Assessment 2 – Coursework Report - Brief

1. Module number	CSN08703
2. Module title	Cyber Security and Cryptography
3. Module leader	Rich Macfarlane
4. Tutor with responsibility for this Assessment	Rich Macfarlane
5. Assessment	Assessment 2/3 – Coursework Report
6. Weighting	50% of module assessment
7. Size and/or time limits for assessment	12-15 pages
8. Deadline of submission	After first 20 working days/4 weeks of module completed. i.e. after all taught sessions
9. Arrangements for submission	Online via Moodle Module page - Turnitin link
10. Assessment Regulations	All assessments are subject to the University Regulations
11. The requirements for the assessment	Resit by repeating the assessment.
12. Special instructions	As per the assessment document.
13. Return of work and feedback	Initial feedback will be emailed within 2 weeks of submission. More detail feedback will be available on request by each student.
14. Assessment criteria	See assessment 2 coursework specification document.

CSN08703 Assessment Specification

Rich Macfarlane

Details

Module name:	Cyber Security and Cryptography
Module number:	CSN08703
Session:	Semester 2, 2017-18
Title:	Botnet Detection and Perimeter Defense
Weighting:	50% of module
Submission:	End of module, online via Turnitin link on Moodle module page

Outline Requirements

Botnets are a particular problem, where bot agents may infect machines inside an organisation's network and connect back to a botnet controller, in order to receive commands and undertake malicious activities. The focus of this coursework is to create a virtualized testbed environment to analyse a particular botnet agent and the communications to its controller, to create and test a detection system to detect its activities, and then to mitigate its use in future with some firewall based defenses.

For this you should:

- Configure a working perimeter network topology with a firewall, DMZ, and host systems as a testbed for the coursework. Secure the VMs by changing login passwords.
- Analyse the operation of the running Bot agent and Botnet controller, including any network scanning by the bot, connections created, and any communications between the bot and controller.
- Create and test a detection system for the Botnet agent and controller using an IDS sensor.
- Create a closed perimeter, firewall policy configuration to prevent future communications for this particular botnet, but allow certain valid traffic, specified in next section.

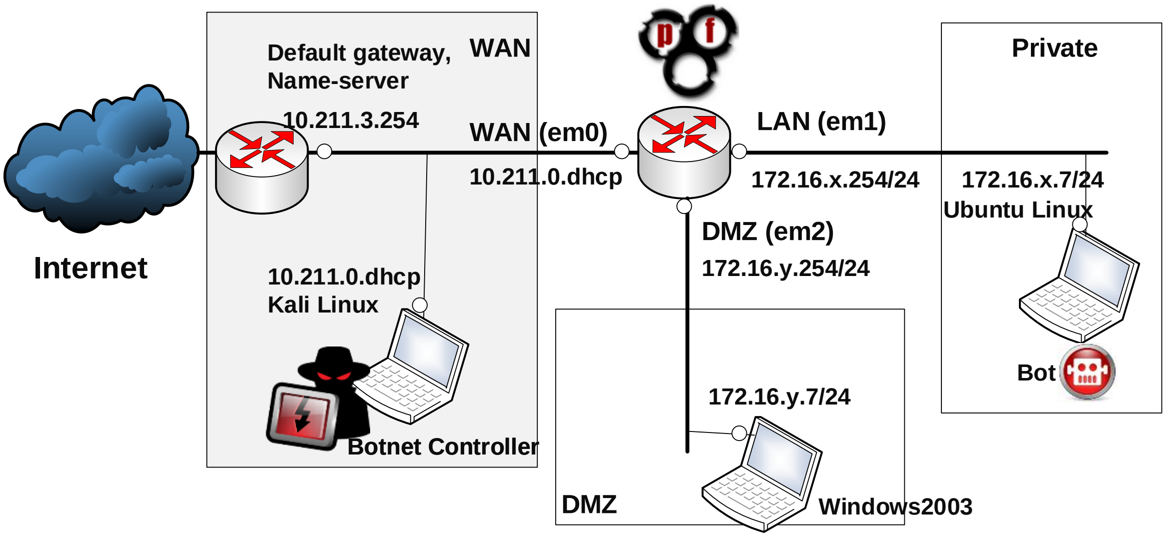

Figure 1: Perimeter Network Architecture

Your network architecture should be similar to that shown in Figure 1, with the VMs provided using two private address spaces specified for the coursework assignment. These addresses will be assigned to through Moodle. The Botnet controller program should run on the external Kali machine and the Bot agent should be run from the internal trusted Private network.

Start by allowing all traffic from the internal network out to the external network so the bot can communicate with the bot controller. Then use this architecture as your testbed to thoroughly investigate and analyse the Botnet activity. Try to plan and be scientific in the experimental method you use and don't simply run it once and report. Static analysis can then be used to compliment the dynamic analysis.

After this, design an Intrusion Detection System (IDS) which will detect the various bot activities, leading to an implementation of a prototype using a Snort sensor running on the internal Linux system. The alerts generated should be useful to a security admin. If you have time investigate tuning the rules.

Once the IDS has been tested, design and create firewall rules to close down the firewall to prevent future botnet activity, possibly highlight/log specific botnet activity, and test the configuration. Create a basic perimeter firewall solution, based around the current topology to provide a public web server from the external network, and Internet access from the internal network, as well as incorporating the botnet firewall defense.

