

David Price P131188 Network Operating Systems And Security Report

by David Price

FILE	4305_DAVID_PRICE_DAVID_PRICE_P131188_NETWORK_OPERATING_S YSTEMS_AND_SECURITY_REPORT_113613_1566645976.DOCX		
TIME SUBMITTED	23-MAY-2018 04:13PM (UTC+0100)	WORD COUNT	3047
SUBMISSION ID	89801250	CHARACTER COUNT	18595

Network Services

**Networking Operating Systems and
Security Report**

M2X8522

Student: David Price

Student number: P131188

Lecturer: Dr Tim Bashford

Table of contents

Table of Figures	3
Introduction.....	4
Background Research	4
Threats.....	6
Denial of Service (DoS)	6
Rogue DHCP Servers.....	7
ARP Spoofing	8
Packet Sniffing	9
Password Cracking.....	10
Conclusion	11
References.....	12
Bibliography	13

Table of Figures

Figure 1 - A diagram of a simple network[4].	4
Figure 2 - Various threats and their implications[7].	5
Figure 3 - Overview of an DoS attack [9].	6
Figure 4 - Rogue DHCP Server attack[13].	7
Figure 5 - ARP spoofing[15].	8
Figure 6 - Packet sniffing in practice[17].	9
Figure 7 - Possible password attacking threats[18].	10
Figure 8 - Estimated time to brute force a password[20].	11

Introduction

This report will analyse scenarios that are considered risks to security of a computer network and outlining these risks with recommendations of how they may be prevented, defended against and consider what cracking tools can be used to help against these risks. Included in this report there will be a brief overview of the common security risks listed and what they do and how they work particularly efficient when attacking a computer network. There will be literature pertained to this field of work which will show more clearly of what occurrences may happen to a computer network that is affected by those considered risks.

Background Research

Network security is vital in society today as networks is used to share sensitive data and resources through nodes inside the network, to prevent any wrongdoing inside the network, governing bodies are there to set restrictions and policies in place that businesses must adopt to prevent any unauthorised access to that data being shared amongst varied nodes within the network. Network security at its core is where “a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses” [1].

Achieving a secured network is important, “it is crucial for organizations to define why they want to achieve computer security to determine how they will achieve it” [2]. The challenging section is there are a vast amounts of local area networks in all different institutions and home where these local area networks are connected to the outside nodes within a network via gateways and wide area networks, by the lack of security within these network that are sharing data and resources, remote computers can use varying methods to retrieve the data being shared. There will be discussion about the types of methods used in this attack in the later section of this report.

The local area network is usually connected to the following:

- Network gateways which gives access
- Network communications
- Network control resources
- Network routers
- Network resources, e.g. databases[3]

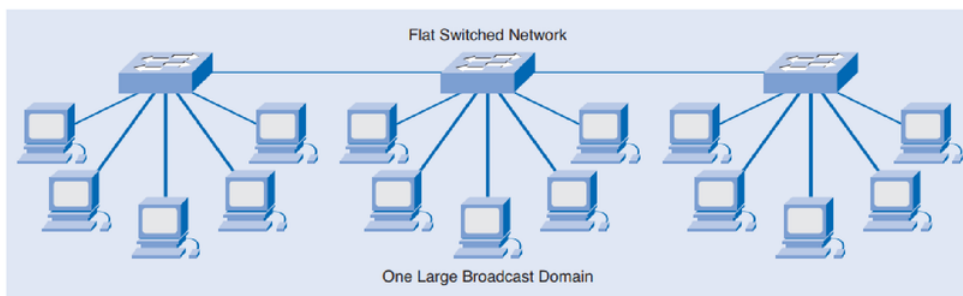


Figure 1 - A diagram of a simple network[4].

