N10214925 Liam Dines N10091190 Jomarcel Nguyen
N10271171 Nickhil Nischal N10221221 Louis Yanagisawa

CAB303 Networks
Group Security Project – Report
Group Name: Project-(D) #5

N10214925 Liam Dines N10091190 Jomarcel Nguyen
N10271171 Nickhil Nischal N10221221 Louis Yanagisawa

Claim of Individual Contribution

Student Number	Name	Claim of Contribution
N10214925	Liam Dines	● 20% of Mitigations section within Discussion ● 20% of Conclusion ● 20% of Recommendations ● 20% of References ● Extensive proofreading, editing and rephrasing of the entire document ● Independent analysis of capture file in Wireshark ● Independent research
N10091190	Jomarcel Nguyen	● 100% of Network Traffic section within Discussion ● 20% of Mitigations section within Discussion ● 20% of References ● Extensive independent analysis of capture file in Wireshark ● Extensive independent research ● Proofreading, editing and rephrasing
N10271171	Nickhil Nischal	● 100% of Executive Summary ● 60% of Introduction ● 60% of Mitigations section within Discussion ● 50% of Technical and Organisational Consequences of the Attack section within Discussion ● 80% of Conclusion ● 80% of Recommendations ● 30% of References ● Independent analysis of capture file in Wireshark ● Extensive independent research ● Extensive proofreading, editing and rephrasing ● Final document formatting, checking and submission ● Organised all group meetings
N10221221	Louis Yanagisawa	● 40% of Introduction ● 100% of Observations Based on Examination of Capture File within Discussion ● 100% of Compromised Security Goal section within Discussion ● 100% of Relevant Vulnerabilities within Discussion ● 100% of Explanation of Attack within Discussion ● 50% of Technical and Organisational Consequences of the Attack section within Discussion ● 30% of References ● Extensive independent analysis of capture file in Wireshark ● Extensive independent research ● Extensive proofreading, editing and rephrasing

N10214925 Liam Dines N10091190 Jomarcel Nguyen
N10271171 Nickhil Nischal N10221221 Louis Yanagisawa

Executive Summary

The presented report provides analysis and evaluation from the network administration team regarding the causation of XYZ company's website attack. The attack was thoroughly investigated and researched. The report finds that a Teardrop Attack was initiated, and outlines analysis conducted surrounding the attack, as well as the process taken to conduct the analysis. Through extensive research, the report also recommends mitigations for XYZ company to implement regarding the attack.

Table of Contents

Introduction

Company XYZ's website is unable to be accessed by users and is instead displaying a 'page cannot be displayed' error. The website is suspected to be under some form of attack and the network administration team has been contacted to investigate. The attack is essential for company XYZ to resolve as it can have detrimental and wide-ranging impacts on stakeholders. This issue not only for their website to function again but to also review their security goals and expectations. From a business perspective, an inoperative website means customers and other stakeholders cannot use or view the website - potentially resulting in business losses. Additionally, other aspects of the company such as servers and databases are also at risk, leading to reliance and data integrity issues. This poses a larger issue that needs to be resolved for the security and wellbeing of the company. The network administration team has been asked to investigate the attack and has taken a systematic approach to investigating. Packets were carefully examined for any anomalies using Wireshark, and research was conducted regarding possible attacks and abnormal packet behaviours.

Discussion

Network Traffic

The Internet Protocol was disrupted. This protocol allows us to link our devices to the internet. A special, numerical IP address is allocated if a device accesses the internet (whether it is a laptop, smartphone or another device). A data packet must be transmitted across the network containing the IP addresses of both devices in order to transmit data from one machine to another through the web (Newton, n.d).

It is the duty of the Internet Protocol to address host interfaces, encapsulate data into datagrams (including fragmentation and reassembly), and route datagrams through one or more IP networks from a source host interface to a destination host interface. The Internet Protocol determines the format of the packets for these purposes and provides an addressing scheme. There are two sections to each datagram: a header and a payload. The IP header contains the source IP address, the destination IP address and other metadata necessary for the datagram to be routed and distributed. The data being transported is the payload. This technique of nesting the payload of information in a packet with a header is called encapsulation (Balasubramanian et al, 2014).

