COMP3500 ASSIGNMENT 2

HARLAN DE JONG | C3349828

TABLE OF CONTENTS

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 an attack on a software system where the exploit has just recently been discovered. Thus, the name 'zero-day', infers that the developers have zero days to fix this exploit as attacks are already undergoing. Often attackers inject code into the system known as exploit code which allows the hacker access to higher permissions and/or important information. The reason that the zero-day attacks are difficult to deal with is because the software developers don't even know that there is a vulnerability until the security is breached. Once the hackers have infiltrated the system, they have a greater amount of control of what they want to do and can do. They have the option to either wait for the best time to utilise the exploit, attack immediately or to sell the exploit onto the dark web. All the aforementioned options available are detrimental to the system as nothing can be done to protect the system until the vulnerability is known, and this is usually too late.

Polymorphism poses an extreme threat to systems and software as malicious code can be hidden from virus scanners and threat detection software via encryption. The polymorphic viruses or worms essentially use a mutation engine that provides a new decryption routine for the malicious program using an encryption key and has the ability to change attributes associated with code when installed on a different system. The reason it does this is because the file scanners will not be able to make correlations to pre-existing known malicious files and will treat the file as safe.

Metamorphism is a method in which malicious code rewrites itself without an encryption key. The metamorphic malware uses various obfuscation techniques to ensure that each instance of itself appear different to the last, these include register renaming, code expansion, code permutation, code shrinking and garbage code insertion. Every part of the code is rewritten and proves harder to detect than polymorphic code as nothing remains the same. The two techniques utilise two techniques to achieve the same result and the use of either ensures further complications arise when trying to detect the malware.

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).

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.

There are 8 steps involved when accessing a website with a URL in the browser:

1. **Search www.google.com into address bar of the browser**
2. **Cache is checked for DNS entry of corresponding IP**
   The Domain Name System (DNS) is an extensive list of all URL's and their corresponding IP addresses. It attempts to find the IP addresses as this is the address that is used when accessing different websites through the server host. The DNS will search 4 different caches:
   1) **Browser cache**. The browser being used currently will have stored previously visited website URL's and IP's. Thus, a DNS search will be run in order to see if google.com is in this list. This would be at the 'John' level of the sample home network in figure 1.
   2) **Operating System (OS) cache**. The operating system also stores a list of DNS records, and the browser can opt to call this system. This would be at the 'John' level of the sample home network in figure 1.
   3) **Router cache**. The router maintains a cache of the DNS records, and this is searched if the IP address hasn't been found. This would be at the 'DHCP' server level of the sample home network in figure 1.
   4) **ISP Cache**. The ISP cache is DNS queried as the last resort. This would be at the 'ISP' level of the sample home network in figure 1.
3. **IP not found, ISP DNS server launches DNS query**
   A recursive DNS query search is activated through the ISP. Essentially the ISP's DNS server will communicate with other DNS servers to find the correct IP address for the google.com search. It does this by sending small packets of data consisting of the destination IP and the reason for the request. The packets are sent through different networks to find the IP for the request at the proper DNS server and returned with correct IP address if found and an error if unable to find. This step occurs on the 'ISP' level of figure 1.
4. **TCP connection with server via browser**
   Assuming the browser has received the correct IP, a new connection will be made between the server and browser. The Transfer Control Protocol (TCP) connection will most likely be used for the http request. Next a three-way handshake using

synchronise (SYN) and acknowledge (ACK) messages will be used for TCP/IP connection.

1) **SYN message sent to server checking for connection availability**
2) **If server accepts connection, server will send SYN/ACK packet back**
3) **SYN/ACK packet will be received, browser sends ACK packet to server**

This three-way handshake ensures a stable and accessible connection for data transmission. This occurs in the 'John' level of figure 1.

5. **HTTP request sent by browser to the web server**
   With a TCP connection established, the browser sends GET requests in order to retrieve the website page. Alternatively, the browser could use a POST request which send data to the server for input data such as forms. This occurs on google.com's end.
6. **Server handles requests and delivers response**
   A request handler deals with the POST and GET requests and sends back an appropriate response.
7. **HTTP response from server**
   The server delivers the webpage and other data in the HTTP response, this includes status code, how to cache page, compression type, etc.
8. **HTML content is displayed by browser**
   The webpage that was initially searched for (google.com) is rendered on the screen by the browser and some static files are stored in the browser cache. This occurs on the 'John' level of figure 1.