A vulnerable implementation of a network in which the administrator hasn't been sufficient in which how the network has been initialised is a major underlying cause which allows the

perpetrator to identify weakness within that network to gain unauthorised access. Essentially network vulnerability “is a flaw in the design or implementation of an information system that could be intentionally or unintentionally exploited to adversely affect an organization’s operations or assets through a loss of confidentiality, integrity or availability” [5].

Vulnerabilities can be found in some software such as the operating system, application software and control software[6], regarding these potential weaknesses within a computer they are usually down to human factors rather than computer or software factors. A network is more likely to be vulnerable caused by the human administrator rather than the software to implement the network.

Threat	Domestic/Foreign	Threat Consequences
E-mail containing virus	Foreign origin, domestic use	Can infect system’s reading email and subsequently spread throughout the organization.
Network Virus	Foreign	Can enter through unprotected ports and affect the entire network.
Web-based viruses	Internal views of external sites	Can affect the system that does the visit and then also affect other internal systems.
Attack on the server	Foreign	If the server is compromised by a hacker he can gain access to internal network systems.
Service rejection attacks	Foreign	If the router is attacked the entire network can fail and external services such as web, email and FTP can be cumbering.
Network User Attack (internal employee)	Internal	Traditional firewall network edge can prevent the attack. Internal segmentation firewalls can help internal damage.

Figure 2 - Various threats and their implications[7].

Threats can harm a network in all different manners, they can range from internal to external attacks. This report will look at the more common attacks a perpetrator might attempt but the attacks vary in how they gain access and what they are able to retrieve once access is gained.

There are ethical penetration tools such as ‘Kali Linux’ which allows ethical hackers to use to penetrate applications which allows them to identify potential weaknesses within a system, within Kali are the same tools that unethical hackers use to steal sensitive data and gain unauthorised access to system/networks in the real-world, whereas these ethical hackers use these tools behind closed doors before an application/network/systems is available to the public where the unethical hackers get their hands on it. Using ethical penetration tools to

identify weaknesses which show what needs to be fixed is vital for a business as it can save them money and embarrassment in the future if their application is hacked in to, it can become very detrimental to the business and their image, ethical hackers can resolve this problem if the potential threat is found quickly and efficiently, more importantly before a hacker gets there, this is vital that the ethical hacker finds weaknesses first.

Threats

The previous section briefly looked into how a computer network can be infiltrated and the components of a network which connects and shares data which the perpetrator is trying to gain access to, this section will consider some of the possible methods and tools an attacker would use to try to gain unauthorised access.

Methods this report will consider are as followed:

- Denial of Service
- Rogue DHCP Servers
- ARP Spoofing
- Packet Sniffing
- Password Cracking

The following sections will consider how each of these methods will work and how to prevent their infiltrations and attacks, also through illustrations will give a clearer insight into how the attacks are initialised and how they are finalised.

Denial of Service (DoS)

Firstly, Denial of Service or (DoS) attacks are used on a network structure to essentially take a server offline or to slow it down this is achieved by sending vast amount of data packets requests which can range in the millions, the attack itself is simple as the tools needed to perform a DoS attacks are available to download on the internet so anyone is capable to use it. The purpose of this type of attack is to consume the victims' resources, this can be things like "network computing and service performance, such as link bandwidth, TCP connection buffers, application/service buffer, CPU cycles"[8]. DoS is a high-volume tool which penetrates systems that have limited resources to handles such high volume of data.

