ICTNWK511 Manage Network Security

Student Learning Guide

Student name:

Tutor name:

Exceptional Education, Inspiring Educators, Outstanding Experience

PO Box 357, Springwood QLD 4127   Ph: 1800 EVOCCA (386 222)   Email: admin@evocca.com.au

Disclaimer

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without the express written permission of Prime Learning Pty Ltd.

No patent liability is assumed with respect to the information contained herein. While every precaution has been taken in the preparation of this book, the publisher and the author assume no responsibility for the editorial quality of this publication. Neither is any liability assumed for damages resulting from the use of the information contained herein.

These learning materials have been prepared for use as part of a structured vocational education and training course and should only be used within that context.

The information contained herein was correct at the time of preparation. Legislation and case law is subject to change and readers need to inform themselves of the current law at the time of reading.

ICTNWK511 Manage Network Security			Created	09/05/2016
Student Learning Guide				
© Prime Learning Pty Ltd	Version #:	1	Last Modified Date:	09/05/2016

CONTENTS

TABLE OF FIGURES

LEGISLATION

Unit Information

Welcome to the unit ICTNWK511 Manage Network Security.

UNIT DESCRIPTION

This unit describes the skills and knowledge required to implement and manage security functions throughout a network.

It applies to individuals with excellent information and communications technology (ICT) expertise who lead the development of strategic reviews of security and provide technical advice, guidance and leadership in resolution of specified problems.

UNIT OBJECTIVES

1. Define a process for designing security
2. Identify threats to network security
3. Analyse security risks
4. Create a security design
5. Design and implement responses to security incidents

FOUNDATION SKILLS

This section describes language, literacy, numeracy and employment skills incorporated in the performance criteria that are required for competent performance.

Skill	Description
Writing	Uses factual information and industry related terminology to develop organisational plans, security policies and document security breaches
Oral Communication	Uses active listening, observational and questioning techniques in order to identify different perspectives and confirm and clarify understanding
Numeracy	Calculates equipment costs in order to assess their business related value
Get the Work Done	Demonstrates a sophisticated understanding of principles, concepts, language and practices associated with the digital world and uses these to troubleshoot and reduce risks Uses digital tools to access and organise complex data and analyse multiple sources of information for strategic purposes Is acutely aware of the importance of understanding, monitoring and controlling access to digitally stored and transmitted information Uses a combination of formal and logical planning processes and an increasingly intuitive understanding of context to plan control methods for managing system security Makes a range of critical decisions in relatively complex situations, taking a range of constraints into account Recognises and addresses complex problems, including systems processes and rapid deployment of solutions to problems involving failure and security incidents

Source: ICTNWK511 Unit of Competency document located at www.training.gov.au

1. Define a process for designing security

Designing security for a network can be done in a multitude of ways, but there are three main phases that need to be looked at"

- Planning
- Building
- Maintaining

Out of the three phases, planning will be the hardest and most in-depth aspect of designing security for a network. This is because there are multiple layers that form a network, these layers are:

- Router
- HW Firewall
- Switch
- SW Firewall/Anti-Virus/Anti-Malware
- Group Policy Objects
- Critical Data

Each layer is a section of the network that requires a level of security. The primary goal is to ensure that the critical data of an organisation is protected at all costs. When designing security there are two distinct areas, the layers above can be split into hardware (router, firewall, switch) and software (firewall, anti-virus/malware, Group policy objects and critical data). Each area protects a network from various threats, with it leading at the router, or end point of the network. This is where attacks normally enter the system, or it is itself an attack point from attacks such as distributed denial of service attacks. There is a lot of information that is required to secure a network properly and, due to the evolving nature of the internet, if you want to maintain a good skill level in security, you will need to research a lot into security.

1.1 DEFINE PLANNING PHASE FOR NETWORK SECURITY DESIGN

Planning of any sort is critical for any project to be considered successful, in regards to network security even more so. The planning phase refers to the ability to estimate where there are potential breaches in an existing network or where they might exist in a brand new network.

The more effort that is put into planning, the higher the chance that the network will be secure. Though, as with anything technological, the system of protection needs to be maintained and updated on a regular basis.

Planning should cover the following main areas:

- Logical
  - Encryption policy
  - Password policy
  - Email and communications
  - Identity
  - Anti-virus
  - Acceptable use policy

    - Remote access
- Hardware
    - Firewall
    - Intrusion detection systems
    - VPN

There are elements of planning such as education of end users that should also be looked into as they are, without meaning too, an entry point into a network. Social engineering is a method of manipulating employees of an organisation to allow an unknown entity access to a system. For example, if a hacker arrives at the front desk of a large corporation with packages for someone, they will be let through from the public area to the private area of an organisation, then with the simple insertion of a maliciously coded USB key, they could plug a drive into a machine and gain access to an aspect of the network. But, if employees are educated to know that certain behaviours are possible, then unknown people will not be allowed into areas they shouldn't be.

1.2 DEFINE BUILDING PHASE FOR NETWORK SECURITY DESIGN

The building phase can also be referred to as the implementation phase, the specific section of the timeline where the planned out security elements are put into operation. The implementation of the building phase can be broken down into two main sections:

- Physical
- Logical

Physical security of network is based upon the ability to actually access the physical components of a network. This includes, but is not limited to, the server room, patch panels, switches, routers, desktop machines and any mobile device that might be attached to the network. It covers wired and wireless device access. An example of physical security, is a locked door scenario to a server room, the room requires key-card access and even then, each implemented device in the network is locked inside server racks which require key access.

Logical security of a network is the implementation of software solutions to prevent damage to the information that is stored within a network. This is where aspects such as group policy objects, anti-virus, intrusion detection systems and firewalls come into play.

1.3 DEFINE MANAGING PHASE FOR NETWORK SECURITY DESIGN

The managing phase is implemented after the building phase, this particular phase of a project is when monitoring and upgrading of the original design is implemented. Monitoring is when the areas in which the security is implemented, be it logical or physical, are constantly reviewed to determine if there have been attacks made to the system, if the current system handles the attacks and examination of areas that need improving based upon the data collected from any network attacks.

If the attack was physical, then a stronger physical security could be implemented, such as surveillance cameras, stronger locks and bio-metric passwords to name a few items. Logical attacks will leave details in log files, which will allow the areas which need securing to be focused on and improved. This could be aspects of closing of ports using a firewall, implementation of Intrusion detection systems and so forth.

The management phase is critical in any implemented project as this is where the strength of the security plan is monitored and its value determined.

Management phase is where the monitoring of the network takes place, log files are to be examined constantly to determine if the network has had any anomalous traffic or network spikes. This is the phase where software is continuously updated and patched, operating system updates are applied and monitored and research into new ways to ensure a network stays secure.

2. Identify threats to network security

2.1 DETERMINE WHY ATTACKS OCCUR

Network attacks occur due to a multitude of different reasons, below is a list of malicious activities:

- Theft of hardware and software
- Ability to corrupt data and services
- Modification of data
- Stealing data, this data could be for financial gain or industrial espionage
- Utilising resources, such as creating zombie bots

The attacks can occur potentially due to the following reasons:

- Political motivation
- Industrial Espionage
- Criminal activities
- Seeking of Fame
- Greed
- Terrorism
- Racism

It's possible to combine the above lists to determine the type of attacker that exists; for example: The attackers are attacking corporation X to steal specific data to on sell to a rival corporation. This would fall under industrial espionage as well as greed.

A lot of the time, attacks are designed to promote the infamy of the hacker. These hackers with high end skills, if they become white hats instead of black hats, are sometimes hired by government agencies to help test networks for security or to break into elements. For example, there was a case in early 2016 that the USA government needed the help of hackers to break into an iPhone that was evidence from a deceased terrorist, the government apparently paid a substantial amount to make get into the phone.

2.2 DETERMINE WHO THE ATTACK MAY COME FROM

An attacker can be anywhere on the planet. With the internet being as vastly distributed as it is, add in the ability to bounce into and out of various networks and remotely control the resources on other machines, attackers have the capability to be in multiple locations, anywhere. So, how does this help when trying to determine where an attack comes from? When given such a wide and diverse selection of machines to choose from.

The primary way to determine the location of an attacker, or at least the machine(s) is to use the log files on the attacked machines. These log files can be located in various locations depending on the operating system being used. If the machine is a linux machine then the files can be located in the /var/log if it is a windows machine, then the log files will be located in the event viewer.

Depending on how you view the information, it can be displayed in a variety of ways. One such method is looking at the data as a hex dump. A hex dump is a method in which information can be viewed, this information is broken down to hexadecimal and, in some cases, it's ASCII counterpart for reading. Hexadecimal is a way of reading binary in an easier format for humans. Let's examine this new information.

ASCII

ASCII is the American Standard Code for Information Interchange, created in 1960 to enable the exchange of information. ASCII was surpassed as the primary character encoding system in 2007 by UTF-8. ASCII allowed for the conversion of Binary, to Octal to Decimal to Hexadecimal to, what is called Glyph. Glyph is the human readable format of information. Binary is the computer readable format of information with Octal being a base 8 method of representing information, Decimal being base 10 and Hexadecimal as base 16. Each of the base numbers will be discussed in the next section.

The ASCII chart can be broken into sections; these sections are based upon how the information is used. The first 32 numbers of the ASCII chart are the control codes, so 0 to 31 with an additional control occurring at decimal value 127. The control codes refer to elements such as null, end of text, the tab, a backspace, the escape and delete. If you look at your keyboard, you will be able to see keys that fall into control codes. Values 32 to 126 correspond with printable characters, these characters are the alphanumeric and symbols that you see on your keyboard.

Below is the ASCII chart.

ASCII Chart

The coloured table cells are the control codes.

Dec	Hex	Glyph		Dec	Hex	Glyph		Dec	Hex	Glyph
0	00	Null		43	2B	+		86	56	V
1	01	Start of Heading		44	2C	,		87	57	W
2	02	Start of text		45	2D	-		88	58	X
3	03	End of text		46	2E	.		89	59	Y
4	04	End of Transmission		47	2F	/		90	5A	Z
5	05	Enquiry		48	30	0		91	5B	[
6	06	Acknowledgment		49	31	1		92	5C	\

7	07	Bell		50	32	2		93	5D	]
8	08	Backspace		51	33	3		94	5E	^
9	09	Horizontal Tab		52	34	4		95	5F	_
10	0A	Line Feed		53	35	5		96	60	`
11	0B	Vertical Tab		54	36	6		97	61	a
12	0C	Form Feed		55	37	7		98	62	b
13	0D	Carriage Return		56	38	8		99	63	c
14	0E	Shift out		57	39	9		100	64	d
15	0F	Shift in		58	3A	:		101	65	e
16	10	Data Link Escape		59	3B	;		102	66	f
17	11	Device Control 1		60	3C	<		103	67	g
18	12	Device Control 2		61	3D	=		104	68	h
19	13	Device Control 3		62	3E	>		105	69	i
20	14	Device Control 4		63	3F	?		106	6A	j
21	15	Negative Acknowledgement		64	40	@		107	6B	k
22	16	Synchronous Idle		65	41	A		108	6C	l
23	17	End of Transmission Block		66	42	B		109	6D	m
24	18	Cancel		67	43	C		110	6E	n
25	19	End of Medium		68	44	D		111	6F	o
26	1A	Substitute		69	45	E		112	70	p
27	1B	Escape		70	46	F		113	71	q
28	1C	File Separator		71	47	G		114	72	r
29	1D	Group Separator		72	48	H		115	73	s
30	1E	Record Separator		73	49	I		116	74	t
31	1F	Unit Separator		74	4A	J		117	75	u
32	20	(space)		75	4B	K		118	76	v
33	21	!		76	4C	L		119	77	w
34	22	“		77	4D	M		120	78	x
35	23	#		78	4E	N		121	79	y
36	24	$		79	4F	O		122	7A	z
37	25	%		80	50	P		123	7B	{
38	26	&		81	51	Q		124	7V	|

39	27	‘		82	52	R		125	7D	}
40	28	(		83	53	S		126	7E	Delete
41	29	)		84	54	T				
42	2A	*		85	55	U				

Binary and Hexadecimal

Hexadecimal is a base 16 system, this system supplies a way of representing 0-15 to a computer, but it is done as single characters, so the format is 0-9 A-F. Basically, a computer understands information in ones and zeros, on and off. They have been written to understand bursts of information, these bursts are referred to as a byte, which is a single grouping of information that is 8 bits. A bit is either 0 or 1, binary.

Binary values can be calculated quite quickly, when using the following table:

128	64	32	16	8	4	2	1

The table covers the ranges of 0-255, this range of numbers can be demonstrated in 8 bits, and is referred to as a byte. From here the byte range goes into kilobytes, megabytes, gigabytes, terabytes and so forth.

Using this table converting a number to binary is just a case of applying a 1 into a value that is smaller than the total. For example, if I wanted to convert the number 54 into binary, you would break it down like this:

128 doesn’t go into 54, therefore it’s a 0

64 doesn’t go into 54, therefore it’s a 0

32 does go into 54, therefore it is a 1. From here, we are left with 54-32, or 22 as we still have a number, we continue on.

16 goes into 22, therefore it’s a 1. Calculate the remainder; 22 – 16 = 6

8 doesn’t go into 6, therefore it’s a 0

4 does go into 6, therefore it’s a 1. Calculate the remainder; 6-4=2

2 does go into 2, therefore it’s a 1. There is no remainder, but 2-2=0

1 doesn’t go into 0, therefore it’s a 0.

To show this in the table:

128	64	32	16	8	4	2	1
0	0	1	1	0	1	1	0

So, 54 is represented in binary as: 0011 0110

As computers speak in binary, base 2, it means that if viewing a string of binary it would be a lot harder to display the information in human readable format. Each 4 number group of binary can relate to a single letter in Hex. Let's take for example a name;

Human format: Bill

Binary Format:

- B: 0100 0010
- i: 0110 1001
- l: 0110 1100
- l: 0110 1100

So Bill, to a computer is 0100 0010 0110 1001 011 1100 0110 1100. To make this more readable for a human, though still simple for a computer it can be written in hex format:

- B: 42
- i: 69
- l: 6C
- l: 6C

Bill in Hex is 42 69 6C 6C.

If you examine the binary code and the hex code, you should see the correlation between the first 4 bits and the first part of the hex code. So, if you take the first letter B, you can break the octet into 2 sets of 4, 0100 and 0010. Performing simple maths on them you can see that 0100 can be converted to the base 10 number 4 and 0010 can be converted into the base 10 number 2. Viewing a computer that is displaying 42 instead of 0100 0010 is a lot easier for a human to read and faster to compare against the ASCII table.

Activity:

Convert the following numbers to binary:

84,111,111,32

101,97,115,121

	128	64	32	16	8	4	2	1
84	0	1	0	1	0	1	0	0
111								

111								
32								
101								
97								
115								
121								

Then convert the binary to hexadecimal

Such as: 0101 0100 = 54

Binary (split into 2 sets of 4)		**Match each set of 4 to a column**		**Final Hex Value**
0101	**0100**	**5**	**4**	**54**

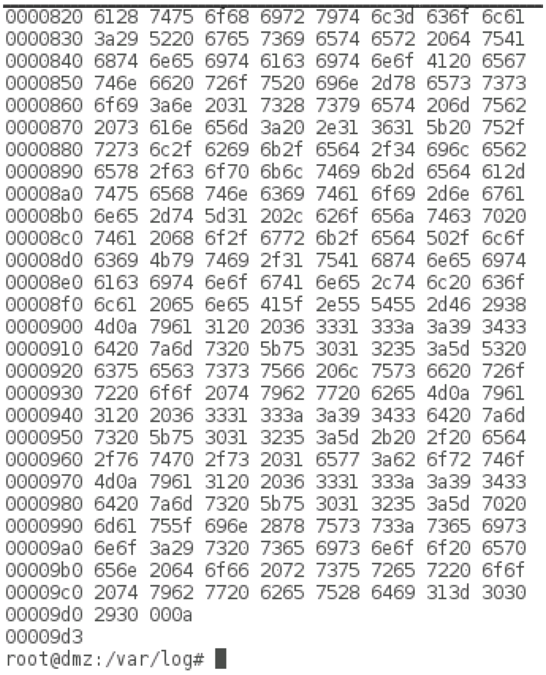
Once you have done this, correlate the Hex code to its relating Glyph off the ASCII chart:

Hex	**Glyph**
54	**T**

Hexdump

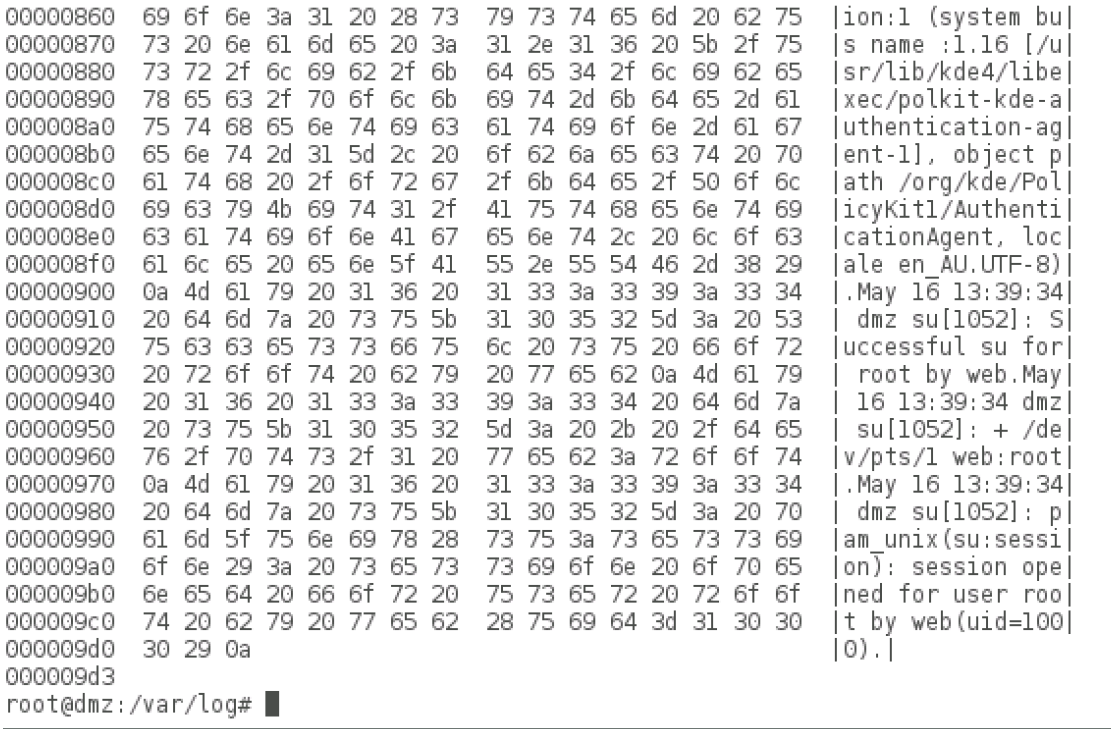
A hexdump is where a file has been viewed in its hex format, this can be done for a variety of reasons, one of them being able to locate where a section of code is that needs to be manipulated for a specific reason through use of a hex editor or if a file has been saved with no extension, it’s possible to view the header aspect of the file to determine what the file type is.