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.

In order to monitor network traffic within a home network, we first need to know that all the traffic goes through a router (in fig. 1 – "Gateway with DHCP Server"). The next step would be to install the open-source packet monitoring software "Wireshark", this will be used for monitoring the traffic on the home network. When initially installed Wireshark will have "promiscuous mode" enabled automatically. At the top left of the window there will be a blue shark fin which indicates starting the network capture process and a red square which stops this process.

Run the capture for as long as necessary and during this time all the traffic across the network will be monitored with attributes such as source, destination, info, etc. As Jack is attempting to monitor John's activity Jack will need to sort the attributes, source and destination by John's IP address which is given "192.168.2.5". If John's IP address is seen in

the “source” column, this means that this is where the packet has come from. If John’s IP address is seen in the “destination” column, this means that this is where the packet supposed to go to.

These default attributes are:

1. **Number** – This is the number of captured packets.
2. **Time** – This is the time at which the packets were captured.
3. **Source** – This is where the packets have come from.
4. **Destination** – This is where the packets are going to.
5. **Protocol** – This the name of the protocol for the packet.
6. **Length** – This is the number of bytes within the captured packet.
7. **Information** – This includes any addition information about the packets.

Through reading all the attributes of specific packets Jack can determine all the traffic that comes through the router and thus transparently monitor John using Wireshark. This will not let John know that he is being monitored which may or may not be the initial intention of the goal.

WHY IS IT DIFFICULT FOR THE ORGANISATIONS TO DEAL WITH INSIDER ATTACKS. GIVE ANY 2 REASONS AND JUSTIFY YOUR ANSWER.

Insider attacks are commonly seen as threats that occur from inside a business. The cause of these attacks can be from malicious intent to plain carelessness and companies need to ensure that these types of risks are handled prior to them happening.

1. **Higher role within the company**

   As an employee that is considered to be within a senior role of a company, they are generally considered to be trustworthy. The issue with this assumption is that senior malicious insiders can exist, and they may use the power that they have gained over the course of working within company for ill intent.

   The reason that this type of insider would be difficult to deal with is because confronting such a high member of the company may come across as belittling in the case that the accuser is wrong. On the flipside, the insider will never openly admit to such allegations as they do not want to be fired. As such a stalemate between workers will arise and without any concrete evidence it would be hard to launch an investigation against the insider. For example, if an intern within a software company notices his supervisor doing something distinctly dodgy with private files on his computer and the intern reports it to someone higher up, the likelihood of people listening wouldn’t be high. Following on,

the intern might not even be able to contact anyone higher than his/her supervisor so reporting may not even be able to take place.

2. **Competence with internal systems and software**

Due to the fact that internal employees use the companies' systems and software on a daily basis, it is assumed they are very familiar with how things operate. With this in mind, malicious insiders will have the capacity to find and tamper with important files of a company for either personal or monetary gain.

This type of insider would be difficult to deal with as due to them knowing all the systems inside out, they have the ability to conceal their malicious tracks. For example, inside a company where many people have permissions to certain documents and something important gets tampered with, the chance of knowing exactly who did it, without any traces left behind is nearly impossible. This exemplifies why companies should prioritise prevention rather than a solution to this problem.

COMPARE THE IMPACT OF DISASSOCIATION AND DEAUTHENTICATION ATTACKS ON THE STATIONS IN WLAN NETWORKS.

Disassociation and deauthentication attacks are a type of Denial of Service (DoS) attack which inhibits the user to be able to access a network particularly in a Wireless Local Area Network (WLAN). This attack works by having a victim connect to a wireless connection (router) and an attempt will be made by the attacker to deauthenticate the victim through various tools. These tools essentially allow the attacker to have information about the router. Once the target victim is found, connected to the network, the attacker will run a command which elicits the victims MAC address. Once that information is known the next step is to disassociate the victim, this is done by running a command which uses the tool plus the victims MAC address. The result of this command being run will have the victim disconnected from the WLAN and attempts to re-join the network will not work until the deauthentication messages are stopped being sent by the attacker.

The impact of these types of attacks are that the disassociation phase results in a victim essentially being tracked and disassociated within a network via finding their MAC address. While on the other hand, the deauthentication phase is what inhibits the victim from maintaining a connection with the WLAN and when both phases work in tandem the impact is significant.

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.

