Information Security Analyst Intern at ONE Bank PLC

by

Soham Ahmed
24141033

A report submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
February 2025

Declaration

It is hereby declared that

1. The internship report submitted is my own original work while completing degree at Brac University.
2. The report does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The report does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. I have acknowledged all main sources of help.

Student's Full Name & Signature:

Soham Ahmed
24141033

Approval

The internship report titled "Information Security Analyst Intern at ONE Bank PLC" submitted by

1. Soham Ahmed(24141033)

In Fall, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on February 08, 2025.

Examining Committee:

Supervisor:
(Member)

Md. Shahriar Rahman
Lecturer
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Mr. K. M. Mohiuddin
Chief Information Security Officer and First Assistant Vice President
Information Security Department
Information Technology Division
ONE Bank PLC

Program Coordinator:
(Member)

Dr. Md. Golam Rabiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Dr. Sadia Hamid Kazi
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

The Information Security Analyst Internship at ONE Bank PLC offers a comprehensive learning experience within the Information Technology division, with an emphasis on the challenging field of information security. This internship offers hands-on training regarding latest security protocols, risk management strategies, and compliance measures vital for safeguarding the bank's not only physical but also digital assets. Throughout the internship, the intern will engage in various activities, including getting hands-on training, monitoring security systems using SIEM solutions, performing vulnerability assessments using industry-standard tools, as well as performing penetration testing in a controlled environment. The role aims deepen the intern's knowledge of information security frameworks and regulatory standards, such as ISO/IEC 27001:2013, PCI-DSS, HIPAA, GDPR etc. Furthermore, the internship will enhance the intern's skills in critical thinking, problem-solving, and effective communication in a professional setting. By the end of the internship, the intern will acquire valuable insights into the operational and strategic dimensions of information security in the banking sector, which will ultimately prepare them for future roles in entry level cybersecurity and IT risk management jobs.

Keywords: Vulnerability Assessment; Penetration Testing; Information Security; Incident Response; ISO/IEC 27001:2013; PCI-DSS; HIPAA; GDPR; Cybersecurity; Assets; IT Risk Management;

Acknowledgement

Firstly, I want to start by praising Almighty Allah for allowing me to complete my internship report without any major difficulties.

Secondly, thanks to my co-supervisor Mr. K. M. Mohiuddin sir and my internship mentor Md. Appel Mahmud Sagar bhaia for their kind support and guidance throughout the process.

Thirdly, thanks to my supervisor Md. Shahriar Rahman sir for helping me clear all my confusions.

And finally, I want to thank my mother for always believing in me. With her prayer I am now on the verge of my graduation.

Table of Contents

List of Figures

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

AI Artificial intelligence

AML Anti-Money Laundering

AWS Amazon Web Services

BoC Behaviors of Compromise

CBS Core Banking System

CIA Confidentiality, Integrity, Availability

CSR Corporate Social Responsibility

DNS Domain Name System

EoC Enablers of Compromise

FTP File Transfer Protocol

$GDPR$ General Data Protection Regulation

GPI Global Payments Innovation

GUI Graphical User Interface

$HIPAA$ Health Insurance Portability and Accountability Act

$HTTP$ Hypertext Transfer Protocol

IoC Indicators of Compromise

IP Internet Protocol

$ISMS$ Information Security Management System

ISO International Organization for Standardization

ISP Internet Service Provider

IT Information Technology

$ITSM$ Information Technology Service Management

KYC Know Your Customer

MFS Mobile Financial Services

MIS Management Information System

$NMAP$ Network Mapper

NTA Network Traffic Analysis

$OBPLC$ ONE Bank PLC

$OSINT$ Open Source Intelligence

OT Operational Technology

$PCI - DSS$ Payment Card Industry Data Security Standard

PT Penetration Testing

RMG Ready-Made Garments

$SDLC$ Software Development Life Cycle

$SIEM$ Security Information and Event Management

$SMAC$ Social, Mobile, Analytics, and Cloud

SME Small and Medium Enterprises

$SMTP$ Simple Mail Transfer Protocol

$SWIFT$ Society for the Worldwide Interbank Financial Telecommunication

TCO Total Cost of Ownership

TCP Transmission Control Protocol

TOR The Onion Router

VA Vulnerability Assessment

VPR Vulnerability Priority Rating

WAF Web Application Firewall

Chapter 1

Introduction

1.1 Preamble

An internship can be regarded as a training period offered by certain companies for helping fresh graduates get familiar with the professional environment. A workplace setting is significantly different from the learning setting we get in our early lives. In the classroom, students don't get the chance to implement their knowledge in a real world scenario. Whereas, an internship can provide a taste of this experience by creating not only an opportunity for practical learning, but also highlighting the importance of collaborative learning and teamwork. In the workplace, each individual possesses a different set of skills. That's why teams work together to combine their knowledge and skills to achieve shared objectives.

The Department of Computer Science and Engineering at Brac University offers three options to students who have completed at least 75 credits: a research intensive thesis, a project or an internship. I always wanted to get myself familiar with corporate life by gaining hands-on experience. The following are the objectives of the internship introduced by the department :

- To acquire necessary understanding of the corporate environment
- To create a bridge between academic knowledge and real-world scenarios
- To fulfill the requirements for the Bachelor of Science in Computer Science (CS) Program

I am honored to be a student of Computer Science and have the opportunity to get an internship in the Information Security Department at ONE Bank PLC, one of the most prestigious banks in the country. From my early life, I was always fascinated by cybersecurity experts and ethical hackers and wanted to work like them. My idol was Edward Snowden, a Russian former National Security Agency contractor who successfully leaked the classified documents that proved the existence of secret surveillance programs. I began my internship on 2nd June, 2024 without any prior experience of the field. Looking back from now, I realize that it was one of the best decisions of my life because I have learned a lot which exceeded my expectations. It was an enlightening journey.

1.2 Purpose of this Document

This report is the overview of the first two months of my internship program that I have conducted in the Information Security Department at ONE Bank PLC and it is prepared as a requirement for the completion of the Bachelor of Science in Computer Science degree, at Brac University. The objective of this report can be divided into two categories:

- General Objective
- Specific Objective

1.2.1 General Objective

This internship report is prepared in order to meet the requirements for the Bachelor of Science in Computer Science degree under the Department of Computer Science and Engineering at Brac University.

1.2.2 Specific Objective

On a more specific note, this report covers the following:

- An overview of the ONE Bank PLC
- Focus on services, work environment as well as facilities provided to the employees of ONE Bank PLC
- A comprehensive discussion of my responsibilities and knowledge gained throughout the six months of my internship

The purpose of this report is to not only track my overall experience of ONE Bank PLC, but also provide a comprehensive overview of the difficulties that I have faced and utilize them as a learning to overcome them further. It also outlines the products and services that ONE Bank PLC offers to its clients and employees.
Furthermore, this report shows my achievements, practical work and professional growth throughout the journey. It can serve as a detailed guideline for future interns seeking to know more about the workplace environment of ONE Bank PLC.

1.3 Methodology

The following report is mainly focused around my personal experience as well as my learning throughout my internship at ONE Bank PLC. I can categorize all the information that was available to me into 2 categories:

1.3.1 Primary Data Source

- My practical experience gained from day to day basis
- Lessons learned from discussions with colleagues, team leaders and my mentor
- Information gathered from formal meetings, audits and seminars

1.3.2 Secondary Data Source

- Official website of ONE Bank PLC
- Internet

Chapter 2

Company Profile

2.1 Overview

ONE Bank PLC started its journey in May 1999 under the Companies Act of 1994 which was registered with the Registrar of Joint Stock Companies as a private commercial bank. The bank is dedicated to providing for its clients. The primary focus of the bank is efficiency, transparency, precision and motivation. ONE Bank PLC aims to reach the peak of excellence through its value and image while manifesting the idea of unity and progress. One Bank PLC provides several savings schemes for deposits from the public and lends funds to important sectors maintaining a certain margin. It follows a risk assessment strategy and ensures compliance while choosing its assets. Along with its focus on the textile and RMG industry, the bank is currently expanding its horizon regarding its non-funded business. It is also trying to expand its SME portfolio.

2.2 Vision

- Rank ONE Bank PLC as a role model in Bangladesh's Banking sector.
- Meet the needs of clients as well as ensure employee satisfaction.

2.3 Mission

- Explore ways to serve better in order to enhance customer service.
- Proactively fulfill social responsibilities
- Regular reviewing of business lines to implement industry best practices.
- Foster a supportive work environment that promotes teamwork and encourages employees to bring their highest potential.

2.4 Services

With the help of innovation and state of the art technology, ONE Bank PLC offers real-time online banking services which include Visa debit and credit cards along

with ATM facilities. Not only that, ONE Bank has E-banking and mobile banking facilities. ONE app is a digital banking service that allows clients to conduct any type of financial transactions using only a smartphone or tablet. It also has OK Wallet which is a Mobile Financial Services (MFS) application that not only allows sending cash to people online, but also recharge mobile talk time, pay utility bills, buy something from favorite shops by only scanning QR code or using an OK merchant payment gateway. It also allows cash-in and cash-out from any of ONE Bank's agent points as well as 107 branches. ONE Bank PLC also has SWIFT (Society for the Worldwide Interbank Financial Telecommunication) for secured interbank financial communication through messaging service. SWIFTgpi (Global Payments Innovation) is a new approach from SWIFT which allows faster and more transparent cross-border payment solution for the clients.

