Appendix A

MSc Cyber Security Engineering

DETECTION OF MALICIOUS ACTIVITIES IN BANKS AND THEIR PREVENTION BY UTILIZATION OF FRAMEWORK PRACTICES AND SECURITY POLICIES

OLUWASEUN DAYO OYENIGBEHIN

SOUTHAMPTON SOLENT UNIVERSITY

SCHOOL OF MEDIA ART AND TECHNOLOGY

SEPTEMBER 2022

Appendix B

SOUTHAMPTON SOLENT UNIVERSITY
SCHOOL OF MEDIA ART AND TECHNOLOGY
DECEMBER 2022

MSc Cyber Security Engineering

Academic Year 2021-2022

Q15731570

OLUWASEUN DAYO OYENIGBEHIN

Detection of Malicious Activities in Banks and their Prevention by Utilization of Framework Practices and Security Policies

Supervisor: Kalin Penev September 2022

This report is submitted in fulfillment of the requirement of Southampton Solent University for the degree of MSc Cyber Security Engineering

Acknowledgment

Firstly, I would like to acknowledge my supervisor Kalin Penev (Associate Prof) who made this research work possible. His guidance and advice allowed me to complete my project by passing through all the stages in sequential manner. I would also like to thank my other supervisor Femi Isiaq who gave guidance in all the stages and proved supportive during research phase.

This dissertation could not get into successful phase without having a support from my parents for which I am extremely thankful for their support and being compassionate with me throughout this whole tenure of the research work. Their wishes have encouraged me to put best of my efforts in the research work.

I am thankful to university staff at the library for their assistance with resources which has really helped me in the completion of this dissertation.

I also want to thank all my lecturers who have guided me about essential knowledge of dissertation work and how the research must be executed in different phases. Without their initial guidance, it would be a difficult task to complete this work in that defined duration

Abstract

The banking sector has progressed from more than a decade for increased consumer interest towards utilization of transaction services through ATM machines, pay orders, demand drafts, cheques and online transactions. Most of the transactions and data access has been made possible by utilization of internet services, applications and computing technology. However, the cyber-attacks have been increased at the same time using different techniques and methods due to which the identities and financial assets of the consumers have not remained safe. Different countries have developed policies and frameworks to ensure the safety of the assets which is beneficial for the government, organizations and people. Since the private sector sometimes do not give careful attention to the system's security, they have to face cyberattacks. The focus of the research is to carryout vulnerability testing for which the website has been formed, and the traffic has been analyzed. The Wireshark software has been utilized to detect different types of vulnerabilities. The results show that the tool has been able to detect different types of vulnerabilities up to 100%, except PING which is 50%, and XSS as well as SQL Inject which are less than 50%. After the security audit, the organizational framework has been suggested which involves three different layers of, securing the assets and their categorization, detecting the threats at different levels, and categorization of the attacks for which exploitation, detection, and control measures are to be taken. In addition to that, the networking framework has been suggested for the cyber expert to monitor, update and control the user activities to save the network from malicious activities. The implementation of both the networks will reduce the cyberattacks and save the banking network from any vulnerabilities

***Keywords**: Cybersecurity, Penetration testing, Wire Shark, Networking policies*

List of Figures

Pilot Project

1.1 Introduction

The banking sector is considered to be the backbone of the economy. The daily-based transactions are carried out in different forms such as demand drafts, cash payments, and cheque payment methods. The modernized banking system has moved from conventional payment methods to online-based technological systems which make utilization of credit cards or debit cards or online payment methods (ICICI Bank, n.d.). The technological developments have provided the benefits of mobility and quickness to both consumers, financial institutions, and banks but at the same time but deserted in the evolution of other risks (Elsinger, et al., 2006). The electronic banking system offers different activities associated with banking which involve the utilization of computer technology and the information technology (IT) sector, thus minimizing the physical interaction among the customers and banking personnel. E-banking making utilization of electronic sources is also referred to as virtual banking, cyberbanking, and home banking. It includes the usage of Automated Teller Machines (ATMs), Real-Time Gross Settlement System (RGST), Internet Banking, Mobile Banking, Smart Cards, and other types of cards (Dr. Umamaheswari K., 2021).

Different types of cyber-attacks have been faced by organizations among which the banking sector is the most prominent one because of having assets of the consumers. Among those cyber-crimes, the prominent ones are hacking, credit card fraud, and keylogging. Whereas, different types of viruses, spyware, water hole, malware-based attacks, and DNS cache positioning are mostly observed (Damico, 2009).

The focus of this pilot project is to observe the networking policies that have been developed by different countries to deal with cyber-attacks in the banking sector. The below sections cover different stakeholders and regulatory policies

1.1.1 Financial Sector and E-Commerce

The stakeholders which are involved in Taxonomy include banking sector authorities, service providers, and professional associates

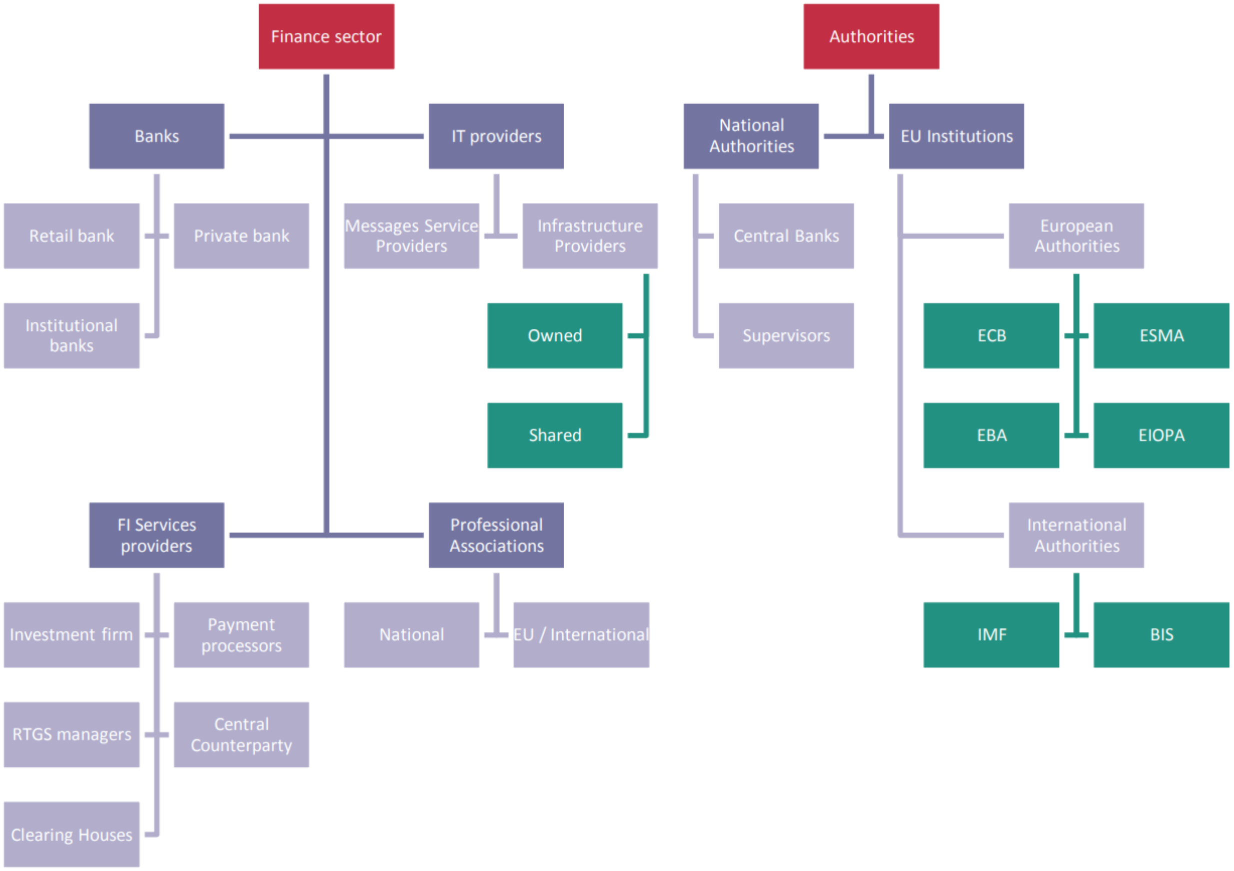


Figure 1.1 Stakeholders involved in the Financial sector (Dupré L., et al., 2014)

The communication flows in the financial sector take place in such a way that the central banks, financial markets, lenders or savers, and borrowers are spenders communicate to retail banks to having

- Safety of financial assets and their storage
- Capabilities of moving the financial assets through transactions
- Provision of accessing the financial instruments related to trades, payments, securities, and funds

The network and information security (NIS) drivers in the financial sector contain three different layers which are governed by IT security (Dupré L., et al., 2014). These three key drivers are

1. External oversight that describes standards as well as regulations having an impact on information security and networks
2. Internal governance has a description of strategic alignment for dealing with business objectives which mainly rely on the architecture of NIS For supporting the business model
3. Operations of NIS have a description of activities being carried out for allowing the actual security to carry out its daily based operations