Penetration testing is a legal way for authorised individuals to attempt to exploit both networks and systems. This type of testing will give developers insight into some of the vulnerabilities before unethical hacking can take place and thus proactively patch the systems. The proper way to conduct penetration testing is as follows.

1. **Legal and authorisation requirements**
   For the testers within the test there are legal requirements that must be agreed upon prior to the attacks. Written consent must be obtained from the developers, the small bookstore will need to agree upon both the risk and scope with the testers, all actions with need to be logged in some way, a time frame for testing and the testers must not work outside the scope.
   There are also legal requirements for the bookstore. These include an understanding of both network and system in question, potential disruptions of services, and problems may not be reported by the penetration testers.
2. **Documentation and logging**
   This is primarily for the penetration testers as they must follow the legal and authorisation requirements listed above that states all actions must be logged and correctly documented. This ensures that an accurate backlog is maintained to refer to later for reporting to the bookstore.
3. **Reconnaissance**
   This step essentially tries to give the testers a background of the bookstore and where exploits may arise. The first step the testers would do is query “www.bookstore.com” in the web and try to understand the company. The next step is to answer the “who is?” question, in this case Domain information about www.bookstore.com would be important. Next answer the “what is the site running” question which entails finding the OS and using site reports. Finally, a website “exploit database” has an archive of exploits that the public can use for penetration testing.
4. **Scanning**
   This phase involves mapping the bookstores network topology, finding weaknesses, and identifying the used services. Tools such as Nesus and Nmap are ways that scanning can be done on the bookstores network to achieve the aforementioned goals.

5. **Penetration**
   This step involves gaining access to the systems and networks through various attacks. These attacks are listed under three categories, application and operating system attacks, network attacks and privilege escalation. The two vulnerabilities the testers should look for in www.bookstore.com are Cross-Site Scripting (XSS) attacks and Distributed Denial of Service (DDoS) attacks as these can be detrimental if not prevented early. The DDoS attacks have the ability to shut down the entire web bookstore thus minimising sales, while the XSS attacks have the ability to make the website visitors information vulnerable and potentially redirect them to a phishing website.
6. **Maintaining access and covering tracks**
   Maintaining access to the bookstore's website can be done via backdoors, spyware, trojans, etc. The testers can also cover tracks by altering the change logs of the actions that take place.
7. **Reporting**
   The reporting phase involves the testers telling the bookstore about all the findings/exploits. The typical format of this report is with an executive summary, a detailed report and raw output, which is the proof of the attacks.
8. **Clean up**
   The clean up is for the testers restore everything as it was and depart with the bookstore once all reporting is finalised.

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.

DESCRIBE THE OPERATION OF STATEFUL FIREWALL OPERATION WITH THE FLOW RULES IN TABLE 1.

A stateful firewall is a network security system that has the ability to capture the entire state of the current network connections. This firewall is used to monitor traffic over the network and analyse the context of various data packets. This network security system is then able to approve or deny access to different kinds of traffic over the network, essentially acting as a barrier between the internet and the local network. If the three-way handshake between the two parties is not successfully completed the packets will not be able to reach the destination and thus blocked. These stateful firewalls are susceptible to Distributed Denial of Service (DDoS) attacks as the number of resources required to maintain such a close eye on all packets across the network is significant.

Viewing table 1. we see:

1. **Row 1**

allow	202.202.202.202	Outside of 202.202.202/24	TCP	>1023	80	any

This means that the “Client Machine 1” is allowed to send packets to an IP address outside of the current local network through the Transmission Control Protocol (TCP), which is connection oriented. The source port is either registered or dynamic while the destination port is 80 which is the Hypertext Transfer Protocol (HTTP) port for web connection. TCP uses a three-way handshake; this is the first step, and a SYN is sent to the server from the “Client Machine 1” to try to attain connection.

2. **Row 2**

allow	Outside of 202.202.202/24	202.202.202.202	TCP	80	>1023	ACK

This means that a server/machine outside of 202.202.202/24 local network is allowed to connect with “Client Machine 1” (202.202.202.202) through the TCP protocol. This indicates the second phase of the three-way handshake where the HTTP port (80) is sending a SYN/ACK to the “Client Machine 1” indicating that clients request to connect with the server was successful and data transfer is possible after connection.

