|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Student Name |  | | Student Number | |  |
| Unit Code/s & Name/s | VU23215 Test concepts and procedures for cyber security | | | | |
| Cluster Name  *If applicable* | N/A | | | | |
| Assessment Type | Assignment  Project  Case Study  Portfolio  Third Party Report (Workplace)  Third Party Report (Peer)  Other | | | | |
| Assessment Name | Cyber security vulnerabilities testing procedures and mitigation strategies | | Assessment Task No. | | 2 of 2 |
| Assessment Due Date |  | | Date Submitted | | / / |
| **Assessor Feedback:** | | | | | |
| **Attempt 1** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| **Student provided with feedback and reassessment arrangements**  *(check box when completed)* | | | Date scheduled for reassessment | | / / |
| **Attempt 2** | Satisfactory | Unsatisfactory | | Date | / / |
| Assessor Name |  | | Assessor Signature | |  |
| Note to Assessor: Please record below any reasonable adjustment that has occurred during this assessment e.g. written assessment given orally. | | | | | |
|  | | | | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assessment Criteria / Benchmarks  ***The evidence submitted demonstrates that the student has satisfactorily:*** | Attempt 1 | | Attempt 2 | |
| **Date**  \_\_/\_\_/\_\_ | | **Date**  \_\_/\_\_/\_\_ | |
| Y | N | Y | N |
| PART 1 - Review of cyber security legislative and regulatory requirements for Australian organisations | | | | |
| 1.1 At least two (2) current cyber security testing have been researched. For each methodology selected, the student has identified its suitability, features and complexity to learn. Table provided has been completed |  |  |  |  |
| 1.2 The testing tools provided have been researched, and a brief description of each, including their strengths and weaknesses, has been presented. The table provided has been completed. |  |  |  |  |
| 1.3 At least three (3) vulnerabilities of the application layer have been identified and explained |  |  |  |  |
| 1.4 Three (3) policies that can be used to minimise the vulnerabilities of the application layer have been identified, reviewed and explained. |  |  |  |  |
| 1.5 At least three (3) physical vulnerabilities of the WLAN have been identified |  |  |  |  |
| 1.6 Current frameworks that can be used to identify application layer vulnerabilities have been identified. |  |  |  |  |
| PART 2 - LAB: Scenario 1 Cyber security common threats and mitigation strategies | | | | |
| Activity 1: Configure the Lab Environment | | | | |
| 2.1 Network settings for three of the five virtual machines (VMs) in the lab environment have been configured according to LAB notes provided. |  |  |  |  |
| 1. Provided the full pathname of the configuration file where the network settings for Kali Linux and Metasploitable are stored. |  |  |  |  |
| 1. Screenshots from Kali and Metasploitable have been provided. Name and date are displayed in the screenshot. |  |  |  |  |
| 1. Screenshots of the output of the command-line from Kali and Metasploitable showing the actual IP address and netmask have been provided. |  |  |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. A screenshot of the contents of the network configuration file from the Ubuntu system has been provided. Name and date are displayed in the screenshot. |  |  |  |  |
| 1. A screenshot of the output of the command-line from Ubuntu desktop displaying the actual IP address and netmask has been provided. |  |  |  |  |
| 1. A screenshot of the ping command to verify end-to-end network connectivity has been provided. The screenshot displays IP addresses of all three systems: Kali, Metasploitable and Ubuntu. |  |  |  |  |
| 1. Summary of steps to troubleshoot basic network connectivity in the network including ping and traceroute commands has been provided. The importance of the commands has been explained. |  |  |  |  |
| Activity 2: Use tools to identify target systems | | | | |
| 2.2 Performed the activities for the second set of lab notes including the use of nmap and amap tools. Table provided completed for the following commands: -sT, -F, -A,sC and -PU |  |  |  |  |
| 1. A screenshot of the output of the nmap command for nmap -sT 192.168.1.100 has been provided. |  |  |  |  |
| 1. A paragraph to describing the command has been provided. |  |  |  |  |
| 1. Screenshot of the output of the nmap -sT command has been provided. |  |  |  |  |
| 1. What information in the nmap outputs gives you the impression that Ubuntu is a client desktop system whereas Metasploitable is a server system? Question answered. |  |  |  |  |
| 1. Used nmap with command-line options: -F, -A, -sC and -PU (one at a time) to scan the Metasploitable system. |  |  |  |  |
| 1. Question answered. What output information for Metasploitable is given by each of these nmap options that is not given by the other options? |  |  |  |  |
| 1. Screenshot of the amap tool retrieving the banner from TCP port 22 of the Metasploitable system has been provided. |  |  |  |  |
| 1. What Application Protocol is running on TCP port 22 of your Metasploitable system? What software and what software version TCP port 22 of your Metasploitable system? Question answered. |  |  |  |  |