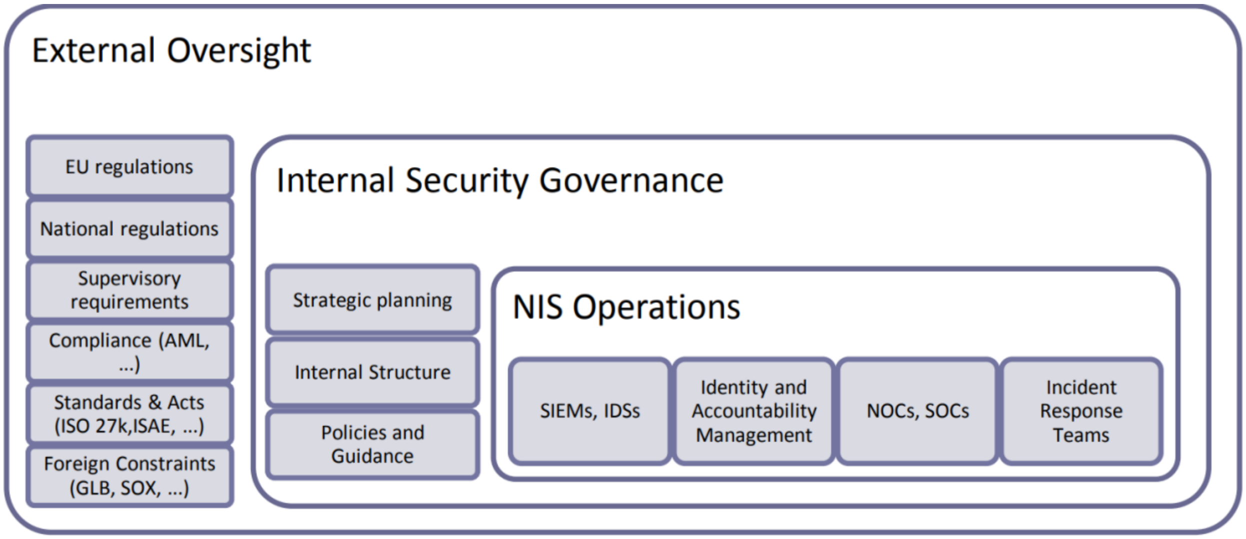


Figure 1.2 Key drivers of NIS (Dupré L., et al., 2014)

The international standards which have been followed by different countries have been formed by the member states for addressing their needs such as

1. Minimum requirements for risk management by the German Federal Financial Supervisory Authority.

   The German Federal Financial Supervisory Authority gives the provision the framework for dealing with different risks and managing them in an efficient way in their financial institutions. The basis of such a framework is EU Directive 2004/39/EC. The framework provides the basis of management responsibilities, requirements for dealing with managing different risks as well as resources associated with technical facilities, personnel, and system, and the development of procedures and plans for dealing with contingencies.
2. Swiss National Bank: The Bank Act 3/2004

The banking act has been found by the Swiss National Bank which clearly focuses on the settlement and observance of different financial instruments

3. European Regulations

   The European regulations have been developed to deal with different aspects such as

   - General Data Protection Regulation – COM (2012) 11 Final
   - Assurance of high level of networking and information security across the union COM (2013) 48Final
   - European Court of Auditors – Financial and Compliance Audit Manual
   - Market on financial instruments – Directive 2004/39/EC
   - Processing of personal data and protecting the privacy associated with electronic communication sector – Directive 2002/58/EC
   - Pursuing and acquirement of business related to credit institutions – Directive 2004/39/EC

1.1.2 Case Study

The electronic banking separate passes through different types of attacks among which the phish or bait is one of the main attack category being employed by the attacker (Ghazi-Tehrani et al., 2021). The phishing attacks are basically carried out by the attacker by the usage of either is spam e-mail or fake web pages. therefore, different methods have been utilized among which one method being employed by (Zhang Y. et al., 2007) was based on development of CATINA model for the detection of HTML and URL having specific type of keywords. Similarly, the forensic study has been carried out by (Bilim A. et al., 2021) for which Commission was made for attacking strategy of the attacker after which their forensic analysis involved preparation of E-banking website to analyze phishing attacks. Therefore, the material that is to be involved contains data set that contained the simple of the problem. after having the data set, that e-mail assist was performed using Wireshark 3.4.3 and HTTrack Website Copier 3.49.2. The case study involved or incorporation of cyber fraudsters that were focused on providing the information to the customer through the website. The HTTrack Website Copier 3.49.2 help in targeting the website for downloading purposes and this suspected content was analyzed. The result was identification of IP address of the attacker and detection of that IP number for reaching the address of the attacker under the procedure of forensic investigations. This case study has been analyzed since the research will be dependent upon using Wireshark tool. Therefore, different tools have been analyzed in the below section after which the research project will be proceeded on using Wireshark tool

1.1.3 Cyber Security Acts – United Kingdom

The countries after the development of standards have also worked on the accountability and regulations related to cyber security and cybercrimes. When it comes to cybersecurity issues, the developed countries have improved economic conditions and technological usage enforce and implement the regulations (World Bank, 2019). The details of the UK having different rules and regulations are provided below

1.1.3.1 UK National Cyber Security Strategy 2016-2021

UK Financial Conduct Authority has commenced the consultation of the certification regime and senior managers for the development of the policy under the individual accountability regime (Cyber Security Organization, n.d.). For the banking sector, UK Competition and Markets Authority have standardized the banking products including ATMs and branches that will have to coincide with EU Payment System directive 2. Moreover, the country has defined a national cybersecurity strategy for 2016-2021 (HM Government, 2016) the goals of which are to:

1. Defend The evolution of cyber threats for ensuring the protection and resiliency of networks systems and data of the UK. the public sector, citizens, and other organizations have to develop resiliency and utilize protection platforms and tools to defend themselves,
2. Deter: Since UK it's one of the hard targets of the cyberattacks, the strategy will be focusing on understanding, investigation, and disruption of or style actions that will be taken against public, private sector and organizations of the country. in regard to that, the country will have ability of taking the actions against the cyber attackers
3. Develop: The country has to develop cyber security industry along with focus on innovations and growth by underpinning the leading research and development in the field of science and technology.

1.1.3.2 UK CBEST – Intelligence led Vulnerability Testing 2.0

The Sector Cyber Team of Bank of England (BoE) published the second version of CBEST that involved different service providers and participants. The policies developed by the organization focused on coordination with the Council of Registered Ethical Security Testers (CREST). The consideration of the testing was ensuring the inclusion of BoEs' Sector Cyber Team provides the assessment of the firm's capability of getting surrounded by cyberthreat and dealing it with intelligence, detection of intrusion, and providing the incident response. Therefore, the main key components included (Paul Williams, 2021)

1. Implementation Guide for an explanation of different activities, phases, and deliverables associated with the assessment of CBEST
2. Service Assessment Guide for providing the information uh related to assessment criteria and allowing the participants to assess different threats and make usage of penetrating testing services provided by CREST
3. To make an understanding of operations associated with cyber threat intelligence which provides different standards for producing and consuming the threat intelligence for the execution of vulnerability tests in compliance with the CBEST program

1.1.3.3 UK Government Cyber Security Regulation and Incentives Review

The country has defined Cyber Security Regulation and Incentive Reviews in 2016 for the protection of £1.9 billion for the UK president in cyberspace for the Department of Digital, Culture, Media, and Sport (DCMS). The review has been made for the development of additional incentives and regulations for boosting the management associated with cyber risk across a large scale. The amendments have been made by the development of a yearly based incentive review to tell the latest version of the policy paper has been published in 2022. Now, the government has intervened across four different policy areas which are foundations, market incentives, capabilities, and accountability. The foundation's section gives guidance, information, and standards along with inclusion of campaigns. the capabilities deal with the skill development, market incentives deal with economic and consumer drivers, and that is section deals with accountability and regulation (GOV.UK, 2022)

Therefore, the country will be focused on meeting and overcoming the challenges and threats associated with cyber security in the banking sector

1.2 Networking and Security Tools

In the cyber security, the software has been categorized as network security monitoring tools, encryption tools, antivirus software, network defense wireless tools, web vulnerability scanning tools, PKI services, managed detection services and penetration testing. The cyber resilience is necessary for stopping every threat while working at the same time for the minimization of impact of successful cyber-attack. The cyber security tools allow to carry out e-mail communications and business transactions without any disruption. Different tools available in the market are Intruder, Syxsense, Perimeter 81, LifeLock, System Mechanic Ultimate Defense, Wireshark, Webroot, BluVector and so on (Software Testing, 2022). The discussion about all these tools have been provided in sub-sections below

1.2.1 Wire Shark

Wireshark is one of the widely utilized network protocol have any capability of analyzing the activities of network at microscopic level and is considered as a standard across different government organizations, small and medium enterprises, and educational institutions. The project for the security purposes was initiated in 1998 by Gerald Combs. The features of the tool (Wireshark, n.d.) include