2.5 Certifications

2.5.1 ISO/IEC 27001:2013

ISO/IEC 27001:2013 is a globally renowned standard for information security management which outlines the requirements for not only continual development, but also implementation and maintenance of an Information Security Management System (ISMS). This standard provides a step-by-step approach towards managing confidential company information by ensuring CIA triad which is confidentiality, integrity and availability through a process called risk management. It has a total of 114 controls listed in Annex A which is later organized in 14 control categories. These controls are building blocks of a detailed framework that is capable of managing information security risks.

ISO 27001 Domain	Number of Controls	Annex
Information Security Policies	2	A5
Organisation of Information Security	7	A6
Human Resources Security	6	A7
Asset Management	10	A8
Access Control	14	A9
Cryptography	2	A10
Physical and Environmental Security	15	A11
Operational Security	14	A12
Communications Security	7	A13
System Acquisition, Development and Maintenance	13	A14
Supplier Relationships	5	A15
Information Security Incident Management	7	A16
Information Security Aspects of Business Continuity Management	4	A17
Compliance	5	A18

Figure 2.1: 14 Control Categories of ISO/IEC 27001:2013 [7]

ONE Bank PLC has received the ISO/IEC 27001:2013 certification from a Tier-1

accreditation body on August 18, 2024. The certificate is valid until August 17,2025.

Figure 2.2: ISO/IEC 27001:2013 certificate

2.5.2 Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI-DSS) is basically a set of regulations designed to establish a secure environment for processing, storage and transmission of any payment card information which includes credit, debit as well as prepaid cards. The goal of PCI-DSS is to protect cardholder information while minimizing the risk of credit card fraud. There are in total of 12 requirements of PCI-DSS.

Figure 2.3: PCI-DSS requirements

ONE Bank has the PCI-DSS compliance certification which was issued on 20th August, 2023.

Figure 2.4: PCI-DSS certification

2.6 Green banking

As an environmentally responsible bank, ONE Bank PLC's eco-friendly initiative towards building a greener future and sustainable environment include:

- Implementing in-house environmental management practices
- Conducting and promoting eco-friendly activities for raising awareness
- Sticking to Environmental Risk Management guidelines
- Introducing green banking products as well as services
- Providing funding for green projects and initiatives
- Supporting customers and Employees for becoming more environmentally responsible
- Supporting eco-friendly as a part of CSR activities
- Creating alliances with NGOs and other environmentally focused organizations in order to further advance green banking initiatives.

2.7 Office Schedule

Business hours are usually the hours during the day in which general official activities are conducted. ONE Bank PLC follows a strict working schedule. There are 5 working days in a week, starting from Sunday to Thursday, from 10:00AM to 6:00PM.

2.8 Recruitment process

Recruitment process differs from position to position. For my case, I had to submit my CV along with the forwarding letter issued from my university to the Head of HR. Upon acceptance, a small interview was taken by the Managing Director. After that, I was transferred to the Information Technology Division where the Head of the Information Technology Division conducted a second interview for assigning me to a suitable department. That is how I was selected for Information Security Department.

2.9 Information Technology Division

Key aspects of the Information Technology Division of ONE Bank PLC include:

2.9.1 Core Banking Systems:

It is responsible for managing essential operations like transaction, customer accounts as well as loan processing.

2.9.2 Online and Mobile Banking:

It allows customers to create and access accounts, make transaction, pay bills as well as apply for loans through digital platform.

2.9.3 Data Center and System Management:

It involves planning, monitoring, maintenance and security of the data center to ensure the availability, reliability and efficiency of banking services.

2.9.4 Network Management:

It ensures the secure and reliable communication within the bank's network through administration and control of the network infrastructure. It involves monitoring, configuration, maintenance and security of the bank's network to ensure its reliability, performance, and security.

2.9.5 In-house Software Development, Maintenance and Support:

Develops and maintains software to automate processes. The main goal is to enhance customer experiences while complying with regulations. This includes system integration, security measures as well as quality assurance.

2.9.6 Risk Management:

It helps identify and manage credit related, market related as well as operational risks using the help of algorithms and dedicated software which ensures informed decision-making and resilience.

2.9.7 Data Management, Analytics, and Reporting (MIS):

It uses state-of-the-art analytics tools to manage vast amounts of data while improving risk management, detecting fraud as well as enabling targeted marketing tactics.

2.9.8 Database Management/Administration:

It manages database systems in order to store it securely while maintaining stability and compliance with regulatory standards.

2.9.9 Compliance and Regulatory Requirements:

IT systems facilitate compliance with several standards like anti-money laundering (AML), Know Your Customer (KYC) and other legal standards through automated monitoring and reporting tools.

2.9.10 Digital Banking Services:

It leverages models like SMAC (Social, Mobile, Analytics, Cloud) in order to enhance customer experience and cost reduction, making banking more customer-friendly and agile.

2.9.11 Information Security Management:

ONE Bank implements robust IT security measures like firewalls, encryption, SIEM (Security Information and Event Management), Vulnerability assessment to protect sensitive data and prevent cyber attacks.

2.10 Information Security Team

The information security team consists of 3 employees:

- Mr. K. M. Mohiuddin (Chief Information Security Officer and First Assistant Vice President, Information Security Department)
- Md. Zamal Sikder (Manager and Senior Principal Officer, Information Security Department)
- Md. Appel Mahmud Sagar (Assistant Manager and Senior Officer, Information Security Department)

2.11 Environment and Security

- Every floor main door is always locked and requires Bio-metric scan as well as employee key card to open
- BYOD (Bring Your Own Device) is strictly prohibited by the office
- Printers and Photocopiers record activity log
- The Bank runs on Intranet network, with heavy restriction to websites including YouTube, Facebook, Instagram, etc.
- Closed-Circuit Television Cameras are operating 24/7 in the office premises.

Chapter 3

Training and Initial Work Plan

3.1 Training on General Awareness of Information Security and Cybersecurity

The first training I received from my department was the Training on General Awareness of Information Security and Cybersecurity. It was a comprehensive training which allowed me to learn industry best practices to safeguard information and build a robust defense against cyber threats to protect bank assets as the bankers typically deal with sensitive information everyday. Some important takeaways from the training include:

3.1.1 CIA Triad

- Confidentiality: Only authorized persons can access the information
- Integrity: The information is complete and accurate. And protecting information from being changed by unauthorized parties
- Availability: The information is available whenever authorized access is required

Figure 3.1: CIA Triad [3]

3.1.2 ISMS

ISMS is a documented management system consisting of a set of security controls that protect the confidentiality, availability, and integrity of assets from threats and vulnerabilities. By designing, implementing, managing, and maintaining an ISMS, organizations can protect their confidential, personal, and sensitive data from being compromised.

Figure 3.2: ISMS

3.1.3 7 Layers of Cybersecurity

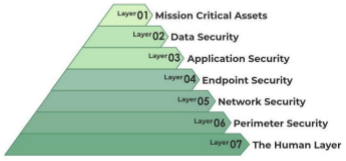


Figure 3.3: 7 Layers of Cybersecurity [6]

3.1.4 Information Security vs Cybersecurity

There is a common misconception that information security and cybersecurity are the same thing. It is partially true. Because the realm of information security is a lot larger than cybersecurity which includes the security of overall landscape including physical and digital whereas, cybersecurity works with only the security of only the cyber realm.

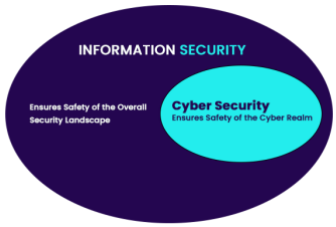


Figure 3.4: Information Security vs Cybersecurity

3.1.5 Social Engineering

Humans are considered as the weakest link because no matter how strong is someone's firewall, antivirus, Intrusion Detection System or cryptography, humans will still be vulnerable than computers as they are prone to mistakes. and Social Engineering is a concept that involves manipulating people into performing actions or divulging confidential information. Similar to a confidence trick or simple fraud, the term applies to the use of deception to gain information, commit fraud, or access computer systems.

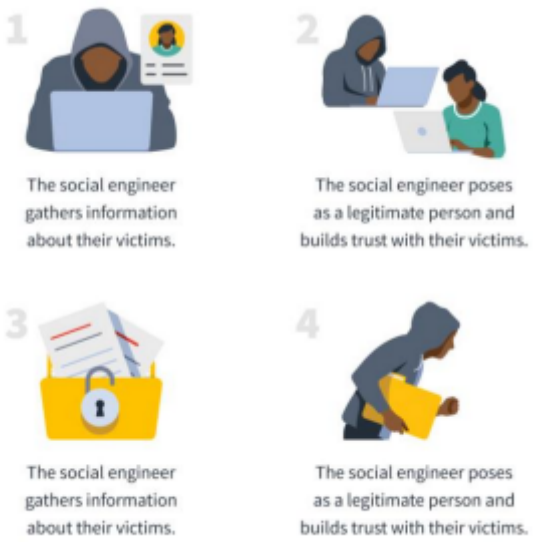


Figure 3.5: Social Engineering

3.1.6 Common Cybersecurity Threats

The common cybersecurity threats an organization faces include viruses, malware (ransomware and spyware), phishing, Password Attacks, DDoS attacks, Man in the middle, Drive-By Downloads, Malvertising, Rogue Software etc.