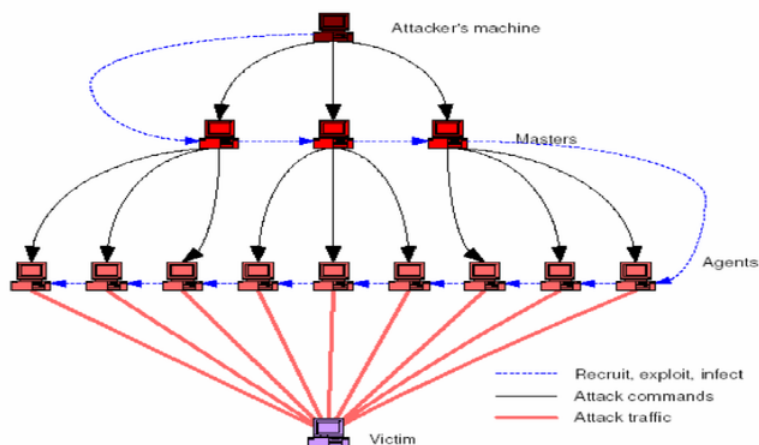


Figure 3 - Overview of an DoS attack [9].

The consequences for this attack are troublesome:

- Harmful for an institution in which relies on a server being online
- Immediate impact to the victim/business
- Costly to fix

There are many prevention techniques against this type of attack, by adjusting certain aspects of their system or network can stop these very subtle but harmful attacks. The main “DDoS defence system is to relieve victim’s resources from high volume of counterfeit packets sent by attackers” [10]. Some methods/tools that can help prevent or completely discontinue the attack are as followed:

- Adjustment of firewall settings
- Null route the target
- Network behaviour analysis
- IPS software threat prevention

These methods/tools listed will prevent and limit the damage caused and stop any more damage being inflicted which then allows time for the server to restart or for it to be fixed entirely depending on the amount of damage that has been caused.

Rogue DHCP Servers

Secondly, Rogue DHCP Servers is a server within a network that has an administrator of the network has no control over, DHCP allows devices to obtain an IP address dynamically once connected to the network. “This service automates the assignment of IP addresses, subnet masks, gateway and other IP networking parameters” [11]. The attacker will act as the DHCP server which then can assign wrong default gateway, wrong DNS server and wrong IP address to the connected devices. By having a device connected to these applications which are wrong will allow the attacker to gain unauthorised access to devices data and resources, “a rogue DHCP server might be able to redirect traffic to another site” [12].

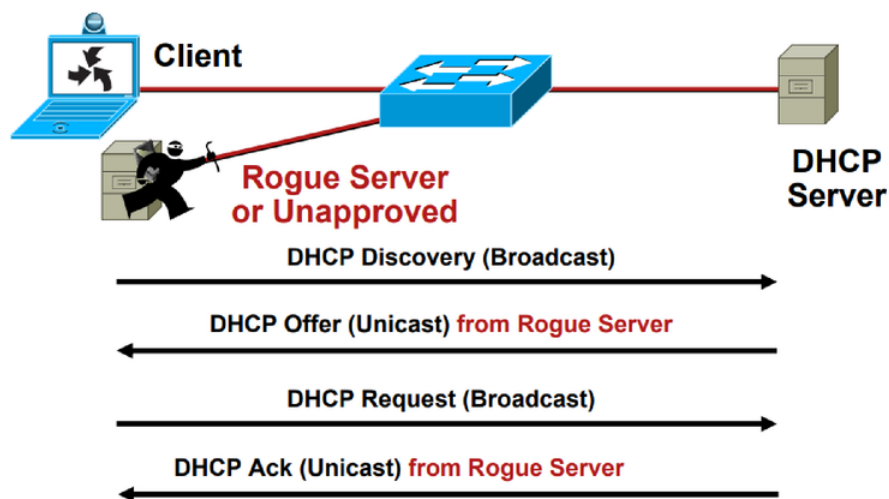


Figure 4 - Rogue DHCP Server attack[13].

There are tools available to identify the rogue server within the network, these tools will help identify and prevent any more damage or unauthorised access to data and resources, such as:

- DHCP snooping which drops traffic that deemed to be unstable or unacceptable
- DHCPDump to find IP address if there are no snooping on the switches within the network
- Temporarily disable the DHCP server and connect a device and follow the route to what server it reaches to identify the rogue server
- “Rogue DHCP servers can be mitigated by DHCP Snooping features”[13]

This attack is essentially a ‘man in the middle’ attack, in which the attack alters and hides behind someone or something else and acts unethically, more commonly used for eavesdropping which neither party knows what is happens.

