

Dale Griffiths MSc Project Proposal

by Dale Griffiths

FILE	2832_DALE_GRIFFITHS_DALE_GRIFFITHS_MSC_PROJECT_PROPOSAL_9 3935_1442902760.DOCX (476.39K)		
TIME SUBMITTED	08-MAY-2019 11:24 PM (UTC+0100)	WORD COUNT	4577
SUBMISSION ID	106704391	CHARACTER COUNT	25053



RESEARCH PROPOSAL

CONSTRUCTING A SECURE ENTERPRISE
NETWORK

Section 1 Introduction

1.1 Introduction

This report is based within the computer network security field, the report is written on the topic of constructing a secure enterprise class network. This report is utilised to conduct research into previous studies and experiments within this field. This research will enable the author to understand how others have conducted the same type of project. The author will additionally conduct research into constructing a secure class enterprise network, penetration testing, attacks and solutions. This report will allow the author to provide the background research and give the author the understanding required to complete the project.

1.2 Project Title

The project title being utilized for this project proposal is constructing a secure enterprise network. The purpose of this project proposal is to conduct a final project within this field for the MSc computer networks and security degree.

1.3 Background of the Project

The author has previously conducted a project on constructing a secure home network for an undergraduate degree, the author wanted to further this project and that is how the project was decided upon. This project is essentially in two parts firstly investigating building an enterprise network, then conducting penetration testing and implementing solutions to secure the network. What is an enterprise network and how is it different to a home network? An enterprise network is a large-scale network, this network is constructed to allow an enterprise a communication method, it is utilized to provide employees access to company resources however it provides three main points integrity, security and reliability. These are critical within an enterprise network due to data protection laws company data must be kept confidential, this usually means encrypted within a computer network.

Within enterprise networks there are several stages to implementing security. The first stage is to implement a firewall. Firewalls are utilized to create a list of rules to allow or deny a packet entering the network. It is becoming more common within enterprise networks to have both internal and external firewalls. The reasoning behind this is companies are spending money building secure networks however, forgetting to secure the internal network from an inside attack. The next stage is to utilize a router with strong security. The next stage is to have wireless authentication to authenticate users and devices, simple wireless WPA2 security is not strong enough to secure a network. The final step is to implement security products to secure the network and end devices including email scanning as this is a common vector for phishing attacks.

1.4 Project Aim

The aim that is being utilized within the project proposal is to understand how enterprise networks are designed and constructed, this will enable the author to understand how to test the exploits that exist within enterprise networks and provide preventions to strengthen the security that exists within the network.

1.5 Project Objectives

The project objectives is to conduct research and investigate how enterprise networks are designed and build. This will enable the author to investigate how an enterprise network can be attacked with different threats and how the network can be secured.

- Research enterprise networks
- Research penetration testing methods
- Research different attacks & preventions that can be utilized within the project
- Plan and construct an enterprise class network consisting of more than 30 networking devices
- Conduct the penetration testing and provide solutions to attacks

Section 2 Literature Review

2.1 Introduction

This section is utilized for the documentation of the research that is being conducted to enable the author to understand the proposed project. The information will be gathered on enterprise networks, network devices, network attacks, network defences and penetration testing. The author then documents work that can be related to the proposed project. This literature review will not contain all the network attacks and defences that will be utilized within the project but give a demonstration on some that will be utilized within the proposed project.

2.2 Enterprise Networks

Enterprise networks are an essential part of modern businesses and most businesses would not be able to operate without them. Enterprise networks have similarities to a home networks however an enterprise network consists of many devices both networking and end devices. An enterprise network has one major difference to a home network, this is the implementation of maximum security to ensure the organisation complies with data protection laws. This is the reason why enterprise networks are typically harder to attack than others as there is a strong security implementation implemented within the network. Cisco provide some of the best enterprise networking equipment available, for this reason the author hopes to conduct the project utilizing cisco networking equipment.

2.3 Network Devices

2.3.1 Routers

A router is utilized to attach a local area network LAN to a wide area network (WAN), this is commonly to the lease line provider. Depending on the network configuration routers are typically the entrance and exit points of the network. Enterprise class routers typically have strong authentication and cryptography. High end routers can additionally support IPS, IDS, VPN and firewalls to create a strong entrance point to the network.