IP addressing includes assigning host interfaces with IP addresses and related parameters. The address space, including the assignment of network prefixes, is split into sub-networks. Both hosts, as well as routers whose main role is to move packets across network boundaries, perform IP routing (Cisco, n.d). Routers interact with each other through specially designed routing protocols, either internal gateway protocols or external gateway protocols, as necessary for the topology of the routing system (Hedrick, n.d).

Observations Based on Examination of Capture File

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.170.10	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=0, ID=3039) [Reassembled in #3]
2	29.286867	192.168.170.10	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=16, ID=3039) [Reassembled in #3]
3	34.260715	192.168.170.10	192.168.170.8	ICMP	60	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)
4	169.578640	192.168.170.35	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=0, ID=ddac)
5	173.424260	192.168.170.35	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=8, ID=ddac)
6	179.215367	192.168.170.35	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=16, ID=ddac)
7	185.958505	192.168.170.35	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=32, ID=ddac)
8	309.435036	192.168.170.55	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=0, ID=2dff) [Reassembled in #10]
9	314.526007	192.168.170.55	192.168.170.8	IPv4	60	Fragmented IP protocol (proto=ICMP 1, off=16, ID=2dff) [Reassembled in #10]
10	319.547831	192.168.170.55	192.168.170.8	ICMP	66	Echo (ping) request id=0x0000, seq=0/0, ttl=64 (no response found!)

Figure 1: PCAPNG file

The packets in the PCAPNG file (Figure 1) provided consist of ten packets, two of which are 'Echo (ping) request' and the other eight are 'Fragmented IP protocol'. Fragmented IP protocol packets 1 and 2 are reassembled into ping packet 3 and packets 8 and 9 are reassembled into ping packet 10, while packets 4,5,6 and 7 are not reassembled at all. The packets all had destinations for XYZ's website, IP address 192.168.170.8, and came from various sources but all the source addresses were in the 192.168.170.0/24 range.

Statistics

Measurement	Captured	Displayed	Marked
Packets	10	10 (100.0%)	—
Time span, s	319.548	319.548	—
Average pps	0.0	0.0	—
Average packet size, B	61	61	—
Bytes	606	606 (100.0%)	0
Average bytes/s	1	1	—
Average bits/s	15	15	—

Figure 2: Packet statistics

The rate of packets (Figure 2) was not particularly high at around 32 seconds per packet and were spaced over a 320 second interval. All packets had a length of 60 bytes with the exceptions of packet 10 that had 66 bytes, resulting in an average packet size of 61 bytes. All the fragmented IP protocol packets had 8 or 16 bytes of data and the echo ping requests had 24 and 32 bytes of data. From these initial observations, nothing seems to be out of the ordinary and no malicious activity can be detected.

Some abnormal behaviour that was present is the lack of variation in the packets coming in. All the packets coming in are either IPv4 Fragmented IP packets or ICMP Echo Ping Requests which is strange because usual data transmission associated with a website consists of a variety of packets with a range of protocols such as HTTP, TCP, ICMP, ARP, etc. Another concern is the lack of outgoing packets. In normal IP protocol behaviour, it is normal to see many incoming and outgoing packets at a fast rate but what is observed here is much different. Firstly, the packet rate is quite slow for a website with average packets per second only being recorded as 0 by the Wireshark statistics page and a packet arriving around every 32 seconds. Secondly, out of all the packets provided all of them incoming are seen as the destination addresses for every

packet is XYZ's website address and none of the packets have a source address from the website. This behaviour indicates that company XYZ's servers are down as it is not attempting to communicate with anyone else and is only slowly receiving packets from an external source.

```
[Expert Info (Warning/Protocol): Source MAC must not be a group address:
```

Figure 3: Source MAC warning

Other abnormal behaviour observed in the file was the source address of the packets, shown in Figure 3. At first glance there seems to be no issue as the source IP address seems to be from a legitimate source and maybe even on the network, if the slash notation is 28 or lower, but on further inspection the MAC address raises some concern. When viewing the source MAC address, Wireshark raises a warning that "Source MAC must not be a group address" - and this is present for all packets. This is concerning as the sender may be attempting to hide its real address and posing as a legitimate and safe address by sending from a group source address.

