website Title PCR Retail

Date Added 16/03/2016 16:22:15

Modified 16/03/2016 16:22:15

Attachments

- Snapshot

FORECAST: THE INTERNET OF THINGS, WORLDWIDE, 2013

Type Web Page

URL <https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide>

Accessed 22/03/2016 10:57:53

Abstract The Internet of Things will include 26 billion units installed by 2020, with revenue exceeding \$300 billion, mostly in services, in 2020. It will result in diverse end markets.

Short Title Forecast

Date Added 22/03/2016 10:57:53

Modified 22/03/2016 10:57:53

Attachments

- Snapshot

HOW A 'DENIAL OF SERVICE' ATTACK WORKS

HOW TO AVOID ATTACKS THAT EXPLOIT A WEB BROWSER VULNERABILITY

Type Web Page

URL <http://searchmidmarketsecurity.techtarget.com/tip/How-to-avoid-attacks>

Accessed 14/04/2016 11:37:32

Abstract Learn how to stop attacks that exploit a Web browser vulnerability. To host-based intrusion detection systems, use a Web proxy and do not u

Website Title SearchMidmarketSecurity

Date Added 14/04/2016 11:37:32

Modified 14/04/2016 11:37:32

Attachments

- Snapshot

KALI LINUX TUTORIAL: HACK A WEB BROWSER USING BEEF

Type Blog Post

URL <http://www.picateshackz.com/2015/09/kali-linux-tutorial-hack-web-brow>

Accessed 12/04/2016 11:22:32

Abstract BeEF was developed by a group of developers led by Wade Alcorn. B to explore the vulnerabilities in browsers and test them. In particular, B to cross-site scripting (XSS) and other injection attacks.

Blog Title PicaTesHackZ: IT Security | Ethical Hacking | Penetration Testing

Short Title Kali Linux Tutorial

Date Added 12/04/2016 11:22:32

Modified 12/04/2016 11:22:32

Attachments

- Snapshot

NEWS RELEASE | INFOBLOX

Type Web Page

URL <http://ir.infoblox.com/phoenix.zhtml?c=251270&p=irol-newsArticle&ID=1943472>

Accessed 22/03/2016 11:14:57

Date Added 22/03/2016 11:14:57

Modified 22/03/2016 11:14:57

Attachments

- News Release | Infoblox

NEXT BIG THING: PREPARING FOR THE INTERNET OF THINGS IN THE

Type Web Page

URL <http://www.information-age.com/technology/mobile-and-networking/12>

Accessed 22/03/2016 10:57:57

Abstract Smartphones and tablets have rapidly changed the way we live out compared with the potential of the Internet of Things

Short Title Next big thing

Date Added 22/03/2016 10:57:57

Modified 22/03/2016 10:57:57

Attachments

- Snapshot

PROVOS.PDF

Type Attachment

URL https://www.usenix.org/legacy/event/hotbots07/tech/full_papers/provos/provos.p

Accessed 12/04/2016 11:19:27

Date Added 12/04/2016 11:19:27

Modified 12/04/2016 11:19:29

SECURITY - WHY IS IT BAD TO HAVE OPEN PORTS? - SUPER USER

Type Web Page

URL <http://superuser.com/questions/82488/why-is-it-bad-to-have-open-ports>

Accessed 11/04/2016 16:06:32

Short Title security - Why is it bad to have open ports?

Date Added 11/04/2016 16:06:32

Modified 11/04/2016 16:06:32

Attachments

- Snapshot

THE INTERNET OF THINGS AND ITS IMPACT ON ENTERPRISE NETWO

Type Web Page

URL <http://www.information-age.com/technology/data-centre-and-it-infrastru-networks>

Accessed 22/03/2016 10:58:03

Abstract How businesses need to make changes to their infrastructure in orde
Things

Date Added 22/03/2016 10:58:03

Modified 22/03/2016 10:58:03

Attachments

- Snapshot

TOP 7 NETWORK ATTACK TYPES IN 2015

Type Blog Post

URL <http://www.calyptix.com/top-threats/top-7-network-attack-types-in-2015-so-far/>

Accessed 12/04/2016 17:20:23

Date Added 12/04/2016 17:20:23

Modified 12/04/2016 17:20:23

Attachments

- Snapshot

WHAT EVERY BUSINESS MUST KNOW ABOUT THE INTERNET OF THING

Type Web Page

URL <http://www.information-age.com/technology/mobile-and-networking/12%E2%80%A8>