2.3.2 Switches

A switch can be utilized for multiple devices to be connected into a single enterprise network. There are three typical switches found within enterprise networks these are core, distribution and access switches. The core switches are utilized to route traffic that is entering and exiting the network, these are the expensive and have many ports. Both core and distribution switches can consist of over 500 ports. Distribution switches are utilized to handle routing within the network between different virtual local area networks (VLAN). Access switches are what connects the end devices to the network. These are typically between 24 and 48 ports that are connected to the distribution layer of the network. The access switches are where the VLANs are implemented, these increase security within the network as they segregate traffic into smaller networks. E.G. A network could consist of sales, accounting and guest VLANs, each would be separate providing a more secure network to the end user.

2.3.3 Access Points

[1] Wireless access points are utilized to provide wireless access to the users within the network. Wireless access is becoming more common due to the convenience of not having physical wires connecting the end devices. Wireless networks are typically less secure than wired networks as they do not require a physical connection to the network. The author aims to implement a radius server to provide authentication to wireless clients. This should help provide a more secure connection to that of just a WPA2 password.

2.4 Network Defences

2.4.1 Antivirus

[2][3] An antivirus is a software that is designed to defend a workstation from viruses, malware, ransom ware and spyware. Antivirus is software that runs in the background process of a workstation with real time detection, it scans every process for threats and when detected it automatically removes the threats.

2.4.2 Virtual Private Network (VPN)

[4][5] A VPN is utilized to establish a connection from one location to another in the form of an encrypted connection. Once a connection is established the client is seen only connecting to the VPN destination, this is then used to communicate with the internet hiding the client's information. Different VPNs use different security hashing methods and recommendations are different for different applications.

2.4.3 Firewalls

[6][7] A firewall is the first line of defence within a network. A network firewall is utilized to both allow and drop packets with different protocols. Firewalls additionally help to identify open ports within a network and secure them from attackers. Enterprise networks are commonly adding additional firewalls both the inside and outside of the network. The reasoning for this is attacks are becoming more common from within the organisation, filtering internal traffic utilizing a firewall further protects the network from attacks.

2.5 Network Attacks

2.5.1 Denial of Service Attack

[8]–[11] Denial of service attacks (DOS) is conducted by installing malware onto victims' devices this then attacks the device and creates a zombie that can be controlled by the attacker. Denial of service attacks contain hundreds of thousands of devices. The attack is carried out against a single resource with the aim to deny access to the resource. This type of attack is hard to trace back to the origin as there are so many users who were zombies, the devices who are zombies usually have no idea that they had been attacked and the device was utilized for a DOS attack. This attack is commonly utilized against large organizations with the aim to stop them from operating, costing the organizations massive sums of lost revenue and unhappy customers.

2.5.2 Keylogger

[12]–[14] A keylogger is utilized by attackers to record keystrokes input on devices. A keylogger is usually installed as malware, this can send the inputted keystrokes to an email address created by the attacker. The attacker can then access all usernames and passwords utilized to obtain unauthorised access to bank accounts and confidential customer and company data. An antivirus with real time detection should detect a keylogger, however setting up users with the correct privilege levels additionally will prevent this.

2.5.3 Password Cracking

[15]–[17] Password cracking utilizing the brute force method to obtain passwords to access different devices and accounts. This password cracking method is very effective however, it is very slow at breaking passwords. This method of password cracking will only work if the wordlist being utilized contains the exact password used for that being cracked, it must match identically. This method of password cracking works best against weak passwords as complex passwords take too much time to break. A strong password storage algorithm additionally needs to be implemented to secure the passwords as research has identified this is a common weakness.

2.6 Penetration testing

[18]–[20] Vulnerabilities and exploits can be identified by conducting penetration testing. The testing should be performed with a real-world scenario on a network and obtain as much information as possible. There are two different methods of penetration testing automatic and manual. Research has identified that one or the other is not enough, penetration testing should consist of both manual and automatic testing. This will ensure a more threats are identified during the penetration testing process.

2.6.1 White Box Testing

[21][22] white hat hackers are the ethical hackers. This is someone who conducts a penetration test however they have the network owner's full permission to do so. A white box tester will document all penetration tests conducted and state the vulnerabilities found. This type of attacker will additionally provide solutions for the vulnerabilities found during the testing. A white box tester is very well paid.