Compromised Security Goals

If Company XYZ does not already have them, we would recommend creating security goals. These goals would encompass Confidentiality, Integrity and Availability. From the current situation at least one of these goals has already been compromised - availability. This has been compromised as the company's assets, in this case the website, are not continuously accessible to relevant stakeholders as the website is currently unreachable. Confidentiality, keeping company information secure, and integrity, guaranteeing that company information is not modified by unauthorized users, may have been compromised by this suspected attack but not enough information has been revealed at this point in time to confirm.

Relevant Vulnerabilities

This attack may have been exacerbated by vulnerabilities in company XYZ's servers. Firstly, it is seen that the server is still receiving data after it has been down which is a serious issue that has to be addressed. Because the server is still allowing data to come in it means malicious packets can still come through and cause problems on the server. If attacks are still allowed to come in while the website is down, it makes it very difficult for the server to recover or be repaired. Thus, the server should not let any packets come through whilst it is down. Secondly, all the incoming packets have a group address, signalling that these are from illegitimate addresses, but the server still allows these packets to come through which is concerning. To avoid this issue the server should filter out and inspect packets that have a suspicious source address to mitigate the damage that can be done by them.

Explanation of Attack

Fragmentation has been a frequent source of security vulnerabilities in IPv4. With fragmented IPv4 packets, the layer 4 header information for the second through to the last fragment is not available. In intermediate nodes (such as firewalls and routers) and end nodes (such as user computers), the fragmentation and fragment reassembly phase may produce unintended and harmful behaviors (Tomsho, 2019).

This is an issue as IPv4 Fragmentation requires a lot of resources on the intermediate routers and receiver's behalf. When data is sent it must be fragmented as every network has a Maximum Transmission Unit (MTU) which specifies the largest number of bytes a single packet can have on the particular network. If a packet is too large it is up to the routers to fragment it and the intermediate router uses its resources to fragment the packet. Furthermore, the router must create fragment headers, compute checksums, coping the original packet into the fragments and other overhead requirements. Once the packets arrive at the host's destination it is on the host to assemble the fragments, using up a lot of its own resources to complete this task. These processes can be exploited as all the computational burden is on the routers and receiver, not on the sender, so senders can send malicious packets to purposely disrupt the routers and receivers (Tomsho, 2019).

First one of these exploitations is intentionally sending large amounts and large sized packets to disrupt receiver resources. The larger the packet the more times it must be fragmented by the routers and assembled by the receiver, costing a large amount of resources on their behalf. Coupled with the fact that these packets can be sent in large volumes in a short amount of time, servers and devices can quickly be overrun and crash from these types of attacks (Singh et al, 2016).

Another exploit is sending malformed packets that exploit TCP/IP vulnerabilities. TCP/IP have many rules and processes that must be followed otherwise bugs can occur and cause the servers to crash. Purposely sending packets that defy these conventions is a common form of attack and most likely the attack we have witnessed in the XYZ business case. Furthermore, the fragmentation and assembling process has a lot of vulnerabilities as well and can become a target itself (Lin, 2013).

A Teardrop Attack is a form of IP Fragmentation DoS attack which exploits the TCP/IP fragmentation reassembly code. This is done by sending intentionally pre-fragmented and mangled packets with overlapping data that cause an overload in the network or device's resources (AL-Musawi, 2012; Hovav & D' Arcy, 2003; Lin, 2013; Singh et al, 2016). In the data we have been given, the packets are neither large nor high in volume but have used IP fragments with overlapping data to overload the system. When a packet is fragmented, the routers add an offset number to the fragments to inform the assembler of what order the packets need to be reassembled in. Purposely sending already fragmented packets with incorrect offset values causes the packets and data to overlap and causes the assembler to crash as the computer is unsure about what to do with the overlapping packets (Singh et al,, 2016; Solanker et al, 2015).

