Module Code: Network Forensics

Module Title:	Network Forensics
Assignment Type:	Practical and Report (max 800 words)
Project Title:	CA 1 – Network Security Configuration and Report
Project Date:	**28th** March 2018
Assignment Compiler:	Greg South, gsouth@cct.ie
Weighting:	Marks out of 20%
Due Date:	**8th April 2018 @ 11.55pm**
Method of Submission:	**Packet Tracer & Report via Moodle Upload**.
Group or Individual:	Individual assignment

Assignment Introduction

You work for an IT Consultancy firm in Dublin City Centre known as ICT Solutions. You have been assigned to a client to undertake a short term networking and security project for the next week(and a bit!). The deadline to complete this project is the 8th April 2018 @11.55pm. The client has some strict timelines and needs this work to be completed on time!

In short, the client would like practical help with their network and also some guidance (in the form of a report). This assessment will test your ability to configure, secure a network against unauthorised logins and popular LAN attacks. It will also provide an opportunity to apply best principal security practices on a network level in the form of a written report.

About the client

The client is a small Dublin based financial organization (creditbank.ie) and have asked for your assistance with improving their current configuration on their network. They have engaged in a project which has two phases.

Phase 1 is the immediate improvement of their current practical security posture (this is hands on work which they would like you to complete ASAP). Phase 2 is a report proposal to improve their security posture for their network and also the implementation of a their new website. Phase 2 is your advice on what your recommendations are.

Phase 1: Download the packet tracer file and read the instructions carefully inside. Make any changes you feel appropriate to meet the requirements.

Phase 2: Provide security recommendations to help improve the security of their network. In addition, the webserver is yet to go live what network security and application recommendations would you provide before it does so. Remember for this part of the project you don't have to implement these changes (only recommendations are required in report).

What you will need to upload to Moodle:

1) Packet tracer file (saved as your student name)
2) Report (max 800 words).

This is an individual take home assessment and must be completed and uploaded to Moodle within the timeframe allocated.

Specific Requirements

Examine the network in the topology. The IT manager of the Creditbank has provided you with the following information and requirements:

Basic IP addressing is configured, however, some configuration is required by you. More details of this is provided in the Packet Tracer file.

You are required to configure the Routers and Switches on the LAN and WAN side. Just for your own knowledge, the bank staff currently sit on the NETWORK1 subnet and visitors to the bank (auditors etc) sit on the GUEST side.

As a proof of concept configure ONLY switch 2 and DublinRouter (unless it says otherwise) with the following. Creditbank will roll out security settings themselves on other network devices.

- Configure DHCP for both networks (GUEST and NETWORK1) as specified in Packet Tracer. Ensure PC0 can communicate with PC7. PC0 (and any other PC on NETWORK1 only) should be able to visit the webpage of www.creditbank.ie from the browser within Packet Tracer.
- Configure all devices with passwords (password below) to secure login from console, to enter privileged mode (enable password) and also remote access. Note: ensure all switches / routers are configured with SSH ONLY. As a temporary measure, they would like all switch/router passwords to be 'creditbank' until they have launched their password policy.
- Configure devices to require a minimum of 8 characters for passwords.
- Configure the switches to protect against any Layer 2 attacks. Configure switch ports so they will only accept traffic from the devices currently connected to them.
- Shutdown any ports on switches/routers that don't need to be enabled.
- Configure a suitable message of the day to instruct potential unauthorized users that the device is the property of Creditbank and only authorized users are permitted.
- Configure any other settings on switch 2 and DublinRouter you think will make the devices more secure. (HINT: look back over previous labs to get ideas e.g. portfast, bpduguard).
- Configure on the DublinRouter, add a default route based on the network. This route could be used to route all traffic to the ISP that matches any and all IP packet destinations as a last resort. Give an example of what this default route could be? Write your answer here.
- Configure an appropriate summary route to use to route back traffic from the ISP to the DublinRouter sites? (The big objective is to allow traffic to travel from Dublin branch (from either NETWORK1 or GUEST) to Galway branch and travel back again. You can test this with ping.
- Configure on the Galway Creditbank branch inter-vlan routing between the sales and HR teams. The IT manager has asked you to implement router on a stick configuration to allow these different departments to be able to communicate between one another.

Marking Scheme Summary

Description	Weighting
Phase 1: LAN and device security settings (Packet Tracer file)	0 to 10 marks
Phase 2: Report clearly explains network and security recommendations for Creditbank. This will include diagrams and references.	0 to 9 Marks
In the Appendix of your report includes running-config of: switch 2 Dublin Router ISP router Switch 4	0 to 1 Mark
TOTAL	**0 to 20 Marks**