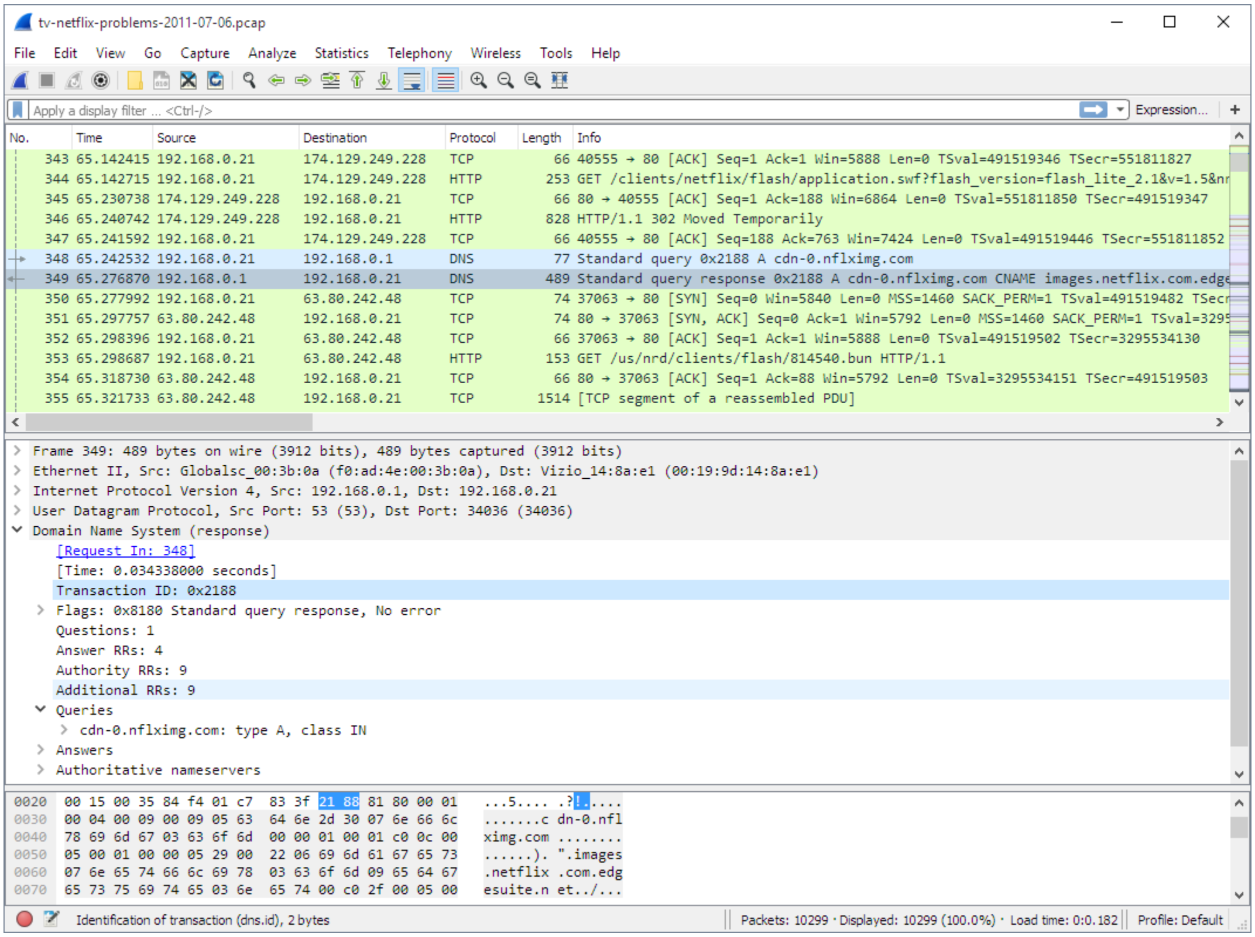
- Deep inspections of thousands of protocols
- Offline analysis and life capture
- Standard browser
- Operating capability on different platforms including Linux, Mac OS, Windows and several other platforms
- Capability of providing visualized form of network activities using graphic user interface (GUI)
- Richness of voice over internet protocol analysis
- Capturing capability of compressed files

- reading capability of live data from different resources such as IEEE 802.11, ATM, Token Ring, Ethernet, Bluetooth, FDDI, and USB which varies depending upon the platform that is being utilized
- Capability of exporting the output in terms of CSV, XML, and plaintext
- Support to the protocols by decryption which may include WPA/WPA2, Kerberos, IPSec and SSL/TLS

The company has managed to to get different awards which include McAfee SiteAdvisor, ACM Software System Award and PC Magazine – Editor’s Choice

Figure 1.3 Logo of Wireshark (Wireshark, n.d.)

The random programming image of the WireShark is provided in figure below


tv-netflix-problems-2011-07-06.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...

```
No.   Time      Source          Destination     Protocol Length Info
  343 65.142415 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519346 TSecr=551811827
  344 65.142715 192.168.0.21    174.129.249.228 HTTP      253 GET /clients/netflix/flash/application.swf?flash_version=flash_lite_2.1&v=1.5&nr
  345 65.230738 174.129.249.228 192.168.0.21    TCP        66 80 → 40555 [ACK] Seq=1 Ack=188 Win=6864 Len=0 TSval=551811850 TSecr=491519347
  346 65.240742 174.129.249.228 192.168.0.21    HTTP      828 HTTP/1.1 302 Moved Temporarily
  347 65.241592 192.168.0.21    174.129.249.228 TCP        66 40555 → 80 [ACK] Seq=188 Ack=763 Win=7424 Len=0 TSval=491519446 TSecr=551811852
  348 65.242532 192.168.0.21    192.168.0.1     DNS        77 Standard query 0x2188 A cdn-0.nflximg.com
  349 65.276870 192.168.0.1     192.168.0.21    DNS       489 Standard query response 0x2188 A cdn-0.nflximg.com CNAME images.netflix.com.edge
  350 65.277992 192.168.0.21    63.80.242.48    TCP        74 37063 → 80 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=491519482 TSecr
  351 65.297757 63.80.242.48    192.168.0.21    TCP        74 80 → 37063 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SACK_PERM=1 TSval=3295
  352 65.298396 192.168.0.21    63.80.242.48    TCP        66 37063 → 80 [ACK] Seq=1 Ack=1 Win=5888 Len=0 TSval=491519502 TSecr=3295534130
  353 65.298687 192.168.0.21    63.80.242.48    HTTP      153 GET /us/nrd/clients/flash/814540.bun HTTP/1.1
  354 65.318730 63.80.242.48    192.168.0.21    TCP        66 80 → 37063 [ACK] Seq=1 Ack=88 Win=5792 Len=0 TSval=3295534151 TSecr=491519503
  355 65.321733 63.80.242.48    192.168.0.21    TCP      1514 [TCP segment of a reassembled PDU]
```

```
> Frame 349: 489 bytes on wire (3912 bits), 489 bytes captured (3912 bits)
> Ethernet II, Src: Globalsc_00:3b:0a (f0:ad:4e:00:3b:0a), Dst: Vizio_14:8a:e1 (00:19:9d:14:8a:e1)
> Internet Protocol Version 4, Src: 192.168.0.1, Dst: 192.168.0.21
> User Datagram Protocol, Src Port: 53 (53), Dst Port: 34036 (34036)
v Domain Name System (response)
    [Request In: 348]
    [Time: 0.034338000 seconds]
    Transaction ID: 0x2188
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 4
    Authority RRs: 9
    Additional RRs: 9
  v Queries
    > cdn-0.nflximg.com: type A, class IN
  > Answers
  > Authoritative nameservers
```

```
0020  00 15 00 35 84 f4 01 c7  83 3f 21 88 81 80 00 01   ...5.... .?!.....
0030  00 04 00 09 00 09 05 63  64 6e 2d 30 07 6e 66 6c   .......c dn-0.nfl
0040  78 69 6d 67 03 63 6f 6d  00 00 01 00 01 c0 0c 00   ximg.com ........
0050  05 00 01 00 00 05 29 00  22 06 69 6d 61 67 65 73   ......). ".images
0060  07 6e 65 74 66 6c 69 78  03 63 6f 6d 09 65 64 67   .netflix .com.edg
0070  65 73 75 69 74 65 03 6e  65 74 00 c0 2f 00 05 00   esuite.n et../...
```

Identification of transaction (dns.id), 2 bytes

Packets: 10299 · Displayed: 10299 (100.0%) · Load time: 0:0.182 | Profile: Default

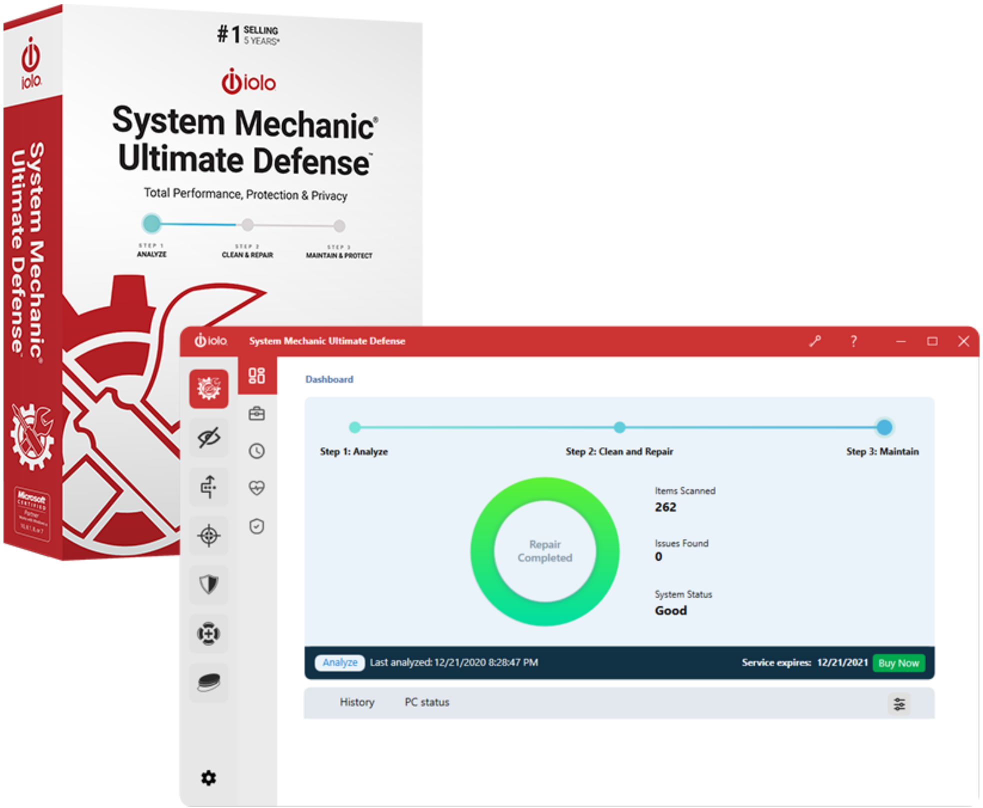
Figure 1.4 Wire Shark illustration

1.2.2 System Mechanic Ultimate Defense

The System Mechanic Ultimate Defense is based on boosting up total performance of the system and providing the privacy and protection to the user (IOLO, n.d.). Six major functions being performed by the tool are

