**Lecturer’s Name:** Mark Melling

**Assessment Title:** Final Assessment – Corona Fightback Solution

**Work to be submitted to:** Blackboard

**Date for submission of work:** 2/5/2021

**Place and time for submitting work:** 23:59 Blackboard

**To be completed by the Student**

**Student’s Name:** Mark McGuinness

**Class:** Computer Security & Digital Forensics – Year 3

**Subject/Module:** Secure Network Services

**Word Count (where applicable):** 2,250 words

**I confirm that the work submitted has been produced solely through my own efforts.**

**Student’s signature:** Mark McGuinness **Date:** 2/5/2021

|  |
| --- |
| **Notes**  **Penalties:** The total marks available for an assessment is reduced by 15% for work submitted up to one week late. The total marks available are reduced by 30% for work up to two weeks late. Assessment work received more than two weeks late will receive a mark of zero.  **Continuous Assessment:** For students repeating an examination, marks awarded for continuous assessment shall normally be carried forward from the original examination to the repeat examination.  **Declaration:**  I declare that this work is entirely my own and does not contain the words or ideas of someone else, whether published or not, without specific acknowledgement by relevant referencing. I have read and understood the LYIT Plagiarism Policy on the “Student & Academic Policies” section of the LYIT Website and understand plagiarism to include:   * Direct copying of text, images and other materials (electronic or otherwise) from a book, article, fellow student’s essay, handout, web page or other source without proper acknowledgement. * Claiming individual ideas derived from a book, article etc. as one’s own and incorporating them into one’s work without acknowledging the source of these ideas. * Overly depending on the work of one or more other sources without proper acknowledgement of the source, by constructing an essay, project etc., extracting large sections of text from another source and merely linking these together with a few of one’s own sentences.   I understand that it is my responsibility to familiarise myself with and to follow the Institute’s Assessment Regulations. I acknowledge that Incidents of alleged plagiarism and cheating are dealt with in accordance with the Institute’s Assessment Regulations and that penalties will be applied if I breach this policy.  **Signed:** Mark McGuinness **Date:** 2/5/2021 |

**Network Report – Corona Fightback Solution**

**Introduction:**

For our final assessment, we were tasked with designing & securing a network for a fictional company called ‘Corona Fightback Solution’. The company in question have roughly 215 hosts, 200 comprised of staff & 15 making up application servers in both the ‘Medical’ & ‘Marketing’ department. The network is to be subnetted on a class B network (172.16.0.0/16), by department.

In this document, I will outline the design process & security measures of the ‘Corona Fightback Solution’ network. I will attempt to explain the reasoning behind each decision made, in an informative & rational manner.

**Network Topology:**

Diagram

Description automatically generated with low confidence

***‘Corona Fightback Solution’ Network***

To provide some context on the overall network layout, I structured it as if there were two separate offices of this company. One in ‘Letterkenny’ & the other in ‘Derry’, with them both converging at the ‘Internet Service Provider’ (ISP). Although a bit out of the realms of reality due to the limited number of interfaces on a switch, I split up the six departments evenly amongst the buildings & had each of them on a ‘router-on-a-stick’ setup.

The departments are represented with three devices each. The ‘Medical’ & ‘Marketing’ departments have the first member of that department visualised as a PC. The first & last application servers of the department are the two devices following. I assigned the last usable addresses of each subnet to the servers, as to allow wiggle room for additional PCs in the further future. The rest of the departments are represented with just three PCs. I kept the number of devices to a minimum, so as to not take the focus away from the system’s functionality.

This in turn kept the structure simple, both for the viewer and for the VLANs to follow.

The ‘ISP’ cloud contains the ‘ISP’ router , ‘EmailServer’ & ‘WebServer’. The servers are located on a LAN called ‘IT Services’, and these devices are located on a network of 184.168.10.128/25. The ‘IT Services’ switch was not implemented with VLANs, nor trunked as there was only one LAN the switch was concerned with.

**VLANs & WANs:**

With there being six departments and with two serial connections on the routers, there will be six VLANs & WANs to follow. The IP addressing scheme of the VLANs & WANs can be found in the Excel sheet ‘Corona Fightback Solution’. I colour co-ordinated the departments in the packet, to match that of the LANs found in the IP addressing scheme Excel file.

**Routers-** For the routers, I settled with the 2811 models as they had the potential to create VPN tunnels for a network and only contained interfaces that were going to be made use of. In fact, two ‘WIC-1T’ modules had to be installed on each router to have access to Serial interfaces.

Sub-interfaces were configured on the ‘Derry’ & ‘Letterkenny’ routers to accommodate for the default-gateways of the VLANs. ‘Letterkenny’ housed VLANs 10 – 30, whereas ‘Derry’ housed VLANs 40 – 60. These sub-interfaces must be encapsulated, so that the router can successfully communicate with the VLANs.

Graphical user interface, text, application

Description automatically generatedGraphical user interface, text

Description automatically generated  
***Sub-interfaces on routers ‘Letterkenny’ & ‘Derry’***

The Serial interfaces of the routers were initiated with the addresses outlined in the Excel document, to have the WANs up & running. However, a routing protocol must be configured for communication to occur across the routers.