2.6.2 Black Box Testing

[21][22] This style of penetration testing is conducted by an individual without any internal network knowledge. This style of penetration testing is illegal and is preformed by attackers to obtain a financial gain.

2.6.3 Grey Box Testing

[23][24] An individual who is known as a grey box attacker is someone who conducts penetration tests without the owner's permission. The attacker will just perform the testing for fun and provide the organisation with full details of the exploits found. However sometimes this type of attack can be utilized to blackmail organisations into paying the attacker to rectify the exploits that were identified within the testing.

2.7 Related work

The paper "Design and Develop Hands on Cyber-Security Curriculum and Laboratory" by Dongqing Yang [25], has four objectives create an enterprise network, penetration testing, hardening the network and performing an audit. Developing an enterprise network, the paper looks at creating a virtualised network within a laboratory environment. The network consists of three sections, outside, DMZ and Inside. The attacker is on the outside of the network demonstrating an attack over the internet to the demilitarised zone (DMZ). The DMZ consists of a single server operating windows server 2012. The internal network consists of the typical networking devices found within enterprise networks. The router, DMZ and inside are separated by utilizing a firewall. The paper then goes on to talking about penetration testing and what attacks should be conducted these include a man in the middle attack, wireless cracking, hacking cisco routers, firewall evasion, password cracking. The paper then suggests hardening the network to prevent the security breaches and how to conduct an audit. This paper relates to the project the author is planning as it suggests a method that could be utilized to construct a virtual enterprise network and conduct a penetration test.

The paper "A study on penetration testing process and tools" by Hessa Mohammed and Zaher Al Shebli [26], investigates the different types of penetration testing that can be conducted. The paper looks at external testing, internal testing, router penetration, firewall penetration and application testing. The paper identifies that it is essential not just to conduct a single penetration test from the outside but to conduct several on critical aspects of the network. External testing is important to ensure that the network is secure from external attacks. Internal testing is important to ensure that an employee or customer cannot access anything confidential or attack the network and end devices. Router penetration testing is important as identified in the last paper, in enterprise networks routers tend to have many of the security applications within them. If there is a weakness within the router it is critical to identify and implement a solution to secure the network. Firewall penetration testing is important as it will identify misconfigurations and it is usually the first line of defence to prevent an attack. Application penetration is important within organisations as these applications store and have access to confidential company information. The paper additionally recommends tools like Nmap, Beef, Metasploit, Nessus and Cane and Able to conduct the penetration testing. This paper relates to the project the author is planning as it suggests a method that could be utilized to conduct some of the penetration testing and provides some tools that can be utilized.

The paper "Security Assessment via Penetration Testing: A Network and System Administrators Approach" by Nishant Shrestha[27], investigates the difference between automated and manual penetration testing. The paper additionally provides some penetration testing frameworks that could be utilized by the author to conduct the penetration testing. There are additionally several tools that could be utilized within the penetration test that will be conducted. The tools include Nessus, open vulnerability assessment systems, open vas, Metasploit Framework and Backtrack. This paper relates to the project the author is planning as it suggests a method that could be utilized to conduct some of the penetration testing and provides some tools that can be utilized and provides information relating to automated and manual penetration tests.

2.8 Conclusion

This section of the report has outlined research that has been conducted upon similar work to the proposed project. The author has additionally looked at related work and justified why each section of the relayed work is related to the project. The final project will additionally include further attacks and solutions that are not discussed within the literature review. The author demonstrated examples of the types of attacks and solutions within the literature review. The final project will cover a large amount of research on different penetration tests that can be performed.

Section 3 Research and Development Methods

3.1 Research and Development Methods Introduction

This section of the report will be utilized to consider the research methodology required to conduct the project proposal. This will additionally cover what development method will be used within the project. This chapter will additionally cover risks, limitations and anything that is required to prevent the risks and limitations becoming issues. The last part of this chapter will be utilized to consider how the evaluation will be made to see if the aims and objectives have been met. Figure 1 is utilized to demonstrate the research onion; the research onion provides the author with a possible project plan that can be utilised for every stage of the project from research to experiment and finally evaluating the results.