3. **Row 3**

allow	Outside of 202.202.202/24	202.202.202.203	TCP	>1023	80	any

This means that a server/machine outside of 202.202.202/24 local network is allowed to connect with web server www.foodchain.com (202.202.202.203) through the TCP protocol. This is the first phase of a TCP three-way handshake where a server/machine under either a registered or dynamic port number is attempting to access the HTTP port (80) of the foodchain webserver. The TCP three-way handshake will follow with the IP address outside of 202.202.202/24 sending a SYN to the foodchain webserver to initiate potential connection.

4. **Row 4**

allow	202.202.202.203	Outside of 202.202.202/24	TCP	80	>1023	ACK

This means that the www.foodchain.com webserver (202.202.202.203) with port 80 is allowed to send packets to an IP address outside of 202.202.202/24 with port >1023 (registered or dynamic). The second phase of the TCP three-way handshake will follow as the foodchain webserver will have received the SYN and will respond

with a SYN/ACK to state that connection is possible and data transfer can be made after successful connection.

5. **Row 5**

allow	202.202.202/24	Outside of 202.202.202/24	UDP	>1023	53	-

This means that all servers/machines within the 202.202.202/24 local network (www.foodchain.com & Client Machine 1) with port >1023 are able to send packets to servers/machines outside of IP address 202.202.202/24 with port 53 under the UDP protocol. Port 53 indicates the Domain Name System (DNS) which helps with matching domain names to IP addresses. The User Datagram Protocol (UDP) is not connection oriented unlike TCP and the data packets are just sent to the IP address outside of 202.202.202/24 without any guarantee they will make it.

6. **Row 6**

allow	Outside of 202.202.202/24	202.202.202/24	UDP	53	>1023	-

This means that all servers/machines outside of 202.202.202/24 local network with port 53 are allowed to send packets to servers/machines inside of local network 202.202.202/24 with port >1023 under the UDP protocol. As there is no handshake within UDP there is no SYN/ACK transfer.

7. **Row 7**

deny	all	all	all	all	all	all

This means that all other IP addresses that are not listed above, are not able to send packets and maintain a connection to the servers/machines within the local network that the stateful firewall is protecting (202.202.202/24). This is a good preventative measure that ensures no malicious packets of data are sent to the "Client Machine 1" and food chain web server and only good, known connections are allowed to.

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 attacker was to send a SYN/ACK message before the google web server, the connection between "Client Machine 1" and the attacker would not be successful. This is because the stateful firewall has policies that prevent the attacker from sending packets to the client machine. In row 2 of the table, it states that only IP addresses outside 202.202.202/24 AND with port 80 (HTTP) will send a SYN/ACK message. Since the attacker is

not a web service on port 80 and instead just a machine it will be blocked by the firewall. This is the intention of row 7 as all other attempted connections that don't satisfy rows 1-6 will not be allowed to connect with the "client machine 1". Thus, no connection will be made between the attacker and client machine.

REFERENCES

5 Common Types of Website Attacks. Sectigo® Official. (2022). Retrieved 22 May 2022, from https://sectigo.com/resource-library/what-are-the-5-most-common-attacks-on-websites.

Deauthentication/Disassociation attack. Cyber Security Labs. (2022). Retrieved 22 May 2022, from https://cybersecuritylabs.wordpress.com/2014/02/01/wireless-networks-deauthenticationdisassociation-attack/.

Define a firewall rule for use in policies | Deep Security. Help.deepsecurity.trendmicro.com. (2022). Retrieved 22 May 2022, from https://help.deepsecurity.trendmicro.com/10_1/on-premise/Protection-Modules/Firewall/create-firewall-rules.html.

How to capture HTTP traffic using Wireshark, Fiddler, or tcpdump | Atlassian Support | Atlassian Documentation. Confluence.atlassian.com. (2022). Retrieved 22 May 2022, from https://confluence.atlassian.com/kb/how-to-capture-http-traffic-using-wireshark-fiddler-or-tcpdump-779164332.html.

What happens when you type a URL in the browser and press enter?. Medium. (2022). Retrieved 22 May 2022, from https://medium.com/@maneesha.wijesinghe1/what-happens-when-you-type-an-url-in-the-browser-and-press-enter-bb0aa2449c1a.

What is a Zero-day Attack? - Definition and Explanation. www.kaspersky.co.uk. (2022). Retrieved 22 May 2022, from https://www.kaspersky.com.au/resource-center/definitions/zero-day-exploit.

What Is an Insider Threat | Malicious Insider Attack Examples | Imperva. Learning Center. (2022). Retrieved 22 May 2022, from https://www.imperva.com/learn/application-security/insider-threats/.