University of Gloucestershire

CT4010: Computers & Security
2023-2024 BSc Computer Science

Completed Date: 4th May 2024

Table of Contents

Analysis of Investigate Tools

During the investigation to detect and analyze an unknown vulnerability within OceanView's network which caused a concerning breach on one of the servers, a full capture pcap data file was provided and thoroughly analyzed using Wireshark to understand the foundations of the data packets within the network before, during and after the breach, how the unknown vulnerability affected the network and better security measures to reduce the chances of a successful breach within the network.

Using Wireshark & It's Features

To open the pcap file, a data packet analyser software was appropriate. Wireshark was used as it is currently free and it is user-friendly made available for many platforms (Nath, 2015). However, it provides many advanced features which would be difficult for beginners, and it is complex when carrying out advanced analysis.

It provides several features such as packet capture, allowing Wireshark specific information on a packet's source and destination Internet Protocol addresses and ports along with the protocol header. Additionally, other features include filters on IP addresses, the different protocols, ports, etc and in-built protocol analysers to identify suspicious patterns within the traffic such as data loss which will be useful to help find malicious data packets and detect the type of malicious attack using the expertise on protocols and networks (Nath, 2015).

Sharma (2024) explains two limitations which Wireshark provides such as intrusion detection limitations meaning that it is unable to locate and detect stealthy attacks that use "low-and-slow techniques or advanced evasion methods" as the software does not have built-in signatures to track specific types of attacks or vulnerabilities that specialized intrusion detection system tools would detect. The second limitation is Wireshark's purpose as a "post-event analysis tool so an attack could occur in-real-time and cause significant damage before anything could be done however for this investigation this is not necessary (Sharma, 2024).

Wireshark also has some limitations as a network security tool.

- **No real-time detection:** One of them is that it does not provide real-time detection of ongoing attacks. Wireshark is mainly a post-event analysis tool that allows analysts to examine packet captures after they have been collected. This means that analysts may not be aware of an attack until it is too late or has already caused harm. To overcome this limitation, analysts may need to use other tools that provide real-time detection and alerting of network attacks, such as **intrusion detection systems (IDS)** or firewalls.
- **Intrusion Detection Limitations:** Another limitation of Wireshark is that it may not detect certain attack patterns that are detected by specialized IDS tools. Wireshark is not a dedicated IDS tool and does not have built-in rules or signatures for detecting specific types of attacks. For example, Wireshark may not be able to detect stealthy attacks that use low-and-slow techniques or advanced evasion methods. To compensate for this limitation, analysts may need to use other tools that have more sophisticated detection capabilities and features, such as Snort or Suricata.

Process of the Investigation

Labelling the IP Addresses & Standard Ports

- 172.16.0.8 -> HewlettPacka_bf:91:ee (HP) [MAC: 00:25:b3:bf:91:ee]
- 64.13.134.52 -> Cisco_31:07:33 (Cisco Router) [MAC: 00:26:0b:31:07:33]
- 172.16.100.26 -> VMware_07:ae:27 (Server) [MAC: 00:0c:29:07:ae:27]
- 192.168.100.202 -> HewlettPacka_bf:91:ee [hijacked]
- 12.153.20.41 -> Cisco_31:07:33 & HewlettPacka_bf:91:ee
- 74.125.95.147 -> Cisco_31:07:33
- 172.16.0.107 -> Dell_c0:56:f0 (Dell) [MAC: 00:21:70:c0:56:f0]

113 port -> identification request to verify TCP connection between devices
53 port -> DNS requests and responses
80 & **143** port -> HTTP requests and responses
21 port -> FTP requests and responses
22 port -> SSH requests and responses
23 port -> Telnet requests and responses
143 port -> IMAP requests and responses