Here is an example of a hexdump



```
0000820 6128 7475 6f68 6972 7974 6c3d 636f 6c61
0000830 3a29 5220 6765 7369 6574 6572 2064 7541
0000840 6874 6e65 6974 6163 6974 6e6f 4120 6567
0000850 746e 6620 726f 7520 696e 2d78 6573 7373
0000860 6f69 3a6e 2031 7328 7379 6574 206d 7562
0000870 2073 616e 656d 3a20 2e31 3631 5b20 752f
0000880 7273 6c2f 6269 6b2f 6564 2f34 696c 6562
0000890 6578 2f63 6f70 6b6c 7469 6b2d 6564 612d
00008a0 7475 6568 746e 6369 7461 6f69 2d6e 6761
00008b0 6e65 2d74 5d31 202c 626f 656a 7463 7020
00008c0 7461 2068 6f2f 6772 6b2f 6564 502f 6c6f
00008d0 6369 4b79 7469 2f31 7541 6874 6e65 6974
00008e0 6163 6974 6e6f 6741 6e65 2c74 6c20 636f
00008f0 6c61 2065 6e65 415f 2e55 5455 2d46 2938
0000900 4d0a 7961 3120 2036 3331 333a 3a39 3433
0000910 6420 7a6d 7320 5b75 3031 3235 3a5d 5320
0000920 6375 6563 7373 7566 206c 7573 6620 726f
0000930 7220 6f6f 2074 7962 7720 6265 4d0a 7961
0000940 3120 2036 3331 333a 3a39 3433 6420 7a6d
0000950 7320 5b75 3031 3235 3a5d 2b20 2f20 6564
0000960 2f76 7470 2f73 2031 6577 3a62 6f72 746f
0000970 4d0a 7961 3120 2036 3331 333a 3a39 3433
0000980 6420 7a6d 7320 5b75 3031 3235 3a5d 7020
0000990 6d61 755f 696e 2878 7573 733a 7365 6973
00009a0 6e6f 3a29 7320 7365 6973 6e6f 6f20 6570
00009b0 656e 2064 6f66 2072 7375 7265 7220 6f6f
00009c0 2074 7962 7720 6265 7528 6469 313d 3030
00009d0 2930 000a
00009d3
root@dmz:/var/log# █
```

As you can see, there is a lot of information, but nothing that is extremely useful at first glance. Using the above methods, you could break the hex into its various glyphs to attempt to read what the data is. The above dump was done using the hexdump command on a Debian machine. Supplying the –C attribute to the command, so it is hexdump –C <filename> The output now looks like:

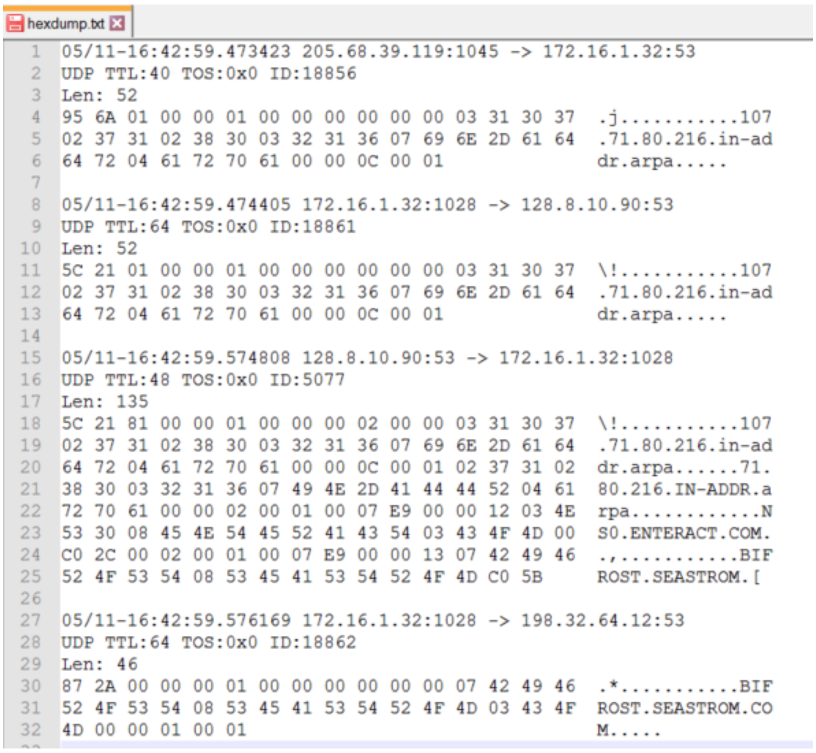


```
00000860  69 6f 6e 3a 31 20 28 73  79 73 74 65 6d 20 62 75  |ion:1 (system bu|
00000870  73 20 6e 61 6d 65 20 3a  31 2e 31 36 20 5b 2f 75  |s name :1.16 [/u|
00000880  73 72 2f 6c 69 62 2f 6b  64 65 34 2f 6c 69 62 65  |sr/lib/kde4/libe|
00000890  78 65 63 2f 70 6f 6c 6b  69 74 2d 6b 64 65 2d 61  |xec/polkit-kde-a|
000008a0  75 74 68 65 6e 74 69 63  61 74 69 6f 6e 2d 61 67  |uthentication-ag|
000008b0  65 6e 74 2d 31 5d 2c 20  6f 62 6a 65 63 74 20 70  |ent-1], object p|
000008c0  61 74 68 20 2f 6f 72 67  2f 6b 64 65 2f 50 6f 6c  |ath /org/kde/Pol|
000008d0  69 63 79 4b 69 74 31 2f  41 75 74 68 65 6e 74 69  |icyKit1/Authenti|
000008e0  63 61 74 69 6f 6e 41 67  65 6e 74 2c 20 6c 6f 63  |cationAgent, loc|
000008f0  61 6c 65 20 65 6e 5f 41  55 2e 55 54 46 2d 38 29  |ale en_AU.UTF-8)|
00000900  0a 4d 61 79 20 31 36 20  31 33 3a 33 39 3a 33 34  |.May 16 13:39:34|
00000910  20 64 6d 7a 20 73 75 5b  31 30 35 32 5d 3a 20 53  | dmz su[1052]: S|
00000920  75 63 63 65 73 73 66 75  6c 20 73 75 20 66 6f 72  |uccessful su for|
00000930  20 72 6f 6f 74 20 62 79  20 77 65 62 0a 4d 61 79  | root by web.May|
00000940  20 31 36 20 31 33 3a 33  39 3a 33 34 20 64 6d 7a  | 16 13:39:34 dmz|
00000950  20 73 75 5b 31 30 35 32  5d 3a 20 2b 20 2f 64 65  | su[1052]: + /de|
00000960  76 2f 70 74 73 2f 31 20  77 65 62 3a 72 6f 6f 74  |v/pts/1 web:root|
00000970  0a 4d 61 79 20 31 36 20  31 33 3a 33 39 3a 33 34  |.May 16 13:39:34|
00000980  20 64 6d 7a 20 73 75 5b  31 30 35 32 5d 3a 20 70  | dmz su[1052]: p|
00000990  61 6d 5f 75 6e 69 78 28  73 75 3a 73 65 73 73 69  |am_unix(su:sessi|
000009a0  6f 6e 29 3a 20 73 65 73  73 69 6f 6e 20 6f 70 65  |on): session ope|
000009b0  6e 65 64 20 66 6f 72 20  75 73 65 72 20 72 6f 6f  |ned for user roo|
000009c0  74 20 62 79 20 77 65 62  28 75 69 64 3d 31 30 30  |t by web(uid=100|
000009d0  30 29 0a                                          |0).|
000009d3
root@dmz:/var/log# █
```

If we do a quick comparison, the first set of numbers 69 6f 6e when the hex is compared to the ASCII chart, they do translate into ion. Which, thanks to the –C attribute has already occurred, this in turn makes it far easier to read through specific elements.

Tracking an External entry to a network

Knowing that a computer works in this format and that it is viewable makes it possible to examine certain file to trace activity. If there is a need to trace activity, then the object is to look for something that is out of place, if someone is entering your network, then there will be an IP address that will be indicative of this entry, let's look at the following hexdump.



```
05/11-16:42:59.473423 205.68.39.119:1045 -> 172.16.1.32:53
UDP TTL:40 TOS:0x0 ID:18856
Len: 52
95 6A 01 00 00 01 00 00 00 00 00 00 03 31 30 37  .j...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

05/11-16:42:59.474405 172.16.1.32:1028 -> 128.8.10.90:53
UDP TTL:64 TOS:0x0 ID:18861
Len: 52
5C 21 01 00 00 01 00 00 00 00 00 00 03 31 30 37  \!...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01              dr.arpa.....

05/11-16:42:59.574808 128.8.10.90:53 -> 172.16.1.32:1028
UDP TTL:48 TOS:0x0 ID:5077
Len: 135
5C 21 81 00 00 01 00 00 00 02 00 00 03 31 30 37  \!...........107
02 37 31 02 38 30 03 32 31 36 07 69 6E 2D 61 64  .71.80.216.in-ad
64 72 04 61 72 70 61 00 00 0C 00 01 02 37 31 02  dr.arpa......71.
38 30 03 32 31 36 07 49 4E 2D 41 44 44 52 04 61  80.216.IN-ADDR.a
72 70 61 00 00 02 00 01 00 07 E9 00 00 12 03 4E  rpa............N
53 30 08 45 4E 54 45 52 41 43 54 03 43 4F 4D 00  S0.ENTERACT.COM.
C0 2C 00 02 00 01 00 07 E9 00 00 13 07 42 49 46  .,...........BIF
52 4F 53 54 08 53 45 41 53 54 52 4F 4D C0 5B     ROST.SEASTROM.[

05/11-16:42:59.576169 172.16.1.32:1028 -> 198.32.64.12:53
UDP TTL:64 TOS:0x0 ID:18862
Len: 46
87 2A 00 00 00 01 00 00 00 00 00 00 07 42 49 46  .*...........BIF
52 4F 53 54 08 53 45 41 53 54 52 4F 4D 03 43 4F  ROST.SEASTROM.CO
4D 00 00 01 00 01                                M.....
```

Figure 1 Hexdump

Figure 1 Hexdump shows that there is a lot of things occurring, in this instance, this screen shot is of a red hat 6.0 system, that was hacked into and a recursive DNS probe was implemented, this recursive DNS enabled the system to do a buffer overrun which then allowed the hacker to generate elevated accounts into the network.

Using the hexdump, you can tell that the internal network is running on the private IP range of 172.16.x.x, if we run through the hexdump, you'll see the following external IP numbers:

- 205.68.38.119
- 128.8.10.90
- 198.32.64.12

With 3 external IP addresses present, what needs to be done is to see which IPs were used to enter the system. So, now we work through each line of the hexdump to determine what is going on. The first line showing 205.68.38.119:1045 -> 172.16.1.32:53 has logged that the external IP entered the system using port 1045, port 1045 is the fpitp port, otherwise known as the fingerprint image transfer protocol. And hit the internal system through the DNS port, 53. This is a good indication of the entry IP of the attacker, but we'll check the other ones just to be sure.

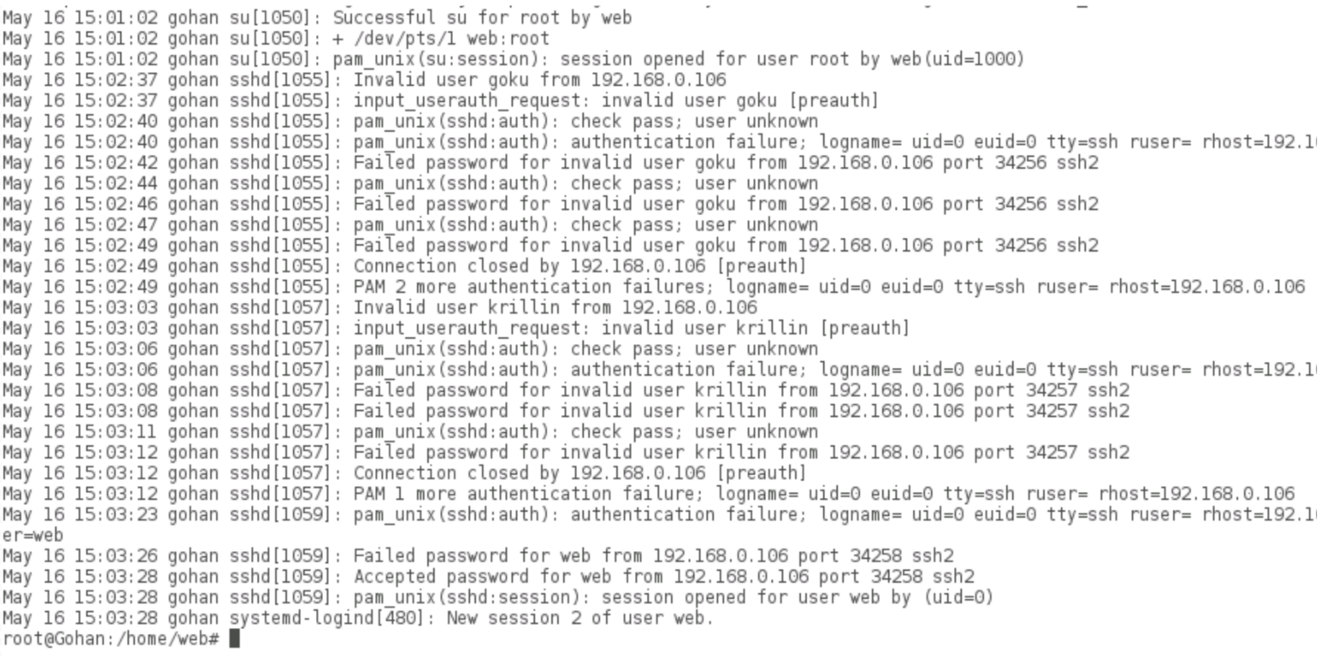
Reading down through the hexdump, the machine 172 initiates a connection to the 128.8 machine; so our local machine has now connected to an external machine. The next incoming IP is the 128.8 machine coming back into the internal machine. From which an outgoing connection is once again made from 172 to 198.

So, the attacker entered the network from the 205 range, and then instigated a recursive DNS attack from the internal machine out and back in again. As such, we now know where the attacker came from and can blacklist the IP as needed.

Tracking Internal traffic

Tracking internal traffic isn't as simple as looking for an external IP address connecting to a machine that it should have access to, though it still falls under the same situation of need to be able to view log files and determine an instance where the traffic that is being generated is inconsistent with normal machine traffic.

In this case, on a Debian system, looking at the auth.log file stored in /var/log is a good way to start. For example, let's look at Figure 2 Auth.log Dump.



```
May 16 15:01:02 gohan su[1050]: Successful su for root by web
May 16 15:01:02 gohan su[1050]: + /dev/pts/1 web:root
May 16 15:01:02 gohan su[1050]: pam_unix(su:session): session opened for user root by web(uid=1000)
May 16 15:02:37 gohan sshd[1055]: Invalid user goku from 192.168.0.106
May 16 15:02:37 gohan sshd[1055]: input_userauth_request: invalid user goku [preauth]
May 16 15:02:40 gohan sshd[1055]: pam_unix(sshd:auth): check pass; user unknown
May 16 15:02:40 gohan sshd[1055]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.1
May 16 15:02:42 gohan sshd[1055]: Failed password for invalid user goku from 192.168.0.106 port 34256 ssh2
May 16 15:02:44 gohan sshd[1055]: pam_unix(sshd:auth): check pass; user unknown
May 16 15:02:46 gohan sshd[1055]: Failed password for invalid user goku from 192.168.0.106 port 34256 ssh2
May 16 15:02:47 gohan sshd[1055]: pam_unix(sshd:auth): check pass; user unknown
May 16 15:02:49 gohan sshd[1055]: Failed password for invalid user goku from 192.168.0.106 port 34256 ssh2
May 16 15:02:49 gohan sshd[1055]: Connection closed by 192.168.0.106 [preauth]
May 16 15:02:49 gohan sshd[1055]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.0.106
May 16 15:03:03 gohan sshd[1057]: Invalid user krillin from 192.168.0.106
May 16 15:03:03 gohan sshd[1057]: input_userauth_request: invalid user krillin [preauth]
May 16 15:03:06 gohan sshd[1057]: pam_unix(sshd:auth): check pass; user unknown
May 16 15:03:06 gohan sshd[1057]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.1
May 16 15:03:08 gohan sshd[1057]: Failed password for invalid user krillin from 192.168.0.106 port 34257 ssh2
May 16 15:03:08 gohan sshd[1057]: Failed password for invalid user krillin from 192.168.0.106 port 34257 ssh2
May 16 15:03:11 gohan sshd[1057]: pam_unix(sshd:auth): check pass; user unknown
May 16 15:03:12 gohan sshd[1057]: Failed password for invalid user krillin from 192.168.0.106 port 34257 ssh2
May 16 15:03:12 gohan sshd[1057]: Connection closed by 192.168.0.106 [preauth]
May 16 15:03:12 gohan sshd[1057]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.168.0.106
May 16 15:03:23 gohan sshd[1059]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=192.1
er=web
May 16 15:03:26 gohan sshd[1059]: Failed password for web from 192.168.0.106 port 34258 ssh2
May 16 15:03:28 gohan sshd[1059]: Accepted password for web from 192.168.0.106 port 34258 ssh2
May 16 15:03:28 gohan sshd[1059]: pam_unix(sshd:session): session opened for user web by (uid=0)
May 16 15:03:28 gohan systemd-logind[480]: New session 2 of user web.
root@Gohan:/home/web# █
```

Figure 2 Auth.log Dump

Figure 2 Auth.log Dump is the auth.log file of a machine called Gohan, if you examine the above image, you can see that there were attempts to connect to this machine using the accounts krillin and goku. Now, if the machine was normally one that was connected to that wouldn't raise much of a concern, as this is quite possible behaviour of users forgetting their password. The part that does raise concern, is that the attempts where from the same IP address, 192.168.0.106 and was then closely followed by a successful connection by the user web. In which the user web now had two sessions opened as can be seen in the last line.

So, the points of concern are:

- Multiple attempts at login
- All attempts from the same IP
- A second session created for the web user

As an administrator, you would then access the 192.168.0.106 machine and start to work through that machines log files. This will enable identification of the user that is logged in to the machine and also assist in the discovery of if the machine was accessed from an external entity.

So, when tracking an internal IP, you would always work backwards from the machine that was first seen as attacked until you are either on a machine that was attacked by an external entity or one that has no more connections to it.

If you have a diagram of the network, it will assist in discovering the path, if you like machines up via the log file path.

So, let’s link the Internal and external machines, that we have been discussing to see the network. We will swap the 172.16.1.32 IP to 192.168.0.106. In this manner, the network would look like the following Figure 3 Trace Network.

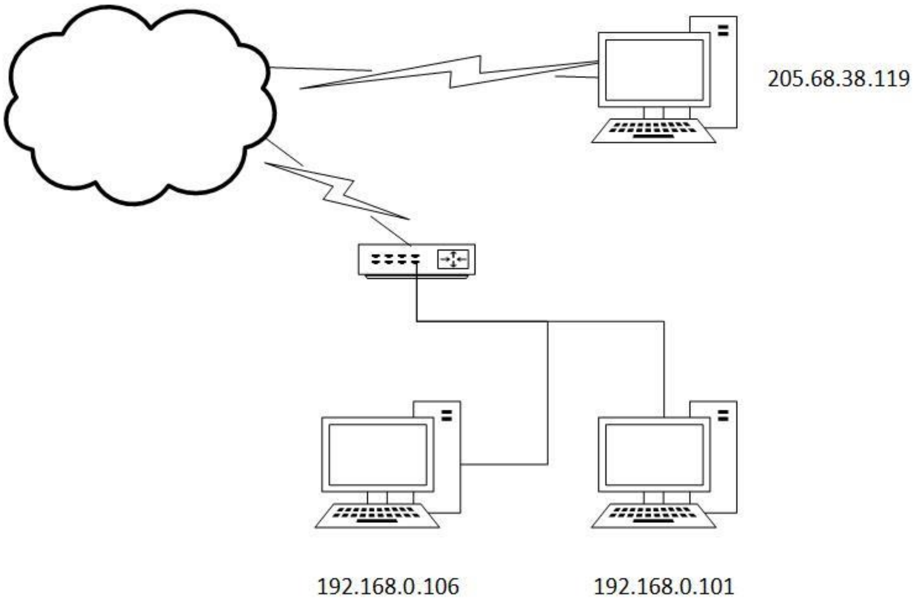


Figure 3 Trace Network

Now, if we trace the log files, we get to map the attack like this Figure 4 Attack Path.

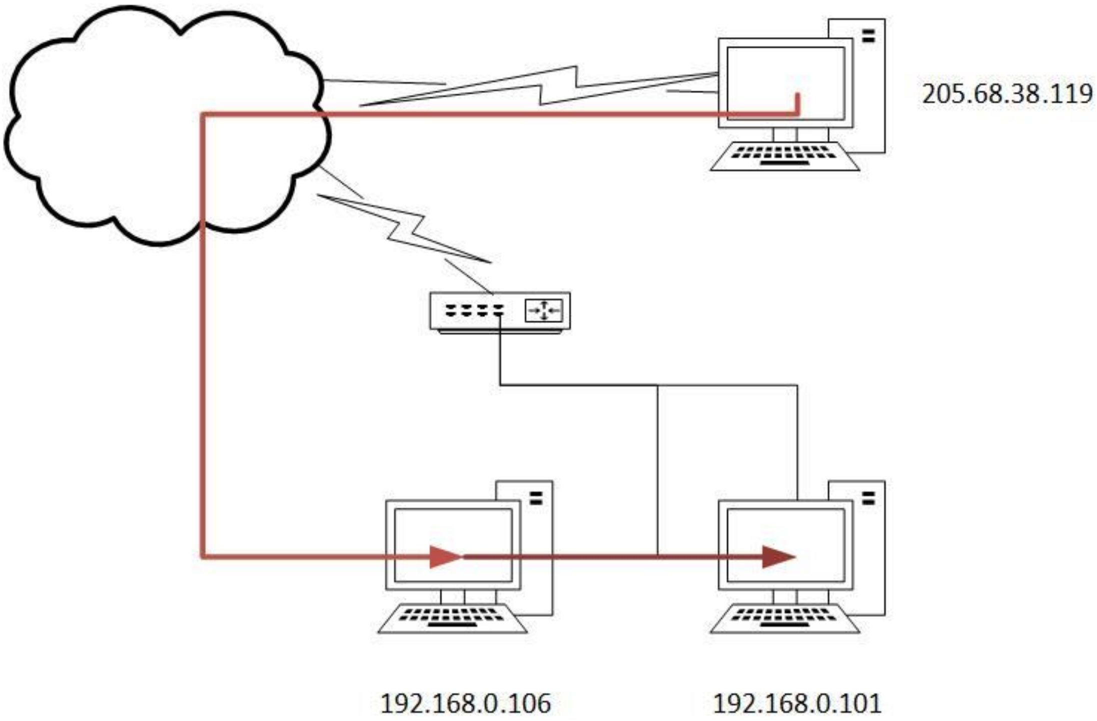


Figure 4 Attack Path

When you see an attack vector coming in like this, you can see why the need for logging incoming traffic is very important in network security. And the ability to backtrack through log files to determine the entry vector on a network is just as important.

2.3 ANALYSE COMMON TYPES OF NETWORK VULNERABILITIES

In a network, no matter how well planned out, there is bound to be some security areas that have been missed. These areas are sections of the network that can be located in both physical and logical situations.