| 1. Explain the ethical hacking principle that tells you to only use the nmap and amap tools on networks where you have permission to do so, or on networks which you control yourself. Question answered. |  |  |  |  |
| Activity 3: Use Wireshark to monitor, capture and analyse network traffic | | | | |
| 2.3 Used Wireshark network sniffing tool to analyse the captured network traffic in the file TCP\_Example.cap. |  |  |  |  |
| 1. What TCP port is the web client using in the HTTP conversation? Question answered. |  |  |  |  |
| 1. Based on the contents of the HTTP conversation, what operating system is on the client and what web browsing software is being used? Question answered. |  |  |  |  |
| 1. Is it the client or the server that initiates the closing of the TCP connection in the HTTP conversation?   What evidence in the captured traffic leads you to this conclusion? Questions answered. |  |  |  |  |
| 2.4 Used Wireshark network sniffing tool to analyse the captured network traffic in the file UDP\_Example.pcapng. |  |  |  |  |
| 1. Described how to filter and display only the UDP traffic in the captured traffic. |  |  |  |  |
| 1. Described how to display the contents of UDP packet #1169 in the captured traffic. |  |  |  |  |
| 1. In UDP packet #1169, what DNS query is the client making? Question answered. |  |  |  |  |
| 1. Based on your traffic analysis, what is the answer to the DNS query in UDP packet #1169? Question answered. |  |  |  |  |
| Activity 4: Analysing HTTP conversations | | | | |
| 2.5 Performed the activities in the fourth set of lab notes to use the Wireshark tool to capture and analyse HTTP network conversations. |  |  |  |  |
| 1. A screenshot displaying three packets in the three-way TCP opening handshake from the web client on Kali to the IIS web server on Windows 10 has been provided. |  |  |  |  |
| 1. Description of why the TCP flags are turned on the opening handshake has been provided. |  |  |  |  |
| 1. A screenshot displaying the three packets in the three-way TCP closing handshake has been provided. |  |  |  |  |
| 1. Description of why the TCP flags are turned on the closing handshake has been provided. |  |  |  |  |
| 1. A screenshot of the HTTP conversation with the three client requests to fetch three documents from the IIS web server has been provided. |  |  |  |  |
| 1. Description of the HTTP conversation with the three client requests to fetch three documents from the IIS web server has been provided. |  |  |  |  |
| 1. A screenshot of the HTTP conversation from the Windows 10 web client to the Apache web server has been provided. |  |  |  |  |
| 1. Description of the HTTP conversation from the Windows 10 web client to the Apache web server has been provided. It includes server, version and operating system name. |  |  |  |  |
| Activity 5: Performing denial of service attacks | | | | |
| 2.6 Performed the activities in the fifth set of lab to use the Wireshark tool to capture and analyse Telnet conversations and denial of service attacks. |  |  |  |  |
| 1. A screenshot of the Telnet Application Layer conversation between Kali and the Windows 7 system has been provided. |  |  |  |  |
| 1. Questions answered. What sensitive information has been sent by the Telnet client to the server in plain text (i.e. not encrypted)? Explain why this is a security risk if a third party was able to sniff the network traffic. |  |  |  |  |
| 1. Three questions for this section have been answered. Explanation provided for how the SSH protocol is a lower security risk than the Telnet protocol in this situation. |  |  |  |  |
| 1. A screenshot showing the open TCP ports on the Windows 7 system has been provides. It includes the student name. |  |  |  |  |
| 1. A screenshot of the output of the “dos.py” denial of service script as it attacks the Windows 7 system has been provided. It includes the student name. |  |  |  |  |
| 1. A screenshot of the ten TCP SYN packets that were sent in the DoS attack, with the details of the TCP fields shown has been provided. |  |  |  |  |
| 1. Questions answered. What are the values for the Sequence number, the Windows size, and the TCP segment length in the packet in the above screenshot? |  |  |  |  |
| 1. A screenshot of some of the attack packets which are SYN packets sent from the fake IP address - after running “ettercap” DoS against the Windows 7 system has been provided. |  |  |  |  |
| 1. At least three ways that could mitigate TCP SYN DoS against a system have been described. |  |  |  |  |
| The meaning of the terms “RFC documents” and “BCP documents” have been explained. |  |  |  |  |
| 1. One RFC document and one BCP document that deals with DoS mitigation have been identified. |  |  |  |  |
| Activity 6: Performing Man in the Middle attacks | | | | |
| 2.7 Performed the activities in the sixth set of lab notes for this unit to use the arpspoof and dsniff tools to perform a man in the middle attack. |  |  |  |  |
| 1. Questions answered. Explain how arpspoof convinces a client and server that they are still communicating directly with each other when they are not. Identify which layer of the OSI model is in action. |  |  |  |  |