Analysing the Data Packets

Packet 1 to Packet 2005

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	172.16.0.8	64.13.134.52	TCP	58	36050 → 443 [SYN] Seq=0 Win=3072 …
2	0.001539	172.16.0.8	64.13.134.52	TCP	58	36050 → 143 [SYN] Seq=0 Win=3072 …
3	0.001597	172.16.0.8	64.13.134.52	TCP	58	36050 → 3306 [SYN] Seq=0 Win=2048…
4	0.001650	172.16.0.8	64.13.134.52	TCP	58	36050 → 199 [SYN] Seq=0 Win=3072 …
5	0.001703	172.16.0.8	64.13.134.52	TCP	58	36050 → 111 [SYN] Seq=0 Win=1024 …
6	0.001755	172.16.0.8	64.13.134.52	TCP	58	36050 → 1025 [SYN] Seq=0 Win=4096…
7	0.001807	172.16.0.8	64.13.134.52	TCP	58	36050 → 995 [SYN] Seq=0 Win=1024 …
8	0.001861	172.16.0.8	64.13.134.52	TCP	58	36050 → 587 [SYN] Seq=0 Win=1024 …
9	0.001913	172.16.0.8	64.13.134.52	TCP	58	36050 → 53 [SYN] Seq=0 Win=3072 L…
10	0.001965	172.16.0.8	64.13.134.52	TCP	58	36050 → 5900 [SYN] Seq=0 Win=1024…
11	0.063797	64.13.134.52	172.16.0.8	TCP	60	53 → 36050 [SYN, ACK] Seq=0 Ack=1…
12	0.065271	172.16.0.8	64.13.134.52	TCP	58	36050 → 21 [SYN] Seq=0 Win=4096 L…
13	0.065341	172.16.0.8	64.13.134.52	TCP	58	36050 → 113 [SYN] Seq=0 Win=4096 …
14	0.126832	64.13.134.52	172.16.0.8	TCP	60	113 → 36050 [RST, ACK] Seq=1 Ack=…

Figure 1 – TCP connection between HP and Cisco device

Figure 1 shows data packets where most of the packets have the source IP address of 172.16.0.8 (highlighted in blue), the source port of 36050 (highlighted in purple), the destination IP address of 64.13.134.52 (highlighted in green) and the destination source ports of the Cisco router ports.

A connection is established between the HP computer and the Cisco router of the network, resulting in the two devices communicating with one another by the Transmission Control Protocol. This is seen throughout Packets 1 to 528. Multiple

packets are transferred using the non-standard 36050 and 36051 ports to several different standard and non-standard Cisco router ports from the HP device. For example, the 113 port for identification/authorization services and the 53 port for Domain Name System requests. Packets 47 and 118 are described to be forcibly terminating and resetting the TCP connection between the two devices, probably due to issues with the destination device which is suspicious. Multiple packets such as packet 529 results in a TCP retransmission of DNS queries followed by another forced termination of the TCP connection from packet 571.

571	3.132131	64.13.134.52	172.16.0.8	TCP	60	113 → 36061 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Figure 2 – Forced termination and reset of TCP connection

The TCP connection between the HP device and the Cisco router is active again, going through several different queries however at Packet 632, a second TCP retransmission of HTTP queries and requests occur. It continues until the router sends Packet 1233 to the HP device with the 70 ports. The 70 port is associated with an old protocol called the Gopher protocol which is responsible for the requests of retrieving documents over the Internet. This infer that the new consultant opened a document. A third TCP retransmission of Secure Shell requests and responses indicate poor communications with the devices relating to the SSH, resulting in a vulnerability of the context of the data. The final packet that will provide a stable TCP connection between the HP devices and the Cisco router is Packet 2005.