Here is a list of potential vulnerabilities:

- Logical
    - Email: Ability to get malicious code inside the system where an authenticated user can run the code.
    - Websites: Ability to allow authenticated users to infect previously secured systems
    - Weak passwords: Easily guessed passwords, can allow for an authenticated user to login
    - Missing patches on Servers: This is where security patches are not applied to publicly discovered flaws and a hacker can locate the entry point to the network.
    - Misconfigured firewalls: Opened holes in the firewall to allow attacks access to the system
    - DOS/DDOS: Denial of Service/Distributed DOS, this is where a network’s access to the net is removed, due to it being overwhelmed

by constant machine requests and hence using all of a particular resource.

- Physical
    - USB drives: portable device that can contain malicious code
    - Laptops: Mobile devices, that have the ability to run a full suite of attack software to break or enter a network.
    - USB Devices: Like a USB drive, a USB device can have internal memory that could be used to store malicious code
    - Social Engineering: Employees being fooled to supply access, very similar to internal connections.
    - Internal connections: Employees can grant access to non-secured people who are dressed to look the part.
    - Mobile devices: can be used to locate access points such as wireless access points, and run specific software designed to damage a network.
    - Wireless Access points: Easily discovered access to a network, to enable additional attacks

As one would expect, when dealing with differing areas of security, there will be differing ways in which that security vulnerability can be addressed.

Logical vulnerabilities can be addressed by doing the following set of actions:

- Always updating security patches; these patches can be for operating systems, routers, switches and applications.
- Misconfiguration of systems can be limited by ensuring that the staff that deal with the devices are trained and attend conferences to maintain currency.
- Network security elements like DDOS, are a little trickier to deal with when compared to virus's and malware, as this can involve introducing high end hardware and manipulation of records to resolve. But, it is not a normal occurrence for a small to medium sized business. Though, this still resolves education on the technical end for the client.
- Virus's and malware fall under the capability of ensuring that all software applications are updated and users are educated in methods of how machines can be infected.

Physical vulnerabilities can be addressed by looking at the following set of actions:

- Education of end users, this is potentially the hardest part to achieve, as a normal user will always think "it'll never happen to me" and, unfortunately, until it does, they don't always want to learn or change what they know. Education of users covers the following areas:

    - Social Engineering: Recognising and handling social engineering. Identifying of individuals and their behaviour to determine the validity of the individual.
    - Device management: Use of external items such as USB keys or USB devices, that may have been used in differing machines.
    -

- Internal connections; in this manner the levels of security that employees have should be monitored and controlled. This also means logging activity and determining if there is any malicious activity.
- Wireless access points: The security of these devices should be maintained and logged as they are an entry point into the network, which doesn't require a physical connection, so to speak.
- Mobile devices: Machines that log in, or attempt to log in to the network should be monitored for malicious activity.

2.4 DETERMINE HOW ATTACKS OCCUR

One of the best ways to determine how to prevent access to a network, is to think like an attacker and determine entry vectors in the network. Based off the following list of items we'll examine a couple of potential attack vectors.

- Logical
  - Email: Ability to get malicious code inside the system where an authenticated user can run the code.
  - Websites: Ability to allow authenticated users to infect previously secured systems
  - Weak passwords: Easily guessed passwords, can allow for an authenticated user to login
  - Missing patches on Servers: This is where security patches are not applied to publicly discovered flaws and a hacker can locate the entry point to the network.
  - Misconfigured firewalls: Opened holes in the firewall to allow attacks access to the system
  - DOS/DDOS: Denial of Service/Distributed DOS, this is where a network's access to the net is removed, due to it being overwhelmed by constant machine requests and hence using all of a particular resource.

- Physical
  - USB drives: portable device that can contain malicious code
  - Laptops: Mobile devices, that have the ability to run a full suite of attack software to break or enter a network.
  - USB Devices: Like a USB drive, a USB device can have internal memory that could be used to store malicious code

- Social Engineering: Employees being fooled to supply access, very similar to internal connections.
- Internal connections: Employees can grant access to non-secured people who are dressed to look the part.
- Mobile devices: can be used to locate access points such as wireless access points, and run specific software designed to damage a network.
- Wireless Access points: Easily discovered access to a network, to enable additional attacks

Using the above list of common vulnerabilities, we'll determine a couple of attack vectors on the following network Figure 5 General Network.

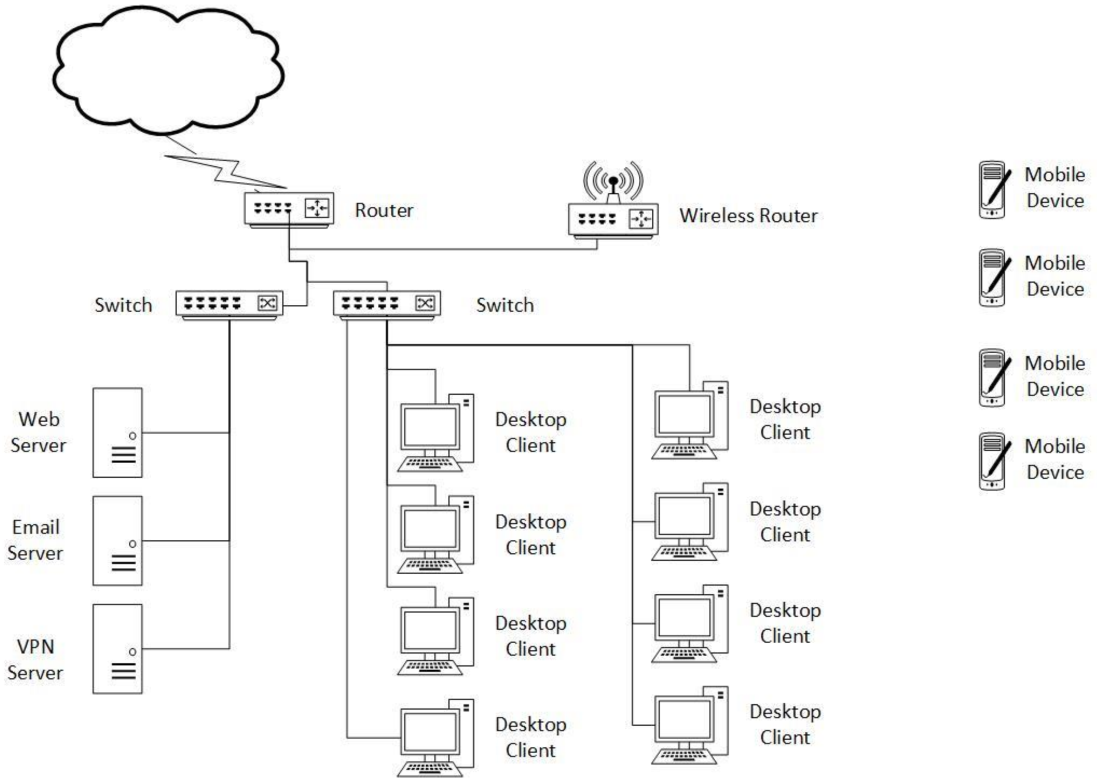


Figure 5 General Network

Examining the above Figure 5 General Network, there are quite a few sections of the network that would be open to potential attack. In fact, like the real world, attacks are based upon a combination of physical and logical strategies to get into a network.

Attack Vector 1: An attack from a mobile device is both physical and logical, the mobile could be used to test the security of the wireless router. And once the security on that has been broken, the hacker could do pretty much do anything they wanted to.

Attack Vector 2: The VPN server is designed to handle incoming requests, as both web and email servers are. If the VPN server is hit with a DDOS, then any remote users for the network would be locked out. As the network is hosting email and web off the same internet connection, then a DDOS has the ability to take down those servers as well.

To assist with determining the attack vector, determine the motive of the hacker.

2.5 DESIGN A THREAT MODEL TO CATEGORISE THREATS

Threat modelling is way of identifying vulnerabilities in a computer network and then outlining measures that can be used to prevent or negate the threats.

The use of threat modelling allows for the network to be examined into differing levels of security and have these specific areas addressed, or at the very least acknowledged as a potential issue.

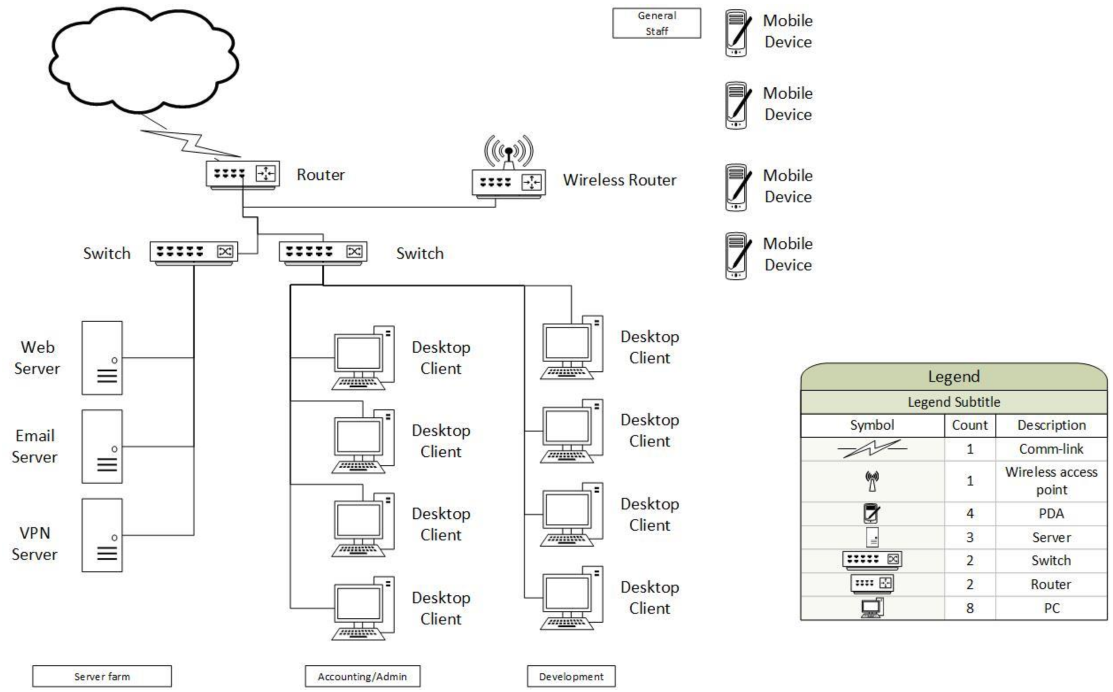
In general, a threat model consists of differing stages.

Threat model stages:

- Identify and document assets
  - This section of the document is where you would locate all assets that consist of the network and document what each item is used for. On a live network you would list hardware and software specifications as well as including the role of the asset;

  - For example, you could indicate there was a server, it's primary role is web development, connected internally, external access not allowed, the following Groups in Active Directory have access to it: Administrators, Web Developers; System; Test Viewers.
- Create an overview of the network
  - In documentation on a threat model, an image linking all of the gathered assets would be viable here. There would be a legend on the image stating what area certain assets are.

- For example,



Legend

Legend Subtitle

Symbol	Count	Description
⚡	1	Comm-link
📶	1	Wireless access point
📱	4	PDA
▯	3	Server
▭	2	Switch
▭	2	Router
🖥	8	PC

Figure 6 Network Legend

- In addition, you would write up roles for each section discussed.

- Identify and document attack vectors
  - In this part of the threat model, you would examine the potential areas of the network in which an attack can come from. So, using the above image, there are attack vectors of:
    - Internet
    - Wireless Router
    - Physical access
- Identify threats
  - With the attack vectors assumed, you can narrow down the potential list of threats that can occur within a certain network. Continuing on with the example network, we'll select one attack vector and identify the threats for it.

  - For Example; Wireless Router. Threats are internet based, primary threat is the ability to broadcast its existence as a network and enable connections. Once connections are established, the connected user has access to the network.

  - There are more, but we'll go with one threat at the moment.
- Document and categorise threats
  - This section of the threat model is categorising the threats that you have identified for the network. This also allows you to determine threat levels for specific threats.

  - For Example; if you have identified the following threats:
    - Virus's
    - Malware

        - DDOS (Distributed Denial of Service)
        - USB Infection
    - You could break them into threat categories
        - High Threat: DDOS
        - Medium Threat: Virus, Malware
        - Low Threat: USB Infection
    - This categorisation allows for an easy way to understand the severity to the company due to the security threat that has occurred.
- Document potential solutions
    - Based on the threats that have been identified, a potential solution can be written up and discussed for each element.

    - For Example; Based off a virus threat, you would write up the following solutions
        - The machine that is infected gets removed from the network
        - The network is scanned
        - All anti-virus software is updated and system re-scanned
        - The infected machine is examined, log files to determine entry vector of virus
        - Machine gets cleaned
        - Machine returned to network
        - Education of end user
- Monitor security
    - This is where the implemented systems are watched to see if there are any resulting attacks.
    - Monitoring Network logs, local machine logs and network logs
- Re-evaluate security
    - Set an end time frame for the current threat model, just to ensure that the content will be kept current with how fast technology changes.

3. Analyse security risks

Analysing security risks is part of the ongoing monitoring and maintenance phase of network security. Though, with time spent during the planning phase to identify potential risks of the network, the implemented network might natively mitigate some risks. For example, implementing a distributed anti-virus system will enable a network to push updates and remotely scan all machines on the network.

There are several steps to determining the risks for a network, as such below are the list of steps.

Risk Analysis steps:

- Identify the scope of the analysis
- Survey and gather the data
- Identify and document threats and vulnerabilities
- Assess current security measures
- Categorise likelihood of threats
- Determine level and impact of threat
- Identify security measures

3.1 DETERMINE ELEMENTS OF RISK MANAGEMENT

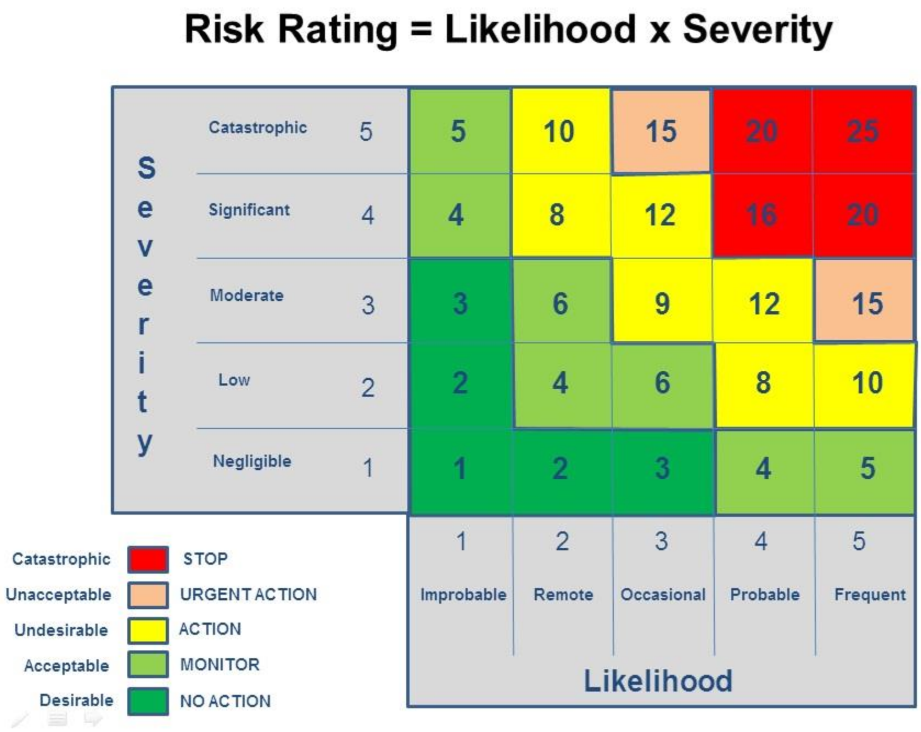
Determining the elements of risk management involves understanding the scenario that the client is in. In general, there will be certain areas in which risks will apply to all scenarios, but most situations will involve their own quirks and as such when determining risks for a client, look at the details that make the client unique.

Some areas in which risk should be looked at

- Router configuration
- Switch configuration
- Server configuration
- Internal access to the machines
- Social engineering
- Viruses, worms, and Trojan horses
- Denial of service attack tools
- Packet replaying and modification
- IP spoofing
- Password cracking

When calculating risks, you can use a risk matrix and legend to assist with determining the status of each risk.

Risk Matrix



Risk Rating = Likelihood x Severity

Severity						
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5
		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
		Likelihood				

Catastrophic	🟥	STOP
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

Risk Legend

Rating	Description
Desirable (1-3)	Impact can be easily absorbed without requiring management effort
Acceptable (4-7)	Impact can be readily absorbed but some management effort is required
Undesirable (8-12)	Impact cannot be managed under normal operating conditions; requiring moderate level of resource and management input
Unacceptable (13-15)	Impact requires a high level of management attention / effort and resources to rectify
Catastrophic (16-25)	Disaster with potential to lead to business collapse and requiring almost total management attention / effort to rectify

When combining the matrix and legend, it is possible to determining the level of impact based off the risk rating. To use the above combination of charts you determine risks by matching likelihood of an incident to the severity and then cross referencing the final number into the legend. The way this is done is that you determine the likelihood and severity, then multiple the numbers to determine the overall rating.

For example, if a client has a desktop machine fail and require replacement. Assuming this was a normal machine with no specific tasks, using the chart you would rate it like this:

Desktop Failure

- Likelihood: Low 2
- Severity: Occasional 3
- Rating: 6, this gives an Acceptable risk

This would be performed on the main elements that are considered at risk in a network.

3.2 DETERMINE ASSETS THAT REQUIRE PROTECTION

The easiest way to determine the primary assets that require protection is to determine the core function of the business. The information that the network supplies for the business, be it raw customer data, sales figures or even repair data for cars; this information is what keeps the business running, and as such needs to be protected.

Let's examine a few scenarios:

Scenario 1: Your client is a car yard, they store all mechanical information in regards to repairs of specific brands on a local server, they run a file share server, an email server and a user server. They have 25 client machines, which link up to the servers to share information, they run specific applications that store client information. This database is stored on the file server. They have a single internet point. They run a wireless system to enable mobile devices to connect to, for themselves and for clients coming in. Access to the wireless is anonymous.

If we work through this scenario, there are multiple locations in which aspects of the network can be attacked, but their primary items that need protection are the servers and the data that they hold. If they are unable to access this mechanical data, then they will be unable to repair vehicles, which is what the company runs on. So, in general, the servers would need significant backups that are tested for integrity, a secondary solution for accessing the information if the primary server goes down. This could be as simple as having the software installed on one of the other servers, but not active, with data being kept up to date on a regular schedule. So if need be, the client machines could be switched over.

Scenario 2: This client is a new accounting business, they have 3 desktop machines with information being shared between them through local shares, there is a single internet connection. They use outlook.com as their email strategy.

Working through scenario 2, the information they have stored all over the place, should be stored in a singular location, which is backed up. Or, to make it easier, the client should have the work synched to the cloud, using a cloud service like OneDrive or dropbox.

Overall, notice the primary trend in the scenarios; it's not the hardware itself that is considered the most critical, it's the raw data, the information that the client uses to communicate and run their business off. Hardware can be replaced reasonably quickly. Data, not so much. So when working with a client, the best idea is to determine where their data is, what is classified as the most important data and how that information can be stored and recovered from.

3.3 CATEGORISE ASSETS AND CALCULATE THEIR VALUE TO THE ORGANISATION

Information is the primary asset of a company, though it's value is immense, when dealing with clients, always put this as the primary asset and design systems to protect it, use local and remote solutions to ensure that the data is kept secure.

When dealing with other assets, this is where auditing comes into play, by auditing, this is where a list of all hardware assets are recorded and maintained to ensure that the client knows, at any point in time, what they have, how much it cost and what the best estimate of replacement value would be. Let's look at a scenario to calculate this information. Using the same scenario from above.

Scenario 1: Your client is a car yard, they store all mechanical information in regards to repairs of specific brands on a local server, they run a file share server, an email server and a user server. They have 25 client machines, which link up to the servers to share information, they run specific applications that store client information. This database is stored on the file server. They have a single internet point. They run a wireless system to enable mobile devices to connect to, for themselves and for clients coming in. Access to the wireless is anonymous.

From this scenario, you will need to break down the hardware assets.:

- Servers x 3
- Desktops x 25
- DSL router
- Switch
- Wireless Router

That's the indicated hardware, notice the addition of the switch and no notification of mobile devices, the client's employees link their own mobile phones to the company wireless network, so not the client's responsibility and the switch will be needed to link up all of the servers and desktop machine. When you are onsite, you would of course have access to the brand of each machine and even the invoice of the hardware itself. So with the information from above, you would be able to display this in the following table:

Item	Price	Amount	Total
Server	$3550	3	$10,650
Desktop	$1400	25	$35,000
DSL Router	$300	1	$300
Switch	$500	1	$500
Wireless Router	$300	1	$300
			$46,750

3.4 CREATE A RISK MANAGEMENT PLAN

A risk management plan is critical to any project, and as such you will need to know how to document all of the risks that you have already identified. Overall, the risk management plan consists of:

- Identify the risk
- Analyse and evaluate the impact
- Mitigate the risk
- Review and maintain the plan

The document itself, should be fluid, as projects tasks change, the risks that might occur will change with them. The document itself should be arranged out like this:

- Cover page
- Project Summary
    - Document Control
    - Opportunity Statement
    - Objectives and Success Criteria
    - Recommended Solution
    - Project Milestones
- Project Risk Assessment
    - Risk Rating Methodology
    - Consequence Legend
    - Risk Identification

- Risk Management Process
    - Organisation
    - Risk management Process and Reporting
- References

The below example is a template for a risk management plan.