| 1. Screenshots of a successful ping from Ubuntu 14.04 to Windows 7, a successful ping from Ubuntu 14.04 to Kali, and the ARP table on Ubuntu have been provided after arpspoof targeting both OS. |  |  |  |  |
| 1. Explanation provided on how the information in the ARP table indicates that an ARP spoofing attack is in progress. |  |  |  |  |
| 1. Screenshots of a successful ping from Windows 7 to Ubuntu 14.04, a successful ping from Windows 7 to Kali Linux, and the ARP table on Windows 7 have been provided. |  |  |  |  |
| 1. Screenshots to confirm that Kali is the man-in-the-middle of the conversation have been provided. Screenshots display HTTP packets with the IP addresses of both Ubuntu 14.04 and Windows 7 systems. |  |  |  |  |
| 1. Explanation of what dsniff can do, and which Application Layer protocols it understands has been provided. |  |  |  |  |
| 1. A screenshot of the output from the dsniff command where it has captured sensitive information via a man in the middle attack has been provided. The output has been explained. |  |  |  |  |
| 1. The difference between DDOS and DOS attacks has been explained. |  |  |  |  |
| Activity 7: Attacking Metasploitable-2 | | | | |
| 2.8 Performed the activities in the seventh set of lab notes for this unit to carry out a Samba Command Execution attack on the Metasploitable-2 system. |  |  |  |  |
| 1. Provided a screenshot of the output from the nmap command that you have run on your Metasploitable-2 system. Name and student number included on the image provided |  |  |  |  |
| 1. Provided a screenshot of the options that are necessary for the usermap\_script exploit. |  |  |  |  |
| 1. Provided a screenshot of the shell acquired from exploiting the samba vulnerability on the Metasploitable-2 system. |  |  |  |  |
| PART 3 - Scenario 2: Demonstrating ethical hacking principles and procedures  TASK 1 Ethical hacking information gathering stage | | | | |
| 3.1 Trojans, viruses and worms that have been spreading in the last 90 days identified. |  |  |  |  |
| 3.2 Explained at least three (3) legal implications of illegal hacking and their consequences. Answer refers to Australian Cyber Crime legislation. |  |  |  |  |
| 3.3 Described at least two (2) system hacking methodologies that can be used in ethical hacking activity in Task 2. |  |  |  |  |
| 3.4 Described, in detail, the fundamentals of penetration testing. |  |  |  |  |
| 3.5 Explained the process involved in footprinting an organisation’s computer system. |  |  |  |  |
| 3.6 Described at least two (2) enumeration methodologies that can be used to acquire usernames. |  |  |  |  |
| TASK 2 - Demonstrating ethical hacking | | | | |
| 3.7 Passive reconnaissance conducted. It includes searching common vulnerabilities and exposures (CVEs), job boards, the organisation’s own website, user groups/bulletin and social networking sites. Screenshots provided. |  |  |  |  |
| 1. Described the ethical hacking process and procedures used in the activity. |  |  |  |  |
| 1. Outlined and demonstrated at least two (2) base-level troubleshooting procedures. |  |  |  |  |
| 1. Outlined and demonstrated the enumeration techniques used to acquire usernames. |  |  |  |  |
| 1. Outlined the footprinting information collected from the organisation. |  |  |  |  |
| 1. Identified the tools used to port scan the network. |  |  |  |  |
| 1. Identified the sniffing tools used and outlined the purpose of the tools. |  |  |  |  |
| 1. Explained what CVEs are and how they can be used in this activity. |  |  |  |  |
| 3.8 A summary of WLAN hardware/software vulnerabilities has been provided and include explanations of how the organisation has addressed those issues and how leaving the WPS ON on a wireless router could be exploited. |  |  |  |  |
| 3.9 Listed some zero-day attacks on DNS servers. Explanation provided for potential vulnerabilities and mitigation plans. Strategy to enhance current policies has been described. |  |  |  |  |
| 3.10 A strategy specifically designed to secure the organisation’s web server has been developed and includes the security of the server itself as well as securing the network. |  |  |  |  |
| 3.11 Explained heuristics-based string analysis and identified the toolsets that could be used to determine the susceptibility towards particular threats. |  |  |  |  |
| 3.12 At least three (3) security vulnerabilities have been identified. For each vulnerability, adequate mitigation strategies have been outlined. |  |  |  |  |
| PART 4 - Scripting for cyber security environments using Python | | | | |
| 4.1 A Python script that pings each host on a given network has been provided and outputs only those hosts that are active. |  |  |  |  |
| 4.2 A program to conduct a passive attack on the network has been provided. The output reveals open ports on the various host servers. |  |  |  |  |
| 4.3 A program to retrieve information from one of the open ports identified has been provided and uses appropriate protocols to access the port. |  |  |  |  |
| 4.4 Three (3) of Python’s third-party libraries for ethical hacking have been identified and a description and its best security features and suitability provided. |  |  |  |  |
| PART 5 - Contingency task | | | | |
| 5.1 An appropriate solution has been provided for the contingency problem presented. |  |  |  |  |