ARP Spoofing

Thirdly, ARP Spoofing is an attack that works in conjunction with how ARP protocol is used, ARP protocol is the way to map IP address to specific hardware by linking them, operating below the network layer. ARP spoofing is where it sends inaccurate ARP protocol messages over a network, this allows the process of obtain device MAC addresses and pairing them with a IP address of another device within the network. “ARP spoofing involves constructing forged ARP request and reply packets. By sending forged ARP replies, a target computer could be convinced to send frames destined for computer A to instead go to computer B.”[14].

ARP spoofing allows the opportunity of other attacks to be initiated, such as a DoS attacks. ARP spoofing gains access to which then other malicious attacking software can be used, these attacks are:

- Denial of Service (Dos)
- Man in the middle (MITM)

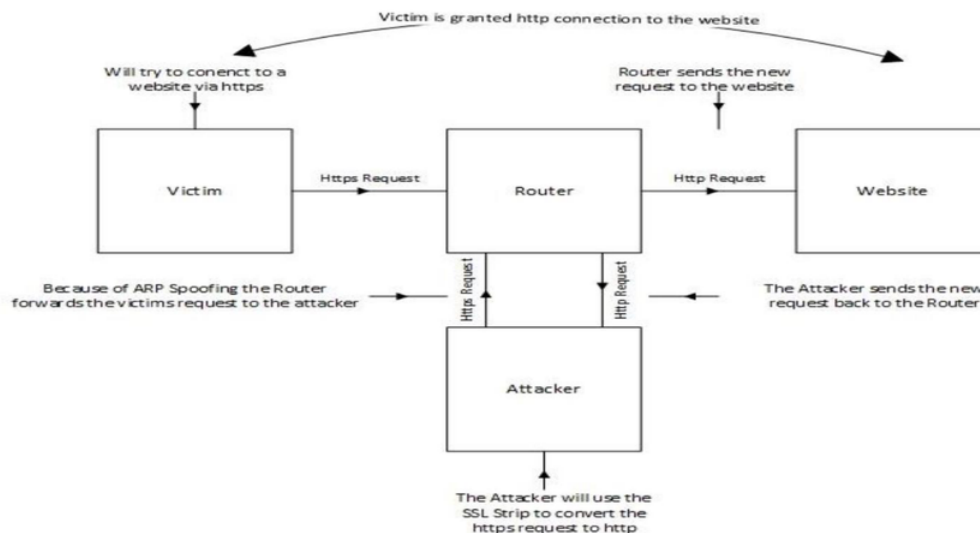


Figure 5 - ARP spoofing[15].

The steps taking when ARP spoofing has been successful on the attackers' end is to try and prevent any wrongdoing and stop the attack from happening, there are methods used for ARP spoofing for detecting and stopping the attack, such as:

- Enabling MAC binding on the switch
- Static routes, spoofed ARP replies wouldn't be noticed

Detecting the spoofing is the other major way of identifying the attacker and where it is coming from etc, there are plenty of free programs available to download over the internet which monitors ARP replies over a network, then save which ARP replies have reached which devices and give a clear overview of what IP address and MAC addresses are connected.

Packet Sniffing

Fourthly, Packet Sniffing is where attackers will monitor and intercept traffic on the network, this 'attack' wasn't initially an attacking software as technicians would use this method to look at networking related issues to identify the problem and act upon the information they would retrieve from packet sniffing. "Packet sniffing is a technique of monitoring network traffic. It is effective on both switched and nonswitched networks." [16].

Packet sniffing helps with:

- Understanding Characteristics of a network
- Who is currently on the network
- Available bandwidth
- Peak network usage times
- Possible attacks
- Unsecured applications[17]

The attack comes down to that not everyone who uses the packet sniffing methods/tools is morally ethical and attackers can use this to intercept data between wired and wireless connections over the network, this can allow attackers to interfere, eavesdrop and access unauthorised data just to name a few reasons attackers use this.