Figure 3.6: Common Cybersecurity Threats

3.1.7 Cyber Hygiene Practices

Everyone should remember these things while leaving office:

- Sign Out all applications
- Shut Down PC and power off all devices
- Lock Desk Cabinet
- Preserve confidential documents
- Clean your Desk

Figure 3.7: Cyber Hygiene Practices [4]

3.2 TryHackMe Certifications

3.2.1 Introduction to Cybersecurity

First course I was instructed to do was the Introduction to Cybersecurity learning path from TryHackMe where I hacked my first application and defended against a live cyber attack in a simulated lab environment. There were 3 modules, and 8 hands-on labs. From this course, I gained knowledge about defensive security and offensive security.

Figure 3.8: TryHackMe Introduction to Cyber Security Learning Path Certification

3.2.2 Pre security

Second course I was instructed to do was the Pre Security learning path which helped me build a solid foundation in the field. There were about 5 modules and 18 hands-on labs. I learned about a lot of things from this course including, network fundamentals, web fundamentals, Linux fundamentals as well as Windows fundamentals.

Figure 3.9: TryHackMe Pre Security Learning Path Certification

3.3 Introduction to Vulnerability Assessment Tools for Future Tasks

ImmuniWeb:

It is a comprehensive cybersecurity platform that offers threat intelligence, application security testing as well as provide compliance solutions. It combines both automated and manual testing methodologies to examine vulnerabilities in web. Not only that, it has the feature of continual monitoring and risk assessment that organizations use to maintain its security posture.

Qualys:

Qualys is basically a cloud-based security and compliance platform used to generate reports regarding the detailed overview of vulnerabilities based on severity levels.

Zenmap:

Zenmap is a graphical user interface for the Nmap network scanning tool. It is used in penetration testing scenarios where the finding open ports of a device to gain access in necessary.

SIEM:

Security Information and Event Management is a cybersecurity approach that records security logs in real-time. SIEM solutions enable organizations to detect, investigate and respond to security incidents by providing a centralized visibility.

3.4 First Task

The initial task given to me was checking the ONE Bank's official website through my home desktop to generate the website security test report through ImmuniWeb. Firstly, I had to create an account with my university email in ImmuniWeb. Then after choosing the website security test, I had to provide the URL of ONE Bank's official website in the tool to generate report and analyze the findings.

Figure 3.10: ImmuniWeb Website Security Test

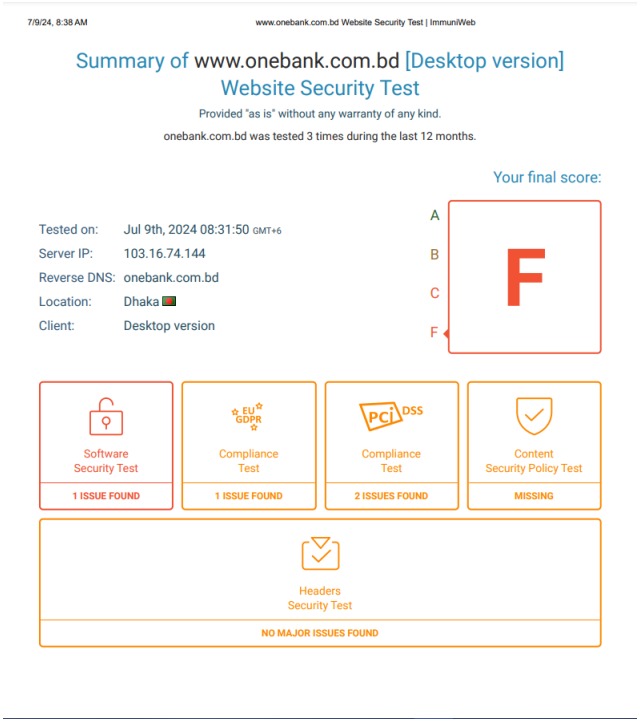


Figure 3.11: ImmuniWeb Website Security Test Summary

After the test, it shows the final score as F which was surprising but my co-supervisor told me this was an expected outcome. So I tried to find out the reason of poor score of such a secured website. There were 4 web software vulnerabilities as well as 1 outdated web software.

Figure 3.12: ImmuniWeb Website Software Vulnerabilities

Not only that, I analyzed the issues further and found a suspicious weakness which was Web Application Firewall was not detected. It was suggesting to implement a WAF to protect against common web attacks. But, I already knew ONE Bank was using an industry standard WAF as well as a core firewall.

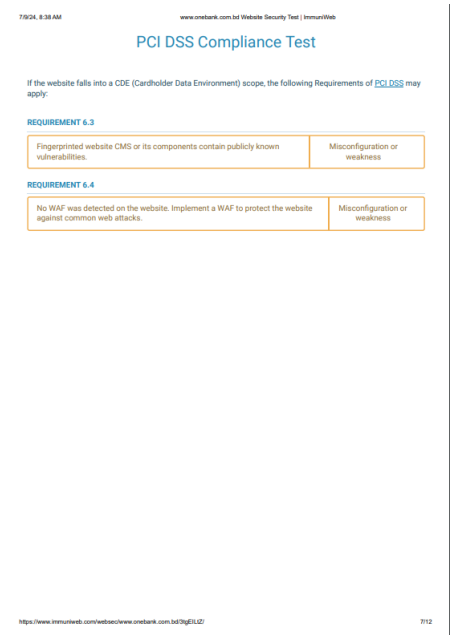


Figure 3.13: ImmuniWeb PCI DSS Compliance Test

Then, I have done the website security test from office desktop in a controlled environment and analyzed ONE app's website and found out the summary had the best score. I noticed that there was clearly a WAF present on the website. Thus, There were also no web software vulnerabilities and PCI DSS weaknesses regarding WAF.

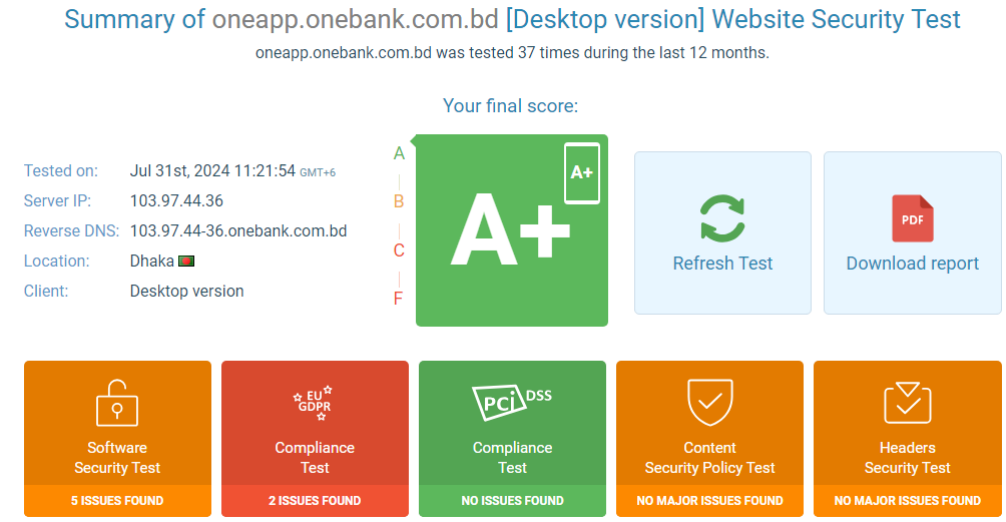


Figure 3.14: Updated Website Security Test summary

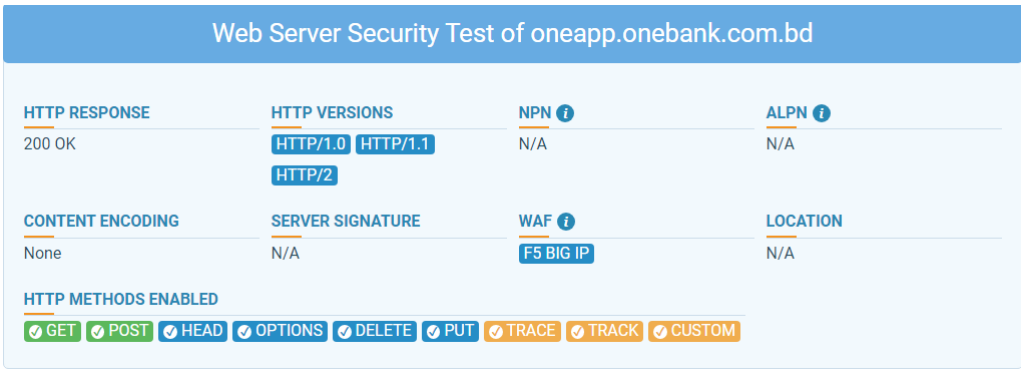


Figure 3.15: Updated Website Security Test results

3.4.1 Key Takeaways

After this task, my co-supervisor made me realize the importance of WAF in an organization and how it interacts with ImmuniWeb reports. Industrial WAFs may identify automated testing tools like ImmuniWeb as a potential threat especially when the tool is performing offensive security tests like penetration testing or vulnerability scanning. If it encounters such network traffic, it might block those requests which gives a false ImmuniWeb report.