EXAMPLE

Example:

DOCUMENT CONTROL

Author

Position	Name
Project Manager	

Revision history

Version	Issue date	Author/editor	Description/Summary of changes
V1		Project Manager	Document Created

Reviewed by

Version	Issue date	Name	Position	Review date

Approvals

Version	Issue date	Name	Position	Approval date

Related documents

Document	Location

TABLE OF CONTENTS

1 Project Summary

This section outlines the project and puts into contexts the objectives that you will provide for your Risk Management Plan. You can include an executive summary of the project here if appropriate.

1.1. Opportunity Statement

Provide the reader with an understanding the overall goal of the project. This can be obtained from the Accove Website Scope.

1.2. Objectives and Success Criteria

This section will outline the Objectives and Success Criteria for the project. Once again this information can be obtained from the Accove Website Scope.

1.3. Recommended Solution

The recommended solution (or a summary if necessary) will be detailed in the Accove Website Scope and can be included here. This section will facilitate the readers thinking as to what the risks may be in the recommended solution the project is setting out to implement.

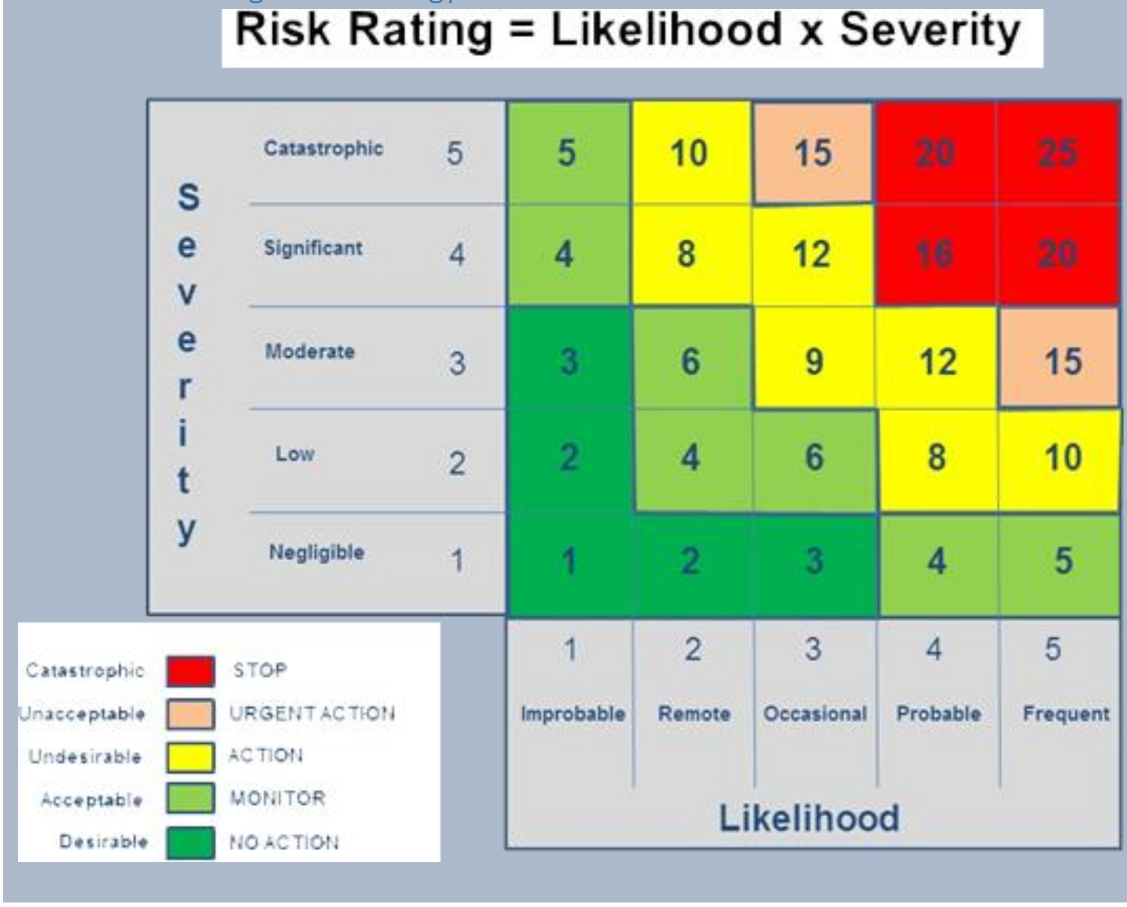
1.4. Project Milestones

The project management plan will detail the key milestones that are required to deliver the project and the associated schedule. Once again this information can be obtained from the Accove Website Scope.

2. PROJECT RISK ASSESSMENT

This section describes the project risk assessment. You may want to include a summary here of the key risks faced by the project (This information can be obtained from the Accove Website Scope.) and the method you have used to rate the risks.

2.1. Risk Rating Methodology



Risk Rating = Likelihood x Severity

Severity		1 Improbable	2 Remote	3 Occasional	4 Probable	5 Frequent
Catastrophic	5	5	10	15	20	25
Significant	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Low	2	2	4	6	8	10
Negligible	1	1	2	3	4	5

Likelihood

Catastrophic	🟥	STOP
Unacceptable	🟧	URGENT ACTION
Undesirable	🟨	ACTION
Acceptable	🟩	MONITOR
Desirable	🟩	NO ACTION

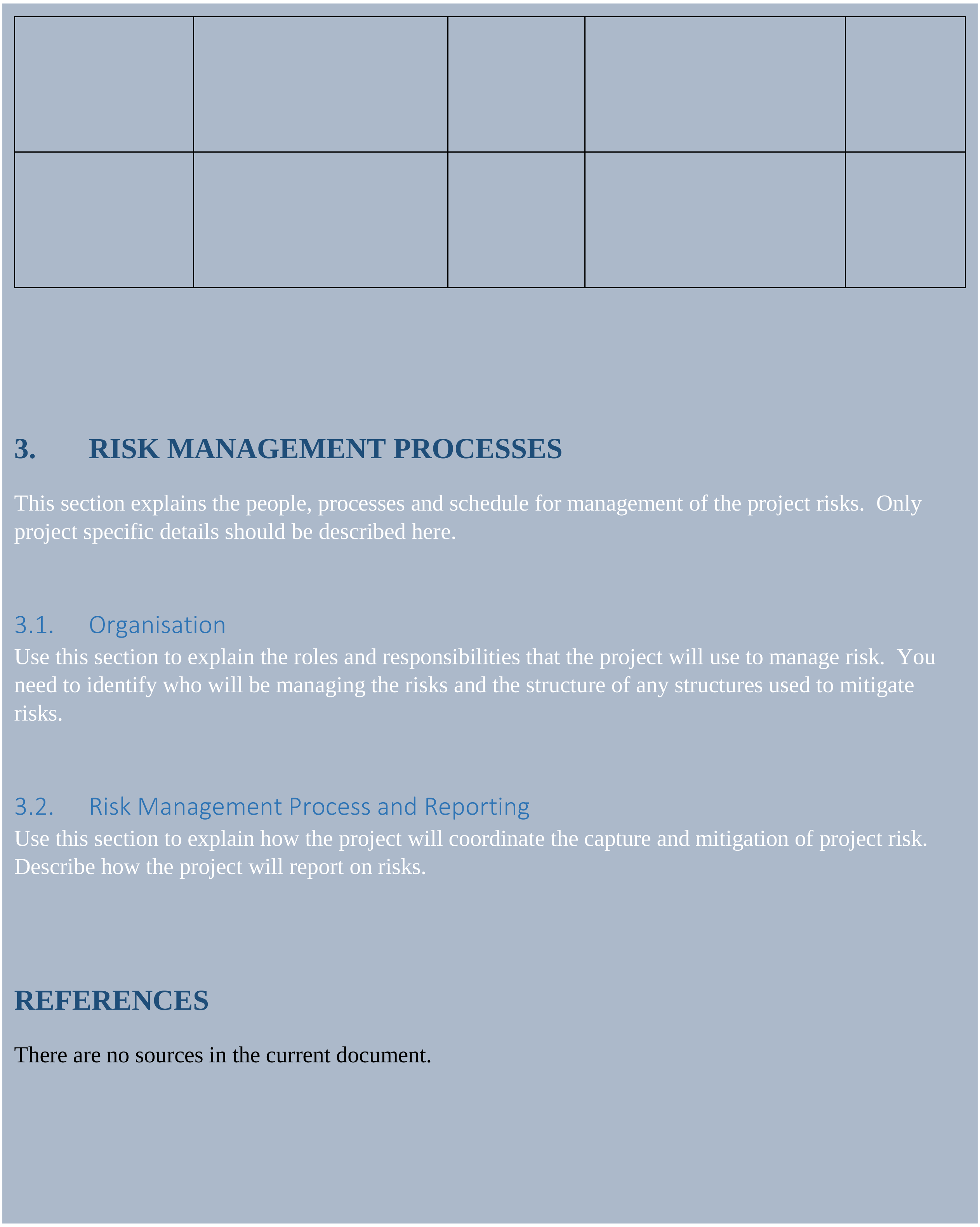
2.2 Consequence Legend

Rating	**Description**
Desirable (1-3)	Impact can be easily absorbed without requiring management effort
Acceptable (4-7)	Impact can be readily absorbed but some management effort is required
Undesirable (8-12)	Impact cannot be managed under normal operating conditions; requiring moderate level of resource and management input
Unacceptable (13-15)	Impact requires a high level of management attention / effort and resources to rectify
Catastrophic (16-25)	Disaster with potential to lead to business collapse and requiring almost total management attention / effort to rectify

2.3 Risk Identification

This section contains a brief description of the known risks and the mitigates. Preliminary and Residual ratings are required.

Risk Summary	Description	Preliminary Risk Rating	Risk Mitigation Description	Residual Risk Rating



3. RISK MANAGEMENT PROCESSES

This section explains the people, processes and schedule for management of the project risks. Only project specific details should be described here.

3.1. Organisation

Use this section to explain the roles and responsibilities that the project will use to manage risk. You need to identify who will be managing the risks and the structure of any structures used to mitigate risks.

3.2. Risk Management Process and Reporting

Use this section to explain how the project will coordinate the capture and mitigation of project risk. Describe how the project will report on risks.

REFERENCES

There are no sources in the current document.

4. Create a security design

Designing for security is an aspect of the initial planning phase for a network. This is where simulating various potential threats to a network need to be created and countered before they are discovered in a live system.

Examples of potential threats:

- Packet Sniffers
- Viruses and Worms
- Spam
- Zombie Computers and botnets
- Password attacks
- Malicious Websites

When designing a network, these areas of potential attack should always have a counter measure in place before implementation. This in turn does effect items such as the overall costing, but when it comes to network security, prevention is far better.

4.1 DETERMINE ATTACKER SCENARIOS AND THREATS

The only way to determine an attackers threat to network security, is to examine the network as a whole entity and then break down the entity into sections of potential entry vectors. To do this, you would have to generate potential scenarios to account for the reason as to why an attacker would target this network. Once you have a reason behind the attack, it is then a case of breaking down potential areas of attack vectors to determine how to get to the information that is desired. Let's examine the following scenario:

Scenario: This client is a local real estate company, they store a database full of information the file server, have remote access to email through the web server and host their own properties. The database contains a lot of personal details and credit card information about their clientele. The router for internet connection is a wireless router, to enable the employees access with their mobile phones.

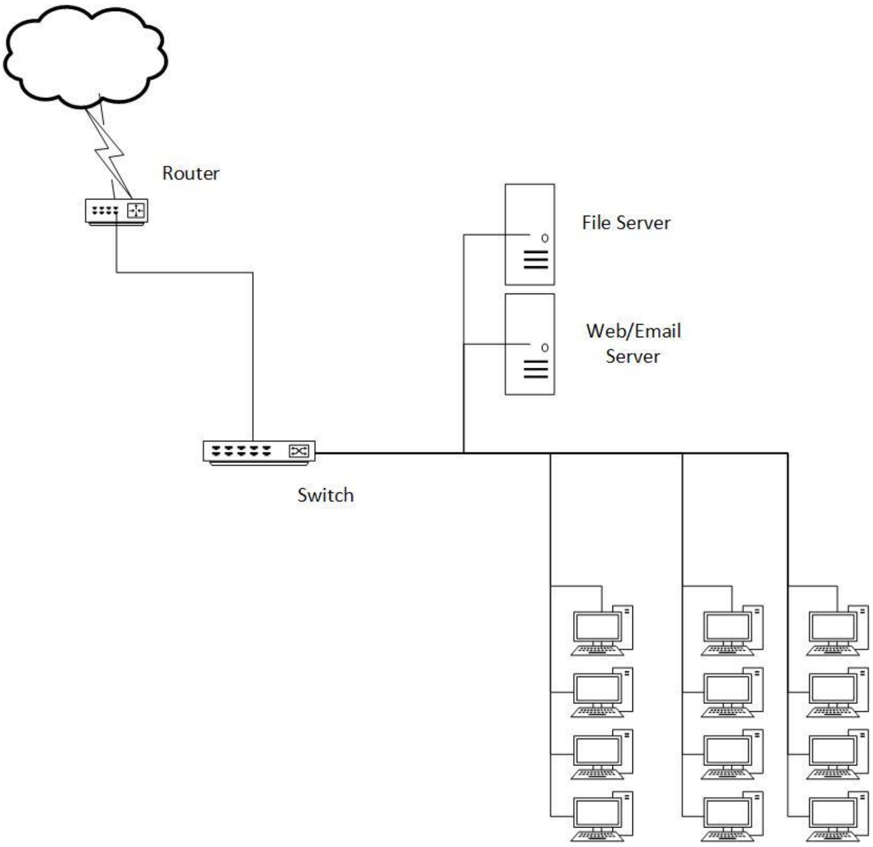


Figure 7 Simple Network

The first thing to determine is the motivation of the attacker, what is it that this particular client has that would be of value to someone. First choice would be the personal information on the clientele, having a list of credit card details enables quite a bit of theft. So, in this scenario, we will work on greed for the attacker.

Let's look at the two main entry vectors into Figure 7 Simple Network, the gateway would be through the internet router, via the wireless access point or through malicious software entering the system via email.

This is of course, not taking into consideration all of the potential attack vectors, but does allow for us to look at the system from these two points. Discovering these two entry vectors, it is easy to see that this is an area that needs to be monitored and kept secure at all points in time.

In general, there are multiple areas in which a network can be attacked:

- Email
- Web
- Physical devices such as usb, Disc
- Virus
- Social Engineering
- Unpatched systems

When examining a network to determine an attacker vector of attack, work through both physical and logical entry points of the network.

4.2 DESIGN SECURITY MEASURES FOR NETWORK COMPONENTS

When it comes to securing a network, the components that construct the network need to be examined for their ability to be configured. Routers and switches, managed switches, all have the ability to have some form of security applied. Most routers have a general firewall with basic settings configured. Though to be confident in the security of a network, you would have to log in and configure the router to exacting standards.

Switches, depending on the type managed, smart or unmanaged also have the ability to be configured. If you have a client that is concerned about network security, then a configured managed/smart switch is, really, the only choice. A secure switch will include the following features:

- Access Control Lists, otherwise referred to as ACLs. An ACL is a set of rules that determine what can and can't be accessed. It allows for specific IP ranges and network address translation for IPs. For example, if you see a router configuration like this:

  ```
  access-list 101 deny icmp any any
  access-list 101 permit ip any any
  ```

  Then the router is designed to block requests such as a ping and still allow for normal traffic to work.
- Virtual LANS, otherwise referred to as VLANs. A VLAN is a logical method of segmenting a network to restrict traffic to one area. For example, you could have a wireless router designed to let visitors to the client's location access the network, this router connects to a switch which has the port and router as a separate VLAN. In this manner, clients that connect to the router can still use the main networks internet connection, but devices on it are unable to see any of the other machines on the network. This segmentation of networks happens a lot in areas such as schools, where you will have everything connecting to the same physical network, but staff, students and admin are logically spilt to ensure that information being transmitted by one group of people, ie admin, is kept separate from the student section of the network.
- Embedded security is another important aspect; in this area the switch is looking at have the ability to encrypt data. In this manner, the information traversing through the network is kept as secure as possible.

As mentioned earlier there are three types of switches, managed, smart and unmanaged.

Unmanaged: An unmanaged switch is a switch that already has a pre-configured setup so that the end user only needs to plug it in and everything just connects. For network that are not dealing with highly sensitive data and just want work, this is a nice easy switch to have implemented. There is no configuration that can be made to this switches.

Smart: A smart switch is an entry level version of the managed switch, it has the features, but doesn't go into as much granular control as the managed switch does.

Managed: A managed switch is the best type of switch to get, as it has the capability of controlling all traffic that travels through it, managed switches have the ability to run ACLs, lock down ports to MAC address and apply Quality of service to parts of the network; for example, ensuring voice traffic has a higher priority to ensure a decent communication link over other traffic.

Let's re-examine the previous network (Figure 7 Simple Network), in which there were two attack vectors, the wireless router and general internet connection. As a reminder, here is the scenario again:

Scenario: This client is a local real estate company, they store a database full of information the file server, have remote access to email through the web server and host their own properties. The database contains a lot of personal details and credit card information about their clientele. The router for internet connection is a wireless router, to enable the employees access with their mobile phones.

To work on securing the network, we need to lock down the core network components, this would be the router and the switch.

Using the wireless router as an attacker vector is indicative of a network not being locked down, and with the router broadcasting its identification. Most wireless routers broadcast their SSID (Service Set IDentifier) to enable devices to be able to locate the router and connect. The drawback to this is that it allows any device that can pick up wireless networks, to know that this wireless network does exist. First layer of device, for wireless routers, is to not let anyone know that the router is even there. As such, disabling the broadcast of SSID is a must. As the client is not sharing its wireless network with its clientele then there is no need for the wireless network to be broadcasting.

The router itself can be locked down with configured firewalls, ACLs and monitored with logs being reported to the servers.

General rules on wireless lockdowns:

- Change the SSID
- Change the password
- Enable WPA2 Encryption
- Enable MAC filtering
- Block WAN requests
- Limit DHCP leases to your devices

Depending on the type of wired router you have you can also harden it against attacks, here is a list of areas that can be disabled to ensure that the router is more secure against attacks:

- Disable unused router interfaces—that's right, find ANY interface that is not in use and make sure you issue the **shutdown** command
- Disable unused services—these typically include:

    - BOOTP
    - CDP
    - Configuration auto loading
    - FTP
    - TFTP
    - PAD
    - TCP and UDP minor services
    - DEC MOP
- Disable management protocols that you are not using—these typically include:
    - SNMP
    - HTTP or HTTPS
    - DNS
- Disable features that are techniques for re-directing your traffic:
    - ICMP Redirects
    - IP Source routing
- Disable features that are techniques for probes and scans in reconnaissance attacks:
    - Finger
    - ICMP unreachable
    - ICMP mask reply
- Ensure security of terminal connections:
    - IP identification service
    - TCP keepalives
- Disable gratuitous ARP and proxy ARP
- Disable IP-directed broadcasts

By locking down the wireless side and wired side of a network, the attack vectors become very limited from external attacks. If you apply internal security to switches you can ensure that a network is as secure as possible, yet still allow the client's employees full range to the internet and resources need to complete their jobs.

If you are dealing with a windows environment, the server in charge of the network, has the ability to apply GPOs (Group Policy Objects). A GPO is effectively a group of rules that can be applied to elements of the network, via user or device groups. Think of it as a tree structure, where a rule applied to the top level filters its way down the base level. GPOs can be used to harden desktop machines against attacks, similar to how we've discussed hardening network components. There are over 3500 elements that can be configured in a GPO for Server 2012 and Windows 8.1

Research: GPO's Server 2012

Read about GPOs:
https://technet.microsoft.com/en-us/library/hh831791(v=ws.11).aspx

In addition to GPOs, when designing security elements, always consider the updates that need to be applied to the desktop machines, as such there might be a need to implement a Windows Server Update Services system. This is a server system that allows for the administrator of a network to actually control when and how operating system and applications patches are applied and when they get pushed out to the client's desktop machines. This in turn saves bandwidth, but also enables monitoring of how up to-date a network is with its patching, as there is logs that inform the administrator if there are machines that are not being patched.

Physical security is something that needs to be taken into consideration when designing a network. For example, if a client has gone with an unmanaged switch and this switch is easy to get to, then all an attacker has to do is plug in a device to start attacking the network as there is nothing preventing this form of attack. This is why switches, routers and servers are generally locked away in racks and sealed rooms to eliminate a physical attack.

When balancing attacker scenario's, it is best to determine the counter measures to them as soon as possible, and implement the solutions securely. A well designed prevention methodology will ensure that actual attacks are minimised.

4.3 OBTAIN FEEDBACK AND ADJUST IF REQUIRED

When you have completed designing a security plan, it is always best to get feedback in regards to what has been decided. When discussing security with a client, one should always try and put a dollar figure on the amount of time and resources that is going to be required to secure a site. The client will respond to how secure they will want the system. For example, if it is a small to medium sized business, they might not like the idea of spending $3000+ on a managed switch when they can get an unmanaged switch for under $200 if they don't see the potential of someone getting into a network.

