ASSIGNMENT/ASSESSMENT ITEM COVER SHEET

Student Name: Brock (FIRST NAME) **Brinkworth** (FAMILY / LAST NAME)

Student Number: 3 3 3 1 9 5 2 Email: c3331952@uon.edu.au

Course Code	Course Title
comp3500	Security Attacks
(Example) A B C D 1 2 3 4	*(Example)* Intro to University

Campus of Study: Callaghan (eg Callaghan, Ourimbah, Port Macquarie)

Assessment Item Title: Security Attacks Analysis and Mitigation Strategie Due Date/Time: 15/05/2022

Tutorial Group (If applicable): Word Count (If applicable):

Lecturer/Tutor Name: Kallol Krishna Karmakar

Extension Granted: ○ Yes ◉ No Granted Until:

Please attach a copy of your extension approval

NB: STUDENTS MAY EXPECT THAT THIS ASSIGNMENT WILL BE RETURNED WITHIN 3 WEEKS OF THE DUE DATE OF SUBMISSION

Please tick box if applicable

☒ *Students within the Faculty of Business and Law, Faculty of Science and Information Technology, Faculty of Engineering and Built Environment and the School of Nursing and Midwifery:*
I verify that I have completed the online Academic Integrity Module and adhered to its principles

☐ *Students within the School of Education:*
"I understand that a minimum standard of correct referencing and academic literacy is required to pass all written assignments in the School of Education; and I have read and understood the School of Education *Course Outline Policy Supplement,* which includes important information related to assessment policies and procedures.

I declare that this assessment item is my own work unless otherwise acknowledged and is in accordance with the University's academic integrity policy available from the Policy Library on the web at http://www.newcastle.edu.au/policylibrary/000608.html
I certify that this assessment item has not been submitted previously for academic credit in this or any other course. I certify that I have not given a copy or have shown a copy of this assessment item to another student enrolled in the course.

I acknowledge that the assessor of this assignment may, for the purpose of assessing this assignment:
- Reproduce this assessment item and provide a copy to another member of the Faculty; and/or
- Communicate a copy of this assessment item to a plagiarism checking service (which may then retain a copy of the item on its database for the purpose of future plagiarism checking).
- Submit the assessment item to other forms of plagiarism checking.

DATE STAMP HERE

I certify that any electronic version of this assessment item that I have submitted or will submit is identical to this paper version.

Turnitin ID: (if applicable)

Insert this way

Signature: Date: 9/05/2022

To copy and paste the completed form into another document use the Adobe `snapshot' tool.

Print Form

THE UNIVERSITY OF NEWCASTLE AUSTRALIA

COMP3500: Security Attacks Analysis and Mitigation Strategies Assignment 2

Table of Contents:

1. What is a zero-day attack and why is it difficult to deal with zero-day attacks? Explain how polymorphism and metamorphism behaviour further complicate the detection of these attacks.

- A zero-day attack is when a developer finds a flaw in their systems which is not yet fixed, and a hacker uses the vulnerability to exploit their way into the system.

- The targets of zero-day attacks are Operating systems, web browsers, office applications, open-source components, hardware and firmware. This means there are many types of targets including individuals on vulnerable machines, individuals with business data, large businesses and organisations, government agencies, and political targets.

- Types of hackers who use this include criminals for financial gain, hackers motivated by political or social causes, hackers doing espionage to spy, and cyberwarfare countries attacking infrastructure

- It is hard to deal with zero-day attacks because the vulnerability is only just become known and therefore still must be figured out and patched. One of the most effective zero-day preventions is to deploy a web application firewall or a network-based firewall which review all incoming traffic and filters out malicious inputs that may be targeting a vulnerability.

- If a zero-day attack has occurred a user may notice their system behaving differently if the intruder has changed the system, if the intruder did not change anything that can be noticed by a user the intrusion will go unnoticed.

- Polymorphic Malware is the most common malware that is widely used in more than 94% of all malware executables. This type of malware changes its identities constantly to not get detected on a system. The types of malwares it most commonly is used in include viruses, worms, trojans, bots and keyloggers.