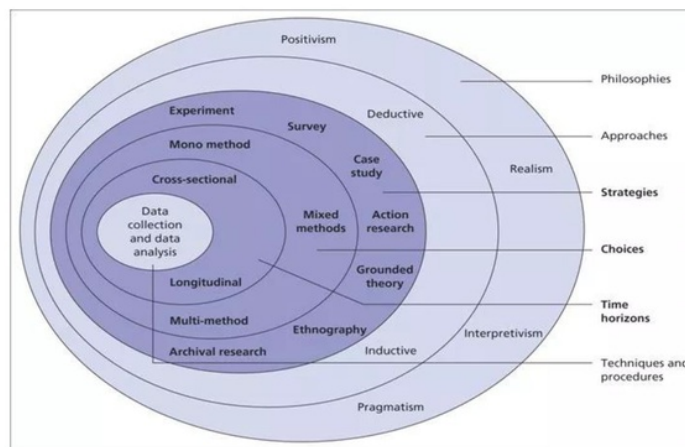


Figure 1 – Research Onion [28]

3.2 Project Philosophy

[29] The philosophy circle of the onion outlines several philosophies that can be utilized for the project proposal. The author has selected positivism to be used within the project proposal. The reason for this choice is that positivism is backed up by scientific evidence in the form of either an experiment or statistically.

3.3 Research Approach

There are several different approaches that could be utilized for the proposed project. Deductive has been chosen as the research approach for the project proposal. The author has chosen deductive as it is utilized when a theory is being tested. This project is based upon a theory that enterprise networks have weaknesses within their security the author aims to prove this when conducting the penetration testing.

3.4 Strategies for Research

This section identifies several different research strategies that could be utilized within the proposed project. Experiment has been chosen as the research strategy to be utilized within this project. The experiment strategy is when the author can change at least one variable to conduct the experiment. The author will be conducting multiple attacks during the penetration testing of the network. This will be the variable that changes, the results will then be recorded for the author to have the ability to compare the findings from the experiments to that of the research. This will enable the author to know whether the attack was successful and as expected from the research.

3.5 Methods for Data Collection

[30] This section identifies several options for the data collection that can be utilized within the proposed project. Observation was chosen as the first data collection method. The reason for this is that when the penetration testing is performed there will need to be observed and documented. The next method identified by the author is has secondary. The reason for this is that the author will be comparing the research that is secondary data to the observations to have the ability to compare the findings with other similar projects.

3.6 Risks and Limitations

There are a few risks and limitations that have been identified, these risks and limitations need to be resolved both before and during the project. The risks that have been identified are

- Not allowing enough time to develop the enterprise network
- The risk of not being able to complete the requirements if the author sets unrealistic plans
- Poor time management

The risks and limitations of the project are all around time management. The use of Microsoft office Project allows for these risks and limitations to be minimised. Microsoft office Project allows the author to create a Gantt chart. A Gantt chart is helpful in providing the author with the critical path. The critical path is vital to ensuring that the project is kept on time at each stage. When building a project plan it is important to allow spare time within each section to allow for delays, E.G. unexpected illness. If this were to happen during the project then it would mean that the project would fall behind schedule, therefore it is critical to allow for slight delays within the planning of a project.

3.7 Evaluation of findings

There are several different methods that will be utilized to evaluate the results of the experiment. The most obvious way is when conducting the attacks to know if they are successful or not. The second method will be comparing the results from the experiment to that of the research conducted within the literature review. The most important evaluation that will be made is if the aim and objectives that were created have been met. This will determine if the project was successful or not.

Section 4 Resources and Planning

4.1 Introduction

This last section is utilized to consider the resources that will be required to conduct the project. It will cover all aspects of the project proposal to ensure that all the resources that are required are highlighted in preparation for the author to conduct the project. This part of the document additionally covers the proposed project plan, the plan that will be created in Microsoft project can be utilized to ensure that all sections are given a deadline. This allows the author to manage the proposed project to ensure that it is completed on time for the deadline.