Modification of ideas and concepts are extremely common and as such talking to clients and discussing ideas and designs with other IT capable peers will enable the plans that you have designed to be of value as they will become more dynamic and meet the clients end needs correctly.

When discussing ideas and concepts, ensure that you create a checklist to cover the important points. Remember to ensure that the client knows about the following types of attack:

- Logical
    - Email: Ability to get malicious code inside the system where an authenticated user can run the code.
    - Websites: Ability to allow authenticated users to infect previously secured systems
    - Weak passwords: Easily guessed passwords, can allow for an authenticated user to login
    - Missing patches on Servers: This is where security patches are not applied to publicly discovered flaws and a hacker can locate the entry point to the network.
    - Misconfigured firewalls: Opened holes in the firewall to allow attacks access to the system
    - DOS/DDOS: Denial of Service/Distributed DOS, this is where a network's access to the net is removed, due to it being overwhelmed by constant machine requests and hence using all of a particular resource.

- Physical
    - USB drives: portable device that can contain malicious code
    - Laptops: Mobile devices, that have the ability to run a full suite of attack software to break or enter a network.
    - USB Devices: Like a USB drive, a USB device can have internal memory that could be used to store malicious code
    - Social Engineering: Employees being fooled to supply access, very similar to internal connections.
    - Internal connections: Employees can grant access to non-secured people who are dressed to look the part.
    - Mobile devices: can be used to locate access points such as wireless access points, and run specific software designed to damage a network.
    - Wireless Access points: Easily discovered access to a network, to enable additional attacks

The checklist you design can be in a simple table format, such as the following:

Area	Issue	Discussed with Client
Logical	Email	□
	Websites	□
	Passwords	□
	Patches	□
	Viruses	□
Physical	Locked Rooms	□
	Key Card Access	□
	USB	□
	Wireless Routers	□
Education	Social Engineering	□
	Viruses	□

When creating this checklist, cover as much of the network design that is needed to ensure that the client understands that they will be safe. Remember, the list will need to be manipulated for the unique needs of a client. For example, a car yard client will not need a checklist in regards to updated dental software.

4.4 DEVELOP SECURITY POLICIES

A policy is a set of rules that list the setup and maintenance of certain aspects of a network. A policy supplies the final result of certain settings of a network, for example, a network policy could specify that all ports on the firewall are blocked expect for ports 80, 25. The document doesn't go into the technical detail on this is implemented, just the end result. This in turn allows the policy to be consistent and work over any form of technology that a client may have implemented on their site.

When writing up a policy, the document will contain the following parts:

- Overview
    - The overview is effectively the same thing as the purpose but, not as detailed, for example, a document about dealing with a firewall, the overview could be written as: "This policy is designed to supply best practices for network security, focusing on firewall protection."
- Purpose
    - A purpose allows for more detail than the overview. So, it would include aspects such as, which ports are left open and a brief explanation of each port, so continuing with the overview concept: "Ports 80(web) and 25(smtp) are being left open on the firewall to ensure correct internet traffic is being supplied to all individuals. Incoming traffic on 80 and 25, will talk to the web server and email server respectively.
- Scope
    - This relates to who the policy is aimed at, if it is aimed a certain department for the client or for the client's entire business. For example: "All employees, contractors, consultants, temporary and other workers at <Name of client's business> must adhere to this policy."
- Policy
    - This is where the policy is stated with as much detail as needed. For example, part of the firewall policy could contain:

        - Firewall disables
            - IP directed broadcasts
            - Incoming packets at the firewall sourced with invalid addresses such as RFC1918 addresses
            - TCP small services
            - UDP small services
- Policy Compliance
    - Here in the document, the areas of where the policy implementation is being monitored, it's time of review and who is in charge of ensuring the policy is enforced. It will also state the potential disciplinary action on non-compliant situations.
- Related Standards, Policies and processes
    - Does the document form part of a larger collection of policies? This is where this information would be listed. For example, the firewall policy is a sub document of the Router/Switch network policy.

- Revision History
    - A simple table in the document, can be found at the end of the document or after the overview to allow for readers to understand how many changes have occurred to the document and how authorised the modifications.

In most cases, when dealing with policy documents it pays to get an overview of the entire network that you need to design policies for. In this manner, it is easier to locate the exact areas in which require points to be made.

5. Design and implement responses to security incidents

5.1 DESIGN AUDITING AND INCIDENT RESPONSE PROCEDURE

Auditing is the ability to document every element in a network. This auditing document allows for the ease of tracking of items as well as a way of determining the financial cost of an item. The financial cost will be based upon the original purchase price of an item, the setup cost and any maintenance costs associated with that item.

An audit document should have the following breakdown of various items, such as:

- Hardware; break down to: cpu, ram, hdd, gpu
- Software; break down to: Operating system, standard applications, anti-virus, specialised applications
- Currency of Software: Are there patches or updates that need to be applied, when was the last time the application was patched
- Revision history: when was the last audit performed

The audit document will need to be as generic as possible and allow for unique modifications based off how a network component can be customised. For example, the server that a client purchases could contain multiple cpus, as such the document should allow for the number of cpus and speed of cpus to be registered. If the machine's image contains outdated software such as Office 2003, then include with the listing of application an area in which notes can be made for in this case, the reason the client might be staying with 2003 is that they have specific macros that have been written for a custom built solution.

Always allow for notes to be placed within the document to indicate discrepancies of a network component or device.

The auditing document allows a client to understand what types of details have been collected on each machine, i.e. the client might have a standard image for all desktop machines, but the audit shows 3 machines that haven't received this image. As such, the client would know to request a work order to update the 3 machines.

To create an audit, there are multiple ways of achieving this. It is possible to download software that will enable the process to be done with a specific time frame quickly. Auditing a client's network means that you need to collect information in the following areas; Hardware, Software, Infrastructure and Data.

- Hardware
    - Hardware auditing is where each item of hardware is located on the premises of the client; details are record and if need be, each item is tagged so that the item can be located quickly.
- Infrastructure

    - Infrastructure is locating and recording information on switches, routers, cabling and wireless devices. As with hardware auditing, you type and details of each device need to be recorded as well as its location.
- Software
    - Software is the recording of each piece of software that is used on a machine, as well as its relevant licensing details. Most business will not buy a blanket license of the adobe suite if there is only a limited number of users who need it for the business. As such, when doing audits, you need to know where this software is installed and how many of the software suites are to be used.
- Data
    - This is one of the most important pieces of a client's network that needs to be audited. Items such as the shares that every user has access to, the location of where each item is on a server or a machine and of course it's backup solution for the client.

Once this information has been collected, it should be done the first time you enter a client's premises, you will be able to make educated estimates on what the client needs to match their strategic goals. If the client needs to add 10, 20 or 50 new machines to their network then you would be able to quickly determine from the paper work if the current infrastructure can handle the increase in machines. As you can imagine, the speed it takes to look up a switch infrastructure for a client is much faster than having to go onto a client's premises to review the hardware manually each time something like this occurs. This ability will increase your skills and reputation as a highly sought after business.

Activity: Do a quick audit on your own network. List only the frequently used items

Item	Type/Location
Hardware	
Infrastructure	
Software	
Data	

Auditing can be a long process, so it is always best to perform an audit of a client's premises as soon as possible, thereby allowing for you to have the knowledge needed to assist the client as soon as possible.

Auditing Software

There are hundreds of different audit software, here is a list of some of the enterprise and popular software.

An incomplete software List:

- Cherwell Asset Management : https://www.cherwell.com/
- Open-Audit: http://www.open-audit.org/
- Spice works: http://www.spiceworks.com/free-software-inventory-audit-tool/
- E-Z Audit : http://www.ezaudit.net/
- Free PC Audit: http://www.misutilities.com/free-pc-audit/index.html

Once you have selected and tested auditing software to determine your preferred type of software, you will have to store the information that you have collected. A lot of businesses will store this information on a database or intranet for ease of access by technicians.

Activity:

Use the E-Z Audit and Open Audit software on your computer and compare the results.

An incident response document is a document that is designed to track and monitor issues that occur within a network. This document should contain aspects of the following:

- Recognize and respond to an incident;
- Assess the situation quickly and effectively;
- Notify the appropriate individuals and organizations about the incident;
- Organize the company's response activities, including activating a command centre;
- Escalate the company's response efforts based on the severity of the incident; and
- Support the business recovery efforts being made in the aftermath of the incident.

As such the document needs to be clearly defined into specific headers, each of these headers allows an auditor to examine an incident response document and determine if the actions followed through were correct. The headers can be:

- Incident Identification information
- Incident Summary
- Incident notification – others
- Actions
- Evaluation
- Follow-up

When designing this type of document tables are a good way to situate the forms that need filling out. An important aspect of the form, and most other forms, is the ability to date and assigned names to it, in this respect, the people who were involved with the incident can be located for additional information as needed.

Example:

Example of the incident identification information form:

INCIDENT IDENTIFICATION INFORMATION	
Date and Time of Notification:	
Incident Detector’s Information:	
Name:	Date and Time Detected:
Title:	Location:
Phone/Contact Info:	System or Application:
INCIDENT SUMMARY	
Type of Incident Detected: ☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Use ☐ Unauthorized Access ☐ Unplanned Downtime ☐ Other	
Description of Incident:	
Names and Contact Information of Others Involved:	
INCIDENT NOTIFICATION – OTHERS	
☐ IS Leadership ☐ System or Application Owner ☐ System or Application Vendor ☐ Security Incident Response Team ☐ Public Affairs ☐ Legal Counsel ☐ Administration ☐ Human Resources ☐ Other:	
ACTIONS	
Identification Measures (Incident Verified, Assessed, Options Evaluated):	
Containment Measures:	
Evidence Collected (Systems Logs, etc.):	

Eradication Measures:
Recovery Measures:
Other Mitigation Actions:

5.2 DOCUMENT SECURITY INCIDENTS

When determining if the template created for documenting incidents is viable, it is always a good idea to test the form through a few iterations of potential incidents. This way the document can be tested against various formats of issues. Both major, in say a server goes down to a minor incident such as machine is infected by a virus.

So, using the template that would have

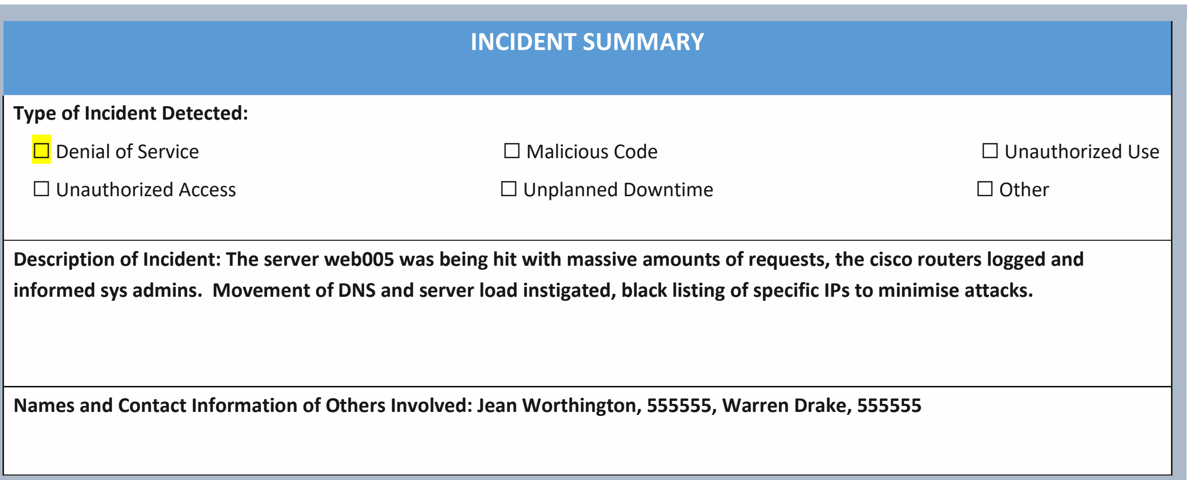
This can be done like this:

Example:

Example of the incident identification information section:

Partial Form fill out for denial of service attack

INCIDENT IDENTIFICATION INFORMATION	
Date and Time of Notification: 23/2/2016 19:37	
Incident Detector’s Information: Scott McCoy	
Name: Scott McCoy	Date and Time Detected: 23/2/2016 17:15
Title: Systems Administrator	Location: West Site Communications hub
Phone/Contact Info:555555	System or Application: DDOS



INCIDENT SUMMARY

Type of Incident Detected:

☐ Denial of Service ☐ Malicious Code ☐ Unauthorized Use

☐ Unauthorized Access ☐ Unplanned Downtime ☐ Other

Description of Incident: The server web005 was being hit with massive amounts of requests, the cisco routers logged and informed sys admins. Movement of DNS and server load instigated, black listing of specific IPs to minimise attacks.

Names and Contact Information of Others Involved: Jean Worthington, 555555, Warren Drake, 555555

Of course, normally the entire form would be filled out. The above is indicative of the information that is expected in a form of this nature.

5.3 IMPLEMENT CONFIGURATIONS ALIGNED WITH INCIDENT RESPONSE PROCEDURE DESIGN

Based off the form in the example shown in 5.1, the bottom of the form indicates the corrective actions that were taken during the resolution of an incident. When there has been a resolution, there is a need to implement the resolution on additional devices to ensure that the chances of the original issue happening again are minimised.

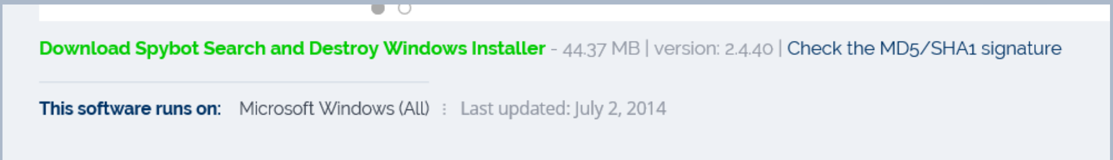
One such incident would be malware attacks, if a single machine was attacked on the network and then resolved, through the use of anti-malware a network response would be all machines on the network would then be scanned for malware.

Configuration and implementation, are dependent on the software that has been located to implement the recovery. The latest software would have to be downloaded on a differing machine, installed onto a usb or onto a network drive of which the machine has access to and then ran, to ensure the system is free from malware. So, in response to a malware infection, do the following activity.

Activity:

Download Spybot ant-malware and run it.

Get the software from here: https://www.safer-networking.org/private/



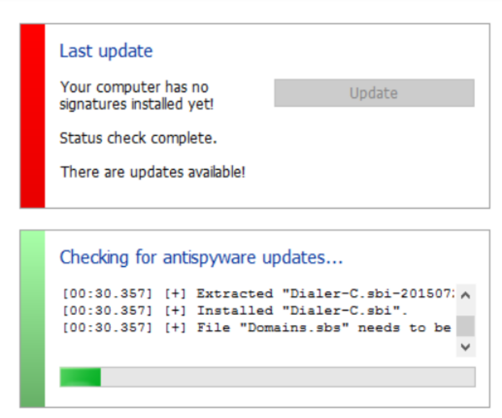
Download Spybot Search and Destroy Windows Installer - 44.37 MB | version: 2.4.40 | Check the MD5/SHA1 signature

This software runs on: Microsoft Windows (All) : Last updated: July 2, 2014

Install and run on your machine, get screen shots of the machine once cleaned,

Eg:

1. **Ensure it is updated:**

   a. 

   Last update

   Your computer has no signatures installed yet!

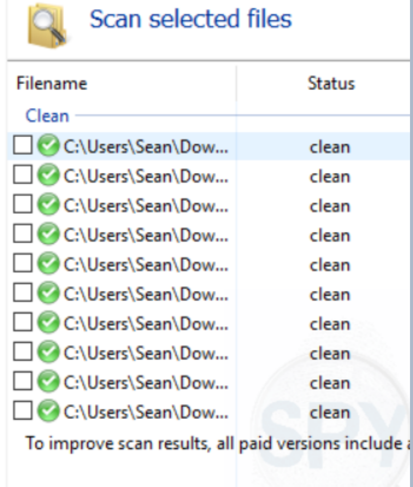
   Status check complete.

   There are updates available!

   Checking for antispyware updates…

   ```
   [00:30.357] [+] Extracted "Dialer-C.sbi-201507:
   [00:30.357] [+] Installed "Dialer-C.sbi".
   [00:30.357] [+] File "Domains.sbs" needs to be
   ```

2. **Runa scan over the system, or specific files, the resultant should be green tick boxes:**

   a. 

   Scan selected files

Filename	Status
Clean	
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean
□ ✓ C:\Users\Sean\Dow...	clean

   To improve scan results, all paid versions include a

When items like this occur, the resolution should be written up and added to the audit trail of the machines that have been examined. It is always a good idea when adding to the documents, what the expected output is going to be as this will then allow for future technicians to understand what to expect from such a run.

5.4 TEST AND SIGN OFF

Before heading out the door it's time to get your paperwork signed to satisfy your own boss. You must find the manager for the site you are working at and get them to sign any documents that you may have that require client sign off.

In cases where there is not staff member authorised to sign off on your work, email the documents to the approver of the original project/design. This person will have the authority to sign off on your work and allow you to complete your paper work for your boss, so that they know you have performed your duties to the client's satisfaction.

Each client is different and unique in what they need, as such, you can have a template sign off form where there is a general item for the client to agree upon and then add additional items that have occurred that are unique to that particular client.

Example: Checklist for Client machine

Below is an incomplete list of elements to indicate that a client machine has been installed and setup.

Task	Completed	Client Agreed
Operating System Installed	□	□
Connected to Network	□	□
Mapped Drives Work	□	□
Printer Access	□	□
Email Setup	□	□
Office Installed	□	□
Adobe Suite Installed	□	□
…….	□	□

A sign off section is a very simple section that you put into a document so that the client recognises that a specific milestone is reached. Depending on the project, this could be used to instigate a payment schedule or resource release.

Sign off sections look like:

Example:

Authorisation

Name	Signature	Date
Owner /Operator		/ /

6. General Knowledge

6.1 RECOGNISE AND DESCRIBE COMMON ICT NETWORKS AND THEIR CONFIGURATION

Networking can be confusing if you don’t understand the basic layout of how it all goes together and communicates. Networks can be broken down into differing topologies and network types.

Topology

Topology is another term that is going to be used within this document a lot; a topology is the term given to the design of a network. This design is the layout of the various devices that are implemented to create the network. There are physical and logical (Signal) topologies; a physical topology refers to the way the devices are connected through actual cabling, where as a logical topology refers to the method in which data traverses the network. Logical topologies are based upon the protocols used for network communication. The primary communication protocol today is TCP/IP.

There are 6 forms of topologies that have been used in the business world, these are bus, star, token ring, ring mesh and tree. Currently the primary ones that are in use are star, mesh and tree.

A Star topology is a network where all of the devices are pointed to a singular device, this central device is normally a switch which is designed to handle the large amounts of data that can be pushed through a network. One of the main advantages of a star network is that if an end device falls off the network, no other device is disrupted. Adding to a star topology is as simple as implementing new wiring to the device location and plugging into the switch. Star networks are the most common form of network. A disadvantage is that if the central communications device is knocked off the network, the entire network is down until it is fixed.

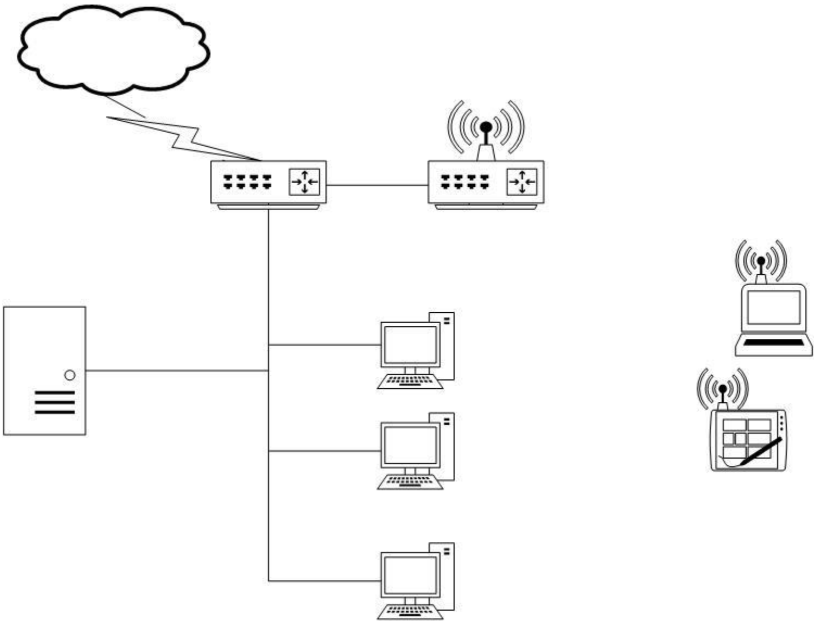


Figure 8 Star Topology

A Mesh network is an extremely reliable type of network, as each device is used to enable the transmission of data. Basically a mesh network is a network where every device is connected to each other. This increases the reliability and security of a network, but it is a far more expensive network to implement. Wireless networks can be used to implement mesh networks as there is no additional media to be assigned. Wireless mesh networks were designed with military applications in mind. Mesh networks use the shortest path bridging algorithm to ensure reliability.