**Switches-** As each end device is directly linked to the switches running to the routers, each port on the switches can be configured to fall among one of the three departments in that building. After doing so, the port connected to the router must be trunked to have the VLANs transfer data out of their assigned switch.

Text

Description automatically generatedText

Description automatically generated  
***Port configurations of switches ‘LAN1’ & ‘LAN2’***

It is worth noting that the default management VLAN (VLAN 1) is not allowed on the switchport trunk, due to security reasons. A management VLAN was instead created on VLAN 99 to lessen any potential harm, which will be touched upon in a later section.

**Router Rip:**

Since the network is being designed for a company with less than 250 hosts, Router RIP Version 2 was chosen. Although OSPF is a greater protocol in terms of offering further distances for packets to travel, the client company is a SME (Small Medium Enterprise) so that 15 hop-limit will never hinder the network (GeeksforGeeks , 2020).

Router RIP V2 was configured on ‘Letterkenny’, ‘Derry’ & ‘ISP’ routers as evident from the screenshot:

Text

Description automatically generated

***All subnets visible on ‘ISP’ router thanks to Router RIP V2***

When configured correctly, Router RIP V2 should allow PCs to ping across from ‘Letterkenny’ to ‘Derry’, and vice versa.

**DHCP:**

For this activity, it was outlined in the documentation to use a service to allocate some IP addresses in the network. Dynamic Host Configuration Protocol was used to fulfil this.

Upon learning of the possibility of setting a router interface to take on the role of a DHCP server, I decided to use it. First reason was because only a few departments located on one router would make use of the service, so burdening either the ‘EmailServer’ or ‘WebServer’ with it did not make much sense. Second reason was I found it easier to grasp than the DHCP service configuration in a physical server, as it was something akin to creating VLANs. I

Although it is not specified, I did assign the same DHCP setup on the accompanying switch to make sure addresses would be assigned appropriately. The IP addresses for each end device in ‘Technical’, ‘Manager’ & ‘Receptionists’ were set using the DHCP service. I situated DHCP on the ‘Derry’ router over ‘Letterkenny’, as I was advised not to use the DHCP service to assign server IPs.

**DNS & HTTP:**

Both the DNS & HTTP were setup on the ‘WebServer’, as they were services that complemented one another and it allowed all users on the network access to it via the ‘ISP’ router.

The DNS, ‘www.fightback.ie’, was assigned with the IP of the ‘WebServer’, 184.168.10.253. Two HTML pages were then created for use with the HTTP service, ‘index.html’ & ‘contactUs.html’. These were personalised by me, rolling with the theme of ‘COVID-19’ help services as a whole.

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application, email

Description automatically generated  
***Pages greeted by the user on ‘www.fightback.ie’***

**Email:**

The service on the ‘EmailServer’ was configured with the domain name ‘fightback.ie’, and all PC users were declared with a username & password. These details, including email address & mail server, were used to configure each PC’s email in their desktop.

Testing the capability of the service was as simple as sending an email from one PC to another and checking if the email was received.

Graphical user interface, application

Description automatically generated

***Confirmation that the Email service works***

**FTP:**

The File Transfer Protocol service allows files to move from a client to a server. In the FTP service, you can dictate what user has which permissions on that FTP server. The FTP service was enabled on each of the application servers in ‘Medical Research’ & ‘Marketing’. On each server, an ‘admin’ & a PC user was implemented. The PC users were only given ‘Read’, ‘Write’ & ‘Rename’ permissions, with ‘admin’ having them, and the added abilities to ‘Delete’ & ‘List’ files.

Graphical user interface, application

Description automatically generatedGraphical user interface, application, table, Teams

Description automatically generated  
***FTP configuration on ‘AppServer\_1’ & ‘AppServer\_11’***

By entering the “ftp <FTP Server IP address>” into the command prompt of a PC, you can test the login credentials & permission of the authorised user. Screenshot below is an attempt on deleting a file, while logged-in as ‘Staff\_1’:

Text

Description automatically generated

***‘Delete’ permission denied from ‘Staff\_1’ user, by FTP server***

**Security Measures:**

To preserve a network’s functionality as much as possible & it’s data confidential are the key goals when implementing security. Some of the security measures put in place into this network I have previously dealt with before, like ACLs, Management VLAN, SSH. While others, like firewalls & VPNs were new ventures undertaken by me.

Prior to starting on the more substantial pieces of security like outlined above, I formed some basic security on the routers & switches. Elements such as line console passwords, privileged passwords, message of the day banner & a password encryption service were setup.

**ACLs/Firewalls:**

I had planned on implementing Access Control Lists (ACLs) onto the network’s switches & routers. However, there were difficulties implementing standard ACLs, let alone extended.