3.4.2 Lessons Learned From Second Test

- Firstly, ImmuniWeb can work perfectly In a controlled environment, administrators can temporarily whitelist or allow access to ImmuniWeb's IP addresses or user agents in the WAF configuration that keeps the scanning activities unblocked.

- Secondly, adjusting WAF rules that are responsible for blocking third party scans can be modified or disabled to ensure a perfect testing environment which typically happens for a comprehensive security audit.

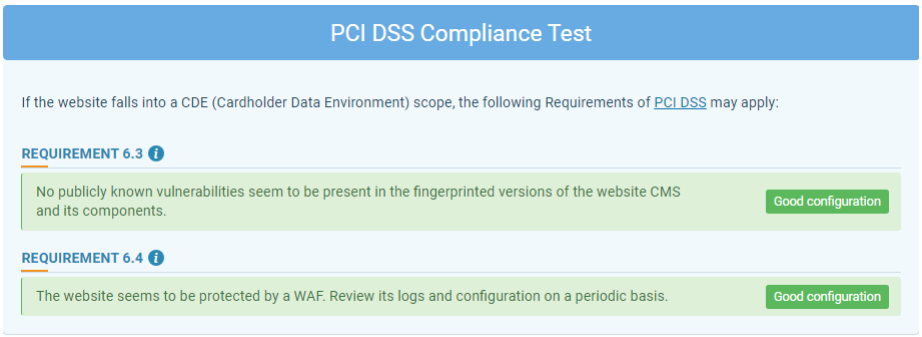


Figure 3.16: Updated PCI DSS Compliance Test

- Finally, running tests in a staging environment where WAF is configured differently to allow testing without interfering with live production traffic.

3.4.3 Future Work

After this testing and learning phase, my co-supervisor sir registered me for the ISC2 Certified in Cybersecurity (CC) Exam and training. the certification is typically not free. It costs about 199 US dollars. But I got the opportunity to get it through an offer that was going on at that time. ISC2 offered Online Self-Paced Training and exams to one million people. After passing the exam, I have to pay 50 US dollars annual fee to finally become a member of ISC2 and get certified in cybersecurity. There are in total of 5 domains. Domain 1 covers security principles, domain 2 covers business continuity, disaster recovery and incident response concepts, domain 3 covers access control concepts, domain 4 covers network security and domain 5 covers security operations. Not only that, I have enrolled in the Google Cybersecurity Professional Certification of Coursera. It requires completing a total of 8 courses covering fundamental topics like Python programming, SQL, Linux, IDS, SIEM and a lot more. These courses will prepare myself for the CompTIA Security+ Examination in the future. According to my co-supervisor, my future tasks will include generating report with Qualys, performing penetration testing in a controlled environment using Zenmap as well as collecting and analyzing logs using SIEM solution.

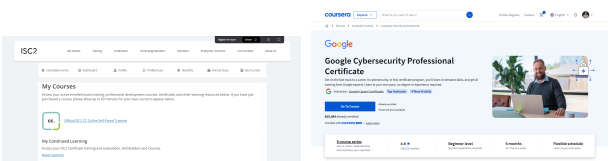


Figure 3.17: Future Work

Chapter 4

My Contributions

4.1 Qualys

My first official task involved performing a vulnerability assessment on a server using Qualys. Qualys is a renowned provider of cloud-based cybersecurity as well as compliance solutions. It provides an integrated suite of tools with a user-friendly GUI for managing and securing the overall IT infrastructure. It offers various services including vulnerability management, real-time threat detection and compliance assessments. Organizations like ONE Bank PLC prefer Qualys as it provides security and compliance through operating as a cloud platform. As a result, depending heavily on on-premises hardware or software installations is not necessary.

4.2 Key Features of Qualys

4.2.1 Vulnerability Management

Qualys not only scans IT assets including servers, workstations of applications to detect vulnerabilities but also provides detailed reports highlighting the severity of threats and mitigation techniques.

4.2.2 Web Application Security

It can protect against vulnerabilities including SQL injection and cross-site scripting. WAF can also be integrated using included tools.

4.2.3 Policy Compliance

It can assess applications and systems for compliance related issues and take necessary measures by monitoring configuration baselines to ensure continuous conformity with industry standards like PCI-DSS, HIPAA, GDPR etc.

4.2.4 Cloud Security Assessment

It not only provides visibility into cloud environments like AWS, Azure, Google Cloud but also, detects and handles any form of vulnerabilities, misconfigurations and compliance issues in cloud space.

4.2.5 Endpoint Detection and Response (EDR)

It detects and immediately responds to any form of threats targeting endpoints such as desktops, laptops as well as mobile devices.

4.2.6 Global Asset Inventory

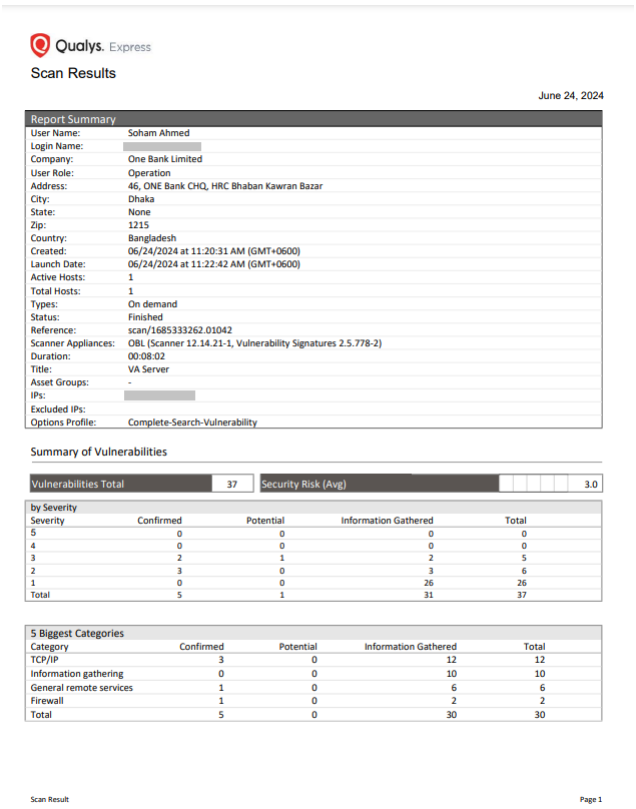
It can maintain a database containing all forms of hardware and software asset information including software versions, licensing, model number, potential risks throughout not only in the cloud space but also on-premises and hybrid environments.

4.2.7 Container and DevSecOps Security

It scans containerized applications for vulnerabilities as well as offers detailed security insights during the software development lifecycle (SDLC)

4.3 Vulnerability Assessment and Report Generation

I was instructed to run a vulnerability assessment on a particular server using Qualys. As per the scan results, It can be seen that 37 total vulnerabilities are detected and the average security risk is 3.0.



Qualys. Express

Scan Results

June 24, 2024

Report Summary

User Name:	Soham Ahmed
Login Name:	
Company:	One Bank Limited
User Role:	Operation
Address:	46, ONE Bank CHQ, HRC Bhaban Kawran Bazar
City:	Dhaka
State:	None
Zip:	1215
Country:	Bangladesh
Created:	06/24/2024 at 11:20:31 AM (GMT+0600)
Launch Date:	06/24/2024 at 11:22:42 AM (GMT+0600)
Active Hosts:	1
Total Hosts:	1
Types:	On demand
Status:	Finished
Reference:	scan/1685333262.01042
Scanner Appliances:	OBL (Scanner 12.14.21-1, Vulnerability Signatures 2.5.778-2)
Duration:	00:08:02
Title:	VA Server
Asset Groups:	-
IPs:	
Excluded IPs:	
Options Profile:	Complete-Search-Vulnerability

Summary of Vulnerabilities

Vulnerabilities Total	37	Security Risk (Avg)	3.0

by Severity

Severity	Confirmed	Potential	Information Gathered	Total
5	0	0	0	0
4	0	0	0	0
3	2	1	2	5
2	3	0	3	6
1	0	0	26	26
Total	5	1	31	37

5 Biggest Categories

Category	Confirmed	Potential	Information Gathered	Total
TCP/IP	3	0	12	12
Information gathering	0	0	10	10
General remote services	1	0	6	6
Firewall	1	0	2	2
Total	5	0	30	30