This type of attack can be observed in the ping packets of the PCAP file provided. In both instances, the offset value of the Ping packets is 8 while the previous packets that are the fragmented packets used to create the ping have offset values larger than 8. For the ping in packet 3 the previous packet has an offset value of 16 and has 8 bytes of data for so the offset value should be at least 24 so an offset value of 8 is suspicious. Similarly, to packet 10 ping the previous packet has an offset value of 16 and 16 bytes of data so the pings offset value should be at least 32 but it has an offset value of 8. This inaccuracy in the offset value for each of the pings are the result of the teardrop attack. Because the data overlaps from the incorrect offset

values the computer does not know how to react when attempting to assemble the packets thus leading to crashes and explains why the website for company XYZ is not working.

Technical and Organisational Consequences of the Attack

Although DoS attacks like the Teardrop Attack do not usually have serious security implications such as stealing of data and loss of data integrity, there can be many technical and organisational consequences of the attack (Cavusoglu et al, 2004). An inoperative website means that customers, stakeholders and other users cannot access the company's online resources. This causes a decline in website traffic and revenue associated with the company's online activities (Hovav & D' Arcy, 2003). Additionally, when potential customers attempt to visit the website and find it inaccessible, they may lose confidence in the XYZ company. This could lead to a decline in business confidence and negatively impact the company's reputation (Hovav & D' Arcy, 2003).

It is clear that XYZ company has been successfully attacked and their security systems have failed, meaning their defence systems and possibly their reputation have been undermined. If the company's systems are susceptible to this attack, and the issue continues to go unaddressed, they will be vulnerable to similar types of attacks in the future. This also leaves them open to other forms of malicious activity as well, as their security systems do not appear to be capable of warding off even relatively simple attacks. This potential fall in reputation will be detrimental for the business's relationship with other stakeholders, as they would not feel comfortable working with an insecure system (Hovav & D' Arcy, 2003) and invite other hackers to attack their servers.

Rectifying this attack will result in a wide range of labour and material costs, including the detection, containment, and repair of the attacked areas; as well as the provision and implementation of new resources (Hovav & D' Arcy, 2003), potentially causing extensive financial impacts on the XYZ company.

Mitigation Strategies

Mitigation strategies are crucial for XYZ company to establish, as they can reduce the impact of the attack once it is detected; and can strengthen the company's technical infrastructure by minimising impact of the attack. The approach to mitigating the Teardrop Attack depends on the nature and scope of the attack. There are several mitigation strategies which are relevant to the teardrop attack and the XYZ company. The most common mitigation techniques include ensuring that targeted servers are prevented from accessing malicious data packets. This includes reviewing incoming packets via a router, a secured proxy server, firewalls or intrusion detection system to decide if they breach fragmentation rules (Solanker et al, 2015). Such rate limiting or blocking suspicious traffic at the local network are quick and efficient solutions used to mitigate DoS attacks. However, these methods in itself are insufficient as they do nothing about the malicious traffic which is still present on the local network - denying use of the website to real users (Lin, 2013).

Firewalls represent the most common stateful inspection devices. There is a component known as the stateful packet inspection (SPI) engine in stateful firewall solutions. It is often referred to as DPI (deep inspection of packets). This engine provided intelligence to determine and define

connection information and application-level details by looking into the packet flow (AL-Musawi, 2012).

Another mitigation strategy is the use of Pushback. When an attack is identified, a pushback strategy will attempt to determine the source of the incoming malicious traffic or 'bad packets'. Attempts will then be made to block and/or redirect the source of the bad traffic. One option would be to block the hostile IP address but realistically this is difficult to do, so the most common method is to rate-limit and preferentially drop packets that match the characterization of the attacker at a router upstream from the victim. This lets through more good traffic than bad from the upstream router, as well as allowing traffic to flow freely from other unaffected routers (Ioannidis & Bellovin, 2002). A key advantage of using Pushback is that other servers can continue to receive legitimate traffic via a router. Additionally, this strategy allows higher level routers to perform complex analysis to filter out malicious traffic (Lin, 2013). A limitation of the pushback method is that there will be an initial infrastructure outlay cost for the company.