Outline Network Security Perimeter Policy:

- WAN>DMZ Only access to web server on DMZ
- WAN>PRIVATE Prevent any access to private systems from the Internet.
- PRIVATE>WAN Inside network has access to the Internet for Web traffic, and DNS at a minimum
    - Optional challenge PRIVATE>WAN Research and Create an Egress filtering ruleset, to filter out unwanted outgoing traffic

Bot and Controller

The Bot agent and controller programs should be installed on the VMs provided to you. If you wish to create a local virtualised testbed, they will also be available for download here:

www.soc.napier.ac.uk/~40001507/2018_rbot.zip

They can be run on Linux using **mono** or Windows using .NET.

THESE **MUST ONLY BE RUN FROM WITHIN LOCAL VIRTUAL ENVIRONMENTS** AS THEY MAY ACCESS SENSITIVE MACHINE AND NETWORK INFORMATION.

Marking schedule

Research [10 marks]

A brief literature review on botnets and IDS demonstrating an understanding of the topics using research from a variety of sources (cited in the text), and for extra marks include some **critical analysis** (for example highlighting some strengths and weaknesses) and some recent real world examples. Around half a page on each topic would be fine for this section.

[10 marks]

Botnet Analysis [40 marks]

Configure a working perimeter network topology with a firewall, DMZ, and host systems as a testbed for the coursework, based on the addressing specified (see Moodle). For example an annotated network diagram, and some basic configuration/connectivity testing shown and discussed very briefly.

Use this to then analyse the operation of the running Bot agent and Botnet controller, including any network scanning by the bot, connections created, and any communications between the bot and controller. For example screen shots and brief discussion for: botnet components running, analysis tools, outputs and interesting data, tools and outputs of cracking codes. Try to be scientific in your method!

- Dynamic analysis of bot and botnet controller should include:
    - Identifying botnet network connections and traffic. Try filtering out unrelated traffic using appropriate tools such as Wireshark
    - Identify types of traffic, reconnaissance/command and control traffic
    - Identify and **analyse** specific botnet commands and response behaviour
    - Decode botnet traffic/files if necessary – some may be encoded/encrypted! Crack the messages for extra marks and clues to other behavior.

      [30 marks]
    - Challenge: create your own bot traffic so individual commands can be sent and analysed, and use experimental methods to find all possibilities.
- Optional Challenge: To verify your findings from the dynamic analysis of the botnet behavior, try to reverse engineer the bot agent and controller code and statically analyse the code, to compliment/compare results from the dynamic analysis.

[10 marks]

Prototype Defenses Implementation and Testing [40 marks]

This should define an outline prototype implementation of the defences.

- From your botnet analysis, create and test a basic prototype detection system for the Botnet agent and controller using an IDS sensor. Create IDS rules/signatures to detect the bot activity and not excessive many false positives. This section could show the Snort rules with descriptions of how they work, and screen shots of the testing/outputs and discussion on this.

  [20 marks]
- Create a closed perimeter firewall configuration to prevent/highlight future communications for this particular botnet, but allow certain valid traffic (specified in requirements spec'). Again show the configuration/rules and testing using screen shot snippets with short explanation, and any interesting discussion on the findings/outputs.

[20 marks]

References/Presentation [10 marks]

The academic report should be written in a formal style, in 3rd person, and well presented. Full academic referencing of peer reviewed papers, technical papers, books, and web sites, using thorough the Harvard referencing format.

- Reference all materials used, citing every reference in the body of the report.
- All references cited should be listed at the end of the report, using Harvard referencing format.

[10 marks]

The Coursework Report

- The report should be in 11 point text with normal margins.
- It must be typed in English.
- It must be submitted by the date shown above to the link on Moodle. If Moodle is for some reason down when you try to submit, then exceptionally it can be submitted by email to the module leader. This must be by the deadline.
- It must be completely your own work, and all written in your own words.
- The document should have page numbers, and should be submitted as a PDF.
- Total report size is **12-15 pages** plus a 1 page cover (sample cover sheet in Appendix A). Extra pages may not be graded. Cover page, References, and the Appendices are not counted in the page count, but note the Appendices are supporting materials and also typically not graded as part of the main report (so don’t simply appendix all your screen shots!)
- Please ask questions if you have problems.

You can submit the report to Turnitin coursework submission link multiple times. Only the last submission you make will be graded. Be aware there is a 24 hour delay between submissions, to prevent misuse of the service. Check the similarity index generated, and work on keeping this as low as possible, but review what is being highlighted as some things, such as configuration, and references may produce many similarity matches to other work, and so long as the matches are not all from one source, these should not be of concern. If you are in any doubt about your similarity result then please ask.

If you have attempted this coursework before, for example repeating the coursework as a resit attempt, each attempt must be a completely new attempt. Do not use any text from a previous attempt.

Appendix A – Sample Cover Sheet

Botnet Detection and Perimeter Defense

Coursework Submission for CSN08703

Edinburgh Napier University 2017-2018 Trimester 2

Name

Matric No

Month 2018

Appendix B – Feedback Form

CSN08703 Coursework - Feedback Form

Matric No: ________________________

	Comment	Mark
Research		/10
Botnet Analysis		/40
Prototype Defenses Implementation and Testing		/40
References/Presentation		/10

First marker Initials: **Final mark: _______/100**

Additional Comments:

Please note that this mark is provisional, and is provided to give you an indication of your grade. At the end of the module, the quality of all your coursework will be moderated to provide a final grade.

Fail	**Pass**	**Merit**
0-39	40-64	65-100