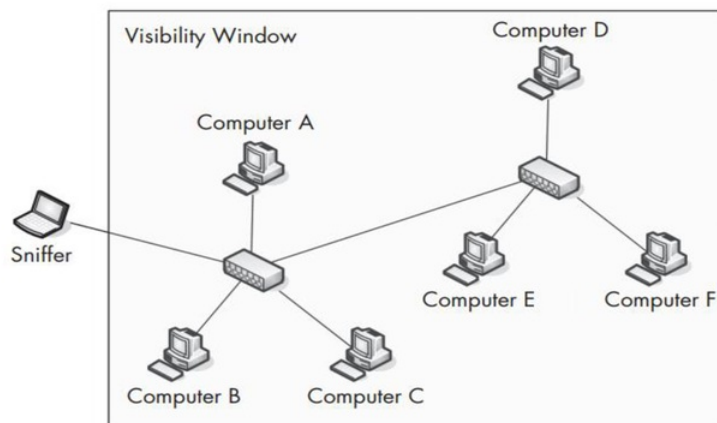


Figure 6 - Packet sniffing in practice[17].

Packet sniffing just like ARP spoofing allows other attacks to take place, the attacks listed below are the outcome of sniffing. These attacks are:

- ARP Cache Poisoning
- CAM table flooding
- Switch port stealing[16]

The defences used when encountering an unauthorised packet sniffing within your network, there are several ways to mitigate and detect these attacks. The defences are:

- Port security enabled on the switch
- Static ARP entries, administrator must create a new entry on every host[16]
- Detection software can listen to ARP traffic and the replies sent and received within the network.

Packet sniffing is highly debated over regarding ethical behaviour, as both technicians and hackers are using it for very different purposes it leads to the question whether it is ethical in the first place, there are laws in place to prohibit any unethical behaviour but there are implications as history shows that even ethical businesses/institutions can use this for unethical reasons. The concern is how easily obtainable the software is for packet sniffing, this allows anyone that owns a PC to use this to eavesdrop and retrieve sensitive data from another party, this questions its illegitimate use and causes concern.

Password Cracking

Lastly, Password Cracking is one of the more common methods of penetration of applications/systems etc, this is mainly because humans tend to use very weak and penetrable passwords, we aren't the best when it comes to remembering password, most people will use the same password for most applications, but trying to remember each individual password becomes complex which is why it is recommended to use software to manage your password in one secure place, but this isn't the solution all the time as human error is still a factor just less likely with this method.

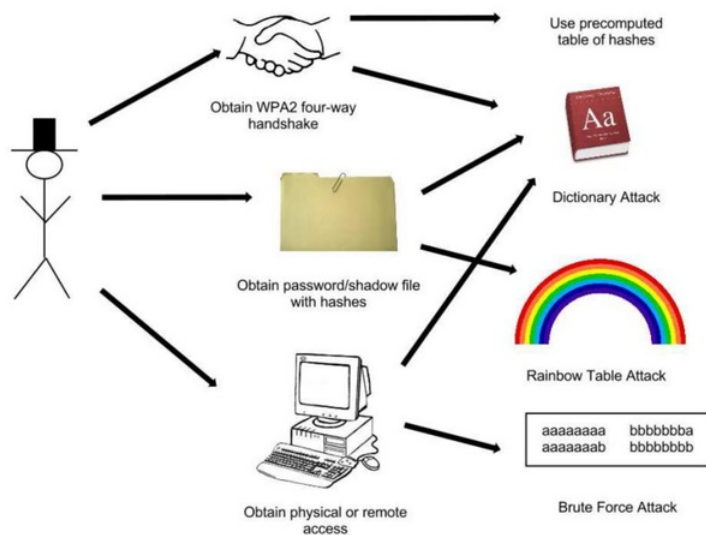


Figure 7 - Possible password attacking threats[18].