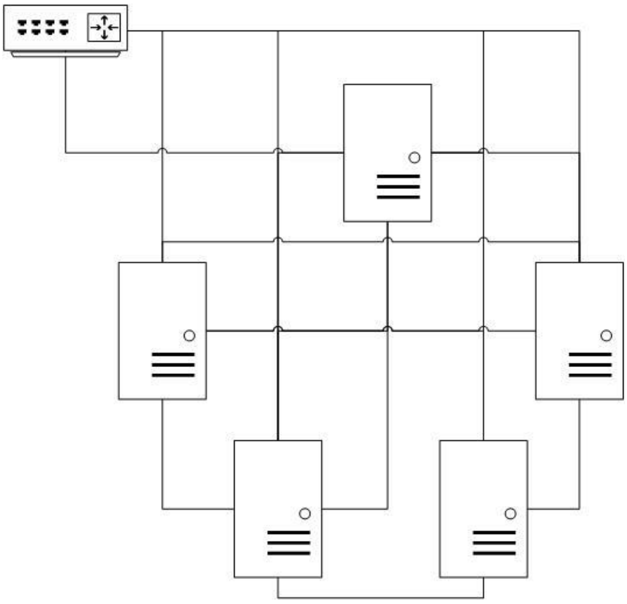


Figure 9 Mesh Topology

A tree topology, is a collection of star topologies connected via a bus topology. A bus topology is a network that has a singular core back bone with nodes linked off it. This is a hybrid network topology which works to use the best of both star and bus technologies. In the case of a tree network, it is a bus topology with star topologies instead of singular nodes, in this manner a singular network can be extended with a core backbone and separate segments to ensure that the data is only propagated in the localised segments, which in turn ensures that the network will do its best at eliminating packet collisions.

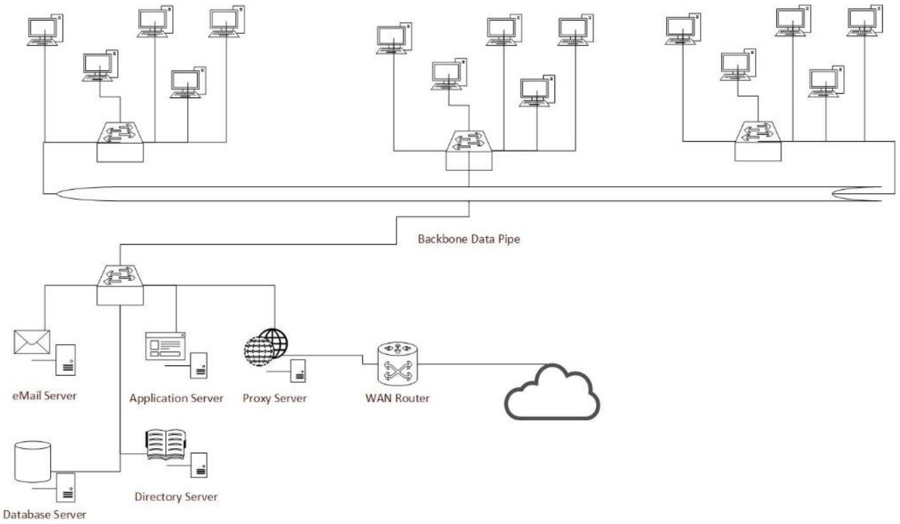


Figure 10 Tree Topology

Historically, ring networks and token ring networks were designed before the use of TCP/IP. A ring network is a closed network with data travelling through adjacent nodes. With a token ring network, this is a protocol that allowed for data to be transported in one direction, through the substitution of a token which could be displaced with data packets.

Network Types

When referring to network types, we are referring to the types of networks that exist in the real world. Terms such as LAN, WAN, WLAN, PAN, MAN, VPN and VLAN are used throughout the industry. So, we will look into each acronym in some more depth.

A LAN is a Local Area Network. A local area is considered to be a close geographically positioned network. Roughly it is one building or office for a network to be dispersed into. In some cases, a single LAN can be dispersed through multiple buildings, if they are all physically connected, in this concept, think of a school. Lots of little buildings all physically connected and yet still in the one single network. A LAN can serve from as many as 2 or 3 people, or up to hundreds of users. In most cases, LANs are a combination of wired and wireless connectivity.

A WAN is a Wide Area Network. A WAN is a widely dispersed geographic network, so city to city or country to country. Communication from Australia to the United States of America is over a WAN connection. The Internet is a WAN.

A WLAN is a Wireless Local Area Network. A WLAN is the same as a LAN, except that the medium for transmission is over the air, via radio signals, specifically the 802.x range. Wireless technology is a great way to expand infrastructure without incurring costs of running cables. Wireless technology transmits data through radio frequencies (RF) or infrared (IR) waves. Normally wireless technology will have a single access point that transmits information, when signals are low, these signals can be enhanced by the introduction of repeaters. A repeater captures the traffic and re-transmits it at full power, thereby increasing the range of the signal.

Wireless technology comes in many different formats, below is some of the data in relation to each particular protocol of wireless.

Protocol	Frequency Used (GHz)	Max Data rate (Mbs)	Release Date
802.11a	3.7 & 5	2	1999
802.11b	2.4	11	1999
802.11g	2.4	54	2003
802.11.n	2.4 & 5	135	2009
802.11ac	5	780	2013
802.11ad	2160	6912 (6.75GB)	2012
802.11ah	0.9		2016
802.11.aj	45 & 60		2016
802.11ax	2.4 & 5		2019
802.11ay	60	Up to 100GBs	2017

A PAN is a Personal Area Network. A personal area network is a network that consists of short range communication, such communication would be done over Bluetooth. A PAN, would be your phone to a Bluetooth receiver, be it either headset or another phone. PAN is a localised wireless network with a range of no more than 10metres when utilising Class 2 devices. It was invented by Ericsson in 1994 and transmits over short distances along the ISM band in the 2.4 to 2.485 GHz range.

Bluetooth comes in 3 classes:

Class	Typical Range (M)
1	~100
2	~10
3	~1

A MAN is a Metropolitan Area Network. A MAN is a combination of LANs that are separated geographically but with the same area, for example, in the same city. If you contemplate a university which has multiple campuses within the same city, but their LAN links are working and communicating as though it was a singular campus. They have LAN segments with a WAN backbone.

A VPN is a Virtual Private Network. Virtual Private Networks are unique in that they can fit in both a software and hardware category though it is common to use a combination of both technologies to get a secure version. A VPN is a secure tunnel that is established between multiple devices, it could be a laptop to a business router which allows a remote user to access a business network. There are a couple of different forms of VPN, hub and spoke, point to point and full mesh topologies. The information transmitted between the two end points of a VPN are encrypted.

Figure 11 Multi-VPN shows an example of both hardware and software VPN connectivity. The routers are linked by a hardware VPN, for example the image is indicative of a router to router connection, for example a Cisco 881 to Cisco Pix. The red software solution is a combination, for example using the inbuilt VPN software in windows to authenticate to a router to allow for access to the internal network.

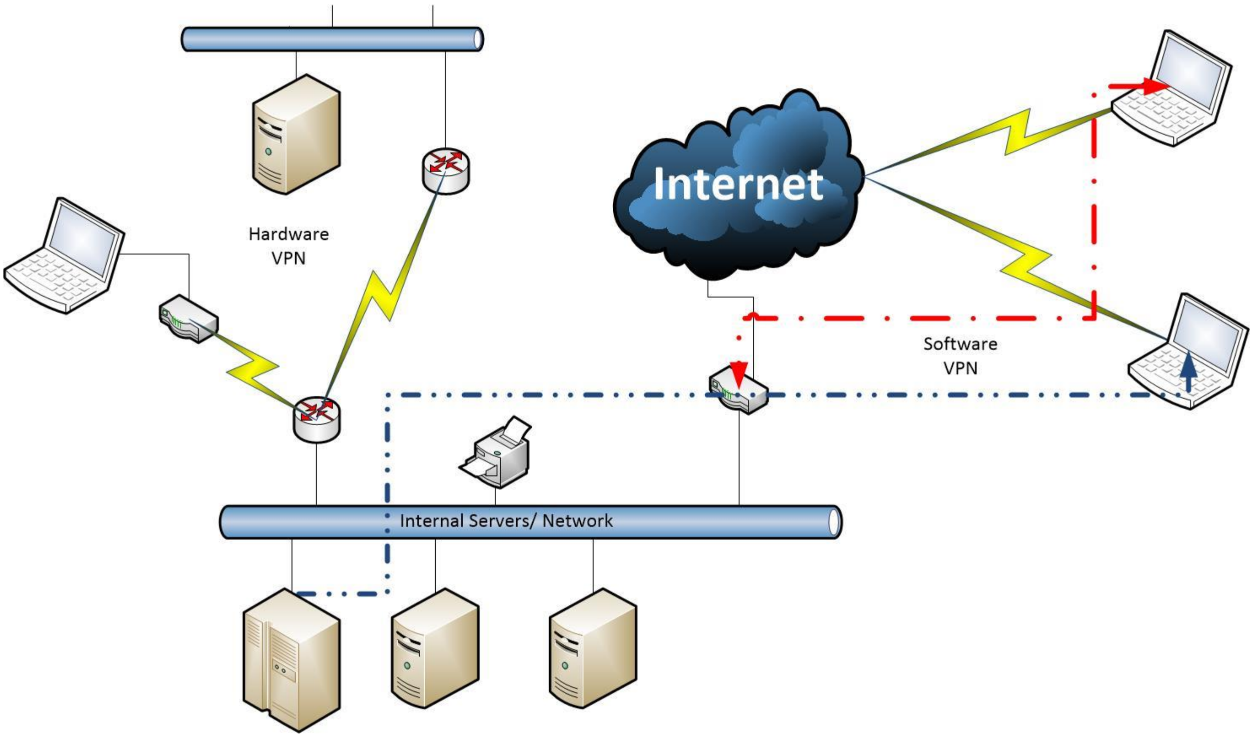


Figure 11 Multi-VPN

The blue software solution, is an example of a client using their software, being piped through to an internal server that would then deal with the authentication of the user. For this to occur, the router in question would have to have the correct ports open to allow the data to flow correctly.

Research: Research Cisco's VPN solutions.

Examine the routers Cisco have listed on their website and determine the level of hardware needed for a 5, 10, 100 person office. Research the requirements needed to implement a VPN solution from client laptop to Cisco router.

All data transmitted over this secure tunnel is encrypted, to ensure that communication works between these devices, you will have to ensure that the firewalls open up the following protocols and ports:

Windows	
Protocol	Port
PTPP	1723
PTPP Pass though / GREE	47
L2TP over IPSEC	1701 and TCP/UDP 500
SSTP	443
Open VPN	

TCP	443,943
UDP	1194

Reflect: *Scenario:* A manager needs to be able to take his laptop on the road and yet still be able to access the companies secure files for work. You've been contacted to come up with a solution for the situation.

Solution: In this case, the laptop will have to be set up with secure software, an example of this is virtual private network (VPN) software. A VPN creates an encrypted tunnel from one end point to the other. As with most I.T. solutions, there is more than one way to achieve this. The most common versions of VPN software are: Cisco VPN, Microsoft VPN and Open VPN.

A VLAN is a Virtual Local Area Network. A VLAN is a logical LAN, in this manner, you can separate a LAN without the need of purchasing new hardware or running extra cable. A VLAN introduces segmentation on the same segment of a network, it allows for scalability, security and network management for an existing network.
As topology segments can be classified as either physical or logical topologies, an easy way to recall this information is based on how the segment is implemented. LAN, WAN, WLAN are all physical implementations. There is cabling and a transmission medium. Topologies such as VPN and VLAN are logical in design as the structure can be changed without a modification to the physical hardware implemented.

6.2 IDENTIFY AND DESCRIBE NETWORK ATTACKS, VULNERABILITIES AND RELATED WEAKNESSES OF INSTALLED INFRASTRUCTURE, INCLUDING: SECURITY TECHNOLOGIES

Security Technologies are designed to enhance and protect an investment in technology. This can be digital or physical in nature. Examples of digital security technologies are: Mobile application wrappers, encryption and Multi-factor authentication. Biometric authentication is a good example of physical security as it requires a physical item to enable authentication.

- Mobile Application Wrappers: This technology allows for an enterprise to add security and management features to an application. This allows for security to be applied to applications on devices that do not fall under a company's security policy, such as Bring Your Own Device (BYOD) scenarios.
- Multi-factor Authentication: Also referred to as two factor authentication. This is where the user requires multiple methods of authentication to ensure that they validate the security level of the users, this is can be done as username/password and a code that is sent to either email or phone.
- Biometric Authentication: This technology involves the use of a physical attribute of the user to provide authentication. This can be done as fingerprint, voice, or iris scanning. Some examples are Windows hello in windows 10, this has the ability to use iris scan on the phone, facial recognition on a desktop and fingerprint via a fingerprint reader.

- Encryption: Encryption isn't new technology; it has been present since 100BC where Julius Caesar used it to ensure the messengers didn't read or understand his messages. Encryption is critical in keeping data secure. There are two main methods of encryption, Symmetric key and Asymmetric key. Symmetric is a single key shared with Asymmetric involving public and private keys to ensure encryption.
- Logging: Has been around since computers were first used, though it's not so much the logging but the method of reading and understanding logging that is vital to security. Zero day threats are only discovered via logging of systems.

6.3 IDENTIFY AND DESCRIBE NETWORK ATTACKS, VULNERABILITIES AND RELATED WEAKNESSES OF INSTALLED INFRASTRUCTURE, INCLUDING: EMERGING SECURITY ISSUES

Security issues are going to be a concern no matter how advanced a system becomes, as the more complex an item is, there will always be a vector in which the programmer missed something. And that something, can be exploited in ways that were never conceived of in the original design.

Zero Day: This is a vulnerability that is exploited on the same day it has been discovered, it has the ability to render defenceless software, hardware and even firmware.

Ransomware: This is where malicious software can gain access to a computer/network and it does one of two things, the first one is that it encrypts the data on the machine and the machine can be unlocked if the owner of the machine pays a certain amount of money or, the second is that the machine has an unlockable lock screen so the user can't get to the operating system.

The current top ransomware is:

- Ransom:HTML/Tescrypt.E
- Ransom:HTML/Tescrypt.D
- Ransom:HTML/Locky.A
- Ransom:Win32/Locky
- Ransom:HTML/Crowti.A
- Ransom:HTML/Exxroute.A
- Ransom:Win32/Cerber.A
- Ransom:JS/FakeBsod.A
- Ransom:HTML/Cerber.A
- Ransom:JS/Brolo.C

Research:

Read more about ransomware here:
https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

http://www.tomsguide.com/us/ransomware-definition,news-18745.html

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-evolution-of-ransomware.pdf

6.4 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: AUDITING AND PENETRATION TESTING TECHNIQUES

Penetration Testing

Penetration testing is a technique where a computer system is attacked to determine if there are any weaknesses or vulnerabilities that can be located to compromise the system. In general, a penetration test identifies and prioritises security risks, these risks can be located in the networks endpoints and applications. By implementing penetration testing, weaknesses in a network can be located and removed without any actual data loss for the client.

The benefits of penetration testing are:

- Avoid costly network downtime
- Manage any located vulnerabilities
- Ensure that the corporate image and customer loyalty stay undamaged

Each network is unique to what it needs to achieve, even though there are some areas in networking that can be classified as the same, as such, simple things like password guessing, social engineering, attempting to send employees of a client to specific web pages.

Research:

Research more about penetration testing:

http://www.pentest-standard.org/index.php/Main_Page

Auditing Techniques

Auditing is key to ensuring that you know what all elements exist within a network, auditing covers the physical components and examination of network traffic. This recording of all elements allows for new elements to be easily discovered, these elements being unknown network traffic, a machine cpu suddenly maxing out for no apparent reason is indicative of that machine being infected. As you can tell, auditing is a way of ensuring that the unknown traffic or unknown system utilisation gets noticed, once noticed, then the machines in question can start to be examined to see if the traffic is just unique for that particular time frame or something more sinister in design. The best time to audit, is as soon as the network goes in, as with everything being new and fresh to a client's location, all items are still known with no "forgotten" machine hidden a corner performing some esoteric task that is vital but no one knows why. If, you need to audit a network that already exists, then the audit can be done with existing software. There are hundreds of different audit software, here is a list of some of the enterprise and popular software.

An incomplete software List:

- Cherwell Asset Management : https://www.cherwell.com/
- Open-Audit: http://www.open-audit.org/
- Spice works: http://www.spiceworks.com/free-software-inventory-audit-tool/
- E-Z Audit : http://www.ezaudit.net/
- Free PC Audit: http://www.misutilities.com/free-pc-audit/index.html

Once you have selected and tested auditing software to determine your preferred type of software, you will have to store the information that you have collected. A lot of businesses will store this information on a database or intranet for ease of access by technicians.

When auditing, audit the network via its capability, but also in the role that it is going to be used in. For example, you might have 6 machines in admin that are exactly the same in hardware specification as the 8 machines in development. But it is easier to locate and manage resources if they are split into admin and development instead of saying 14 desktop machines.

Auditing also allows for a network administrator to locate the flow on effect of a vulnerability if found. For example, using the same 14 machines listed above, if one machine was infected with malicious code it would be safe to assume that the other machines would be able to be infected, and as such preventative measure could be put into place and those systems checked.

Auditing network logs is also a vital part of ensuring a network stays safe and that a benchmark of a clean system is recorded. When you have a benchmark for a network, it is far easier to locate discrepancies when they occur. Areas in which a network should be audited:

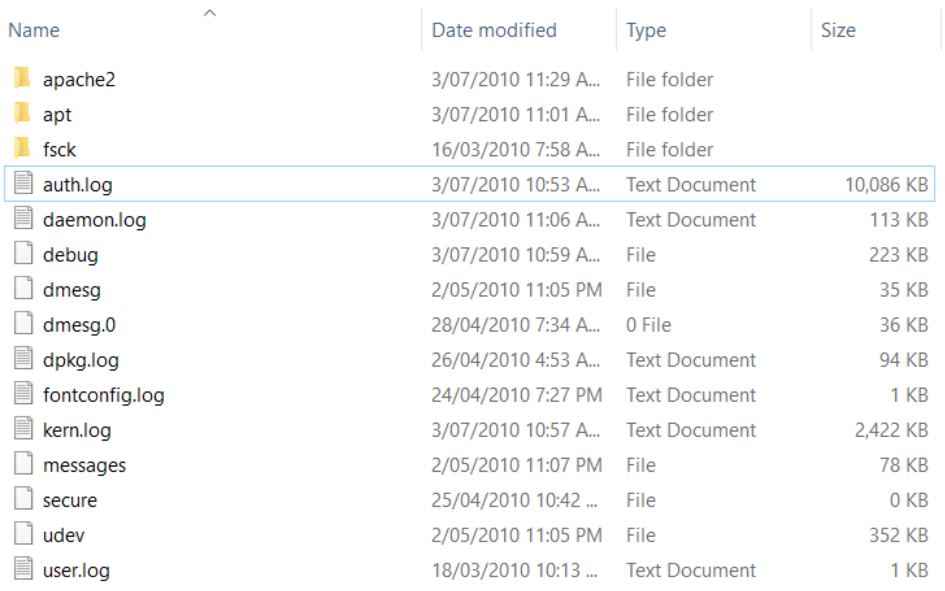
- Risk Assessments
- Policy Assessments
- Social Engineering
- Security Design review
- Security Process review
- Document review
- Technical review

Each area should be examined and audited for currency, this is to ensure that a network continues to stay current with being secure.

6.5 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: LOGGING ANALYSIS TECHNIQUES

The ability to read and examine network logs are a critical skill that is useful when it comes to determining what has been occurring on a computer. A log file records the raw data and doesn't filter out the information, as such, when you are looking at log files to determine what has been occurring on the network, then you need to have a few techniques down.

If you've never seen a collection of log files, this is what is located in the /var/log folder:



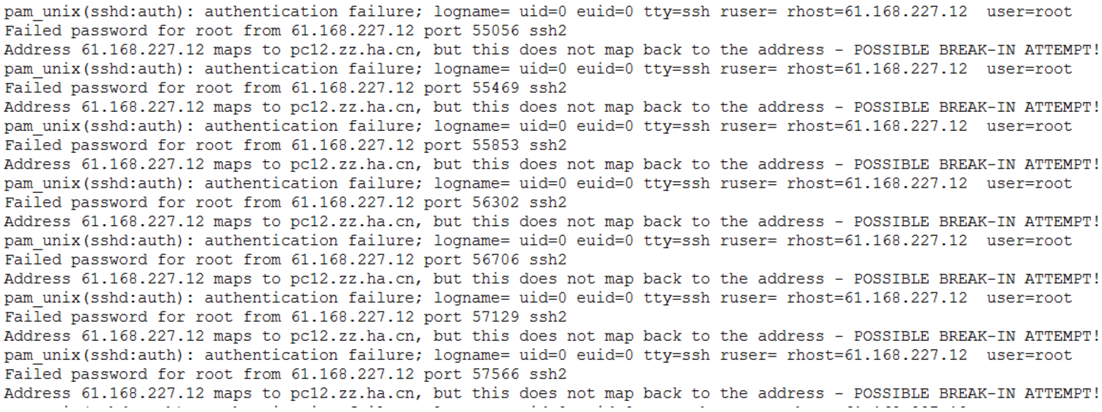
Name	Date modified	Type	Size
apache2	3/07/2010 11:29 A...	File folder	
apt	3/07/2010 11:01 A...	File folder	
fsck	16/03/2010 7:58 A...	File folder	
auth.log	3/07/2010 10:53 A...	Text Document	10,086 KB
daemon.log	3/07/2010 11:06 A...	Text Document	113 KB
debug	3/07/2010 10:59 A...	File	223 KB
dmesg	2/05/2010 11:05 PM	File	35 KB
dmesg.0	28/04/2010 7:34 A...	0 File	36 KB
dpkg.log	26/04/2010 4:53 A...	Text Document	94 KB
fontconfig.log	24/04/2010 7:27 PM	Text Document	1 KB
kern.log	3/07/2010 10:57 A...	Text Document	2,422 KB
messages	2/05/2010 11:07 PM	File	78 KB
secure	25/04/2010 10:42 ...	File	0 KB
udev	2/05/2010 11:05 PM	File	352 KB
user.log	18/03/2010 10:13 ...	Text Document	1 KB

Figure 12 Log Files

Figure 12 Log Files is a copy of the var/log folder transferred over to windows. So, with this selection of files, you can grab a copy from https://honeynet.org/sites/default/files/files/sanitized_log.zip so you can view the same sanitised files.