- Metamorphic malware is more advanced than polymorphic malware, they disguise their malicious code to avoid detection from anti-malware services which makes them more difficult to detect and remove. An example of a metamorphic malware is the virus called Zmist which was discovered in the early 2000s by a Russian author named Z0mbie. This was the first known use of the technique code integration which merged the separate code of Zmist and a target application. The detection of these viruses is more difficult because they disguise themselves, but it is not impossible, and dictionaries are updated to help find these viruses.

2. Consider sample home network shown in Figure 1. John and Jack are connected to Internet using Gateway with built-in DHCP server provided by their Internet Service Provider (ISP).
a. John is trying to access www.google.com using web browser on his laptop.
Explain the background operation in the web browser which enables John to access the google.com server.

- The laptop will first try to request for an Ip address by running a DHCP protocol to obtain the IP Address from the local DHCP server in the router and that should also come with the other information required. The laptop's Operating System creates the DHCP request and then puts the UDP ports to request the IP Address message which is placed into an IP datagram. If the IP Address is not found, the IP datagram is then placed into the Ethernet Frame which is then broadcast to all devices attempting to connect to the DHCP server. This broad cast Ethernet frame is the first packet sent from the laptop out of the internal network to the Ethernet switch. When the router gets the Ethernet frame broadcasted which will have the dynamic host configuration protocol request in its interface, the IP datagram is extracted from the frame. The payload id de-multiplexed to UDP and DHCP and the message is extracted from the UDP segments. The DHCP server can allocate data in the classless Inter-Domain Routing range, and this is used in DHCP ACK Message with the IP address and DHCP server IP and put into the IP Datagram with the UDP segment. Once the DHCP ACK frame is sent via switch to the router it forwards the Ethernet frame to output leading to the laptop.

- Once the laptop receives the DHCP ACK, it extracts the IP datagram from the ethernet frame, the UDP segment from the IP datagram, and the DHCP ACK message from the UDP segment and this data is installed in the IP forwarding table. The laptop then creates a DNS query message which has the website URL, putting the question in Ethernet frame which is sent to the router gateway. Though the DNS knows the IP address through the DHCP ACK, it does not know the MAC address. The laptop now creates an ARP protocol and ARP query which gets an ARP reply with the corresponding MAC address to the IP address. Once the laptop receives that ARP reply it extracts the containing frame to find the MAC address of the gateway router. The laptop now addresses the Ethernet frame with a DNS query to the gateway routers Mac address. Once it receives the frame and extracts the required information, it uses border gateway protocol to extract and determine the outgoing interface.

- Now there is a three-way TCP handshake between the laptop, the website and the destination gateway router. The border gateway protocol again is used to obtain and determine the forwarding table information. The TCP SYNACK message arrives at the website and required information is extracted and a TCP SYNACK segment is generated inside the link layer frame and sent to the first hop router. That is then forwarded through all the networks and reaches the laptop, the browser creates an HTTP GET message and requests the TCP segment. The website replies with the HTTP response message and finally the laptop is connected to the website and loads it.

b. Jack wants to transparently monitor all the online activity of John. Describe how Jack can monitor all the online activities of John in the home network.

- If he wants to monitor John's online activities transparently, he must advise him that all his online activity will be monitored. To monitor all the online activities, Jack can use network monitoring tools. Wireshark can be used to monitor network activity.

- To capture data packets in Wireshark, Jack needs administrator privileges. Then the right network must be chosen and a location within the network is needed to capture the data packets. There are two modes of data capturing in Wireshark which include promiscuous and monitor. Promiscuous mode sets the capturing area to only what is chosen by the user. Whereas monitor mode is used by Linux systems, and it sets the wireless interface to capture as much of the network activity as possible.

- As the data is being recorded by Wireshark, the user can filter out irrelevant information or information which is not useful to them at any given time. This can help the user find the relevant and crucial information needed for many different reasons.

- To monitor the network activity in Wireshark, Jack will need to select a network interface he wants to use to capture the packets of data. Once he chooses a network interface, data packets that are coming into and out of the network interface will be shown. The details that are included in each packet include an ID number, Time, Source Ip Address, Destination IP address, Protocol, Length and information that shows what type of application it is and what application it is changing or updating.