'Brute Force' also commonly called Dictionary attack is a common cracking tool this is essentially throwing all possible entries at it in iterations, a way of performing this would be to get a library of passwords or common words and forcing each of these to get past the password authentication. This is considered a low-level threat as the premise is an attacker is using computational power to gain entry. "A complete brute-force attack that includes all letters, numbers, special and printable characters can in theory guarantee a 100% success rate"[19]. as the success rate is 100% but is very time consuming, the more complex and sophisticated a password is the longer it'll take to crack.

Time to brute force password space, assuming 10,000 attempts per second			
	Lowercase (26 letters)	Uppercase, lowercase, digits (62 characters)	Uppercase, lowercase, digits, punctuation (94 characters)
Length = 5 characters	19 minutes	1 day	8 days
Length = 6 characters	8 hours	65 days	2 years
Length = 7 characters	9 days	11 years	200 years
Length = 8 characters	241 days	692 years	19,000 years
Length = 9 characters	17 years	42,000 years	1.8 million years

Figure 8 - Estimated time to brute force a password[20].

As the strengths of passwords are usually dependant on the user themselves, defending against password cracking tools can be quite the hassle as users mainly choose easy to remember than complex password which are harder to crack. Apart from creating stronger password with different characters and symbols, as the chart above shows it's inevitable for a password to prevent a brute force attack but the best option is to make it more complex which will delay the inevitable outcome of a brute force attack. Through human laziness and errors, we as a species are more likely to use the same password and username on more than one occasion for different websites, this goes into the hackers' advantage when wanting to gain access to different accounts of the user over a series of different websites, by using the same password and username will give the hacker more leverage and the user has more to lose just from pure laziness when choosing a password and username.

Conclusion

This report has looked at network security threats, considered the potential outcomes and dangers that are occurred when dealing with these threats. There has been evidence shown of how to prevent these attacks and a brief description of how they work, as technology is adapting and growing quicker than before there will always be a new and complex way of retrieving unauthorised data over a computer network, this will be an on-going arms race. Keeping updated about the newest technology breakthroughs and what new threats there might be is a good way to stay secure and be cautious of what information you take in. This report has shown what the possible threats are today, whereas tomorrow there could be newer threats exposed, research and adapt to new potential threats by making systems more secure and harder for an attacker to gain access.