The primary file in the collection is the auth.log file. The auth.log file contains all of the systems authorisation information, this includes user logins and any authentication attempts that were made.

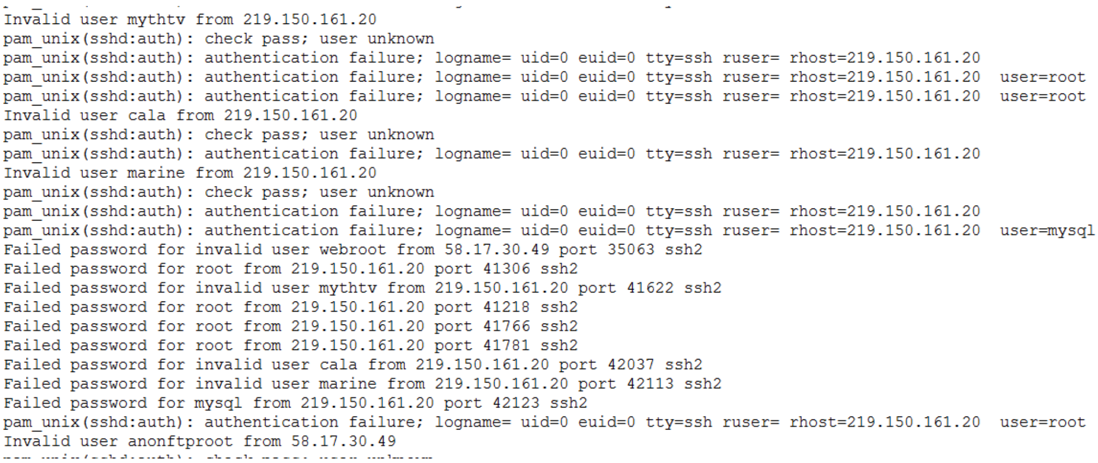
The log file we are looking at contains a lot of information, a quick scroll of the file indicates there is 102165 lines of log file to scan, this is a lot of information to review, during the scan, you will have noticed areas of the file like this:



```
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 55056 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 55469 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 55853 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 56302 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 56706 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 57129 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=61.168.227.12  user=root
Failed password for root from 61.168.227.12 port 57566 ssh2
Address 61.168.227.12 maps to pc12.zz.ha.cn, but this does not map back to the address - POSSIBLE BREAK-IN ATTEMPT!
```

Figure 13 Auth.log Capture 1

And



```
Invalid user mythtv from 219.150.161.20
pam_unix(sshd:auth): check pass; user unknown
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20  user=root
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20  user=root
Invalid user cala from 219.150.161.20
pam_unix(sshd:auth): check pass; user unknown
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
Invalid user marine from 219.150.161.20
pam_unix(sshd:auth): check pass; user unknown
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20  user=mysql
Failed password for invalid user webroot from 58.17.30.49 port 35063 ssh2
Failed password for root from 219.150.161.20 port 41306 ssh2
Failed password for invalid user mythtv from 219.150.161.20 port 41622 ssh2
Failed password for root from 219.150.161.20 port 41218 ssh2
Failed password for root from 219.150.161.20 port 41766 ssh2
Failed password for root from 219.150.161.20 port 41781 ssh2
Failed password for invalid user cala from 219.150.161.20 port 42037 ssh2
Failed password for invalid user marine from 219.150.161.20 port 42113 ssh2
Failed password for mysql from 219.150.161.20 port 42123 ssh2
pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=219.150.161.20  user=root
Invalid user anonftproot from 58.17.30.49
```

Figure 14 Auth.log Capture 2

Figure 13 Auth.log Capture 1and Figure 14 Auth.log Capture 2 indicate that there was a lot of attempts to get into the system, both of which take up a majority of the log file, so to find any useful information we need to eliminate or hide repeated lines. To do this, we can use a free piece of software called highlighter; https://www.fireeye.com/services/freeware/highlighter.html . Use this program to open up auth.log. Using this program, we can clean up the log file by removing redundant information, this information is:

- Invalid user
- Failed password for invalid user
- Authentication failure
- User unknown
- Check pass; user unknown
- Failed password for root from
- Failed password for
- Session closed for user
- Session opened for user root
- POSSIBLE BREAK-IN ATTEMPT

Each of these lines are providing information in the log file about what occurred, but they don't supply the right type of details. After removing the lines from the log file which contained the above key phrases, the log file has significantly dropped in size from 102165 lines to 1520.

Next, what we start looking for is indicators of compromise, as we've managed to clear up quite a bit of the log files that would be classified as redundant information, unless we need to do more statistical research.

Now we look for potential breaches. Using the highlighter program, select the term "Accepted password for root" and highlight all incidents of this. This indicates 28 items where this has occurred, and as such, the log file records what has been occurring around those logins. There are IP addresses that could be blacklisted, for example here are a few lines that were in the log file:

- Accepted password for root from 121.11.66.70 port 33828 ssh2
- Accepted password for root from 122.226.202.12 port 40209 ssh2
- Accepted password for root from 61.168.227.12 port 43770 ssh2
- Accepted password for root from 188.131.22.69 port 1844 ssh2
- Accepted password for root from 190.167.74.184 port 60992 ssh2

If the IP addresses are not known to be safe, then there is a high probability that each one of those addresses are external attackers getting into an already compromised system.

Another line to check for is new user. This then lets you track down the accounts that have been created, and if they weren't created by the admin, you know they are dummy accounts. Here are a few examples from the 11 new user accounts:

- new user: name=wind3str0y, UID=1004, GID=1005, home=/home/wind3str0y, shell=/bin/bash
- new user: name=fido, UID=0, GID=1004, home=/home/fido, shell=/bin/sh
- new user: name=messagebus, UID=108, GID=117, home=/var/run/dbus, shell=/bin/false
- new user: name=dhg, UID=1003, GID=1003, home=/home/dhg, shell=/bin/bash

Another aspect is to check if anything has been installed. As the primary technician on a server, you would be responsible for installing and maintaining a server structure, so when you see elements being installed onto the system, then there is cause to be concerned. Below are a few lines that show installations that occurred:

- sudo: root : TTY=pts/1 ; PWD=/home/dhg/psybnc-linux/psybnc ; USER=root ; COMMAND=/usr/bin/apt-get update
- sudo: root : TTY=pts/1 ; PWD=/home/dhg/psybnc-linux/psybnc ; USER=root ; COMMAND=/usr/bin/apt-get install alien
- sudo: root : TTY=pts/1 ; PWD=/home/dhg/eggdrop1.6.19 ; USER=root ; COMMAND=/usr/bin/apt-get install tcl8.4 tk8.4
- sudo: root : TTY=pts/1 ; PWD=/home/dhg/eggdrop1.6.19 ; USER=root ; COMMAND=/usr/bin/apt-get install tcl8.5-dev
- sudo: root : TTY=pts/1 ; PWD=/home/dhg/eggdrop1.6.19 ; USER=root ; COMMAND=/usr/bin/apt-get install eggdrop

As you can tell by looking at the new user accounts and software that was installed, the account dhg, the network is not looking so secure anymore.

In summary, the best logging technique is to log everything, but then learn how to filter out the additional noise in the log file when determining what is relevant to the current situation. This pattern mining technique is generic and will work on most system log files, though just know that each location will have specific items that should examined for, i.e. email system compromise, web system compromise and so forth.

6.6 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: ORGANISATIONAL NETWORK INFRASTRUCTURE

Network infrastructure is the physical and logical aspects of the components that define a network. Ensuring that both areas are protected and secure are critical to any network. There are a number of areas in which a threat can effect an entire organisation, here are 3 such threats:

- Deliberate threats; these are the threats that are being purposely aimed at the network, such as viruses, malware, Trojan horses, hacker attempts, social engineering
- Environmental Threats; these particular threats are out of the control of any network administrator, items that fall into this category are fires, floods and other natural disasters.
- Accidental threats; an accidental threat is normally an issue that has occurred without anyone actually meaning for it to occur, items such as this would be like a user accidently removing files, renaming files and changing information that should not have been changed.

Dealing with these threats are aspects that should be determined during the evolution of the network. Environmental threats are capable of eliminating entire physical networks and data, as such, the primary method of ensuring that information is kept secure during such an event is to ensure that the information of a company is stored safely away from a single point of impact. This can be as simple as having rotating tape backups that are removed on a daily basis and stored in a different part of the city, or to a more common variation nowadays is the implementation of cloud based backups of data. The distributed method of cloud based storage is perfect for ensuring that data will not get lost or destroyed in a singular event.

Accidental threats are human error. This is always bound to happen within an organisation and the larger the organisation, the more likely it will occur. The best way to ensure that the effects of this are minimised is to enable specific methodologies of data recovery. A very simple way of ensuring that end user's data is kept safe, is to have the end user save their data into a remote folder on the server. I.e. in this manner, with GPOs, it is possible to map the end users folder structure to the server, so, instead of the user have having a file structure for the documents folder like c:/users/%name%/documents the documents folder would be mapped to \\serverName\%user%\documents. The server would have versioning control, so that if the end user accidently re-wrote a particular file, it would be possible to go back a version to recover missing data. And, the server would be maintaining backups to a tape and synchronisation to a company cloud solution, such as Onedrive or Dropbox.

Deliberate threats are the main reason as to why security of networks becomes paramount. Simple steps can be done to prevent all but the most determined attack. These steps are:

- Education; educating an employee on how to safely use email and websites, i.e. don’t click on a link you don’t know or wasn’t sent by a trusted source. Do not install applications unless authorised, social engineering works in the following manner, always get a manager to assist when allowing access to the network for an unknown person.
- Anti-virus/Anti-malware; These systems should be implemented and updated on all machines. Monitoring of this type of software is also important, as most enterprise variations allow for a centralised management suite, so if a single machine didn’t receive the latest updated software, this updated could be pushed to the client.
- Group Policy Objects (GPOs); From a server point of view, restricting what can be occurring on a desktop machine can be critical in ensuring that an end user won’t be able to accidently infect a machine by installing random software is important. Also locking down aspects of what the user can and cannot do, will ensure that uniformed end users won’t make system causing mistakes.
- Access levels; these levels can be implemented using GPOs. Once implemented, you will be able to have areas of a network that a user won’t be able to access. For example, if the client is a car yard, the mechanic who requires only email and access to specialised software, doesn’t need access to accounting files and as such, using a GPO, this type of security can be implemented.
- Physical Security; This is where servers, switches, routers and other network components are locked away in secure areas to ensure that no one can just access them. Locked doors, lockable cabinets are all good ways of implementing this.
- Logical Security; This is where network components can be configured to only allow known machines, switches and routers can be locked down to mac addresses. So no one can just plug a machine into the network and get access. VLANs would be implemented to segment the network ensuring that a shared resource such as internet connection can exist, but machines that belong in accounting or finances in general can’t be seen by a client accessing the wireless network.

Locking machines and networks down is a great way to ensure that the system will maintain safety, but there also has to be a balance formed so that that end users will be able to get work completed with minimal to no hassle. An end user that has to always authenticate when talking to the server, will eventually stop trying to talk to the server and the data will be stored locally. This means that any implementation of security needs to be balanced with the work flow of the company.

6.7 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: CAPABILITIES OF SOFTWARE AND HARDWARE SOLUTIONS

Security solutions can be delivered in both hardware and software variations, a prime example of this is VPN technology. VPNs have the ability to be either hardware or software, i.e. you could have a router to router VPN tunnel which is a purely hardware designed security system, or you could have a client using a VPN client to connect to a VPN server, which is a pure software solution. And, like all things in the computing environment, you can have a mix of the technologies. Such as a client using VPN software to connect to a VPN enabled router.

Another area which is covered in both hardware and software scenarios are firewalls, as we know, firewalls allow for a layer of protection by denying attack vectors through differing ports. As such let's compare:

Hardware Firewall

- Speed; a hardware firewall is designed to be fast and as such it can handle multiple traffic requests at any one point in time.
- Security; Being designed for a singular action, a hardware firewall is locked up and the underlying operating system will have limited vulnerabilities to be exploited.
- Interaction; Once the hardware firewall is configured and set up in the network, it is an isolated element. This isolation means that it does its task and doesn't interfere or manipulate any other aspect on the network.

Software Firewall

- Ease of use; software firewalls are normally configured with user friendly gui's that allow the end user to quickly and easily configure the firewall.
- Flexible; With the advanced interface, software gui's have the ability to be extremely flexible in what they block and how they achieve certain tasks.
- Control; combined with ease of use and flexibility, the software firewall allows the end user to configure and control the firewall settings extremely well.

Things to consider when looking at either a software or hardware firewall, what is it protecting? If it is a single machine, then a software solution works well enough, if there is more than one machine, then a hardware solution is something to consider. Of course, the best solution, and the one that is most common in the industry is the combination of both hardware and software. A normal internet router will come with its own firewall solution built in, which can be configured via the routers web interface, of course it is only designed for low end connection amounts, where as a medium to large business, should be considering a dedicated hardware solution to sit between the internet and intranet. Figure 15 Firewall Network indicates where the firewall sits inside the network.

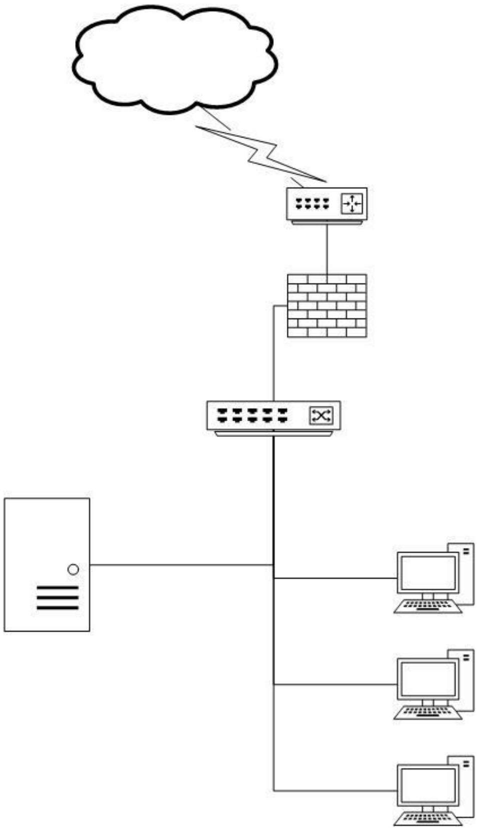


Figure 15 Firewall Network

In all cases, a hardware solution for security is going to be the fastest and most secure, though like any choice for a business, it will come down to the client's desire to spend money.   Companies like Cisco and Juniper are the leading hardware security solutions.

A drawback to software solutions is that if the underlying operating system is infected in anyway, it can be bypassed or overwritten, something that doesn't happen to hardware solutions.

6.8 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: GENERAL FEATURES OF EMERGING SECURITY POLICIES, WITH DEPTH IN SECURITY PROCEDURES

Depth in security, can be treated as a defence in depth scenario. A defence in depth system is a system that has a layered protection around critical systems. So, when designing a security policy for a network, it is advised that there will be many layers of security before an attacker can access the critical data of a network.

As such you can look at a network in the following manner:

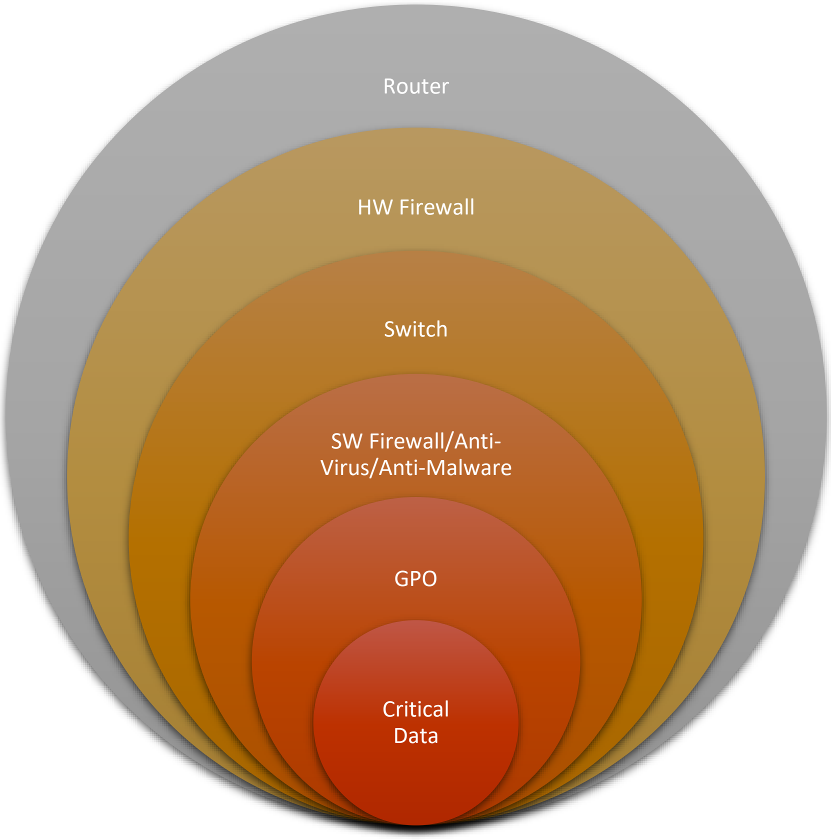


Figure 16 Security Layers

Figure 16 Security Layers represents the layers that an attacker needs to get through in order to access company specific details. Each of these particular layers should have a policy that is always evolving to meet the current threats that exist in the Internet.

When writing the policy for a particular layer, maintain the following document layout:

- Overview
  - The overview is effectively the same thing as the purpose but, not as detailed, for example, a document about dealing with a firewall, the overview could be written as: “This policy is designed to supply best practices for network security, focusing on firewall protection.”
- Purpose
  - A purpose allows for more detail than the overview. So, it would include aspects such as, which ports are left open and a brief explanation of each port, so continuing with the overview concept: “Ports 80(web) and 25(smtp) are being left open on the firewall to ensure correct internet traffic is being supplied to all individuals. Incoming traffic on 80 and 25, will talk to the web server and email server respectively.
- Scope
  - This relates to who the policy is aimed at, if it is aimed a certain department for the client or for the client’s entire business. For example: “All employees, contractors, consultants, temporary and other workers at <Name of client’s business> must adhere to this policy.”

- Policy
    - This is where the policy is stated with as much detail as needed. For example, part of the firewall policy could contain:
        - Firewall disables
            - IP directed broadcasts
            - Incoming packets at the firewall sourced with invalid addresses such as RFC1918 addresses
            - TCP small services
            - UDP small services
- Policy Compliance
    - Here in the document, the areas of where the policy implementation is being monitored, it's time of review and who is in charge of ensuring the policy is enforced. It will also state the potential disciplinary action on non-compliant situations.
- Related Standards, Policies and processes
    - Does the document form part of a larger collection of policies? This is where this information would be listed. For example, the firewall policy is a sub document of the Router/Switch network policy.
- Revision History
    - A simple table in the document, can be found at the end of the document or after the overview to allow for readers to understand how many changes have occurred to the document and how authorised the modifications.

As you can tell from Figure 16 Security Layers, the layers of security go from hardware through to software. Hardware updates are not as fast as software updates when it comes to meeting an emerging threat, as such the policy for covering software security layers should able to adapt and change as required. An example of how software adapts quickly, would be anti-virus software. If a virus has been discovered, a patch to eliminate and remove the virus normally is produced within 24-48 hours. Once the patch is created, a system should be updated and the patch pushed to client machines and each machine scanned. If a policy existed that required elements such as anti-virus updates to be tested, the time delay could potentially enable a network to be infected.

6.9 IDENTIFY AND DESCRIBE NETWORK SECURITY MEASURES, INCLUDING: NETWORK MANAGEMENT AND SECURITY PROCESS CONTROLS

Security process controls for network management is about establishing a consistent method to achieve a pre-determined output. For example, if you design a security policy in a GPO that states the end user needs to change their password every 60 days, then on the 60th day of an account, you would expect to see in the log files a lot of password changes.

When determining elements of security for network management, there are a few phases that need to be implemented, these are:

- Assess; This phase is all about determining the appropriate level of security needed for a network.
- Identify; This section is all about ensuring that the security policies that need to be implemented are in the correct place for the company and that each of the policies are viable and consistent with local laws.
- Evaluate and Plan; This phase is about confirming the pre-design work, ensuring that policies are elevated to the correct level and locating potential issues that will require a rework.
- Deploy; After the planning and identification has all been completed; this is the phase where the polices are deployed to the network.