- Optimization: speeding up of broadband speed, processor speed, memory and hard drives
- Antivirus and malware removal: provision of antivirus capabilities for blockage and removal of newest malwares
- Password management: protection of password and secure usage of credit cards through online platforms
- Cleaning: removal of junk files that slows the computer through PC cleaner
- File recovery: recovery of deleted or lost files through data recovery software
- Privacy protection: shielding of browsing habits and data collection

The preference is given to System Mechanic Ultimate Defense because of its capability of using it personal computers located in homes or organizations, free product support by the company, 30-day money back guarantee, operational capabilities on different versions of Microsoft Windows, and adaptation and reparation of more than 80 million personal computers,



Items Scanned 262

Issues Found 0

System Status Good

Last analyzed: 12/21/2020 8:28:47 PM

Service expires: 12/21/2021

Figure 1.5 System Mechanic Ultimate Defense (IOLO, n.d.)

1.2.3 Intruder

Like other software, Intruder is focused on online will not ability scanning file finding the weaknesses associated with cyber security in their digital infrastructure of the user for our dance of costly breaches of data (Intruder Systems Ltd., 2022). The tool allows

- Scanning of public and private accessible websites, server, end point devices and cloud systems by the utilization of scanning engines
- Finding the vulnerabilities associated with application box, missing patches, weaknesses in encryption, and SQL injection
- Automatic detection of new threats and security of working environment

- Receiving an interpretation of raw data from scanning engines and its conversion into intelligent results
- Generation of security reports providing security ordered send improvement of cyber hygiene
- Extended security and protection services resulting in the reduction of detection time and its fixing

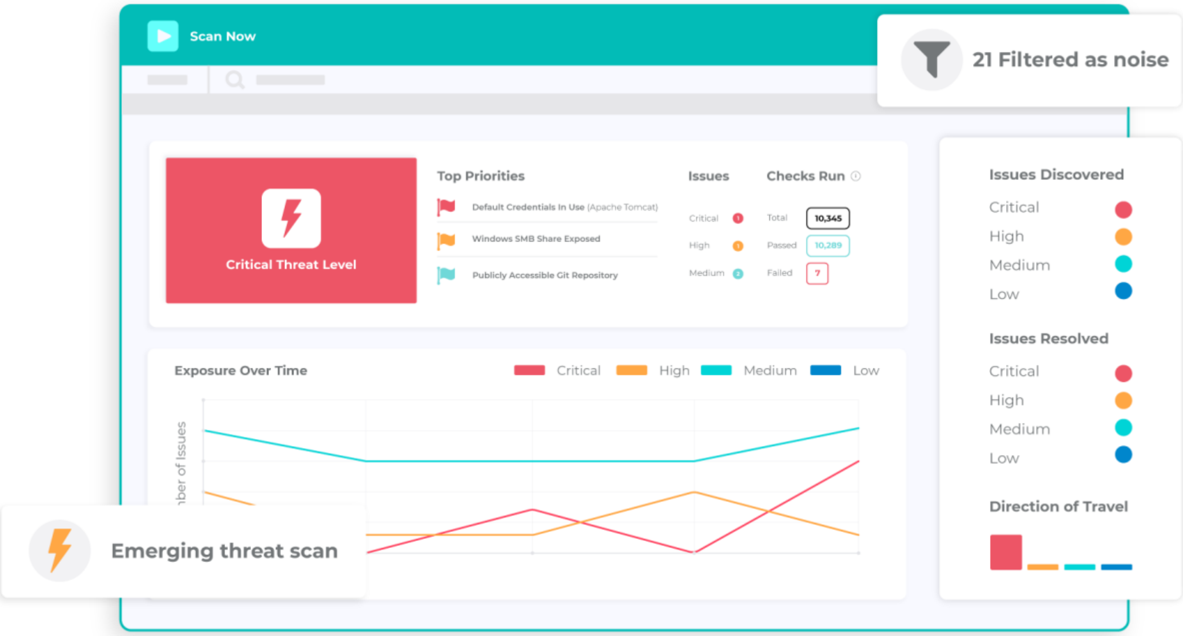


Figure 1.6 Intruder. Io operational illustration (Intruder Systems Ltd., 2022)

1.2.4 Perimeter 81

Perimeter 81 is one of the cyber security detection tools which is used in the field of cybersecurity. the four main services included are Remote Access VPN, Cloud Based VPN Access Network Traffic Control and VPN for Business. The tool had been developed by SaaS experts Sagi Gidali and Amit Bareket and 2018. The inspiration for the development of the tool had come from observance of continuous struggle in the business sector for securing the network architectures and cloud-based storage system. Therefore, the companies were provided by Perimeter 81 to carry out management of their network and acquire security services from just one tool. the company owns more than 2500 customers and is valuation of $1 billion. The main core values driving the company are innovation, transparency, collaboration, accountability, equality, and enjoyment (Perimeter 81, 2018).

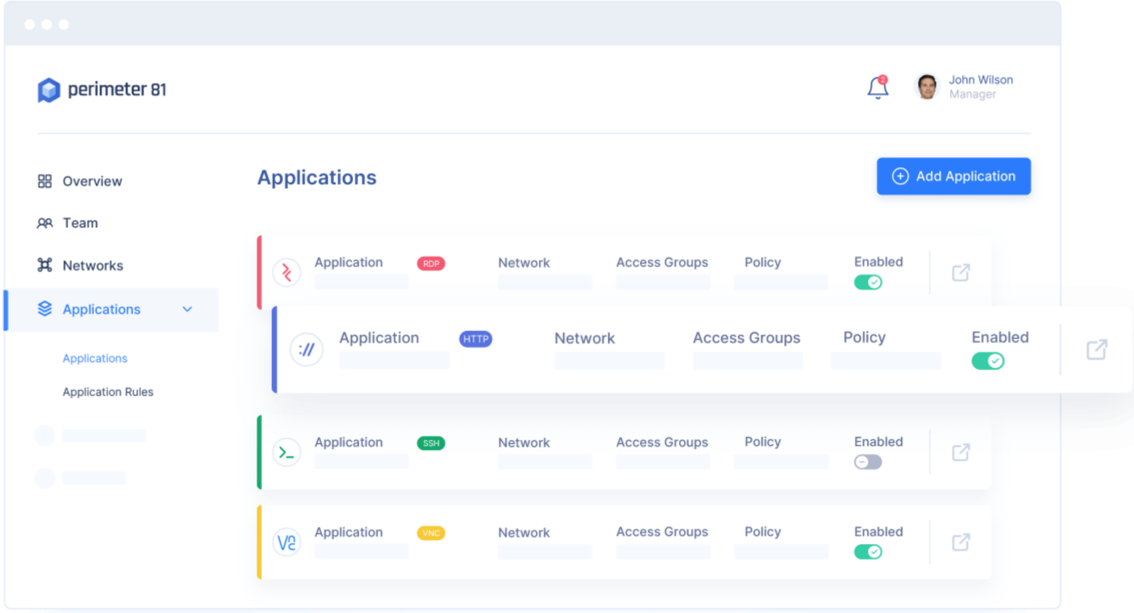


Figure 1.7 Perimeter 81 application panel (Perimeter 81, 2018)

1.2.5 LifeLock by Norton

The Norton company has contributed significantly to the field of security and protection against viruses, malware, and identity theft. Now, the company has been providing LifeLock tool. the key features of LifeLock tool are

- Providing alerts and monitor their activities
- Restoration of identity
- Protection of member

Figure 1.8 LifeLock by Norton (Norton, 2022)

The tool allows easy access by just signing up for LifeLock after which the computer is scanned, and the alert is provided through mobile application, e-mail, and text. The tool resolves the identity theft issue by indulging the restoration specialist and the funds are reimbursed that may be stolen because of identity theft. The company provide coverage of $1,000,000 for experts and lawyers (Norton, 2022).

1.3 Summary

The pilot project focused on providing the literature review about important aspects of banking sector and cybersecurity. It was observed that to ensure the credibility, availability and integrity of the bank, the safety of the assets of the customers has to be ensured. Therefore, it is a duty of an organization or banking sector to provide network and information security by following the rules and regulations at external level, but development of security governance at internal level, and by implementing the security audit on a regular basis. For this purpose, different standards have been studied which includes European directives, Swiss National Bank Act, and European Regulations. Also, the case study has been taken into account for analyzing the phishing attacks that are obtained from the spam emails and other resources. In addition to that, the cyber security acts of United Kingdom have been studied which involves UK National Cybersecurity Strategy 2016-2021, UK CBEST in coordination with Council of Registered Ethical Security Testers, and UK Government Cybersecurity Regulations and Incentives Reviews. The networking and security rules have been reviewed to understand their functionalities and features while focusing on the fact that the research will be involving analysis of the banking website under different types of attacks. So, Wireshark is going to be utilized in final dissertation

Final Research Project

(This page has been left Intentionally)

Chapter 1 – Introduction

1.1 Introduction

The concept of online banking had been introduced by financial institutions in 1980s. The online banking giant momentum in 1990s, and Stanford Federal Credit Union was the first bank in America that offered online banking to all the customers. After the technological innovation got cheap and access of internet got available to everyone, the popularity of online banking was increased by more than 80% in 2000s (Mishra R., et al., August, 2020).