4.2 Required Resources

There are several resources that are required to successfully conduct this project. The author has identified these resources during the research conducted within this report. The project will be built on both physical devices and simulated within high end simulation software. This will enable the author to successfully complete the project. The resources that will be required are:

- Access to 10 physical PC/Laptops
- Access to at least 20 cisco devices including switches, routers, firewalls
- Access to wireless access points
- Access to a Cisco Virtual Internet Routing Lab (VIRAL)
- Access to the internet
- Penetration tools E.G. Kali Linux, Caine & Able
- Access to windows server

4.3 Project Planning

The project planning has been conducted in Microsoft office Project and can be seen in figure 2-3. The project has been split into three sections Literature review, Methodology and Implementation. The tasks that are required to conduct the project have been put into the Gantt chart. The tasks have all been provided with realistic timings.

Task Mode	Task Name	Duration	Start	Finish	Predecessors
★	➤ Requirements and specification	60 days	Mon 03/06/19	Fri 23/08/19	
★	➤ Literature Review	60 days	Mon 03/06/19	Fri 23/08/19	
★	Introduction	2 days	Tue 04/06/19	Wed 05/06/19	
★	Aim & Objectives	2 days	Thu 06/06/19	Fri 07/06/19	3
★	Evaluation of Penetration methods	10 days	Mon 10/06/19	Fri 21/06/19	4
★	➤ Methodology	16 days	Mon 24/06/19	Mon 15/07/19	
★	Development Methods	2 days	Mon 24/06/19	Tue 25/06/19	5
★	Research Philosophy	3 days	Wed 26/06/19	Fri 28/06/19	7
★	Research Strategy	3 days	Mon 01/07/19	Wed 03/07/19	8
★	Data Collection Methods	2 days	Thu 04/07/19	Fri 05/07/19	9
★	Reliability and Validity	3 days	Mon 08/07/19	Wed 10/07/19	10
★	Risk Limitations	2 days	Thu 11/07/19	Fri 12/07/19	11
★	Ethical and Legal issues	1 day	Mon 15/07/19	Mon 15/07/19	12
☒	➤ Implementation	29 days	Tue 16/07/19	Fri 23/08/19	
★	Building a enterprise network	9 days	Tue 16/07/19	Fri 26/07/19	13
★	Conducting penetration testing	9 days	Mon 29/07/19	Thu 08/08/19	15
★	evaluation of findings	8 days	Fri 09/08/19	Tue 20/08/19	16
★	future improvments	3 days	Wed 21/08/19	Fri 23/08/19	17