Scan Result

Page 1

Figure 4.1: Qualys Scan Results Report Summary

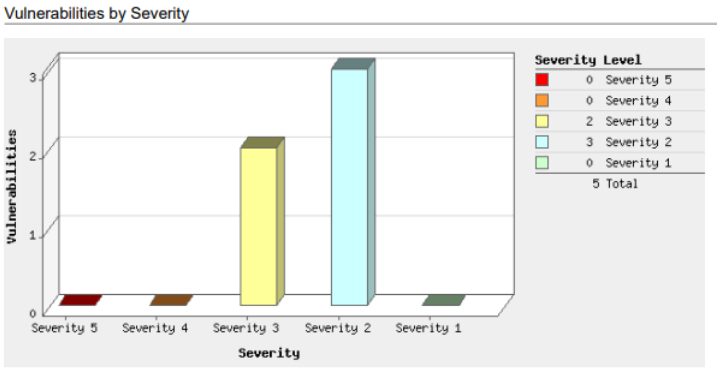
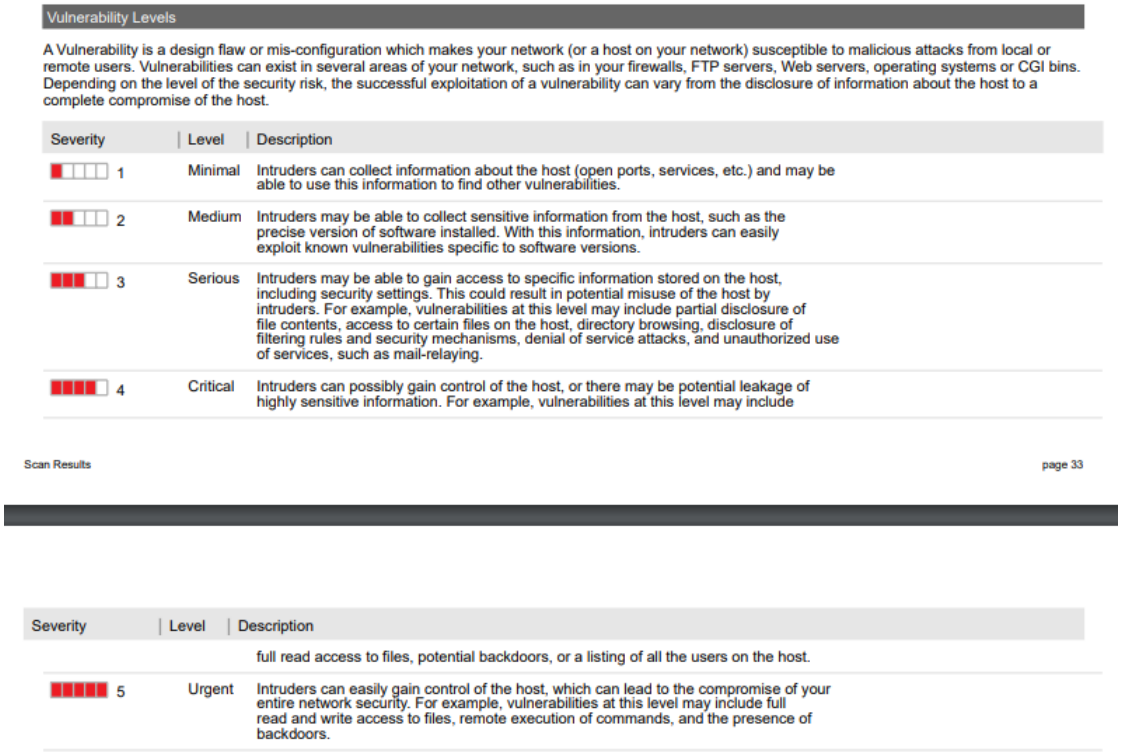


Figure 4.2: Overall Threat Severity Levels

Vulnerabilities are divided into 5 levels of severity starting from level 1. The levels are named in the following manner : minimal, medium, serious, critical and urgent. These are basically a design flaw or mis-configuration which makes the network vulnerable to various malicious attacks from local and remote users. It can exist in several areas of a network including firewalls, FTP servers, Web servers, operating systems of CGI bins.



Vulnerability Levels

A Vulnerability is a design flaw or mis-configuration which makes your network (or a host on your network) susceptible to malicious attacks from local or remote users. Vulnerabilities can exist in several areas of your network, such as in your firewalls, FTP servers, Web servers, operating systems or CGI bins. Depending on the level of the security risk, the successful exploitation of a vulnerability can vary from the disclosure of information about the host to a complete compromise of the host.

Severity	Level	Description
1	Minimal	Intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	Intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	Intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	Intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include

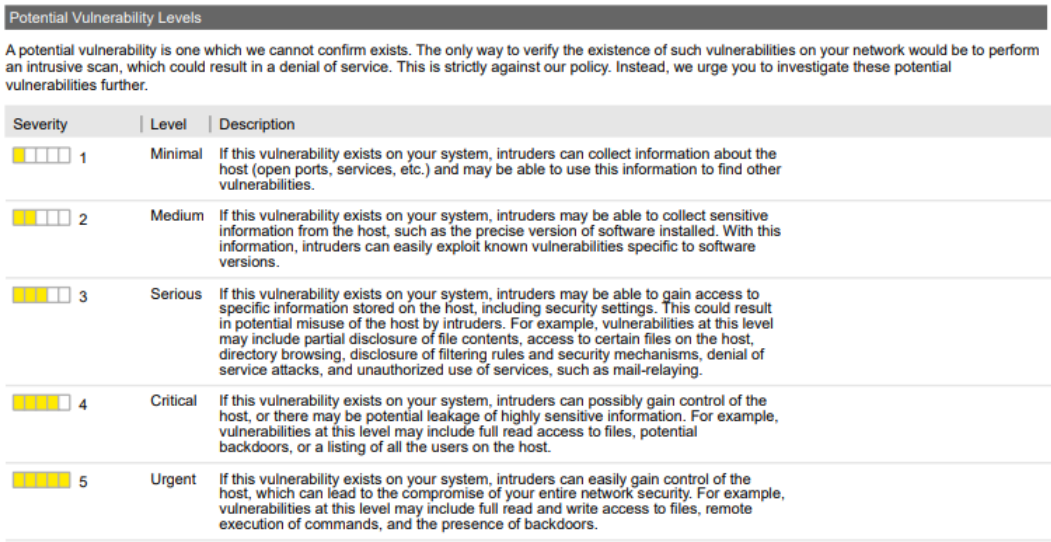
Scan Results page 33

Severity	Level	Description
		full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	Intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Figure 4.3: Vulnerability Severity Levels

There are also potential vulnerabilities which we cannot confirm exists. The only way to ensure its existence is by running an intrusive scan on the network. These are also categorized by severity levels. These forms of vulnerabilities are suggested to investigate further.

Information gathered section includes the visible information about the network related to the host. This includes traceroute information, ISP information, or a list of reachable hosts. The severity levels here also include Network Mapping data, such as detected firewalls, SMTP banners or a list of open TCP services.

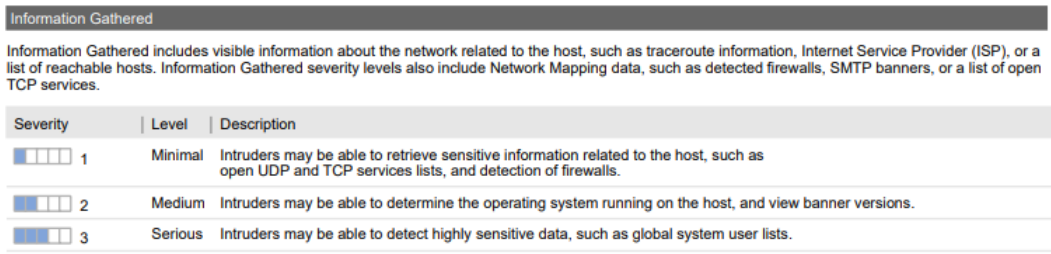


Potential Vulnerability Levels

A potential vulnerability is one which we cannot confirm exists. The only way to verify the existence of such vulnerabilities on your network would be to perform an intrusive scan, which could result in a denial of service. This is strictly against our policy. Instead, we urge you to investigate these potential vulnerabilities further.

Severity	Level	Description
1	Minimal	If this vulnerability exists on your system, intruders can collect information about the host (open ports, services, etc.) and may be able to use this information to find other vulnerabilities.
2	Medium	If this vulnerability exists on your system, intruders may be able to collect sensitive information from the host, such as the precise version of software installed. With this information, intruders can easily exploit known vulnerabilities specific to software versions.
3	Serious	If this vulnerability exists on your system, intruders may be able to gain access to specific information stored on the host, including security settings. This could result in potential misuse of the host by intruders. For example, vulnerabilities at this level may include partial disclosure of file contents, access to certain files on the host, directory browsing, disclosure of filtering rules and security mechanisms, denial of service attacks, and unauthorized use of services, such as mail-relaying.
4	Critical	If this vulnerability exists on your system, intruders can possibly gain control of the host, or there may be potential leakage of highly sensitive information. For example, vulnerabilities at this level may include full read access to files, potential backdoors, or a listing of all the users on the host.
5	Urgent	If this vulnerability exists on your system, intruders can easily gain control of the host, which can lead to the compromise of your entire network security. For example, vulnerabilities at this level may include full read and write access to files, remote execution of commands, and the presence of backdoors.

Figure 4.4: Potential Vulnerability Severity Levels



Information Gathered

Information Gathered includes visible information about the network related to the host, such as traceroute information, Internet Service Provider (ISP), or a list of reachable hosts. Information Gathered severity levels also include Network Mapping data, such as detected firewalls, SMTP banners, or a list of open TCP services.

Severity	Level	Description
1	Minimal	Intruders may be able to retrieve sensitive information related to the host, such as open UDP and TCP services lists, and detection of firewalls.
2	Medium	Intruders may be able to determine the operating system running on the host, and view banner versions.
3	Serious	Intruders may be able to detect highly sensitive data, such as global system user lists.

Figure 4.5: Information Gathered Severity Levels

In the detailed results section of the generated report, all the detected vulnerabilities are shown in a comprehensive manner. Along with the severity level, threat description, impact, solution, compliance issues, exploit-ability as well as results are shown which helps in mitigating these vulnerabilities.

