CSN09112 Coursework Assessment Specification (CW2)

Details

Module name: Network Security and Cryptography

Session: Trimester 1, 2022-2023

Title: Botnet Analysis with Intrusion Detection

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 out on the Internet, 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.

For this you should:

- Setup a cloud instances of your evaluation infrastructure. This should include a Windows server host and a Linux server. Snort should be installed on both machines and will detect network traffic generated by the bot and the controller.
- Analyse the operation of the running Bot agent and Botnet controller, including any network scanning by the bot, activity on the host, network 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.

The controller and the bot should be placed on different hosts, and then enabled to communication. It is then your task to capture and analyse the traffic generated and try and build up an understanding of the requests and replies that are used by the bot and controller. Once you understand the requests and replies, then create a Snort-based IDS detector to detect the presence of the Bot and Controller.

Botnet Bot and Controller

The bot and controller are available for download here:

```
# wget https://github.com/billbuchanan/csn09112/blob/master/week07_dig_cert/labs/certs.zip?raw=true
# mv certs.zip?raw=true certs.zip
# unzip cert.zip
```

It can be run on Linux using mono or on Windows using .NET.

Marking schedule

Research [20 marks]

A brief literature review on botnet operations and IDS demonstrating understanding of the topics using research from a variety of quality sources (cited in the text), and for extra marks include some **critical analysis** (for example highlighting strengths and weaknesses).

Botnet Analysis [40 marks]

Analyse the operation of the running Bot agent and Botnet controller, including any connections created by the bot, host activities on the victim, any communications between the bot and controller, and any network scanning by the bot. For example screen shots and brief discussion for: botnet components running, analysis tools, outputs and interesting data, tools and outputs of cracking codes, with brief discussion.

- Dynamic analysis of bot and botnet controller
    - Identifying botnet network connections and traffic, filtering out unrelated traffic using appropriate tools such as Wireshark
    - Identify types of traffic, reconnaissance/command and control traffic
    - Identify specific botnet commands and responses
    - Decode botnet traffic if necessary – some may be encoded/encrypted! Crack the messages for extra marks
    - Challenge: create your own bot traffic so individual command can be sent and analysed separately
- Challenge: To verify your findings from the dynamic analysis of the botnet behaviour, try to reverse engineer the bot agent code and statically analyse the code.

IDS Detector [30 marks]

- 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.

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.

The Coursework Report

The following outlines some of the details around the submission of the coursework:

- 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 up to 20 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.
- 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.