Figure 2 – Gantt Chart for the proposed project

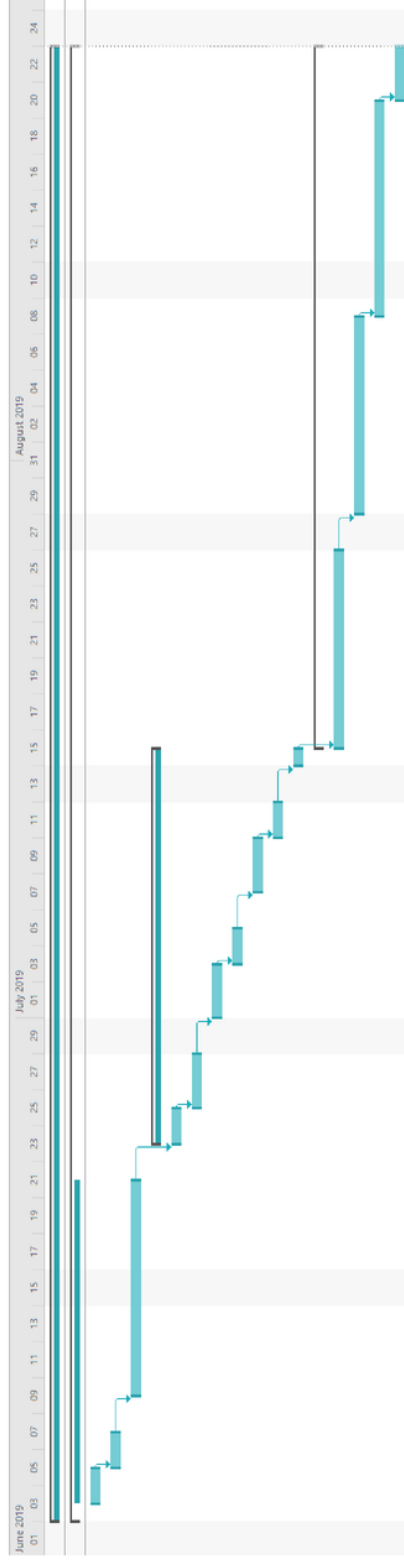


Figure 3 - Gantt Chart Calendar View

References

- [1] M. S. (Mohammad S. Obaidat *et al.*, *WINSYS 2013: proceedings of the 10th International Conference on Wireless Information Networks and Systems: Reykjavik, Iceland, 29-31 July, 2013.* .
- [2] N. B. Vasilyevna, S. S. Yeo, E. S. Cho, and J. A. Kim, "Malware and antivirus deployment for enterprise IT security," in *Proceedings - 2008 International Symposium on Ubiquitous Multimedia Computing, UMC 2008*, 2008, pp. 252–255.
- [3] P. Shahegh, T. Dietz, M. Cukier, A. Algaith, A. Brozik, and I. Gashi, "AVAMAT: AntiVirus and malware analysis tool," in *2017 IEEE 16th International Symposium on Network Computing and Applications, NCA 2017*, 2017, vol. 2017-Janua, pp. 1–4.
- [4] K. M. M. M. Fathima, "A survey on multiprotocol label switching in virtual private networks," in *Proceedings of the International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2018*, 2019, pp. 737–740.
- [5] C. Fancy and L. M. M. Thanveer, "An evaluation of alternative protocols-based Virtual Private LAN Service (VPLS)," in *IEEE International Conference on IoT and its Applications, ICIOT 2017*, 2017, pp. 1–6.
- [6] N. Jiang, H. Lin, Z. Yin, and C. Xi, "Research of paired industrial firewalls in defense-in-depth architecture of integrated manufacturing or production system," in *2017 IEEE International Conference on Information and Automation, ICIA 2017*, 2017, pp. 523–526.
- [7] Z. Ghanbari, Y. Rahmani, H. Ghaffarian, and M. H. Ahmadzadegan, "Comparative approach to web application firewalls," in *Conference Proceedings of 2015 2nd International Conference on Knowledge-Based Engineering and Innovation, KBEI 2015*, 2016, pp. 808–812.
- [8] K. L. Miao, J. W. Zhu, and W. A. Zhang, "Distributed guaranteed cost control of networked interconnected systems under denial-of-service attacks: A switched system approach," in *Proceedings - 2018 33rd Youth Academic Annual Conference of Chinese Association of Automation, YAC 2018*, 2018, pp. 911–915.
- [9] W. Alosaimi, M. Zak, and K. Al-Begain, "Denial of Service Attacks Mitigation in the Cloud," in *Proceedings - NGMAST 2015: The 9th International Conference on Next Generation Mobile Applications, Services and Technologies*, 2016, pp. 47–53.
- [10] S. S. Thakare and P. Kaur, "Denial-of-service attack detection system," in *Proceedings - 1st International Conference on Intelligent Systems and Information Management, ICISIM 2017*, 2017, vol. 2017-Janua, pp. 281–285.
- [11] M. Zhang, J. Bi, J. Bai, and G. Li, "FloodShield: Securing the SDN Infrastructure Against Denial-of-Service Attacks," in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018, pp. 687–698.
- [12] T. O. M. Ali, O. S. A. Awadelseed, and A. E. W. Eldewahi, "Random multiple layouts: Keylogger prevention technique," in *Proceedings of 2016 Conference of Basic Sciences and Engineering Studies, SGCAC 2016*, 2016, pp. 1–5.

