MITS5004 IT Security - 2020S1
Assignment No 3 – Project Work
Critical Analysis of Security Tools

Submission Guidelines:

This assessment task is major assignment and done in groups (3-4 students) and you will be required to work together to apply your knowledge, to analyse critically the tools used in IT security. In this assessment you will work in groups by sharing individual tasks on a major practical based case to analyse and devise solutions to security threats, identify security components needed and implement a solution. This will cover all the four learning outcomes of the unit. All submissions are to be submitted through turn-it-in. Drop-boxes linked to turn-it-in will be set up in the Unit of Study Moodle account. Assignments not submitted through these drop- boxes will not be considered. Submissions must be made by the due date and time. This Assignment-3 is a group assignment and contributes 30% of your unit marks - Critical Analysis of Security Tools (Due in Session 12)

The turn-it-in similarity score will be used in determining the level if any of plagiarism. Turn-it-in will check conference web-sites, Journal articles, the Web and your own class member submissions for plagiarism. You can see your turn-it-in similarity score when you submit your assignment to the appropriate drop-box. If this is a concern you will have a chance to change your assignment and re-submit. However, re-submission is only allowed prior to the submission due date and time. After the due date and time have elapsed you cannot make re-submissions and you will have to live with the similarity score as there will be no chance for changing. Thus, plan early and submit early to take advantage of this feature. You can make multiple submissions, but please remember we only see the last submission, and the date and time you submitted will be taken from that submission.

Your document should be a single word or pdf document containing your report.

Objective(s)

This assessment item relates to the unit learning outcomes as in the unit descriptor. This assessment is designed to improve the ability of students to critically analyse security tools and present their findings. This assignment also provides an opportunity to work in a group and to achieve a joint objective.

Description

Each group is required to critically analyse any 2 security tools from the list and demonstrate the functionality of the tools in a video presentation. The list of tools for the assignment include:

- Hydra
- Maltego
- NMap
- Zed Attack Proxy
- SqlMap
- Metasploit Framework
- Burp Suite
- Nessus
- Nikto
- Snort
- Wireshark
- Siege

The tools need to be launched in Linux terminal (a user could be created for any member of the group).

Each group is required to:

1. Install and launch the 2 security tools in Linux terminal (a user could be created for any member of the group). Screenshots need to be provided with a brief description.
2. Evaluate 4 features of each tool. Description and screenshots need to be provided for each tool.

3. Critically analyse each tool in terms of:
    a) Ease of Use
    b) Performance
    c) Scalability
    d) Availability
    e) Reporting and analytics
4. **Demonstrate the 4 features of the tool in a short video not more than 5 Minutes**. Each student is required to demonstrate 1 feature for each tool. If a student does not demonstrate in the video, the student will not be marked for the demonstration marks

Instructions

These instructions apply to Assignment 3 Group Assignment – Critical Analysis of Network Security Tools. The students are required to form a group comprising of 3 to 4 students from the same session. The group is required to notify the lecturer of the students in the group and the network security tools that they have opted for by the end of week 6.

Submissions

Each group is required to submit a single report and a video presentation on the given link on Moodle. Each student is required to demonstrate 1 feature of each network security tool in the video presentation.

Submit your report to the Moodle drop-box for Assignment 3. Note that this will be a turn-it-in drop box and as such you will be provided with a similarity score. This will be taken into account when grading the assignment. Note that incidents of plagiarism will be penalized. If your similarity score is high you can re-submit your report, but re-submissions are only allowed up to the due date. If you submit your assignment after the due date and time re-submissions will not be allowed.

Please Note: All work is due by the due date and time. Late submissions will be penalized at the rate of 10% per day including weekends.

Your report should be limited to approx. 2000 words (not including references). Use 1.5 spacing with a 12 point Time New Roman font. Citation of sources is mandatory and must be in the IEEE style.

Marking Guide: 75 Marks

Task	Description	Marks
Introduction	This section should include a few sentences which provide an outline of the assignment.	5
Report Layout	The report style, language and structure should be appropriate.	5
Tool Launch	Install and launch the 2 security tools in Linux terminal (a user could be created for any member of the group). Screenshots need to be provided with a brief description.	6
Evaluation	Evaluate 4 features of each tool. Description and screenshots need to be provided for each tool.	16
Analysis	Critically analyse each tool in terms of: a) Ease of Use b) Performance c) Scalability d) Availability e) Reporting and analytics	20
Demonstration	Each group is required to submit a video demonstration of not more than 5 minutes, each member is required to demonstrate 1 feature of each tool.	15
Conclusion	Summary of the report.	4
References	Follow the IEEE style	4

Plagiarism and collusion

All students in the groups are warned that VIT takes a serious stand on Plagiarism and collusion. VIT will apply heavy penalties if individuals and groups are caught in academic misconduct. VIT uses sophisticated TURNITIN software built-in the LMS Moodle system for detecting plagiarism and collusion.

Note: *Turnitin is a text-matching software that checks a student's written work against electronic texts from the Internet, published works (such as journal articles and books), and assignments/reports/articles previously submitted to Turnitin or otherwise elsewhere by other students. So please be warned!*