The cyber-attacks usually fall into the wider category of electronic warfare, security breach, hijacking of human decisions and procedures of national institutions. When it comes to cyber threat, the case further moves to unauthorized access, disclosure, destruction of private data, disruption of service delivery and disclosure of information which will impact the missions, activities, and personal information of an individual and national security at high levels. It is based on four main steps which are identification of target, collection of data offer target, performance of cyber-attack and investigation (Li Y., et al., 2021).

The variation in the type of cyberattack greatly depends upon the development and adaption of computing technologies along with communication systems. The cyber cohesion results in the increment of such acceleration since it has been observed that the variation results in creation of new types of vulnerabilities and responses. The cyber attackers find new methods and modes to deal with latest technological advancements and security systems (Varga et al., 2021). The distribution of cyber assets can be observed in different banking sectors, industrial sectors, and organizations since the transaction of money and information is required related to the consumer. Till now, the banking sectors and other organizations have not assigned cyberspace is to the individuals or organizational groups having high degree of confidence to deal with different threats at internal level, national level, and global level (Al-Ghamdi M., 2021).

The classification and description of different types of threats is essential in data security provision. the classification helps in implementing effective protection against the threats (Hassani H. et al., 2019). So, the mandatory factor is defining and classifying the threats associated with them challenges in dealing with them and formulation of the systems for measurement and management purposes based on the threat type (Shulha O. et al., 2022). Therefore, different protection levels are

a. Physical and organizational protection of data containing information resources by the implementation of different management tactics
b. Hardware and software protection that is concerned with identifying and authenticating the access to the control of user involving auditing, shielding, and logging of security having high privacy assurance
c. Policy implementation for protecting the data by using modernized equipment and IT technology based on different standards and protocols.
d. Procedural protection by taking different measures subjected to management of personnel, protection of digital and physical assets, maintaining the working capacity in response to security breaches end development of plans to restore work
e. Integrated methodologies using different multi-level technologies at organizational levels that involve highly intelligent algorithms and automation tools

1.2 Problem Definition

Security of the network is the main issue for sustainable and reliable operations of the banking system. The loss or breaching of data results in a reduction of customer trust and business loss for the banking system (Sharma, 2012). The banking system still lacks the operational practices defined by some policies, rules, and regulations. At the same time, the requirement of continuous monitoring of the network is not focused which allows the attackers to hack the whole network

1.3 Research Objectives

The objective of this research is to design the policies and implement the practice to ensure the security of the data of a consumer of the banker and at the same time the data of the bank itself. The project will implement operational practices in different private and government organizations for which the important aspects of detecting the attacks and malicious activities will be carried out. The total sum of the objectives of this project are

- Identification of different types of cyber-attacks
- Security risks in the banking sector

- Observation of the cyber security policies being implemented by the UK
- Implementation of technical practices in the banking sector in accordance with the policies
- Testing the network to observe the vulnerabilities to the networking system
- Development of networking policies along with a framework that has to be implement by the Banks to safeguard their control system and ensure its implementation

1.4 Research Issues

The research issues that are going to be addressed in this research project are

a. Research Issue 1: What are the most vulnerable types of cyber-attacks for banks?
b. Research Issue 2: Why cyber security is essential in the banking sector?
c. Research Issue 3: What practices are employed for the detection of malware attacks?
d. Research Issue 4: What will be the impact of the policies and security practices on cyber-attacks, malicious activities and other related vulnerabilities
e. Research Issue 5: What framework can be adapted by the banks to ensure the confidentiality of identity and security of assets and data?
f. Research Issue 6: How operational practices can be implemented in the banking sector?
g. Research Issue 7: What will be the impact of implementing operational practices and research policies?

In order to all the above-mentioned issues, the literature review section will be providing the relevant information. Moreover, the focus will be made on the security tools, operational practices, and testing methods and the role of the cybersecurity manager will be analyzed in reference to the banking sector.

1.5 Research Questions

The research question of the study is

> "How the cybersecurity practices and policies can prevent the network from cyber-attacks, and how the proposed framework can safeguard the network from any kind of vulnerabilities"

1.6 Banking Sector and Cyber Security

Nowadays, the technology has progressed enough to carry out fast transactions at global level. The information modes are not limited among business to business (B2B), but to the business to customer (B2C) as well (Mohd. Khairul Affendy Ahmed et al., 2010). The increased online banking has gained the attention of cyber criminals' interests to the financial gains. The utilization of online banking has also resulted in the acquirement of introduction to different types of threats and vulnerabilities (Stytz, et al., 2005).

The operations and applications of mobile banking is not limited to online transactions only, but also contains management of bank statements, order checking, trading of shares, payments of bills and reviewal of transaction history. It illustrates the fact that the customer is not only concerned with his data, but also carrying out interaction with database and files of the banking system (Narendiran C. et al., 2008). Now, when it comes to the customers, the observation shows that most of the customers have little trust about the mobile devices for carrying out any transactions and are concerned about security level up to some extent. Therefore, the banking systems ensure the satisfaction of the customers by providing authentication methods for allowing the right person to access their services (Yang D. et al., 13-15 June 2010). This involves a third-party involvement in terms of email or text services that allow the customer to pay extra services (for cellular text messages) to the third party and acquire authentication methods (Soni P., July 2010). In order to deal with such issues, the banking system has ensured the authentication using PIN number, username and password, fingerprint system, and so on. The fingerprint system will allow the recognition of the ID and is interconnected with the biometric verification system. Therefore, in case of mobile theft or loss of information, unauthorized access by any means using Internet connectivity to the cybercriminal or any other person can be avoided (Bilal M. et al., September 2011).

The reports have been published to analyze the data breaches in different sectors and their impacts. According to the IBM Security a report titled "Cost of a Data Breach Report 2021", the cost of data breach has rose from $3.86 million to that of $4.24 million having 10% in the average increment of the cost per year. The impact was loss of 38% of the business containing lost revenue to the downtime of the system, increased turnover of the system, increased cost of a business because loss of reputation. With the increased technological innovations and its utilization, the top five countries and regions which remained the Centre of data breach in 2021 were United States, Middle East, Canada, Germany, and Japan. moreover, based on the sectors the top five sectors that were greatly affected in 2021 due to data breach were healthcare facilities, financial sectors, pharmaceuticals, technology, and energy sector. Based on both these factors the top effectives were customers, then employees, intellectual properties, sensitive data, global record and anonymized data of customer (IBM Security, 2021).

1.7 Types of intrusions

There are different types of cyber-attacks, but the potential intrusions that the banking systems have been facing are

1.7.1 Malware

The malware is a type of program which carry out alteration in the modification of the computer system without getting authorized access by the user. Such program propagates among different computers and among different networks. Different types of malwares included worms, viruses rogue Internet codes and script attacks. These malware propagate through online platforms damages the banking system (Natalius, 2018). The impact of malware attack is loss of integrity, confidentiality, and availability of banking system. When it comes to the damage, the analysis can be made for a malware attack in the ATM machine of Ukraine and Russia. The “Trustwave”, the information security provider investigated that different ATMs in Ukraine and Russia had been prone to malicious attacks. While the tests were being carried out is using malicious infections, 20 different ATM machines allowed the attackers for stealing the data, PIN codes and money (Chen T. M. et al., 2004), (Pemble, 2005). Different types of malware attacks (Etaher N. et al., 2014) are

a. Viruses which are self-replicating programs. Such programs carry out modification of file contents, hide themselves within a computer, and are transferred by copying themselves among different machines
b. Worms which are self-replicating as well as self-contained programs. Such programs carry out the performance of destructive actions by invasions of computer (Liu, et al., 2011)
c. Trojan horses appear to be harmless computer programs but contain harmful contents which insert into the machine resulting in the entire damage. One additional factor for this category is the requirement for human assistance for getting spread. this causes the Trojan horses to remain intact on one single device and does not replicate themselves like above two categories. The most famous banking Trojan is Zeus.

d. Spyware is another category of malware the function of which is getting installed on computer for transmission, tracking and reporting of information as well as data of the consumer or internet user having no consent. It appears in the bundle of free access and open software, and performs the function for which it is designed (Sipior, et al., 2005)

1.7.2 Denial of Service Attack

The Denial of Service (DoS) or Distributed Denial of Service (DDoS) is one of the common attacks that the banking system faces. Such attack involves utilization of 100 or more computers for launching the attack on the targeted system. Before the occurrence of an attack, the cybercriminal first builds the attacking network by which the attacker will gain ability to scan the open port containing computer having poor security system such as no antivirus software or firewall presence in the computer (Patrikakis, et al.,). While the attack is being occurred the program gets installed in the computer which continuously propagates automatically for the creation of a large attack at the network level. Such attacks involve the development of infrastructure and utilization of codes for carrying out attacks. The FBI has ranked this attack at third-highest level after terrorism and espionage. The reason at such high ranking is the financial institution or banking system experiencing such attacks would greatly reduce the trust of customers, money, and reputation at the global level (Mohd. Khairul Affendy Ahmed et al., 2010)

1.7.3 Spoofing

One of the attacks in the banking system by which the customers are greatly affected is Spoofing. this attack impersonates a person or a computer by giving false information by utilization of SMS services, emails, IP addresses and URL. Different forms of spoofing are IP spoofing, SMS Spoofing, Web Spoofing, and DNS Spoofing. The two main categories being observed are SMS spoofing and email spoofing. In SMS spoofing, the attacker manipulates the sender number by sending messages. The spoofing attacks through SMS service has caused organizations to not to pursue the SMS services for mobile banking system (Harb H. et al., 2008). In comparison to that, the email spoofing requires the acquirement of IP of the target after which the communication is disabled, the sequence numbers are guessed, the modification of the packet headers is carried out, unauthenticated access is obtained, and desired attack type is planted from the backdoor (Ramesh P. B. et al., 2011).