- [13] A. Solairaj, S. C. Prabanand, J. Mathalairaj, C. Prathap, and L. S. Vignesh, "Keyloggers software detection techniques," in *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, 2016, pp. 1–6.
- [14] M. H. Ahmadzadegan, A. A. Khorshidvand, and M. Pezeshki, "A method for securing username and password against the Keylogger software using the logistic map chaos function," in *Conference Proceedings of 2015 2nd International Conference on Knowledge-Based Engineering and Innovation, KBEI 2015*, 2016, pp. 1071–1073.
- [15] S. Houshmand, S. Aggarwal, and R. Flood, "Next Gen PCFG Password Cracking," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1776–1791, Aug. 2015.
- [16] E. Stavrou, "Enhancing cyber situational awareness: A new perspective of password auditing tools," in *2018 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, CyberSA 2018*, 2018, pp. 1–4.
- [17] E. I. Tatli, "Cracking more password hashes with patterns," *IEEE Trans. Inf. Forensics Secur.*, vol. 10, no. 8, pp. 1656–1665, Aug. 2015.
- [18] G. Chu and A. Lisitsa, "Poster: Agent-based (BDI) modeling for automation of penetration testing," in *2018 16th Annual Conference on Privacy, Security and Trust, PST 2018*, 2018, pp. 1–2.
- [19] A. Tetskyi, V. Kharchenko, and D. Uzun, "Neural networks based choice of tools for penetration testing of web applications," in *Proceedings of 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies, DESSERT 2018*, 2018, pp. 402–405.
- [20] S. Türpe and J. Eichler, "Testing production systems safely: Common precautions in penetration testing," in *TAIC PART 2009 - Testing: Academic and Industrial Conference - Practice and Research Techniques*, 2009, pp. 205–209.
- [21] R. Chopra and S. Madan, "Reusing black box test paths for white box testing of websites," in *Proceedings of the 2013 3rd IEEE International Advance Computing Conference, IACC 2013*, 2013, pp. 1345–1350.
- [22] C. Henard, M. Papadakis, M. Harman, Y. Jia, and Y. Le Traon, "Comparing white-box and black-box test prioritization," in *Proceedings of the 38th International Conference on Software Engineering - ICSE '16*, 2016, pp. 523–534.
- [23] M. Yevdokymenko, E. Mohamed, and P. Onwuakpa, "Ethical hacking and penetration testing using raspberry PI," in *2017 4th International Scientific-Practical Conference Problems of Infocommunications Science and Technology, PIC S and T 2017 - Proceedings*, 2018, vol. 2018-Janua, pp. 179–181.
- [24] Y. Wang and J. Yang, "Ethical hacking and network defense: Choose your best network vulnerability scanning tool," in *Proceedings - 31st IEEE International Conference on Advanced Information Networking and Applications Workshops, WAINA 2017*, 2017, pp. 110–113.
- [25] D. Yuan, "Design and develop hands on cyber-security curriculum and laboratory," in *Proceedings of Computing Conference 2017*, 2018, vol. 2018-Janua, pp. 1176–1179.
- [26] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in *2018 IEEE Long Island Systems, Applications and Technology Conference, LISAT 2018*, 2018, pp. 1–7.

- [27] N. Shrestha, "Security Assessment via Penetration Testing: A Network and System Administrator's Approach," 2012.
- [28] "onion.jpg (715×459)." [Online]. Available: <https://i1.wp.com/www.allassignmenthelp.co.uk/blog/wp-content/uploads/2017/07/onion.jpg?resize=715%2C459&ssl=1>. [Accessed: 08-May-2019].
- [29] D. F. Adamski, "Tools, techniques and philosophies of effective project management," in *IEEE Technical Applications Conference and Workshops. Northcon/95. Conference Record*, 2002, p. 374.
- [30] B. Tie and L. Shufen, "A method for network data collection and processing in the pervasive computing environment," in *SPCA 2006: 2006 First International Symposium on Pervasive Computing and Applications, Proceedings*, 2007, pp. 599–603.

Dale Griffiths MSc Project Proposal

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

Instructor

64/100

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

PAGE 14

PAGE 15

GRADING FORM: NEW ASSESSMENT

ENGAGEMENT WITH LITERATURE

 The background information provided in terms of enterprise networks is very generic and general. It would to see more detail about enterprise network in a more practical way such as relate it to some current enterprise companies and problems/challenges face by them then state some suitable approach to the problem. Appropriate sources used

9

KNOWLEDGE AND UNDERSTANDING

 The aim and objectives are generic and need to be more smart and focus to the particular problem to be solved. The conclusion summed up what the expected outcomes.

9

COGNITIVE, INTELLECTUAL SKILLS

 This is written more like an undergraduate level. Need to be more forceful and critically analyse. I

8

PRACTICAL SKILLS



Some areas are lacking details. More information to justify the selection of testing would be good. The Gantt chart with appropriate timescales for each stage of the project well put together.

30

TRANSFERABLE SKILLS



Correct use of referencing. Flow and written well.

8