529	3.063375	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 53 → 36050

Figure 2 – Packet 529 showing a TCP retransmission of DNS queries

632	3.187263	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 80 → 36050

Figure 3 – Second TCP retransmission of HTTP queries

1963	5.063418	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 22 → 36050

Figure 4 – Third TCP retransmission of SSH queries

Packet 2006 to Packet 2069

2006	9.071680	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 53 → 36050
2007	9.387931	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 80 → 36050
2008	11.0641…	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 22 → 36050
2009	21.0932…	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 53 → 36050
2010	21.4011…	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 80 → 36050
2011	23.0853…	64.13.134.52	172.16.0.8	TCP	60	[TCP Retransmission] 22 → 36050

Multiple TCP retransmissions of DNS, HTTP and SSH queries appear which are most likely caused by network congestion, but an underlying issue of malicious activity could use these retransmissions as a forefront to commit an attack. A potential Denial of Service attack by failing to complete the ACK packets to overwhelm the router with lost or corrupted TCP SYN data packets.

After the several TCP retransmissions, the server and the HP can connect and communicate using the TCP protocol with some packets handled by the HTTP protocol using the 1031 port. These packets seem to be handling several HTTP requests and responses using this non-standard port, especially after the multiple TCP retransmissions therefore the traffic most likely indicates malicious activity using the GET HTTP requests. After Packet 2035, the two non-standard ports: 1032 and

4321 are described to be constantly opened between the HP and the server. This could be done to prevent the malware getting detected. The link which the consultant clicked probably redirected him to a suspicious website, resulting in the consultant's laptop to be hijacked. The compromised laptop connects with the server and transfers over malicious data packets.

At Packet 2051, a Dell device seems to connect and communicate with the Cisco router which has a different IP address for DNS queries for "www.google.com". This Dell device is suspicious, leading to the conclusion that the attacker has gotten access to the OceanView network. Again, the router's IP address changes but still communicates with the Dell device to send and retrieve HTTP requests and responses for a video.

Packet 2070 to Packet 2103

The Dell device constantly communicates with the Cisco router labelled with the IP addresses 12.153.20.41 with DNS queries and responses and 74.125.95.147 with TCP and HTTP queries and responses.

Packet 2104 to Packet 2188

The HP and Dell devices communicate temporarily using the ARP protocol to map out the IP addresses with the MAC address within the network. Afterwards, the Dell device communicates with the router constantly of data packets sending and retrieving HTTP/JSON and TCP queries and responses.

Packet 2189 to Packet 2215

DNS queries and responses from several websites are seen from the data packets transferred between the HP device with the changed IP address of 12.153.20.41 and Dell device.

Recommendations For Network

To improve security within the network, the following security measures could be implemented:

- **Adding Intrusion/Prevention Detection Systems** -> They can prevent TCP retransmissions and potential attempts at IP spoofing while analysing data packets in real-time. Any data packet which seems suspicious will be blocked.

- **Reducing access to certain IP addresses & ports** -> Implementation of firewall to prevent unauthorized communications.

- **Improving staff training** -> Consistent security training of employees should be carried out to help them be more aware on potential common and rare attacks.

- **Commit regular updates to identify vulnerabilities in network ->** Like improving staff training, OceanView should identify potential vulnerabilities within its network to implement better security measures.

Conclusion

In conclusion, the network suffered multiple vulnerabilities which could've led to more serious attacks but if it is constantly improved, it will be harder for several malwares to attack.

Reference List

- Sharma, M. (2024) Ethical Hacking and Network Analysis with Wireshark. BPB Publications