1.8 Malware Detection Methods

The malware detection method is an area of importance for both public and research community. The increased complexities in malware have been resulting in utilization of sophistic techniques to get hidden for avoidance using detection tools. In such scenarios, it is difficult to detect the malware. The techniques that have been utilized for hiding the malware among which the complex ones are polymorphic, packers and metamorphic techniques. To deal with those issues, the need is development of detection methods for detecting and avoidance of malware attacks. The two main techniques for detection of the malware are signature-based techniques and behavior-based techniques

1.8.1 Signature-based Techniques

This technique is based on utilization of set of commands for detecting the malicious program. the commands produce the signature for any detected malware. This method aims at recognizing the malware by every produced signature having emphasized on detecting the behavioral patterns of malware. This technique is widely used in antivirus software. Such software investigates the malware codes, and upon detection the signature is produced. The benefit of signature-based technique is its operational efficiency and availability in the market (Zolkipli M. et al., March 2011).

1.8.2 Behavior-based Techniques

This technique is based on utilization of behavioral methods for detecting the malicious program. such method is concerned with the targeting the basis as well as addresses which are you really the part of such behaviors.

Both methods have their own benefits as well as drawbacks. For example, the signature-based technique requires small time to scan the machine come up and at the same time provides small quantity of false positives. At the same time, such technique has no to reduce capability of dealing with a malware which is not known to this technique. Therefore, that type of malware cannot be detected using the analysis. Similarly, the behavior-based detection method allows detection of polymorphic malware. So, the researchers are focused on development of combined approach or hybrid approach for detection purposes (Zolkipli M. et al., March 2011).

1.9 Conclusions

This chapter focused on historical background of online banking system, advancements and technological sector leading to increased cyber-attacks. Moreover, the network security and damage to banking system because of implementation of cyber practices followed by some policies was defined as the problem for which research objectives were defined. The chapter also took into account the research questions that will provide the basis of development of research methodology. The analysis was also carried out about the banking sector and how the cyber security has resulted in the loss of economic and reputational damage. To observe those facts, the analysis was carried out about different types of intrusions that included malware, denial of service attack and spoofing. Lastly, the chapter focused on basic detection technologies of malware. The study will help in carrying out literature review in the next chapter in which the discussion will be carried out about what research work has been carried out, and what are the policies of U.K to deal with such issues.

Chapter 2: Literature Review

2.1 Introduction

The focus of the chapter will be to discuss different hardware and software trends that have resulted in increased utilization of computing technologies. Therefore, the research will first cover technologies, and then will move to Software Defined Networking (SDN). The comparative analysis will be made for the SDN and conventional networking system. The chapter's discussion will be then diverted to the cyber security networks.

2.1 Emerging technologies and their trends

The emerging trends of information and communication technologies (ICT) having different domains involving big data analytics, cellular technology, social networks, and cloud storages have urged to computer networks utilize high bandwidth having accessibility as well as dynamic management systems (Xia W., et al., 2015). The increased popularity of multimedia systems in both hardware and software forms has increased the demand for big data analytics having diversified sets of data from different resources. In response to the requirements of computer networking domains, the intermediate solution is to invest on development of social network for enhancement of capability of existed computing systems which will be practically a good option for the companies. This can be illustrated by an example of mobile devices that have increased by nearly 1.4 mobile devices per capita from 2014 to 2018 resulting in the dynamic growth of increased utilization of social networks and websites (Barnett T., 2014). When comes to social media comment observation shows that the Facebook users have expanded from 1 million in 2004 to that of 1 billion by 2012. Obviously, all those expansions require proper infrastructure and flexibility in the computer networking system (Xia W., et al., 2015)

2.1.1 Software defined Network

The open networking foundation being a nonprofit consortium has dedicated its efforts in the formation, development, standardization, and commercialization of the SDN. According to the foundation, the SDN is one of the emerging network architectures that involves network control being decoupled as well as forwarded and can be directly programmed (Open Network Foundation, 2012). From the definition comment can be observed that this networking topology is based on two main characteristics which are programming capability and decoupling of data planes as well as control systems. The main feature that separates SDN from Conventional Networking systems involve decoupling of data and control plane, and programmability. In contrast to SDN, the conventional networking system has to define a new protocol for each problem which increases the complexity in controlling the network. The second difference is associated with the configuration among the networking topologies. The SDN topology involves automatic configuration along with centralized validation, which in case of conventional networking systems has to be manually configured in case of occurrence of an error. The performance of SDN network is based on dynamic global control along with cross layer information, which in case of conventional networking has limited information as well as static configuration access. The last name portent feature is innovation which in case of SDN is associated with quick and easy implementation of tools having new ideas, providing testing and isolation environment along with quick upgrades. On contrary to that, the conventional networking system has difficulty in implementing the software having new ideas in the old hardware systems along with limited environment available for testing and standardization. The three-layered model has been shown in figure below

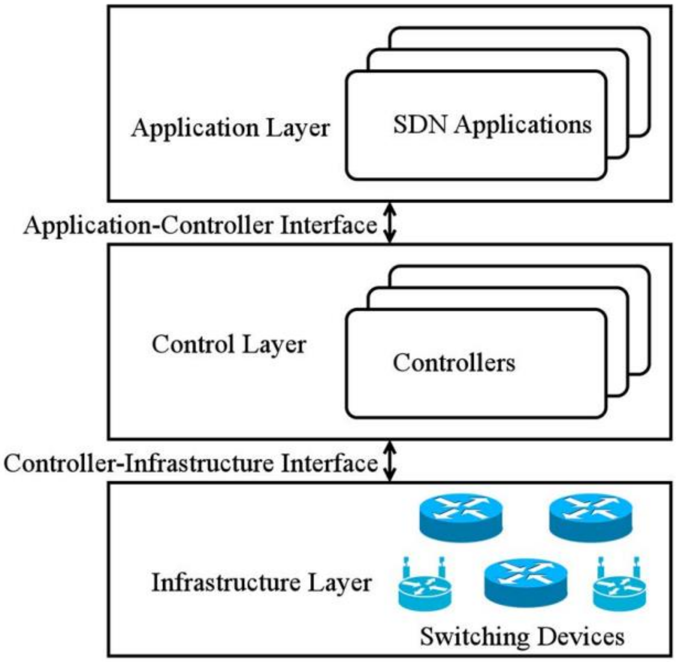


Figure 2.1 Three layered Model of SDN (Xia W., et al., 2015)

2.2 Cyber Security

The cyber security term has been one of the most popular terminologies associated with the cyber attackers, researchers, and academics. The terminology is high broad having its definitions and explanation being subjective found and highly variable (Craigen D., et al., 2014). In order to understand the cybersecurity perspectives.

According to the definition provided by Kemmerer et al., cyber security contains mainly the defensive methods utilize for detecting and throttling the intruders (Kemmerer, 2003). Similarly, Lewis has defined cyber security as the security which involves provision of protecting the computer's network and the information that is contained from getting penetrated as well as damaged from any malicious activity or disruptions (Lewis J. A., 2006). ITU has provided the definition in context with policies and methods according to which cyber security his collection of policies, concepts related to security, tools and safeguards, a risk management approaches, practices, technologies and assurances utilized for protecting the organizational cyber environment, and assets of users (ITU, 2006).

Whatever is the definition, the main focus is on protection of different components which are (Craigen D., et al., 2014)

1. “Asset” which is useful or valuable thing to a person. In case of cyber security systems, it is a cyber space as well as cyber space enabled system
2. “Capability” is associated with the organization involving its procedures, resources and structures for protection
3. “Misalignment” of any position can result in acquirement of incorrect positions are inappropriate happenings that are to be aligned properly
4. “Occurrence” of any event or incident caused by cyber attacks
5. “Organizational” policies and procedures for exploitation of competitive potential of the capabilities and resources
6. “Processes” based on series of actions that helps in protection from cyber attacks
7. “Protection” from getting harmed by exposure of information including assets, identity or any other personal information

8. “Resources” involving tangible and intangible assets that can be utilized for conceiving and implementing the strategies

2.3 Cyberthreats domains

The integration of cyber knowledge is required for not only day-to-day functionality maintenance a letter to technology and economy, but also for the security as well as well-being of the governments, organization, and people, which are prone to attacks because of commercial interests and can result in occurrence of frauds by subject to the variety of assaults. United Kingdom has also been passed through different types of frauds. Therefore, it is necessary to analyze the cyber-attacks by different range, according to which the city challenges evolve that can be related to either ICT networks or equipment (Cornish P., et al., 2009)

2.3.1 Attacks sponsored by States

The interstates sometimes misuse the cybertechnology which is assumed to be a mistake. however, the impact of such attacks is relatively low. It can be illustrated by and attack of Radio Free Europe /Radio Liberty (REF/RL). It involved fake hits of 50,000 in every second. It is assumed to be one of the most sophisticated forms of cyber operations that have been carried out. The main purpose of such attack was to limit the media coverage for opposing the protests against the regime of Aleksander Lukashenko who was the Belarus’s dictator. The activity involved DOS attack (Cummings R. H., 2010). Similarly, another hacking incident occurred by Israeli attackers in September 2000 That involved hacking of websites that are owned by Hezbollah as well as Palestinian National Authority (PNA). The Palestine considered it to be “Cyber Holy War” and retaliated by assaulting the financial and government websites (Cornish P., et al., 2009).