3. Why is it difficult for the organisations to deal with insider attacks. Give any 2 reasons and justify your answer.

- Most organisations do not monitor their internal network traffic and therefore cannot react to insider attacks with knowledge of what type of attack is happening and if an attack is happening and how to deal with that attack.

- The only way to notice an internal attack without the use of network monitoring would be to see changes without authorization to a big enough effect that a larger organisation would have to review. By the time this is reviewed, and steps are put in place to attempt to fix it, the attacker already has the data they were searching for, and they are completely done with the attack.

- If a business is monitoring the network traffic inside the organisation, insider attacks can be overlooked as it can look no different than an employee performing normal activities. With the use of internal network firewalls and network monitoring tools, internal attacks can be prevented, or attacks can be discovered before it is too late. Insider attacks are still very difficult to deal with because they are not expected.

- When monitoring for insider attacks, you want to monitor unauthorised access, violations of organisation policies, internal reconnaissance, data hoarding and data loss. Data analytics can be used to decide whether these violations are insider attacks or just minor incidents or accidents. Records need to be kept when monitoring internal network violations.

4. Compare the impact of disassociation and de-authentication attacks on the stations in WLAN networks.

- A disassociation attack is a type of denial-of-service attack which breaks the wireless connection between the victim's device and their wireless access point. This method is based on the use of a special disassociation frame. Transferring one of these frames to the targeted device breaks its wireless connection to their router, and the wi-fi protocol doesn't need encryption requirements. For one of these attacks to be successful, the hacker only needs the MAC address of the device. Association is a distribution system service.

- A de-authentication attack is another type of denial-of-service attack. This attack is an abuse of the de-authentication messages which are sent from client to AP to de-authenticate from each other. These messages are not authenticated by any cryptographic methods. Therefore, an attacker can send de-authentication message on a victim's behalf cause them to be de-authenticated and lose access to the network. Authentication is a station service.

- The impacts of these attacks end with a very similar result of the victim being denied access to their wireless access point. But the methods in which these attacks use to deny access differ.

5. Consider that a small book store www.bookstore.com managing the orders online as shown in Figure 2. Customers can order the books online by accessing the webserver as a guest user but they do not get any discount on their orders. However, registered customers get 5% discount on their orders. The company has approached you to conduct a penetration testing on their webserver. Describe how you will conduct penetration testing for this scenario. (Hint: State your assumptions. Also, list at least two specific vulnerabilities you would look for in this scenario while conducting the pen testing)

- There are a few different methods for penetration testing of a business' e-commerce website. These include Internal testing, External testing, Client-side testing, wireless testing and targeted testing. For this scenario I would use external testing to test the security from the outside as most traffic will be coming from external sources.

- The steps involved with the penetration testing are to audit the website to pinpoint security flaws and problems, scanning the website for detailed performance, accessing the website fully with penetration methods and exploit the website, and to analyse the security risks and problems then to identify ways to secure the website from these attacks.

- The two specific vulnerabilities that can be exploited in these types of e-commerce websites are SQL injection attacks and cross-site scripting attacks.

- SQL Injection attacks, the union operator is used to attach a piece of malicious code to a query which is originally intended to run the web application, bypassing the need for authentication. The result of the injected code into the original query allows the attacker access to information the user was attempting to access.

- Cross-site scripting attacks work by manipulating a vulnerability in web sites to return malicious JavaScript code to the victims. When the malicious code is run on the victim's browser, the attacker gains access to their account or website they were attempting to access.

- The first thing I would attempt to do to pen test this webserver would be to try sql injection. Sql injection works on database engines that use a dynamic statement that is generated at runtime using parameters password of a web form or URI query string. I need to know how the password and username, or email is stored when the form is sent to check if the information is correct. Once this is known all that is needed is the corresponding sql injection code and access to the victim's account is granted.

- To check if the web page is vulnerable to cross-site scripting attacks, online scanners and scanner applications can be used and they give a detailed description of the vulnerabilities. Once they are found, sql code can be injected into the vulnerable areas with malicious code.