- Threat description provides the context of the vulnerability so that security personnel understand the potential threat
- Impact underlines the business or operational risks associated with the vulnerability
- Solution provides guidance in order to alleviate the threat in an effective manner.
- Compliance section provides the information whether the vulnerability violates any regulatory or compliance standards. This section is given so that penalties related to non-conformity can be avoided

- Exploit-ability section assists by showing the likelihood of a particular vulnerability to be targeted for exploitation.

2 SSL Certificate - Signature Verification Failed Vulnerability — port 3389/tcp over SSL

QID:	38173	CVSS Base:	6.4 [1]
Category:	General remote services	CVSS Temporal:	4.7
Associated CVEs:	-		
Vendor Reference:	-		
Bugtraq ID:	-		
Service Modified:	02/28/2022	CVSS3.1 Base:	6.5 [1]
User Modified:	-	CVSS3.1 Temporal:	5.6
Edited:	No		
PCI Vuln:	Yes		

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection. The authentication is done by verifying that the public key in the certificate is signed by a trusted third-party Certificate Authority.

If a client is unable to verify the certificate, it can abort communication or prompt the user to continue the communication without authentication.

IMPACT:

By exploiting this vulnerability, man-in-the-middle attacks in tandem with DNS cache poisoning can occur.

Exception:
If the server communicates only with a restricted set of clients who have the server certificate or the trusted CA certificate, then the server or CA certificate may not be available publicly, and the scan will be unable to verify the signature.

SOLUTION:

Please install a server certificate signed by a trusted third-party Certificate Authority.

COMPLIANCE:

Not Applicable

EXPLOITABILITY:

There is no exploitability information for this vulnerability.

ASSOCIATED MALWARE:

There is no malware information for this vulnerability.

RESULTS:

Certificate #0 CN=vaserver.obl.com ISSUER:_CN=vaserver.obl.com self signed certificate

Figure 4.6: Threat Description

4.4 Security Information and Event Management(SIEM) Solution

My second task involved using an SIEM solution to collect and analyze logs from various sources like firewalls, servers and applications. The SIEM solution I have worked in during my internship period is basically a suite of cybersecurity tools and platforms developed by RSA Security. Due to confidentiality reasons, I can't disclose the name of the solution. It is designed for comprehensive threat detection, analysis as well as incident response capabilities for organizations. It uses state of the art advanced analytics and threat intelligence as well as a broad range of data sources to improve visibility and perform various security operations.

4.5 Key Features

4.5.1 Network Traffic Analysis (NTA)

In real-time, it can capture and analyze the network traffic in order to detect anomalies and threats.

4.5.2 Endpoint Detection and Response (EDR)

This feature is similar to Qualys. It can not only monitor endpoints for malwares or suspicious activities, but also offer digital forensics for investigating threats and incident response.

4.5.3 Log and Event Management

The solution can collect and analyze logs from sources like firewalls, servers as well as applications in real-time.

4.5.4 Threat Intelligence Integration

It has the capability to utilize global threat intelligence to detect and categorize threats using machine learning models and behavioral analytics.

4.5.5 Incident Response

It has tools in its arsenal to investigate and respond to anomalous activities effectively.

4.5.6 Cloud Security Monitoring

Similar to Qualys, it supports visibility into cloud environments like AWS, Azure, Google Cloud etc.

4.5.7 Scalability and Integration

It is designed such that it can be scaled to monitor small to large enterprises. It has the capability to integrate with other security tools which increases its power even more as an approach towards ensuring cybersecurity.

4.6 Collecting and Analyzing Logs from Threat Hunting Dashboard

My second task involved collecting and analyzing logs using the SIEM solution from the threat hunting dashboard. The threat hunting dashboard provides security analysts a comprehensive overview of potential threats and facilitates proactive investigation through a critical interface. There are several key components.

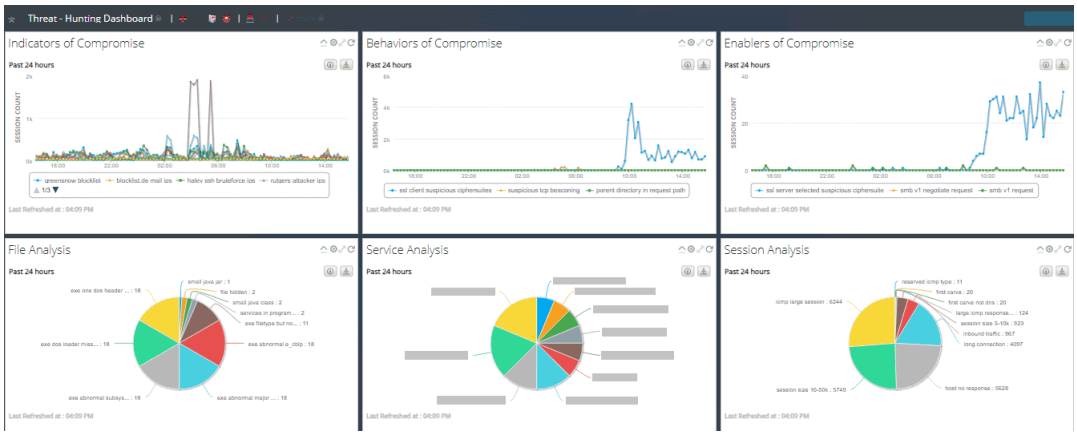


Figure 4.7: Threat Hunting Dashboard

4.6.1 Indicators of Compromise (IoCs)

IoCs show anomalous or malicious activity happened from the past 24 hours. These include malicious IPs, domains, URLs, File hashes incorporated with malware as well as email addresses that are being used in phishing attacks. The main purpose of IoC is to create solid evidence of breach or breach attempts. These are also categorized to validate their risk level using threat intelligence feeds.

4.6.2 Behaviors of Compromise (BoCs)

BoCs show abnormal behavioral patterns of anomalies of the past 24 hours that indicate a compromise. These include unusual login patterns at odd hours or from foreign IPs. The main purpose of BoC is focusing on behavioral analysis to detect threats that IoCs might overlook. It has the capability to detect hidden threats like insider threats or zero-day exploits.

4.6.3 Enablers of Compromise (EoCs)

EoCs show any form of misconfigurations or flaws in the system of the past 24 hours that attackers might leverage to perform exploitation. These include protocols that are unused or open ports, outdated software versions and weak or default credentials etc. The main purpose of EoC is to identify security gaps that need to be managed quickly to reduce the probability of attack by proactive hardening.

4.6.4 File Analysis

It is basically a comprehensive form of inspection of files that are on the network or endpoints. These include file names, sizes, extensions and hashes. The main purpose of file analysis is to identify malicious files that are entering the space. It also helps to understand how files react while executed.

4.6.5 Service Analysis

This analyzes activities across various network services including HTTP, DNS, FTP, SMTP etc. It can detect any form of abnormal spikes in these service usage. The

primary purpose of service analysis is to identify any form of misuse of services like DNS tunneling or spamming emails. It is achieved through monitoring communication patterns.

4.6.6 Session Analysis

It is basically the summary of session level activity including source and destination IPs, duration of a particular session and its data transfer rate, used protocols etc. The main purpose of session analysis is to detect anomalous activity at the session level. It is used to trace the flow of an attack.

4.7 Collecting and Analyzing Logs from McAfee Dashboard

My third task involved collecting and analyzing logs from McAfee dashboard using the SIEM solution. It provides a detailed view of ONE Bank PLC's security environment. There are several key components.

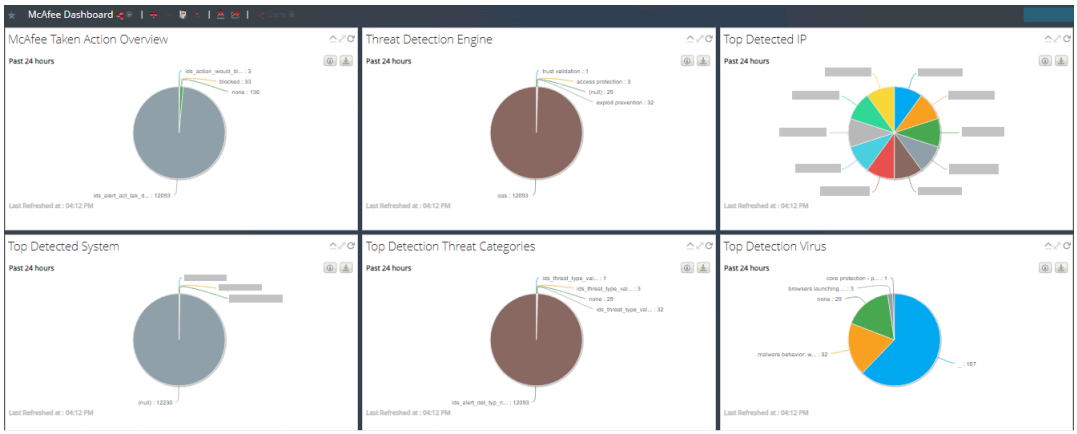


Figure 4.8: McAfee Dashboard

4.7.1 McAfee Taken Action Overview

It summarizes the actions McAfee has taken to alleviate the detected threats including files that have been quarantined to prevent further damage, malicious processes that have been terminated, network connections that have been blocked and finally the alerts that have been generated from the past 24 hours. The main purpose is to assess how McAfee is performing it's security operations in real time.

