AD006 - Associate Degree in Information Technology INTE2643- Cyber Security Foundations

|  |  |  |  |
| --- | --- | --- | --- |
| *Assessment 3*  ***Attack Metasploitable machine using kali tools to gain access remotely*** | | | |
| **Weighting** | 30%  50 Marks | **Due Date** |  |
| **Teacher** | Mohamed Farrag | **Contact details** | [Mohamed.farrag@rmit.edu.au](mailto:Mohamed.farrag@rmit.edu.au) |
| **Individual or Group**  **Assessment** | Individual | | |

|  |
| --- |
| This assessment task is expected to take you a minimum of *(10)* hours. |
| **Introduction:** |
| *Metasploit is a powerful open-source penetration testing framework that facilitates the discovery, exploitation, and validation of vulnerabilities in computer systems. Developed by Rapid7, Metasploit provides a*  *comprehensive set of tools for security professionals, ethical hackers, and penetration testers to assess the security of networks, applications, and systems.*  *For those interested in delving deeper into Metasploit and exploring its extensive capabilities, I recommend visiting the official Metasploit website at* [*https://www.metasploit.com/*](https://www.metasploit.com/)*.*  *On the website, you'll find valuable resources, documentation, tutorials, and community forums that can enhance your understanding of Metasploit and its applications in penetration testing and ethical hacking.*  *In this assignment, the aim is to help you learn by applying what you know in practical situations* |
| **Assessment Objectives** |
| **Part A: Gain Remote Access**  Step 1: Identify Target System  Identify the target system's IP address. Step 2: Select an Exploit  Use Metasploit to identify a suitable exploit for an open port on the target system. Step 3: Configure Payload  Configure a Metasploit payload for remote access. Ensure compatibility with the target system. |