- Those vulnerabilities must be patched, and detailed descriptions of the patches must be given for further examination of the webpage for vulnerabilities should be conducted.

6. Consider simple network shown in the Figure 3 which is protected by stateful firewall and the Table 1 shows policies that are enforced in the firewall.
a. Describe the operation of stateful firewall operation with the flow rules in Table 1.

- A stateful firewall is a firewall that monitors the full state of active network connections within a given network. It is always analysing the context of traffic and packets of data incoming and outgoing in the network. Stateful firewalls have a state table that is used to show previously received packets to compare them to the incoming packets and either allow or deny them accordingly.

- Stateful firewalls are not as fast as packet filters, but they are slower because stateful firewalls are more secure that packet filters. Packet filters do not keep a history of received packets in a data table and they do not know about the relation between the sequential packets. Packet filters do not detect attacks that rely on the sequence of packets with specific bits. To detect these attacks a stateful inspection must occur and that is why stateful firewalls are used.

- The stateful firewall is used to deny access to malicious software and data packets, it also remembers which type of packets are malicious. It keeps a table of all data that goes through it and sets data points to make a profile of safe and malicious connections. When a connection is made the stateful firewall checks the list of attributes collected against that connection and either allows or denies the connection.

- Stateful packet inspection is the technology used in the stateful fire wall, which is used to determine what packets can be allowed through the firewall. This works by examining data in data packets and comparing it to data that has previously passed through the firewall. This keeps track of all connections to the device.

- Stateful firewalls use Transport Control Protocol as its primary protocol for internet connection. There are three stages of the TCP connection which include synchronize, synchronize-acknowledgment, and acknowledgement. This is used in the stateful firewall to identify the parties involved in determining if a connection is malicious.

- A three-way handshake is used to initiate a connection between the devices, which transmits information pertaining to the legitimacy of the devices to trust the other devices to examine the incoming packets for the stateful firewall. These data packets include information such as the source, the destination, sequence of the packets, and the data within the packets to verify the legitimacy of the data being sent and received.

- The difference between stateful packet filtering and stateless packet filtering is that stateless firewalls are designed to protect networks based on static information such as a certain destination and source. Stateful firewalls filter packets based on the context of the connection, whereas stateless firewalls filter depending on the packet of data itself.

b. In Figure 3, consider the case where the client machine 1 has initiated SYN message to Google Web Server and the attacker has responded first with SYN/ACK message to the client machine before Google Web Server. Describe the operation of the stateful firewall for this case scenario with the flow rules in Table 1.

- If the client machine initiated the synchronization message to google web server and a hacker intercepted and responded to it with a synchronization acknowledgement message before google, the interceptor would have been seen as a legitimate party involved in the verifying of malicious and safe programs and packets allowed through the stateful firewall. This would allow the interceptor full access to allow through the firewall any type of file wanted which could give him full access to the device.

References

Jk, R. (2018, March 9). What happens when you type URL in browser? LinkedIn. Retrieved May 8, 2022, from https://www.linkedin.com/pulse/what-happens-when-you-type-url-browser-ramnath-jk-1/

Kaspersky. (2022, February 9). *What is a zero-day attack?* www.kaspersky.com. Retrieved May 3, 2022, from https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Shweta, S., & Meenakshi, M. (2019). Detection and prevention of de-authentication attack in real-time scenario. *VOLUME-8 ISSUE-10, AUGUST 2019, REGULAR ISSUE*, *8*(10), 3324–3330. https://doi.org/10.35940/ijitee.j1217.0881019

Thakkar, M. (2021, April 15). *How to perform penetration testing for e-commerce applications?* KiwiQA. Retrieved May 5, 2022, from https://www.kiwiqa.com.au/blogpost/how-to-perform-penetration-testing-for-e-commerce-applications/

Vargas, J. F. B. (2020, April 13). *What happens when you type google.com or any other URL in your browser and press enter*. LinkedIn. Retrieved May 5, 2022, from https://www.linkedin.com/pulse/what-happens-when-you-type-googlecom-any-other-url-buitrago-vargas/