References

- [1] W. Stallings and T. Copyright, *Cryptography and Network Security : Applications and Standards*, 2013.
- [2] J. E. Canavan and E. John, *Fundamentals of Network Security British Library Cataloguing in Publication Data*, 2001.
- [3] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing , Fourth Edition*. Prentice Hall, 2006.
- [4] Cisco Press, "Introducing Network Design Concepts," pp. 1–48, 2014.
- [5] O. Awodele, E. E. Onuiri, and S. O. Okolie, "Vulnerabilities in Network Infrastructures and Prevention / Containment Measures," 2012.
- [6] M. Abomhara and G. M. Kœien, "Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks," *J. Cyber Secur. Mobil.*, vol. 4, no. 1, pp. 65–88, 2015.
- [7] F. S. Roozbahani and R. Azad, "Security Solutions against Computer Networks Threats," *Int. J.*, vol. 2581, pp. 2576–2581, 2015.
- [8] Q. Gu and P. Liu, "Denial of Service Attacks," *Handb. Comput. Networks*, vol. 3, pp. 454–468, 2012.
- [9] K. Kumar, R. C. Joshi, and K. Singh, "An Integrated Approach for Defending Against Distributed Denial-of-Service (DDoS) Attacks," *Iriss*, pp. 1–6, 2006.
- [10] M. Sachdeva, G. Singh, K. Kumar, and K. Singh, "DDoS incidents and their impact: A review," *Int. Arab J. Inf. Technol.*, vol. 7, no. 1, pp. 14–20, 2010.
- [11] O. S. Younes, "A Secure DHCP Protocol to Mitigate LAN Attacks," *J. Comput. Commun.*, vol. 04, no. 01, pp. 39–50, 2016.
- [12] B. Aboba and S. Chesire, "Dynamic Host Configuration Protocol (DHCP) Domain Search Option." Network Working Group, pp. 1–8, 2002.
- [13] C. Systems, "Understanding , Preventing , and Defending Against Layer 2 Attacks," *Design*, pp. 1–61, 2008.
- [14] Sean Whalen, "An Introduction to Arp Spoofing," p. 7, 2001.
- [15] S. Gangan, "A Review of Man-in-the-Middle Attacks," *Cryptol. Secur.*, no. Mim, pp. 1–12, 2015.
- [16] R. Spangler, "Packet Sniffing on Layer 2 Switched Local Area Networks," *Networks*, 2003.
- [17] C. Sanders, *PRACTICAL PACKET ANALYSIS Using Wireshark to Solve Real-World Network Problems*. No Strach Press, 2011.
- [18] S. Martin and M. Tokutomi, "Password Cracking How Passwords are Stored," *IT Secur.*, pp. 1–11, 2007.
- [19] C. Yiannis, "Modern Password Cracking : A hands-on approach to creating an optimised and versatile attack . Modern Password Cracking : A hands-on approach to creating an optimised and versatile attack," no. May, 2013.
- [20] R. Baloch, "Is It Possible To Crack A Facebook Account?" HackyShacky, p. 1, 2014.

Bibliography

http://www.infosecwriters.com/Papers/BSullivan_Brute_Force.pdf

https://www.ncsc.gov.uk/content/files/MWR_Threat_Intelligence_Case%20Study_BruteForce.pdf

<http://www.ijstr.org/final-print/oct2015/Algorithm-To-Ensure-And-Enforce-Brute-force-Attack-resilient-Password-In-Routers.pdf>

<https://pdfs.semanticscholar.org/presentation/dead/6516c5fd7032220f0bc48e7ef72d6fd1ed7a.pdf>

<http://www.diva-portal.org/smash/get/diva2:833341/FULLTEXT01.pdf>

https://www.researchgate.net/profile/S_Shiva/publication/224123416_A_Survey_of_Game_Theory_as_Applied_to_Network_Security/links/09e415112bb6ddab50000000/A-Survey-of-Game-Theory-as-Applied-to-Network-Security.pdf

http://feihu.eng.ua.edu/NSF_CPS/year1/w9_1.pdf

David Price P131188 Network Operating Systems And Security Report

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

66/100

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5

PAGE 6

PAGE 7

PAGE 8

PAGE 9

PAGE 10

PAGE 11

PAGE 12

PAGE 13

GRADING FORM: SMU GENERIC_GJ

DAVID PRICE

66

RESEARCH-INFORMED LITERATURE

-  A very good number of mostly academically credible sources used. Note that your final source (20) is cited like a book, but is actually a web source - should have a url rather than a page number. Your referencing standard is otherwise correct - but as a general tip, avoid using quotes entirely unless the specific wording of what you're trying to say is important. If you can put something in your own words, it's always better to do so.
- 20**

KNOWLEDGE AND UNDERSTANDING

-  Good evidence of knowledge and understanding - lots of work obviously went into reading about this! It'd be nice to see a bit more mention of low level devices, as per the brief.
- 20**

ANALYSIS

-  Some evidence of snythesis and a limited conclusion drawn. Your conclusion could be a little more developed, relative to the length of the report.
- 15**

PRACTICAL APPLICATION AND DEP.

-  N/A - no marks assigned.

SKILLS FOR PROFESSIONAL PRAC.

-  A fairly well-written and presented report - I like some of the images you've used in particular.
- 11**