|  |
| --- |
| Step 4: Exploit  Execute the exploit and gain remote access to the target system.  **Part B: Copy a File**  Step 5: Gather Information  Identify the file you want to copy from the target system. Step 6: Use Post Exploitation Modules  Utilize Metasploit's post-exploitation modules to interact with the target system. Step 7: Copy the File  Use Metasploit commands or tools to copy the identified file from the target system to the local machine. |
| **Required Setup:**   1. **Virtual Box (VBox):**    * Ensure that you have VirtualBox installed on your system. If not, download and install it from the official website: <https://www.virtualbox.org/> 2. **Kali Linux Virtual machine:**    * Set up a virtual machine (VM) in VirtualBox and install Kali Linux on it. Follow the official installation guide for Kali Linux on VirtualBox: https://[www.kali.org/docs/virtualization/install-virtualbox-image/](http://www.kali.org/docs/virtualization/install-virtualbox-image/) 3. **MSF installed in Kali Linux:**    * Open Kali Linux in VirtualBox.    * Ensure Metasploit Framework (MSF) is installed. If not, install it by running the following commands: sudo apt update sudo apt install metasploit-framework 4. **Metasploitable Virtual machine:**    * Create another VM in VirtualBox to install Metasploitable.    * Download Metasploitable from the official source: https://sourceforge.net/projects/metasploitable/    * Follow the instructions to install Metasploitable on the VirtualBox VM.   **Note:** Ensure that your system meets the minimum requirements for running virtual machines, and always exercise ethical and legal practices when conducting any security-related activities. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Assessment Tasks:** | | | | | | |
| 1. **Configuration: [10 Marks]**    1. Ensure Kali Linux and Metasploitable Linux are installed in VirtualBox. (Screenshots)        * 1. Show the connection between Kali Linux and Metasploitable Linux (Screenshot).        1. **Generating the Target File: [10 Marks]**    1. Apply asymmetric cryptography (RSA) to encrypt the combination of your name and student ID, then store the resulting ciphertext in a file named info.txt.        * 1. Use a steganography tool of your choice to conceal the private key within an image named secret.jpg.      * 1. Save info.txt and secret.jpg in the home/Desktop directory of Kali Linux.      1. ***Establishing Remote Connectivity*: [30 Marks]**    1. Use the MSF framework to scan all open ports on Metasploitable.        * 1. Use one of the open ports to establish a remote session from Kali Linux to Metasploitable.      * 1. Copy info.txt and secret.jpg to Metasploitable.     **\*In this assessment task, you can use AI tools to assist you. All use of AI tools and their outputs should be appropriately acknowledged and referenced. \*** | | | | | | |
| Refer to the assessment rubric for grading.  **Rubric for grading**  **Assessment High**  **criteria Distinction Distinction** | | | **Credit** | **Pass** | **Fail** |  |
|  | Configuration | [8-10 points] [7 points] Kali Kali Linux and Linux and  Metasploitable Metasploitable are running are running successfully in successfully in VBox and both VBox and both machines can machines can ping each other ping each other using terminal. using terminal.  Well documented Not Well  with adequate documented and screenshot as inadequate evidence screenshot as  evidence | [6 points] | [ 5 points] | [0-4 points] |
| (10)  5 marks for | Kali Linux and  Metasploitable are running | Kali Linux and  Metasploitable are running | One or both  machines are not fired up |
| each task | successfully in | successfully in | appropriately in |
|  | VBox but they | VBox but they | VBox. |
|  | can’t ping each | can’t ping each |  |
|  | other. Well | other. Poor |  |
|  | documented | documentation. |  |
|  | with adequate |  |  |
|  | screenshots. |  |  |
| Generating | [8-10 points] [7 points] | [6 points] The | [5 points] | [0-4 points] |
| the Target File (10)  First Task - 4 | personalData.txt personalData.txt  file contains the file contains the  cyphertext of cyphertext of appropriate data appropriate data | plain text was  not formed as  per instruction or embedding | Any one out of  the three tasks  are not done as per instructions | Any two or all  the tasks are  not completed or failed to |
| Marks | as per as per | of private key | and |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Second Task - 4 Marks  Third Task - 2 Marks | instruction. The private key is correctly embedded into secret.jpg and  they are stored in the home directory of Kali Linux. Well documented with adequate screenshot as  evidence | instruction. The private key is correctly embedded into secret.jpg and  they are stored in the home directory of Kali Linux. Not Well documented and inadequate screenshot as  evidence | and is not done appropriately or the files are not stored as per instruction.  [Any one task is not done appropriately] Documentation is clear with adequate screenshots and  annotations | documentation is also not clear. | follow the instruction. |  |
| Establishing Remote Connectivity (30)  10 Marks for each Task | [24-30 points] All three tasks completed + Well Formatted Documentation + Adequate Screenshots with clear annotations | [21-23 points] All three tasks completed + Poor Documentation + Inadequate Screenshots | [18-20 points] Any one task is incomplete + Well Formatted Documentation  + Adequate Screenshots with clear  annotations | [15-17 points] Any one task is incomplete + Poorly Formatted Documentation + Inadequate Screenshots with clear | [0-14 points] Two or all the tasks are incomplete + Poor  Documentation  + Inadequate  screenshots or annotations. |
| **Submission requirements** | | | | | | | |
| *Prepare a report, including a cover page.*  *The report should be professionally formatted, with the cover page containing your name, student ID, unit code, and unit title.*  *Include screenshots of your work with brief annotations for each screenshot. Sequence screenshots logically for clear and distinctive follow-through.*  *Ensure that your report demonstrates original work and avoid copying from others.*  *submit your finished report for Assessment 3 in Canvas by the specified due date. Ensure that the document is saved in either DOCX or PDF format.* | | | | | | | |
| **Academic integrity** | | | | | | | |
| It is important that you submit material which is your own work. The University provides information for  students on academic Integrity through the RMIT website. If you are unsure about academic matters, please be sure to ask your teacher for information. | | | | | | | |
| **Assessment Policy** | | | | | | | |
| *We understand that our students balance the demands of home responsibilities, work life and study commitments. It may not always be possible to hand in assessments on time. The university has policies that allow for late submission, including extension applications and special considerations. Applying for late submission with a valid reason will prevent penalties. Please refer to the Submission, Extension and Special Consideration policies page to find out the process and required evidence to support your request.*  ***Extensions:***  *If you will not be able to meet the due date for an assessment, you may apply to your teacher for an extension of up to seven days by completing the*  *Application of Extension*  [*https://www.rmit.edu.au/content/dam/rmit/documents/Students/Student\_forms/Application-for-extension-*](https://www.rmit.edu.au/content/dam/rmit/documents/Students/Student_forms/Application-for-extension-of-time-to-submit-work.pdf)[*of-time-to-submit-work.pdf*](https://www.rmit.edu.au/content/dam/rmit/documents/Students/Student_forms/Application-for-extension-of-time-to-submit-work.pdf)  *Applications for an extension of time must be received 24 Hrs before the due date for an assessment.* | | | | | | | |

***Special Consideration:***

If unforeseen circumstances beyond your control prevent you from submitting your work on time you may be eligible to apply for special consideration. For further information regarding special consideration, please refer to the

<https://www.rmit.edu.au/students/student-essentials/assessment-and-results/special-consideration>

***Late submission penalty:*** *Deduct 10% of total marks per day late*