2.3.2 Extremism (Ideological & Political)

The terrorism and extremism have also diverted from handling of just guns and other armory to utilization of Internet services, social networks, and dark webs. The terrorists have been involved in cyber-terrorism which involves crimes and hacking applications (The Economist, 2007). One of the most known cyber-jihadists known to the world was Younis Tsouli (Corera G., 2008). The increased popularity of Internet for politics and ideology has explanation in numerous manners. For example, the extremist organization can utilize Internet by diversified activities that are variable based on the origins designing and functionalities. the origins off Internet technology lies in the Cold War and requires insurance of redundancy in both military and government communication system. This allows extremists to get attracted to the Internet system having resiliency as well as anonymity. Another factor is associated with already developed system having global infrastructure by the governments (Barno D. W., 2006)

2.3.3. Organized Crime

UN has defined Organized Crime as the group of three or more persons having existence for a particular time and acting in the concert while aiming at commissioning of one or more offenses that is established in accordance with the convention for direct or indirect acquirement of financial or other type of benefits (The Economist, 2007). The internet technology involving date occasion virtual communication and personal or political activities has made it an important medium for carrying out. It is no surprise that the criminal activities have incorporated utilization of Internet services by using different techniques. While increasing the capacity of transmitting billions of dollars through Internet and other systems, The cybercrimes have tempted for the modernized enterprises of criminals. many applications and software packages have been developed for performing criminal activities lying under the cyberspace.

2.3.4 Individual or low-level crime

The last domain is nonhierarchical spectrum of the cyber threats that are performed using diversified software packages and focus on including into the networks of others by the hackers. When it comes to computers, the analysis shows that acting requires specific sense of balancing the maintenance of which is difficult for some hackers while working in discrete cyber environment. Whereas, for other cyber hackers, there is a lack of coherence. The hacking has been proved to be their central feature that is concerned with a serious types of cyber threats. Whereas, hacking has also been the focus of the media and the archetypical cyber threat for public. Therefore, the need is to realize the dangers associated with the hacking and its dramatization in the technical world (Cornish P., et al., 2009)

2.4 Cyber Security in UK

The United Kingdom has realized the importance of cybersecurity at national level for which the resilience has to be maintained. Therefore, the integration of security, defense, development. and foreign policies (HMG, 2021) provides the national resilience for defining the approach of looking towards the security and prosperity of the country. As the global resiliency has been increasing having dependence on the connectivity and digital devices, the need is to grow the cyber resilience which has to be incorporated as the national effort. Therefore, the National Cyber Security (HMG, 2021) strategy has been developed which is aimed at persuading the objective of seeking the farm establishment of the responsible cyber protection and promotion of the interests of the sovereign country.

2.4.1 Threats

The malicious tools, and types of activities have been evolving because of increased cyber security risks by cyber criminals to nation states. Since the tactics and capabilities have been continuously evolving and have been diversifying, the capability of cyber tools as well as services have been decreasing below the specified threshold for disrupting anyone against the functions and operations of the government. Also, the government has remained the main target having wide variety of malicious actors that have caused 777 incidents among September 2020 August 2021 which have been managed by NCSC (NCSC, 2021), otherwise the public sector could have been affected. This value has been increasing and has not reduced. The major role has been played by ransomware, and both Hackney councils and Redcar & Cleveland have been hit by ransomware in 2020.

2.4.2 Challenges

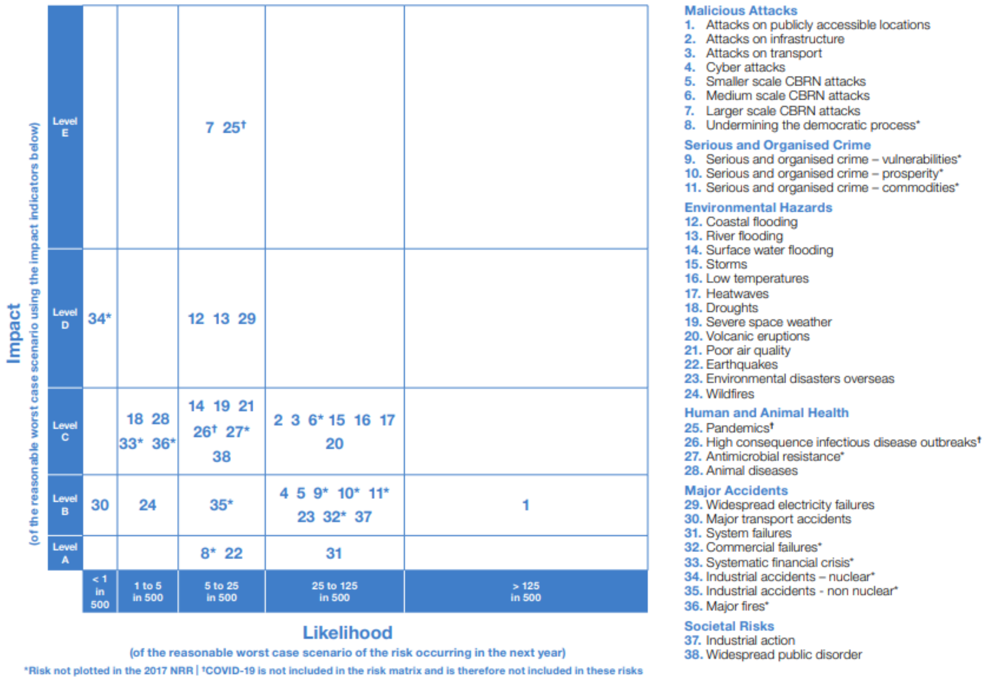
Although, the recognition of the government as well as the understanding about the cyber security risk has evolved, the gaps have been highlighted among the cyber resilience of the government at the specific place and the place where it requires to be. Those gaps have brought the country to meet the minimum cybersecurity standards that have emerged as challenges for the technical departments. At the same time, the maturity level, investments, holding capability and understanding capability of the security of the government organizations has still remained inconsistent. Whereas the size as well as the complexity of the digitalization in the presence of IT technology has been becoming more and more complex. Furthermore, the complex structure of governance, incentives and leverages, improper accountability practices, and mechanisms for sharing the information has made it a challenging task for the government to enhance visibility to the cyber risks at different scales

2.5 The National Risk Register of UK

The United Kingdom has set standards to tackle malicious activities for which National Risk Register (NRR) has been published by HM government in 2020. The edition published in 2020 also concerned the impact of COVID-19 that has great impact on health and wealth of the public. After the publication of national risk register in 2017. The country has faced different challenging incidents which includes terrorist attacks in Streatham and London Bridge, collapsing of Thomas Cook Group and Carillion, winter storm i.e., “Beast from the East”, utilization of chemical weapons in Amesbury and Salisbury, serious floods, and COVID-19 pandemic (HM Government, 2020).

2.5.1 Risk Matrix

The Risk Matix as defined by NRR has been shown below in figure below



Impact
(of the reasonable worst case scenario using the impact indicators below)

	< 1 in 500	1 to 5 in 500	5 to 25 in 500	25 to 125 in 500	> 125 in 500
Level E			7 25†		
Level D	34*		12 13 29		
Level C		18 28 33* 36*	14 19 21 26† 27* 38	2 3 6* 15 16 17 20	
Level B	30	24	35*	4 5 9* 10* 11* 23 32* 37	1
Level A			8* 22	31	

Likelihood
(of the reasonable worst case scenario of the risk occurring in the next year)

*Risk not plotted in the 2017 NRR | †COVID-19 is not included in the risk matrix and is therefore not included in these risks

Malicious Attacks
1. Attacks on publicly accessible locations
2. Attacks on infrastructure
3. Attacks on transport
4. Cyber attacks
5. Smaller scale CBRN attacks
6. Medium scale CBRN attacks
7. Larger scale CBRN attacks
8. Undermining the democratic process*

Serious and Organised Crime
9. Serious and organised crime – vulnerabilities*
10. Serious and organised crime – prosperity*
11. Serious and organised crime – commodities*

Environmental Hazards
12. Coastal flooding
13. River flooding
14. Surface water flooding
15. Storms
16. Low temperatures
17. Heatwaves
18. Droughts
19. Severe space weather
20. Volcanic eruptions
21. Poor air quality
22. Earthquakes
23. Environmental disasters overseas
24. Wildfires

Human and Animal Health
25. Pandemics†
26. High consequence infectious disease outbreaks†
27. Antimicrobial resistance*
28. Animal diseases

Major Accidents
29. Widespread electricity failures
30. Major transport accidents
31. System failures
32. Commercial failures*
33. Systematic financial crisis*
34. Industrial accidents – nuclear*
35. Industrial accidents - non nuclear*
36. Major fires*

Societal Risks
37. Industrial action
38. Widespread public disorder

Figure 2.2 Risk Assessment Matrix (HM Government, 2020)