4.7.2 Threat Detection Engine

This gives me insight regarding the types of threat detection engines and their activity using scanning in real-time, behavioral analysis as well as heuristic analysis. The main purpose is to highlight which engine types are most effective. It also gives necessary information regarding the nature of threats.

4.7.3 Top Detected IPs

This data gives me the information regarding the list of IP addresses that are associated with the highest number of incidents or attack attempts. The purpose of it is to identify not only external but also internal IPs which are contributing to any form of security incidents. It helps me to focus on the critical areas and to take action accordingly.

4.7.4 Top Detected Systems

This highlights the systems around my environment with the most detections. These systems include endpoint devices like laptops, desktops, servers, virtual machines or containers. Compromised or risky systems are easily identified in this log.

4.7.5 Top Detection Threat Categories

It gives me information about threat categories like ransomware, phishing, trojans, adware or spyware etc. The main purpose it to provide insight regarding the threat types that are targeting my environment.

4.7.6 Top Detection Virus

Finally this log lists the specific malware or viruses which are frequently detected. The lists include the names of known threats and the number of instances detected for each form of virus.

4.8 Introduction to Penetration Testing

Penetration testing is basically a form of simulated cyberattack against an organization's systems to identify and exploit vulnerabilities. It is typically performed in a controlled environment in order to evaluate security measures and improve accordingly without harming any of the existing systems. As I have gained a lot of theoretical knowledge during my training phase regarding penetration testing, My co-supervisor K. M. Mohiuddin sir wanted to give me a small practical task which involves the reconnaissance and scanning phase of pentesting which helped me build my interest further in this field. Reconnaissance involves collecting information regarding my target and scanning involves identifying active hosts or open ports. I have performed both of the tasks using Zenmap. Zenmap is basically the official GUI for Nmap (Network Mapper). It is an open source tool used primarily for discovering networks and security audits. The interface is user friendly which makes it easier for utilizing all the Nmap's broad range of features including scanning networks, visualizing scan results as well as managing scan configurations.

4.9 Key Features of Zenmap

- Network Scanning
- Predefined Scan Profiles

- Topology Mapping
- Searchable Results
- Interactive Results
- Command-Line Integration
- Cross-Platform Support
- Comparison of Scan Results

4.10 Port Scanning Using Zenmap

My fourth task involved getting access to an endpoint device and finding its open ports that can be used for exploitation. I have run an intense scan on the target device's IP. After the scan, It gave me all the necessary information including port numbers, port status, services and version. I was advised not to proceed further as it can halt other processes and these types of exploitation shouldn't be performed without ensuring a controlled environment.

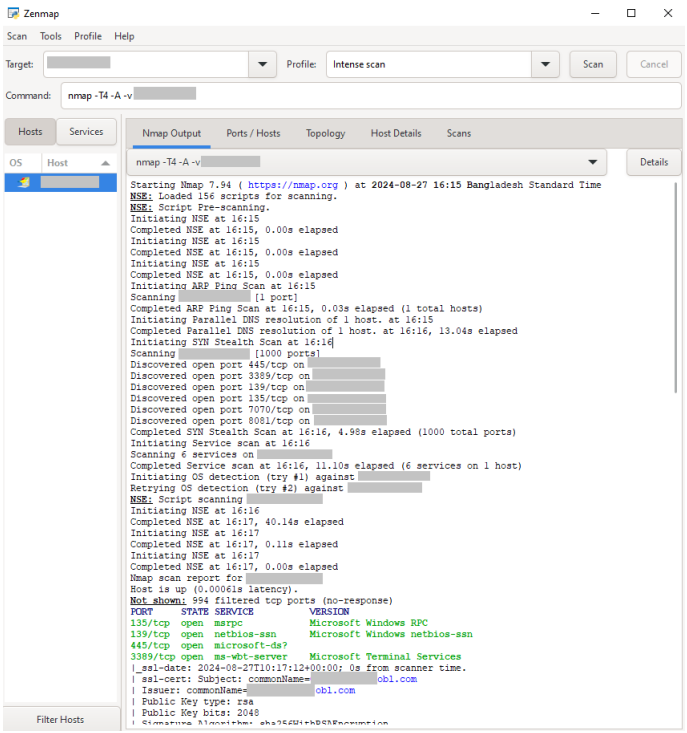


Figure 4.9: Port Scanning 1

As seen in the figure, I have found the open ports of my target IP which are 135, 139, 445, 3389. All the port status is open which can be further used for exploitation. Each of the ports have a particular service running.

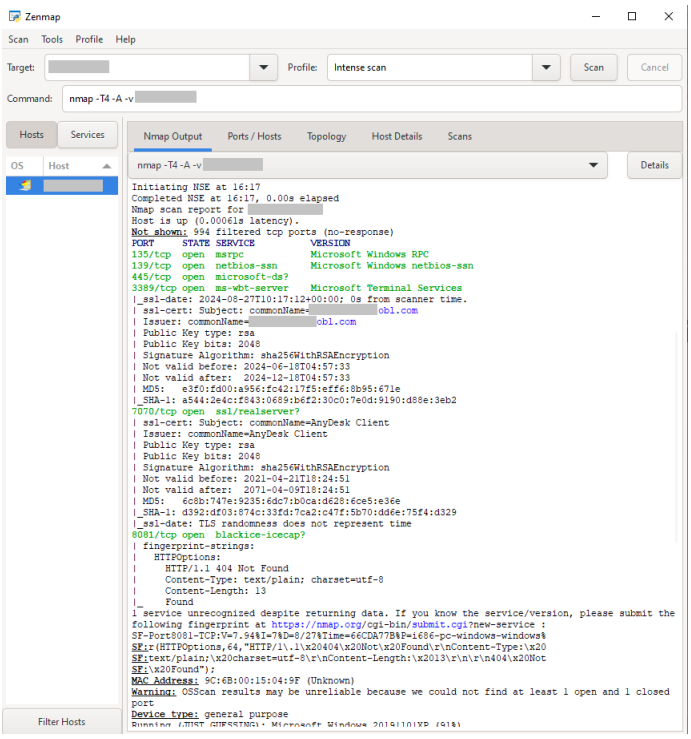


Figure 4.10: Port Scanning 2

4.11 OSINT (Open-Source Intelligence)

My final task was basically a theoretical one. I was instructed to gather as much information as possible regarding OSINT. Open-Source Intelligence is basically a process of gathering and analyzing information which is commonly found in various open sources to generate workable intelligence. It leverages publicly available information to derive actionable insights, often applied in national security and business contexts[2]. The common use cases of OSINT are cybersecurity, law enforcement, competitive intelligence etc.

4.11.1 Sources of OSINT

- Websites and Social Media : Public profiles, online forums like Reddit, social networking sites like Facebook.
- Search Engines : Google, Bing and advanced search operators like Google Dork.
- Public Records : Government databases, legal filings and financial disclosures.
- News Media : Online news articles, blog posts and press releases.
- Geo-spatial Information : Satellite imagery, maps like Google Maps or Google Earth
- Technical Sources : IP address lookup, DNS record etc.
- Dark Web : Information available via TOR networks or other anonymized sources.

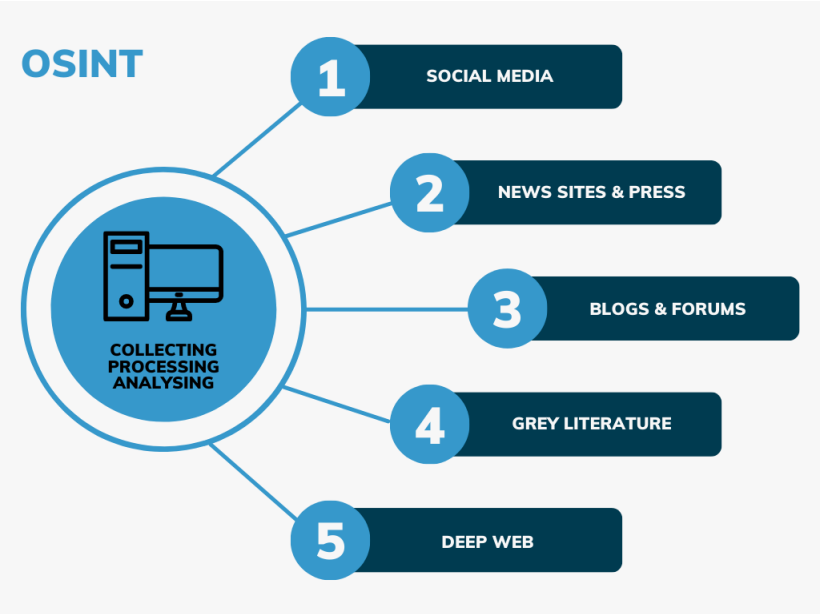


Figure 4.11: Sources of OSINT [5]

4.11.2 Tools Used in OSINT

There are various tools used for OSINT which are Google Dorks, Recon-ng etc. Google Dorks uses advanced forms of query techniques used for searching deep into the web. Recon-ng is basically a framework for initiating surveys through the web.