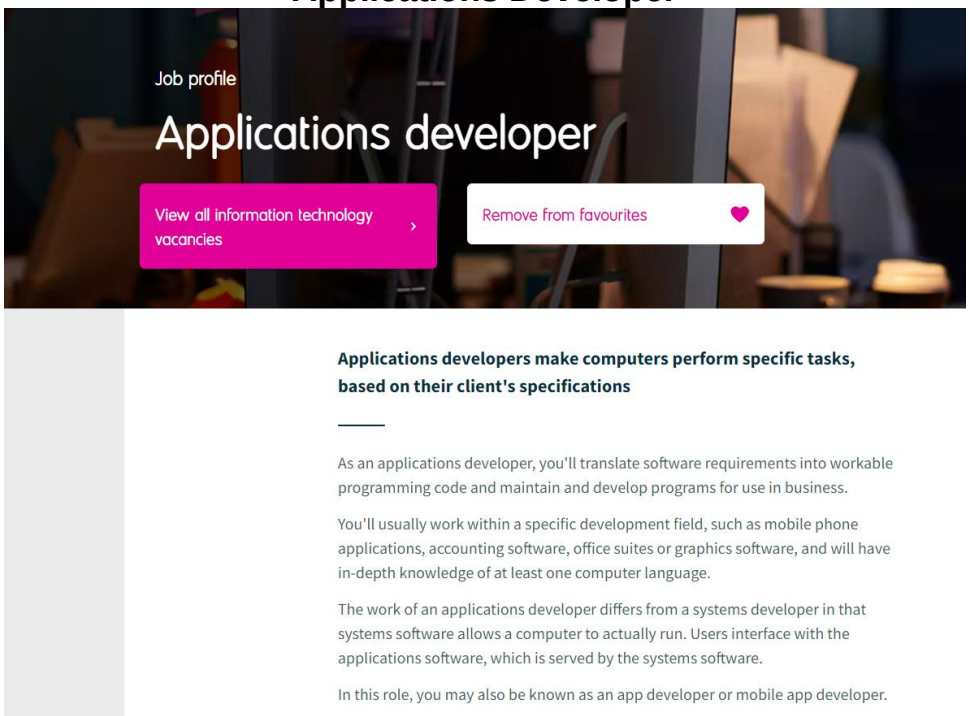
- Anish Nath (2015) *Packet analysis with Wireshark: leverage the power of Wireshark to troubleshoot your networking issues by using effective packet analysis techniques and performing an improved protocol analysis*. Birmingham, Uk: Packt Publishing.

Appendix 1

Identification of desired job roles

To understand and prepare for a potential career in the field of computer science or any other related job industries, research was carried out to identify three potential jobs and plan to understand the responsibilities, experience and qualifications required to be successful within those jobs. Additionally, it will be discussed on why these jobs are suitable.