After trying to troubleshoot these ACL issues, I came across forums mentioning the use of VACLs (VLAN ACLs). As it seemed to appeal more to my current network setup, I tried implementing my defined extended ACL to an access map. However, the command line did not recognise the command ‘vlan access-map’. Upon further inspection, I figured that the switches’ operating systems in packet tracer does not support the ‘access-map’ functionality (Peter Paluch, 2013).

In the end, I settled for firewalls situated on the application servers. I configured it so that only members of the department, which the server belonged to, could ping to it. Anyone outside of it was denied any access to it.

Text

Description automatically generatedTable

Description automatically generated  
***The firewall configured for ‘AppServer\_1’, as well as ‘Accounts\_1’ attempting to ping the server.***

**‘NetMan’ VLAN:**

When configuring a management VLAN on a network, it is of the utmost importance that it stays off the default location of ‘VLAN 1’. As is one of the fundamental rules of security, default settings should always be changed where possible. Hence, I created & assigned an IP to ‘VLAN 99’ interface on the switches, and an accompanying sub-interface on the routers. This VLAN will allow network management to remote into devices like routers & switches, granting them the ability to alter their configurations from a workstation.

**SSH:**

Although remote access can be achieved with Telnet as well, Secure Shell is more secure in that it uses encryption for data transport (Mahesh Parahar, 2020). Key pairs are generated for data transport, with their bit-count decided by whatever number is entered upon ‘Crypto RSA’ start-up. I went with 1,024 bits, as that is required for SSH 2 to operate. Telnet transports data in a plaintext format.

A prerequisite to activating SSH on a device, is registering a user & a password to it (All Answers Ltd., 2018). Finally, the VTY lines will have SSH ready-to-go using “transport input ssh”, and have authorisation be based off of the local profiles on the switch/router. As an added procedure, I set a maximum inactivity timer of 5 minutes:

Text

Description automatically generated

***Line VTY Configurations on routers & switches***

Testing this I found that I was able to successfully gain remote access to both routers, but not the switches. At first, I thought the IP addressing for the ‘VLAN 99’ was the issue, however I was able to remote into the router’s VLAN 99 sub-interface so it could not have been that. Sadly, I was not able to resolve this issue prior to submission.

Text

Description automatically generated

***Using SSH on ‘Staff\_1’ to remote into ‘Letterkenny’ router***

**VPN:**

The final security measure I started on was the data encrypted tunnel of a Virtual Private Network, running from router ‘Letterkenny’, through to ‘Derry’.

What makes site-to-site VPNs possible is the IPsec framework. The SSL framework is another way to encrypt traffic, but they are usually reserved for remote access capabilities. After a bit of research it looked as if tunnel mode was the ideal choice for my situation, because it catered to packet destinations that ran past the end of the IPsec tunnel.

I initialised tunnel interfaces with addresses on both routers, specifying where each started & ended. As depicted on the diagram, the tunnel runs through all three routers. The Maximum Transmission Unit (MTU) of the tunnel is 1476 bytes meaning if any packet exceeds this, it will have to be broken up into multiple packets. The ‘tunnel0’ is up & running on the network, but I was not able to encrypt it, due to running short on time (Online Tutorial, 2017).

**Conclusion:**

When beginning this project, I underestimated the amount of time it would take to simply have cross-site pinging functioning, never mind DHCP or ACLs. By the time I got to VPNs I had to significantly cut the time spent on them down. I may have overreached when it came to security measures, as I could have refined areas with issues, such as the ‘NetMan’ VLAN not allowing SSH access for switches.

Although I was not successful in configuring them, I did take away some knowledge in the fields of VACLs & VPNs, such as how VLANs need to be defined to access maps, and the two main protocols that make up IPsec. I was going to start building on the functionality for the AAA (Authentication, Authorisation & Accounting) service, which would have enforced network policies & further access control on end devices. But in the end, this was scrapped.

My thoughts overall: I thought this was a challenging, but engaging task at that. I particularly enjoyed the designing & service configuration of the network, more than the security end of it. I think it was due to how responsive the services like FTP or Email were, compared to something like SSH. It made issues easier to gage, while dealing with the more tedious tasks of services.

**Bibliography:**

All Answers Ltd. (2018) ‘Security Procedures for a Small Computer Network’, available: https://ukdiss.com/examples/small-computer-network-security-procedures.php#citethis [accessed 2 May 2021].

GeeksforGeeks (2020) ‘Difference between RIP and OSPF’, available: https://www.geeksforgeeks.org/difference-between-rip-and-ospf/ [accessed 2 May 2021].

Mahesh Parahar (2020) ‘Difference between SSH and Telnet’, available: https://www.tutorialspoint.com/difference-between-ssh-and-telnet [accessed 2 May 2021].

Online Tutorial (2017) *Configure VPN in Cisco Packet Tracer* [online], YouTube, available: https://www.youtube.com/watch?v=iLEcE\_8BOd8.

Peter Paluch (2013) ‘vlan access-map not working on cisco router 3600’, available: https://community.cisco.com/t5/switching/vlan-access-map-not-working-on-cisco-router-3600/td-p/2256250 [accessed 2 May 2021].