4.11.3 Advantages of OSINT

As all the information is publicly available on the web, it is a cost-effective strategy. Not only that, It has a larger scope which covers a broad range of data sources. It doesn't require any form of private information because it's legally compliant.

4.11.4 Challenges of OSINT

It is heavily dependent on filtering to extract meaningful data as huge volumes of information is available. Not only that, there is no guarantee of accuracy or authenticity because public data may become outdated, modified or misleading. The debate surrounding whether OSINT qualifies as "true intelligence" is discussed in depth, highlighting its strengths and limitations[1].

4.12 Challenges

During performing my assigned tasks I faced some challenges. Firstly, during the collection and analysis phase using the SIEM solution, I got to learn about all the complex dashboards. Understanding what each metric is doing and their relationship requires training and expertise which can be overwhelming for new analysts. Secondly, reports generated on Qualys are very detailed and take a lot of time to generate. Not only that, understanding the results section and utilizing all the features effectively was a little bit difficult as I am still new to this field. I needed to stay very careful about maintaining confidentiality. But my training and the kind support from the Information security team helped me complete these tasks at ease.

Chapter 5

Alternative Solutions and Comparative Analysis

During my internship, I got the opportunity to use Qualys as my primary vulnerability management and report generation tool as well as a particular SIEM solution for monitoring security systems in real-time. In this chapter, I will explore alternative solutions to these tools and compare them based on their pros and cons. The comparison will be regarding several key factors which include capability set, ease of use, pricing, third-party integrations, learning curve and finally popular companies that use it. The chapter will be divided into two parts. The first part will focus on the comparative analysis of two vulnerability management tools which are Qualys and Tenable. The second part will be based on the comparative analysis of two SIEM solutions which are NetWitness and Splunk. This analysis will determine which solution is more suitable for different types of enterprises.

5.1 Comparative Analysis on Vulnerability Management Tools: Qualys vs. Tenable

Qualys and Tenable are two of the superior vulnerability management solutions that are commonly used by enterprises to identify, assess, and mitigate security risks at ease. However, they have certain distinctive features that make each of them stand out. Both have pros and cons that make them appropriate for certain use cases.

5.1.1 Qualys: Pros and Cons

Pros:

- Qualys is a cloud-based solution and doesn't require on-premise deployment, saving total cost of ownership (TCO)
- It provides comprehensive scanning capabilities including vulnerability scanning of web applications, cloud environments as well as endpoint security
- It offers automated remediation feature for faster response time
- Qualys is capable of strong compliance audits for frameworks like ISO/IEC 27001:2013, PCI-DSS, HIPAA, GDPR etc.

- Qualys integrates with major cloud platforms like Microsoft Azure, Google Cloud and AWS to ensure visibility and security compliance [8]
- It offers flexible annual subscription plans starting from 295 US dollars for small enterprises all the way up to 1995 US dollars for larger enterprises [8]
- More than 60 percent of the Forbes Global 50 enterprises like Cisco, DuPont, Sabre, Microsoft, Sony Network Entertainment depend on Its continuous security solutions [8]
- Offers self-paced training courses with certifications

Cons:

- susceptible to man-in-the-middle attacks
- As Qualys doesn't use domain registry protection, it is vulnerable to domain hijacking
- The user interface has a steep learning curve which requires proper training for effective usage
- Though the pricing is flexible, it is a modular form of pricing structure where additional features increase TCO
- Certain vulnerability detections may be a false positive and require manual verification
- As it is a cloud-based platform, it has limited offline scanning capabilities

5.1.2 Tenable: Pros and Cons

Pros:

- Tenable offers a diverse array of scanning capabilities including agent-based, agent-less and passive scanning options to choose from
- It has a feature called Vulnerability Priority Rating (VPR) which effectively ranks vulnerabilities based on real-world exploit-ability, reducing the need for redundant remediation efforts
- Provides a large asset coverage. It has the capability to scan IT, OT as well as cloud environments
- Tenable's GUI is the best in the industry. It uses HTML5 interface with user-friendly elements of navigation which significantly increases the product's ease of use [8]
- It has the capability to integrate with SIEM solutions, ITSM and cloud-native security tools
- Tenable customers have free 24/7 online access to Tenable University which provides self-serve courses on Tenable's entire product lineup [8]

- It has approximately one million users and more than 20,000 enterprise customers throughout the world including the U.S. Department of Defence, Visa, BMW, Adidas and Microsoft [8]
- No risk of domain hijacking like Qualys

Cons:

- Tenable.sc can cost up to 20,000 US dollars excluding annual maintenance fees. It can be a hefty investment for organizations with a tight budget [8]
- Though the GUI is easy, it requires expertise to configure and utilize properly
- It is also vulnerable to man-in-the-middle attacks
- It is limited in compliance related features which makes it less ideal for regulatory-driven industries

5.1.3 Suitability (Qualys vs. Tenable)

After the analysis, It is apparent that Qualys is an ideal solution for cloud-based and regulatory-driven enterprises which require automated remediation workflows for faster response.

On the other hand, Tenable is the perfect solution for organizations that require risk-based vulnerability prioritization, broader coverage of assets as well as options regarding on-premise or hybrid deployment.

5.2 Comparative Analysis on SIEM Solutions: NetWitness vs. Splunk

Security Information and Event Management (SIEM) solutions are vital for real-time threat detection, log management, and incident response. Though NetWitness and Splunk serve identical purposes, they have some distinct features which are ideal for different types of organizations according to the requirements.

5.2.1 NetWitness: Pros and Cons

Pros:

- It offers security monitoring in a proactive manner by using a method called behavioral analytics as well as machine learning
- It provides deeper visibility through its NTA features which collect and analyze raw network packets
- The security alerts provided by NetWitness are based on real-world threat feeds
- It offers detailed data view through dashboards to security analysts which can be further customized according to preference

- NetWitness provides automated incident response capabilities

Cons:

- The logs are very detailed and it requires expertise in threat hunting and forensic analysis to analyze and take action accordingly
- As it processes data in real-time, it demands high computational power
- Licensing is very expensive which can be difficult for SMEs to maintain
- Compared to Splunk, the user base is limited

5.2.2 Splunk: Pros and Cons

Pros:

- Splunk provides massive log data ingestion capabilities which is suitable for large enterprises
- The interface is user-friendly compared to NetWitness. It offers intuitive search along with visualization tools
- It detects anomaly and responds automatically using advanced analytics
- Splunk has better third-party integration. It can also integrate with cloud services
- It has a very large community with a strong support network and proper documentation

Cons:

- The pricing is dependent on data volume. It can be costly for deployments to a large extent
- It doesn't support NTA features or packet capture capabilities like NetWitness
- Though it is user-friendly at the basic level, it needs expertise for deeper customization

5.2.3 Suitability (NetWitness vs. Splunk)

After the analysis, it is evident that NetWitness is ideal for enterprises which require digital forensic capabilities, network traffic analysis as well as advanced threat hunting.

On the other hand, Splunk is suitable for large enterprises requiring analytics based on machine learning and AI, scalability, log management in real-time, diverse array of third-party integrations as well as a supportive community forum.

However, the selection between these solutions are dependent on factors like the size, budget, security maturity, use cases of an organization.

Chapter 6

Conclusion

During the six months of my internship, I have developed both theoretical as well as practical knowledge in Information Security. I tried to document every experience precisely. I have learned that security breaches can happen from people inside the organization. Before performing any tests, my team constantly reminded me of the best security practices along with maintaining the code of conduct for confidentiality purposes.

I have been exposed to simple scenarios in the first part of my internship which helped me build my foundation in information security. This later prepared me for more complex and real-world scenarios which include vulnerability scan and report generation with Qualys, port scanning using Zenmap as well as detect, investigate and respond to security incidents by analyzing logs using SIEM solution.

I have started this internship on the 2nd of June, 2024. It is a six month long contract and it has ended on the 11th of December, 2024. Overall, the journey was both fun and challenging. I will always be grateful towards my team because they always motivated me to gather as much knowledge as possible and made cybersecurity an interesting field to me. I never thought I would choose this field as my specialization before this.

Bibliography

[1] A. S. Hulnick, "The dilemma of open sources intelligence: Is osint really intelligence?," 2010.

[2] N. A. Hassan and R. Hijazi, *Open source intelligence methods and tools*. Springer, 2018.

[3] CyberOne, *What is the cia triad?* URL : https://cyberone.security/what-is-the-cia-triad/, Feb. 2019.

[4] Joe Hopler, *It cyber hygiene: Why it's important, and duo's role in securing everyday access*, URL : https://duo.com/blog/it-cyber-hygiene-why-its-important-duo-role-securing-access, Dec. 2022.

[5] DLR Projektträger, *New osint report highlights security gaps in academic institutions*, URL : https://www.safeguarding-science.eu/news/new-osint-report-highlights-security-gaps-in-academic-institutions/, Nov. 2023.

[6] GeeksforGeeks, *7 layers of it security*, URL : https://www.geeksforgeeks.org/7-layers-of-it-security/, Mar. 2023.

[7] Gowsika, *Iso 27001 controls: A guide to implementing annex a controls*, URL : https://sprinto.com/blog/iso-27001-controls/, Sep. 2024.

[8] UpGuard, *Tenable vs. qualys*, URL : https://www.upguard.com/blog/tenable-vs-qualys/, Jan. 2025.