Accessed 22/03/2016 11:40:14

Abstract Every business needs an IoT compliance strategy, even if connected c

Date Added 22/03/2016 11:40:14

Modified 22/03/2016 11:40:14

Attachments

- Snapshot

WHAT IS BRUTE FORCE CRACKING? - DEFINITION FROM WHATIS.CO

Type Web Page

URL <http://searchsecurity.techtarget.com/definition/brute-force-cracking>

Accessed 12/04/2016 10:03:26

Abstract Brute force cracking is method used by application programs to crack (DES) keys, through exhaustive effort (using brute force) rather than e

Website Title SearchSecurity

Short Title What is brute force cracking?

Date Added 12/04/2016 10:03:26

Modified 12/04/2016 10:03:26

Attachments

- Snapshot

WHAT IS CONFIGURATION MANAGEMENT (CM)? - DEFINITION FROM V

Type Web Page

URL <http://searchdatacenter.techtarget.com/definition/configuration-manage>

Accessed 18/03/2016 15:16:20

Abstract Configuration management (CM) is the detailed recording and updating and networks, including all hardware and software components.

Website Title SearchDataCenter

Short Title What is configuration management (CM)?

Date Added 18/03/2016 15:16:20

Modified 18/03/2016 15:16:20

Attachments

- Snapshot

WHAT IS NETWORK MANAGEMENT SYSTEM? - DEFINITION FROM WH

Type Web Page

URL <http://whatis.techtarget.com/definition/network-management-system>

Accessed 16/03/2016 16:22:21

Date Added 16/03/2016 16:22:21

Modified 16/03/2016 16:22:21

Attachments

- What is network management system? - Definition from WhatIs.com

WHAT IS PENETRATION TESTING AND WHY IS IT IMPORTANT?

Type Web Page

Author Alan Pearson

URL <http://www.securityinnovationeurope.com/blog/what-is-penetration-testing->

Accessed 14/04/2016 11:54:51

Abstract Click to learn more about what a penetration test entails, and why they're i

Date Added 14/04/2016 11:54:51

Modified 14/04/2016 11:54:51

Attachments

- Snapshot

WHAT IS PENETRATION TESTING AND WHY IS IT IMPORTANT?

Type Web Page

Author Alan Pearson

URL <http://www.securityinnovationeurope.com/blog/what-is-penetration-testing->

Accessed 14/04/2016 12:27:55

Abstract Click to learn more about what a penetration test entails, and why they're i

Date Added 14/04/2016 12:27:55

Modified 14/04/2016 12:27:55

Attachments

- Snapshot

WIRELESS NETWORK MANAGEMENT

Type Web Page

URL <https://www.cs.utexas.edu/~lili/projects/wireless-management.htm>

Accessed 16/03/2016 16:21:45

Date Added 16/03/2016 16:21:45

Modified 16/03/2016 16:21:45

Attachments

- Wireless Network Management

ZONEALARM BY CHECK POINT - AWARD WINNING PC PROTECTION, PROTECTION, AND MUCH MORE.

Type Web Page

URL <http://www.zonealarm.com/security/fr/browser-security/online-threats.htm#>

Accessed 12/04/2016 17:20:24

Date Added 12/04/2016 17:20:24

Modified 12/04/2016 17:20:24

Attachments

- ZoneAlarm by Check Point - Award winning PC Protection, Antivirus, Firewall, Anti-

Type Web Page

URL <https://www.ietf.org/rfc/rfc2975.txt>

Accessed 18/03/2016 15:32:35

Date Added 18/03/2016 15:32:35

Modified 18/03/2016 15:32:35

Attachments

-

Type Web Page

URL <https://www.ietf.org/rfc/rfc2975.txt>

Accessed 18/03/2016 15:37:06

Date Added 18/03/2016 15:37:06

Modified 18/03/2016 15:37:06

Attachments

-

Type Web Page

URL <http://www.cnet.com/news/how-a-denial-of-service-attack-works/>

Accessed 11/04/2016 15:45:42

Abstract One by one, leading sites on the Web have been brought to their knees by so-called denial of service attacks. This article explains to you how such attacks work and how companies can prevent them.

Website Title CNET

Date Added 11/04/2016 15:45:42

Modified 11/04/2016 15:45:42