Some areas in which security polices can be implemented are:

- Physical computer security
  - Computers are kept secure, this can be done in a multitude of ways, locked rooms, attached to desks, monitored security cameras. Key card access to labs or office equipment.
- Network security
  - Network security is where there is hardware designed to keep out intruders, such as firewalls, intrusion detection systems (IDS), vpn, vlan, anti-virus, anti-malware, group policy objects (GPOs), username/password combinations, file security and so forth.
- Data security
  - Securing data is achieved by implementing secure and authenticated file systems, having software protect the data, ensuring that backups both onsite and offsite are taking place. Enabling authentication of users and folders, implementing version control for critical documents.
- Contingency and disaster recovery plans and tests
  - These policies are planned responses to potential identified threats to a network. So, what happens during a fire/flood/earthquake/building disaster? Where is the data stored? How do you recover this information, what's the timeline on getting the business back on its feet? The creation of these plans and policies are designed to get a business back on its feet after a disaster.
- Computer security and awareness training
  - Education of users is critical as attacks of a social engineering nature can be removed through the proper education and identification of what and how these types of attacks can occur. This training will also limit the amount of potential virus and malware infections that can occur due to users not blindly installing applications.
- Security management and coordination policies
  - Policies of a security nature and coordination allow for a business to enhance the general security of a network. These policies inform and control the response to any particular incident.
- Compliance of software
  - By ensuring the compliance of software as a policy this enables systems to be updated through network management to ensure that

any vulnerabilities that are discovered are dealt with in a timely manner. An aspect of this is also ensuring that all systems in place in a network are the same, for example, if a company is using Office 365 as its default implementation of an office suite then word's default saved document is a docx, having a small part of the company implementing word 97 .doc documents shouldn't occur as the company on a whole is using the current standard. By ensuring compliance, this mismatch of file formats would not occur.

During the identification phase, each of the above listed notes should be areas in which identification and planning should take place.

As you can see, securing a network is more than just flipping few switches, as such there are quite a few areas that need to be examined and delved into to ensure that a network you manage is secure. The primary aspect of implement a s security process control is to ensure that the output at the end of its implementation falls within an expected range. Anomalies outside this range are indicative of areas that require further investigation and as such, might be indicative of a potential system attack.

6.10 EXPLAIN NETWORK SECURITY IMPLEMENTATION RISK MANAGEMENT PLANS AND PROCEDURES, INCLUDING: NETWORK SECURITY PLANNING

Planning network security is an obligation of a network administrator. There are a couple of ways of looking at it, but the primary reason is that the more secure a network is, the less time an administrator will spend putting out fires and be able to concentrate on ensuring that the network performs and grows to handle the load of the organisation. If an organisation is always running up-to-date anti-virus software and the endpoints are designed to prevent incoming attacks, then small outbreaks of virus infections within the network should be limited quite a bit, if not eliminated from occurring and this overall, is good for business. A network is a critical tool for allowing an organisation to create a profit and the longer a network or element on a network is down, then an organisation is wasting money, this in general is always a bad thing.

Security planning, at the end of the day, indicates documentation. As this documentation will need to be used by many other people within the organisation, as such when planning out the security, there are some areas that need to be examined.

Areas within a security plan:

- Security risks
    - A listing of potential risks that can occur. Physical and logical.
- Security strategies
    - Mitigation planning of the risks that were identified.
- Public access strategies

    - Determination of if the network infrastructure is to be shared with the public in anyway, an example of this is free wifi for clients that are waiting on a service the organisation is supplying.
- Authentication policies
    - What levels of authentication exist, password/username policies, does remote access into the network exist?
- Information security strategies
    - How is data secured? Is it encrypted? Does email and web traffic require encryption or special authentication policies applied to it?
- Administration policies
    - Monitoring of the network, ability to detect and resolve suspicious activity. A chain of command, so to speak, of where breaches and intrusion to the network are brought up.

Once these elements have been determined, the security policies need to be shared with all executive members of the organisation. This ensures that in case of a potential disaster, the plans and resolution procedures are well known and not restricted to a singular point of failure.

Network security planning documentation will have the following structure:

- Overview
    - The overview is effectively the same thing as the purpose but, not as detailed, for example, a document about dealing with a firewall, the overview could be written as: "This policy is designed to supply best practices for network security, focusing on firewall protection."
- Purpose
    - A purpose allows for more detail than the overview. So, it would include aspects such as, which ports are left open and a brief explanation of each port, so continuing with the overview concept: "Ports 80(web) and 25(smtp) are being left open on the firewall to ensure correct internet traffic is being supplied to all individuals. Incoming traffic on 80 and 25, will talk to the web server and email server respectively.
- Scope
    - This relates to who the policy is aimed at, if it is aimed a certain department for the client or for the client's entire business. For example: "All employees, contractors, consultants, temporary and other workers at <Name of client's business> must adhere to this policy."
- Policies
    - This is where the policy is stated with as much detail as needed. For example, part of the firewall policy could contain:

        - Firewall disables
            - IP directed broadcasts
            - Incoming packets at the firewall sourced with invalid addresses such as RFC1918 addresses
            - TCP small services
            - UDP small services

- Policy Compliance
    - Here in the document, the areas of where the policy implementation is being monitored, it's time of review and who is in charge of ensuring the policy is enforced. It will also state the potential disciplinary action on non-compliant situations.
- Related Standards, Policies and processes
    - Does the document form part of a larger collection of policies? This is where this information would be listed. For example, the firewall policy is a sub document of the Router/Switch network policy.
- Revision History
    - A simple table in the document, can be found at the end of the document or after the overview to allow for readers to understand how many changes have occurred to the document and how authorised the modifications.

In addition, depending on what the policy is specifically about, then appendices and images can be implemented through the document to ensure ease of reading for non-technical individuals.

6.11 EXPLAIN NETWORK SECURITY IMPLEMENTATION RISK MANAGEMENT PLANS AND PROCEDURES, INCLUDING: IMPLEMENTATION

Implementation of plans, the stepping stone to finalisation of a project, well, not quite as there is always maintenance for projects. But implementation is critical to ensuring that the designed plans for network security are valid. When dealing with network security, the risks can be great, attackers have the ability to eliminate all stored data of an organisation, or hold that organisation for ransom depending on the attack that was employed.

To eliminate potential risks, the planning of risks need to be implemented, a well thought out plan allows for various resolutions to be created based upon a singular concept. For example, late 2015 and early 2016, there have been multiple hospitals in the USA that have been held to ransom due to allowing malicious software into the network and preventing the hospital administration the ability to recover and access data. Ransomware is a reasonably new threat that has shown to be highly effective in generating a large amount of risk for organisations. Mitigating this particular risk, can be done by the following implementations:

- Software solutions
    - Operating Systems
    - Anti-virus / Anti-malware
    - Application patches
- Hardware solutions
    - Firewall
    - IDS
- Monitoring
    - Log files for network traffic
    - Log files for authorisation attempts

As discussed through this learning guide, effective implementation of risk management is to be pro-active in monitoring network capability and traffic, reporting and examining any anomalous activity and ensuring all computer network equipment is kept up to date.

To ensure that implementation is done correctly, testing of the systems need to occur. If there is a potential risk of a Distributed Denial of Service attack, then, after work hours. A simulated response technique should be implemented. So, moving from one net connection to another, determining the time it takes to block specific IP ranges, hardening up endpoints and the like. Testing an implementation is critical to ensuring its value to the end user. And, all networks are unique in what they need to serve to the organisation that implements them, this is the area that needs to be tested to ensure it is a viable solution.

6.12 EXPLAIN NETWORK SECURITY IMPLEMENTATION RISK MANAGEMENT PLANS AND PROCEDURES, INCLUDING: COST ANALYSIS AND BUDGETING.

To conduct a costing, this would occur after the network has been selected, with the segment resources already being determined. Once this has been done, then comes the part of sourcing the material, supplies and services.

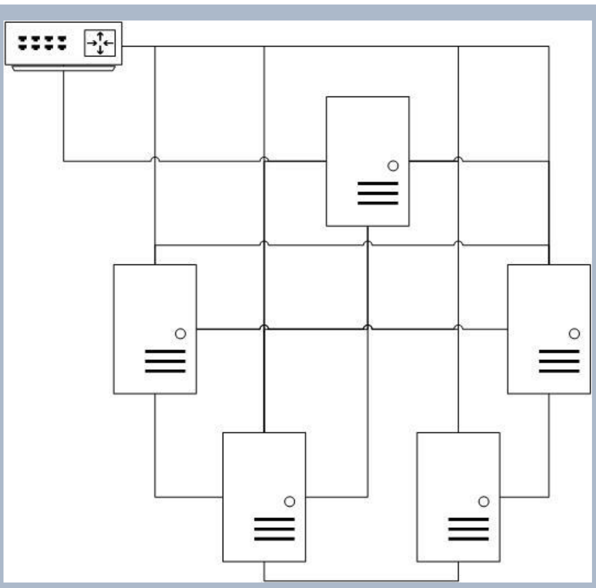
Recall that the topologies mainly used now days are star, mesh and tree. A quick review, star is your standard LAN layout with all of the hosts connecting to a singular point in the network, which is primarily a switch. This switch can be used to segment the LAN into different VLANs as required, but it is an intelligent device that can handle broadcasts and collisions correctly. A mesh topology is where all of the devices are connected to each other, which if course, will increase the cost of implementation. Depending on the need this can be quite useful if you need to generate a redundancy within the network for large amounts of data. Finally, the tree layout is a layout that connects star topologies to a singular backbone line; Ensuring that all LAN segments are responsible for the collisions and traffic in each segment without effecting other star branches, but still enabling data transfer from one star topology to another.

Let’s delve into breaking down each of these topologies into real world scenarios. First, let’s look at a mesh topology from the perspective of an enterprise sized business.

Example: Mesh Topology

Enterprise sized business which deals with the stock market, they data scrap the system and collect data, and this data is then used to implement changes for their clients. To ensure that they have maximum uptime and redundancy for the data they have collected, the have implemented a mesh topology in the server room.

The company has 5 servers dedicated to the data scrapping. The topology would look like this:



With each server having 5 network links, 4 to the other servers and 1 to the switch. In this example, let’s assume that everything is close to each other to make wiring reasonably easy.

With this in mind, let’s look at the break down for this topology. Prices are generalisations.

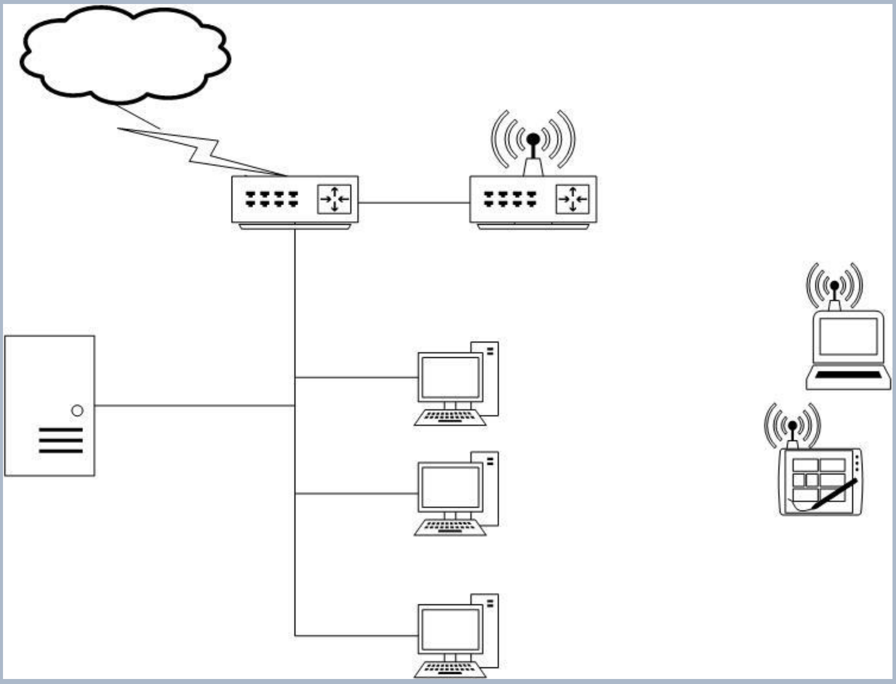
	Item	Pricing	Total Pricing
Mesh Topology	Servers x 5; custom build, high end (5 GB NICs each)	$77,000each	
	Cable 2m x 16	$100	
	Switch	$500	
	Patch Panel	$50	
	Rack	$200	
	Labour to Install and Configure	$5000	
	Software (Operating System, firewall, etc.)	$20,000	
			$410,850

Mesh topology designs and implementations are expensive, the server generalisations contained specialised NICs that contained 4 ports at GB speeds, and each card was approximately $1500. When doing costing, always remember to add in the potential labour cost of the installation. In this case, the mesh network was all taking place in a single room; if a mesh network was expanded to multiple machines spread throughout a building, the cost would dramatically increase.

Star topologies are the most common topology, this is the topology designed with a central device that handles communication between host machines. Assuming you have multiple devices hooked up to the one internet connection at home, you are running a star topology. Let's look at an example of a simple star topology.

Example: Star Topology

In this example, we will look at a small office that contains a server, 3 workstations, 1 laptop and 1 tablet that connect to the network. It has a single ADSL 2+ connection which feeds into a wireless router.



As you can see from the diagram, all of the devices connect to a single device that then enables them to communicate with each other and to the Internet. The method of communication is both wired and wireless, the medium of data transmission is irrelevant to the logical network topology.

With this in mind, let's look at the break down for this topology. Prices are generalisations.

	Item	Pricing	Total Pricing
Star Topology	Server	$8,000each	
	Cable various lengths x 5	$50	
	Wireless Switch	$200	
	Labour to Install and Configure	$500	
	Software (Operating System, firewall, etc.)	$500	

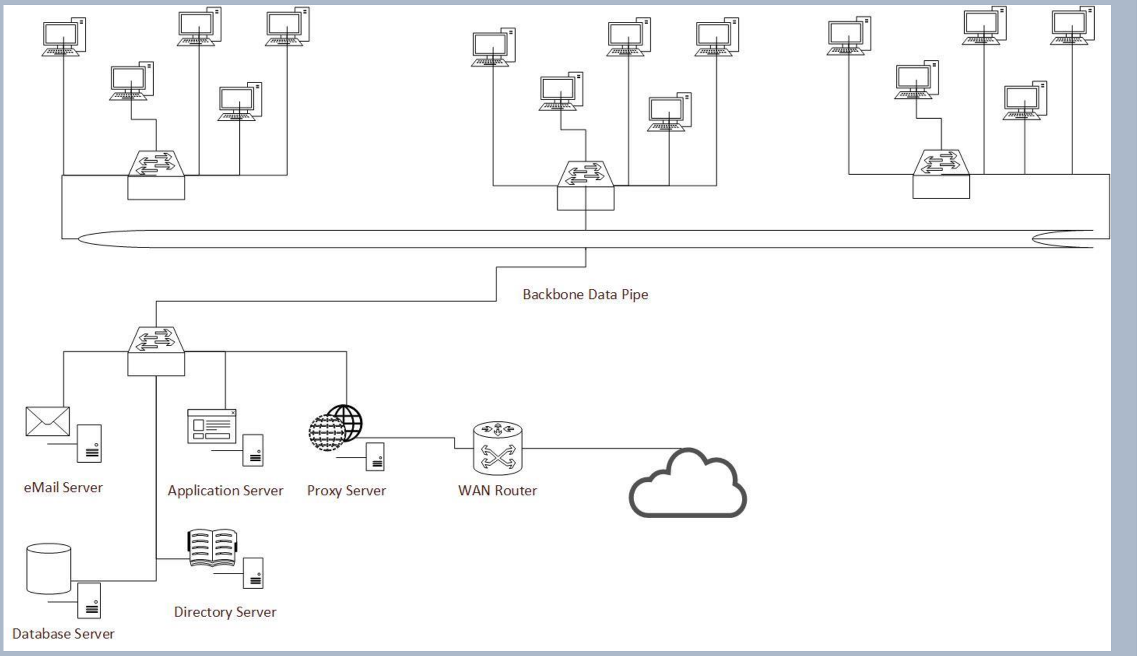
			$9,250

The primary advantage to this particular network, is that devices can be added or removed without disrupting any other host on the network. This flexibility has allowed for Star topologies to be the prominent network topology in the industry.

The final topology to examine is the tree topology. This is a singular backbone that has star networks coming off it. Large institutes like universities or colleges would have this, as would most large businesses. The main advantage of this is that every host has access to all of the core resources of the network, and yet the individual segments can be used to handle collisions and internal broadcasts.

Example: Tree Topology

In this example, we will just examine the overall concept of the network and make some pointers in where items would be purchased.



As you can see form the diagram, there are 4 sections to the network, each segment is a star topology connected to a singular backbone link. Each section is capable of being taken off the network without disrupting other hosts, items such as the application and database servers can be run through VLANs for specific segments which in turn would introduce an internal security system.

The way you would plan and cost this is to calculate each segment separately and then introduce the backbone pipe in to the network, to establish the linkage for the network. A better solution than the above diagram would be to have each of the services feed into the back bone separately instead of through their own network segment. But for illustrating a tree topology, this shows how you can implement such a design.

There is a lot that can be done and costed for the different topologies, so, when deciding a topology make sure that it works with the network options that the client has, with ensuring that the plan will fall into the client's budget.

Activity: Determine and design a topology with costing.

You have been contact by a client to implement a network, they are a single office which is spread over two floors, if need be the floor space can run wiring solutions. All staff members require access to the file/print/database/proxy servers that are stored on the 2nd floor. There are 40 employees in the office, and each have phones and tablets in which they are allowed to connect to the network to use the resources.

Generate a table containing the estimated resources and topology used.

Topology	Item	Pricing	Total Pricing

Queueing constraints are something to consider when working on costing out a network. The constraints are based upon the amount of data that can be pushed through a network, and hence determining its scalability. For a more in depth examination of queueing networks, read the paper "Queuing networks with population size constraints (http://www.cs.utexas.edu/users/lam/Vita/Jpapers/Lam77a.pdf).

To make it easier to work with, we can use the calculations we have previously looked at to understand how a network would handle data loads.

If we are running a 1GB network with 1ms latency and a standard 64Kb packet size then, the following would be expected:

	Latency	Calculation	Bits per second	MB/s

Internal Network	1	524288/0.001	524288000	524.29

This is the theoretical optimum network speed, and this is per second transmission with no collisions. Now days, most machines and switches are bought with GB adaptors, this allows for the tremendous speeds of transmissions you can see.

When working on scalable networks, you take a base amount of traffic and then increase it to see what level the network can no longer handle the traffic at optimum speeds. For example, if the network was transmitting less than 524MB a second, then a GB backbone is sufficient, if the network needed to transmit greater than 524MB per second, then the backbone needs to be increased. A single GB network, would be ramped up to a 10GB network, in this way not only would it cover a much greater throughput but also allow for some future growth on transmission size.

Budgeting for a network, with a focus on security is indicative of putting resources at the gateway of the network, as such, it will be expensive as the devices that are designed to handle high end attacks are highly specialised.

When dealing with cost analysis for a network design, there are a couple of areas that need to be examined, these are the direct costs and the indirect costs, below is a couple of lists covering both those areas:

Direct Costs

- Computer equipment
- Communication equipment
- Common carrier line charges
- Software
- Operations personnel costs
- File conversion costs
- Facilities costs (space, power, air-conditioning, storage space, offices,etc.)
- Spare parts costs
- Hardware maintenance costs
- Software maintenance costs
- Interaction with vendor and/or development group
- Development and performance of acceptance test procedures and parallel operation
- Development of documentation
- Costs for backup of network in case of failure
- Costs of manually performing tests during a system outage
- Security and control
- Personnel

Indirect Costs

- Personnel training
- Transformation of operational procedures
- Development of support software
- Disruption of normal activities
- Increased system outage rate during initial operation period
- Increase in the number of vendors

As you can see, there are a lot of areas in which the total cost of ownership (TCO) fall into play. In most networks, there is a singular budget that will encompass aspects such as IT. This budget is designated to covering all of the points listed above, and in some cases, the system is going to less than perfect due to the limited amount of money that will be spent on it. In some cases, the requests are more than the budget, and as such, compromises need to be made. In some cases, it might be possible to loan from the next year's budget, this is dependent upon the client.

Example: You've been requested to do a cost analyse on the following budget plan.

- **Budget: $35,000/year**

Requirements: 2 x Servers ($5,000), 10 x Desktop ($1,500), Software – Desktop ($800 per machine), Software – Server ($2,000 per machine), Hardware firewall ($600), IDS ($1200)

Calculate costing:

Item	Element Cost	Amount of Items	Cost	Overall
Server	**5000**	**2**	**10000**	
Desktop	**1500**	**10**	**15000**	
Software – Desktop	**800**	**10**	**8000**	
Software – Server	**2000**	**2**	**4000**	
Firewall – Hardware	**600**	**1**	**600**	
IDS	**1200**	**1**	**1200**	
				38800

As you can see, from the quick calculations, there is going to have to be compromises made in the system. As without adding elements such as training, installation, maintenance the budget has already been surpassed.

In the industry, this is where you would analysis the systems in depth, as in do all machines require that specific software? Does the company need a hardware firewall, if they run an IDS? Can the server software be modified and still maintain the correct stability the client is after?

References

There are no sources in the current document.