The final key mitigation strategy is to use a 'cleaning centre'. All traffic is redirected to and from the cleaning centre, which performs required traffic cleaning when destination hosts are under attack. This method operates at the ISP level, which differs from operating at the individual enterprise network level. Hence, a major advantage of the cleaning centre is that associated equipment and security expert costs are substantially reduced, as they are spread across different enterprise customers. Furthermore, due to the magnitude of the cleaning centre, attack traffic can be easily absorbed. Meaning that network packets do not need to be dropped (Lin, 2013). A limitation of the cleaning centre is that because it operates on the ISP level, it will be more difficult to implement and will also take longer to implement.

Conclusion

The XYZ company has undergone an attack which caused their website to become inoperative. The network administration team carried out thorough analysis and research - including examining packets in Wireshark to determine the type and severity of the attack. It was determined that XYZ Company was the victim of a Teardrop Attack, a type of Denial of Service attack performed by sending intentionally mangled packets containing overlapping data causing the network to crash. Without mitigation or further action, the attack would have a substantial negative impact on the company. The network administration team also explored and recommended implementable mitigation strategies which are clearly outlined below.

Recommendations

After extensive analysis and evaluation of possible mitigation methods of the Teardrop Attack, we recommend that XYZ implement a combination of the 'Blocking Suspicious Traffic' and 'Pushback' mitigation strategies. The first strategy will prevent future teardrop attacks from occurring - allowing the system to recover and protect against future attempts. Moreover, Pushback will target the malicious traffic currently on the network and will allow XYZ company's website to recover faster, effectively mitigating the attack.

These have been deemed the optimal choices for XYZ company as they are some of the quickest and most effective mitigation strategies that the company can implement. Both strategies are comparatively low cost and can easily be integrated into current infrastructure, making them the most cost-effective solution as well.

It must be noted that the mitigation strategies suggested may not be 100% effective as the world of online security is constantly evolving. It is hard to predict what kind of attacks the business may be the victim of in the future and to that end, we recommend XYZ constantly remain vigilant for hostile web activity directed towards their online assets.

References

AL-Musawi, B. Q. M. (2012). Mitigating DoS/DDoS attacks using iptables. *International Journal of Engineering & Technology, 12*(3), 101-111. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.419.2480&rep=rep1&type=pdf

Balasubramanian, V., Ho, S., & Vovk, V. (2014). Chapter 12 - Network Traffic Classification and Demand Prediction. In Dashevskiy, M., Luo, Z. (Ed.), Conformal Prediction for Reliable Machine Learning (1st edition, pp. 231-259). Morgan Kaufmann. https://doi.org/10.1016/B978-0-12-398537-8.00012-2

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. *International Journal of Electronic Commerce, 9*(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Cisco. (n.d). *IP Addressing: IPv4 Addressing Configuration Guide, Cisco IOS XE Release 3S*. Chapter: Configuring IPv4 Addresses. https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_ipv4/configuration/xe-3s/ipv4-xe-3s-book/configuring_ipv4_addresses.html

Hedrick, C. (n.d). *The TCP level*. General description of the TCP/IP protocols. https://www.ifa.hawaii.edu/users/gmm/intro_ip/index.html

Hovav, A., & D' Arcy, J. (2003). The Impact of Denial-of-Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review, 6*(2), 97–121. https://doi.org/10.1046/J.1098-1616.2003.026.x

Ioannidis, J., & Bellovin, S. M. (2002). Implementing pushback: *Router-based defense against DDoS attacks.* https://doi.org/10.7916/D8R78MXV

Lin, D. (2013). Network Intrusion Detection and Mitigation Against Denial of Service Attack. *University of Pennsylvania Department of Computer and Information Science Technical*, *13*(04), 5. https://repository.upenn.edu/cis_reports/981/

Singh, K., Singh, P., & Kumar, K. (2016). A systematic review of IP traceback schemes for denial of service attacks. *Computers & Security, 56*, 111–139. https://doi.org/10.1016/j.cose.2015.06.007

Solankar, P., Pingale, S., & Parihar, R. (2015). Denial of Service Attack and Classification Techniques for Attack Detection. *International Journal of Computer Science and Information Technologies*, *6*(2), 1. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.735.6902&rep=rep1&type=pdf

Tomsho, G. (2019). *Guide to Networking Essentials* (8th ed.). Cengage Learning.