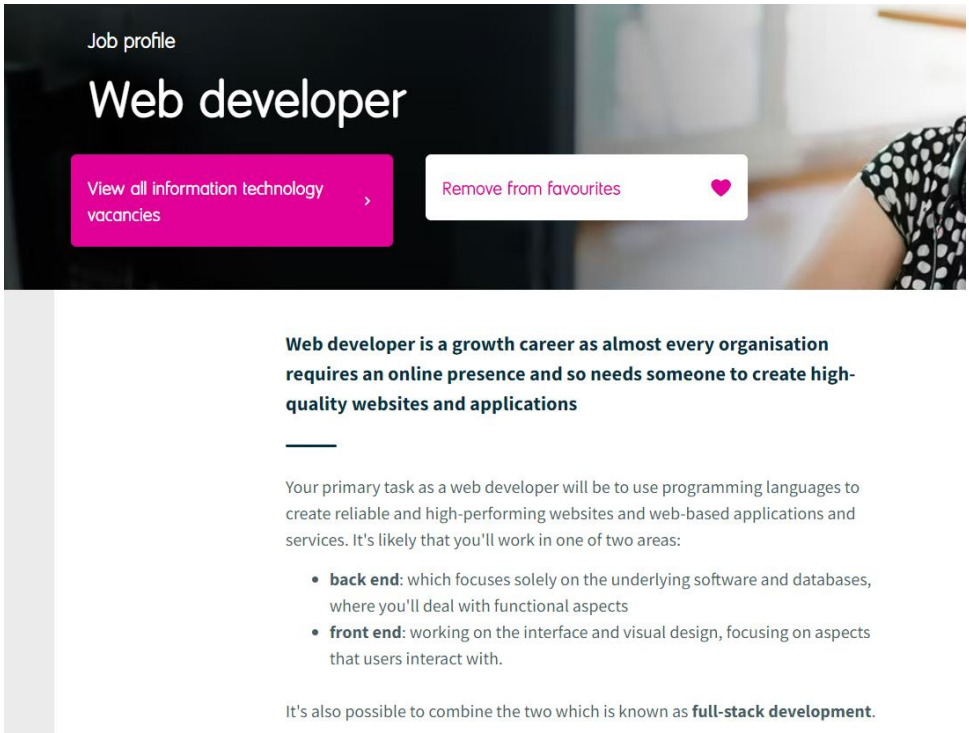
Applications Developer



The first potential job role which I am interested to work together is an Applications Developer who will specialize with mobile devices that are compatible with the Android operating system. Application developers work within a specific development field and convert the software requirements from clients into reliable programs using a programming language. The main responsibilities include communications with clients and other colleagues during the software development process, develop programs by coding in a programming language, test the program, produce documentation and manuals and constantly maintain and improve program.

I have begun learning Java for one of my university modules as a 1st year however it can be used to develop Android mobile applications in Android Studio. However, I have limited knowledge on Java and any other development frameworks for Android mobile phones which can be improved when I start developing experience and getting the relevant qualifications. This experience can be completed by doing a year in industry or freelance for clients.

Web Developer

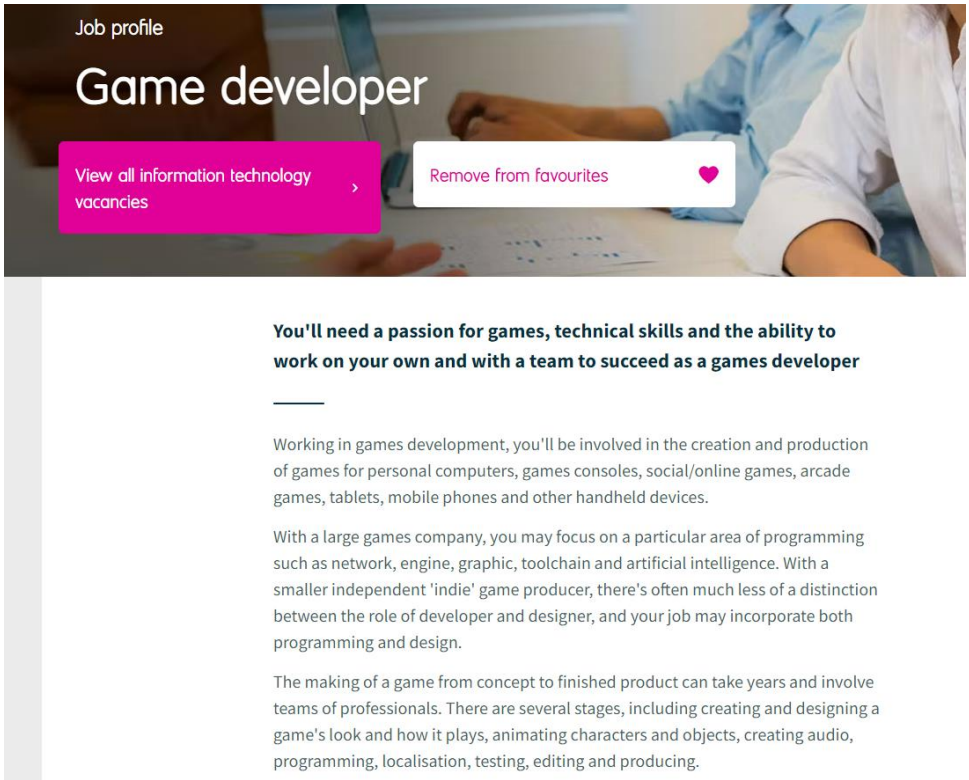


This is the second potential job role which I aim to involve myself in as an option. Web developers are responsible for the creation of high-quality websites, and Application Programming Interfaces. I would become a web developer who would most likely work on the client-side or the frontend of a website. This solely focuses on the appearance and interaction of the website with users. The main responsibilities include are the development of websites using HTML, CSS and a frontend programming language like JavaScript or TypeScript, design features, test websites for different factors such as compatibility, fix bugs in website, produce and maintain databases and document reports, code and manuals.

The roadmap to become a web developer for frontend development includes learning HTML, CSS and JavaScript with a development framework. General and technical knowledge of databases is required. Currently I have learnt both aspects of client-side and server-side web development from one of my 1st year university modules which provides experience. Experience which employers would look at:

- Freelancing
- Independent Web Projects
- 12-month Placement Year
- Part-time, full-time or self-employment

Game Developer



The final potential job role that will be mentioned is a game developer. A game developer is like the last two job roles which includes the creation of games for multiple devices using programming. As a game developer, it is preferable for me to design and produce games using Unity and the programming language C#. This is because I have had considerable amount of experience using Unity for a year.

The main responsibilities of a game developer:

- Designing and developing video games using programming language
- Testing and reviewing code
- Maintaining and improving code
- Collaboration with clients, colleagues and other designers

To become a game developer, I would need to have lots of general and technical knowledge on the video game industry, understand and be able to implement the game development process and several experiences. Like the other two job roles, experience can be achieved through independent projects such as indie game development, a year in industry, part-time employment or freelancing.

Appendix 2

UNIVERSITY OF GLOUCESTERSHIRE

YOUR Future PLAN

My Future Plan

Name: Somto Ezeoke

Date: 30th January 2024

Personal Mission Statement:

I strive to involve myself within a suitable and optimistic work environment within the computer science industry. To achieve this reality I will continue learning, represent and update my technical and transferrable skills. Ideally I do not focus on an ideal salary, only acheiveing success within the field.

My interests and motivations:

1. Programming
2. Stock Investing
3. Gym

My top skills:

1. Problem-Solving
2. Critical Thinking
3. Adaptability

My possible career options:

1. Applications Developer
2. Web Developer
3. Game Developer

	Relevant skills I have now	Skills I need for this career option	What I need to do to develop these skills
Applications Developer:	Such relevant skills which I have equipped relating to the job role include analytical thinking, problem-solving, patience and the technical ability to code using a specific high-level programming language. I aim to apply these skills into the role to develop and maintain mobile apps.	*Several skills required for this job role are analytical thinking, skill to use a high-level programming language, knowledge on the SDLC methodologies, problem-solving and other transferrable skills like working under pressure. A degree in a computer-science related field is needed and/or part-time/voluntary experience.*	*Other skills required are an expertise in mathematics, creativity, working under pressure, attention to detail and abilty to communicate and collaboration. I aim to improve or attain the majority of these skills through personal projects and experiences. During my first year, I will look for a summer internship.*
Website Developer:	*The only revelant skills I have which potentially relates to this job role is analytical thinking and problem-solving which are significant skils however I am ambitious to learn more techincal skills relating to website development.*	*Technical skills and expertise are needed such as understanding HTTP, how websites operate, expertise in HTML, CSS and a client and server side language along with producing a database. Other skills include attention to detail, problem-solving, organisatopn, communication skills, teamwork and working independently.*	*I need technical skills along with the ability to communicate and work as a team with different designers and developers. Such technical skills include knowledge on client-side and server side languages, frameworks and database management systems which can be obtained through my web development module by learning and interacting with others.*
Game Developer:	*Organsational skills, problem-solving and updated knowledge on the video game industry.*	*A strong sense of self-motivation and ability to work independently is a significant skills along with technical skills to use a range of high-level programming languages. Other skills include teamwork, creativity, attention-to detail and communication.*	*Mentioned before, I need to work on teamwork, creativity and have a stronger expertise in programming languages associated with game development such as C# and C++. I can improve this by indenpendently learning, learn through my university modules and get experience such as freelancing or part-time.*