According to risk assessment matrix of the National Risk Register, the likelihood of the events for malicious attacks has great impact. For the first attack on public assets, the economic impacts ranges less than £10 million, and the fatalities can range among one to 8. Similarly, the evacuation and shelter impact can vary for the size of people and days which can be of three days for 50 people. Similarly, the environmental or contamination damage can range up to one month and the electricity supply can be disrupted. lastly, for that attack, there is the chance of moderate damage to the relationship of UK with other countries. The likelihood is among 125 to 500 for that first attack. (HM Government, 2020)

The seventh malicious attacks which involve Chemical, Biological, Radiological, and Nuclear (CBRN) attack has highest impact of level E. For that attack, the economic impact would be more than £100 billion having fatalities more than 1000. Moreover, the public perception about that attack would be prolonged and vulnerable, the environmental impact would be realized throughout the region for more than five years having significant damage to the relationship of the UK with other countries (HM Government, 2020)

2.5.2 Strategy

In order to counter the terrorism, the strategy has been defined by government of UK which is aimed at reducing the risks associated to the personal information as well as assets of the UK (HM Government, 2020) citizens that is based on 4 main strands which are

1. Prevention: it is focused on stopping the people to become terrorists or support any extremism or terrorism
2. Persuasion: it is focused on stopping the terrorist attacks
3. Protection: it is focused on strengthening the protection against any type of terrorist attack
4. Preparation: it is focused on mitigation of the impacts of the terrorist attacks if they or unstoppable at any instance

2.6 Previous Detection Approaches

2.6.1 Computer Vision Techniques

Different approaches have been utilized by the researchers for detecting Denial of Service attacks. One such method has been devised by Tan Z., that focuses on computer vision techniques (Tan Z., et al., 2014). Instead of utilization of statistical analysis and machine learning, the developed method focused on treating the traffic records in terms of images for which the detection of that of dos attacks is being carried out as a problem of computer vision. The multivariate correlation analysis approach has been integrated for depiction of accuracy in maintenance of traffic records of the network, and to carry out conversion of the records into that respective images. That images of the traffic records have been utilized by the author for observing the proposed system under dos attack. So, the dissimilarity measurement system proposing the detection of dos attack has been termed as Earth Mover’s Distance (EMD). The purpose of EMD is to take into account the matching of a cross been and ensures the provision of accurate evaluation of the dissimilarities among the Distributions when compared with well-known dissimilarity measures like Minkowski form distance Lp and X^2 statistics. For the evaluation of the proposed method, the cross validations have been conducted by utilization of KDD 99 dataset as well as ISCX 2012 IDS Evaluation Data set. The detection results obtained by the system for DoS attacks provided 99.95% of the detection accuracy on that of KDD 99 dataset, and 90.12% on that of ISCX 2012 IDS while processing approximately 59,000 traffic records in each second.

2.6.2 Analysis of DoS attacks and their Implementation

The determination along with analysis of three main types of DoS attacks including distributed DoS (DDoS), The Ping of Death and TCP SYN Flood determined by (Elleithy K., et al., 2006). The Ping of Death had been simulated on windows 95 computer, and TCP SYN Flood attack was simulated on MS Windows 2000 Server. For the demonstration of DDoS, the zombie program has been simulated that carried The Ping of Death along with it. For establishment of the communications through TCP protocol, the session was initiated that contained three-way handshake among the source host that sent the TCP packet for hosting the SYN flags, the destination host responding to the host by sending the TCP packet along with ACK flags and SYN flags, turn the source host sending destination. The implementations for development of three case scenarios were carried out for which the determination was made for the number of damages. The funding shown that the attack was stealthily covert as well as delivered quite easily. Whereas DDoS attack was quite powerful in comparison to other two types of attacks.

2.6.3 Analysis of different DDoS attacks and impacts of Layers

The report published by defense Advanced Research Projects Agency, focused on assessment of DoS attacks (DARPA, 2001). With that report published analysis of different types of attacks including Octopus, Snork, UDP Storm, TCP SYN Flood attack and ARP Cache Poison. From the observation, it was found that the affected layer associated with Octopus attack was application, and the transportation layer was the affected layer for Snork, UDP Storm and TCP SYN Flood. Whereas for the ARP Cache Poison attack, the datalink layer was affected.

For the examination of Octopus attack, that bottle had been developed and run nine times for which for important parameters of time out, maximum connections, attacks starting and ending time had been set. The first case contained time out of 30 seconds having 500 connections for which the starting time was 1000s and the ending time was 2200s. For the ninth case, the timeout duration was increased to 300 having maximum connections of 1500 having same starting and ending time. For that attack command the two main measures of effectiveness that were kept our outage time during and attack, and the probability of the denied service. The results being developed shown that the attacker had easy access to adjust the impact of the adjustments by setting up the rate at which the requirements of the resources are to be fulfilled. At the amount of 10 requests for each second, the probability of the denied service was below 0.2 that could increase with an increment of the attacking rate.

For the ARP Cache Poison attack, the observation was made for impact of the attack during the variation of the delay among the attacker after getting the request, and the response of poison being sent. Another factor that was taken into consideration for determination of the impact was inclusion of the method of server that updated ARP cache as well as frequency of updating that ARP cache. It is to be noted that that duration varied based on the operating system. So, the main parameters were ARP request being sent from the server, ARP response being received by the server, the network delay occurring among the ARP request being sent and received, different points that could get poisoned by the response, and the transaction duration among the client and server for completion. The simulation had been done for 12,000 seconds while considering the fact that the attack could occur between 1000s to 10,000s. The results shown that the more is the time out associated with ARP cache, the smaller is the attack's effectiveness.

TCP SYN Flood Attack that is commonly known to be a zombie attack had been analyzed in terms of performance for which the APL Subnet model had been passed through modification. It involved a reduction of the clients to half and increasing the traffic loading of the client. This modification resulted in the reduction of memory utilization in OPNET. After that, the small network had been formed for attacks that contained zombie systems. The analysis involved six different cases having variable queue sizes, connection timeouts, and SYN attack rate. The measures of effectiveness that were taken into analysis were duration of an attack, impact on different services and probability of denied services. For the better observation of the results, the variation had been carried out queue timeout (by 15s, 90s, and 180s), varying the size of queue (by varying the size up to 1024, 4096, and 8192 queue size), and varying the SYN rate From 5000 packets per second to 10,000 packets per second. For all those variations, the results shown that the PDS was maximum for time out of 180 seconds, queue time out of 180 seconds, and queue size of 4096. Whereas the results of SYN rate showing that the packets per second did not affect the PDS.

The UDP Storm attack was determined by configuring the 104-node network for which all the hosts were connected to the local area network (LAN) through a switch. moreover, the modification had been made for placing the additional stress on the network. additionally, the increment of the traffic throughout the network had been carried out while the reduction of size of a queue and speed of processing were managed. This test contained three main analytical parameters of network switching, involvement of hosts in flooding, and data communication link among the switch and individual hosts. The 100 Mbps switching topology was captain to consideration while providing the maximum packet size of that of 1500 bytes. The requirement of host for forwarding 8333 packets in each second was fulfilled by utilization of the datalink. The analysis involved development of nine scenarios having different switching speeds and sizes of the switching queue. The consideration finally involved active participation of one client which was known to be an active client in the attack. The results shown that with an increased pairs of active and passive clients, the flood attack was decreased. Similarly, for the size of a query, the increment of the kb queue also observed a reduction of the impact of an attack, and lastly the observation for both active and festive clients illustrated the fact that the increment of the switching speed caused increased attack.

2.6.4 Hammer Model for assessing the Cognitive Radio DoS Attacks

The cognitive radio next utilization of uh news portion of wireless spectrum which are also known as white space and operates in the region of unused portions which allow to limit other devices from getting interfered. With the advancement of radio technology, the existing networks depending on wireless technologies have been undergoing radical change in the way they operate. The main difference between devices operating on traditional wireless systems and cognitive technology is that the traditional devices are bound to fixed frequency and fixed set of protocols when compared with the cognitive radio technology having capability of operating at multiple frequencies and wide variety of protocols that can be changed at any time. The impact of using cognitive devices is increased authentication, security mechanisms and integrity verifications. The research involving hammer model focused on assessment of the potential attacks on the cognitive radio systems. The vulnerabilities word determined for prevention of the communication through the system in that of specified bands by completely denying the device to allow the communication or induction of harmful interference to the users through DoS attacks (Sethi A., et al., 2008).

2.6.5 Artificial Intelligence Approaches

The detection by the execution of artificial intelligence is mainly dependent upon the collection of the data. Such technology has capability of improving the performance of the tests that is based upon the previous outcomes. therefore, some rules have been set for the government of the data and the results obtained are robust and is dependent upon the attributes related to parallelism, uncertainty, fault tolerance and inaccuracy. The AI based methods you really employ machine learning (ML) for performance of such tasks (Bashar A. K., et al., 2019). It includes different models such as Bayesian networks, fuzzy logic, genetic algorithms, K-nearest neighbors' techniques, neural networks (NN), support vector machine and software agent.

The statistical approach involves utilization of parametric methods, and nonparametric methods. The parametric methods involve operational methods (involving multivariate correlation analysis), statistical methods (involving confidence ranges for which statistical properties are determined), and spectral methods (involving utilization of high dimensional datasets for detecting the applications). Whereas nonparametric methods involves change aggregation trees (CATs) technique, D-Ward approach (by monitoring continuously the bidirectional flow of Internet and local traffic), Markov method (for monitoring the changing states of the networks) and flow feature value (FFV). Moreover, regression analysis, static regression, time-based monitoring are other parametric methods.

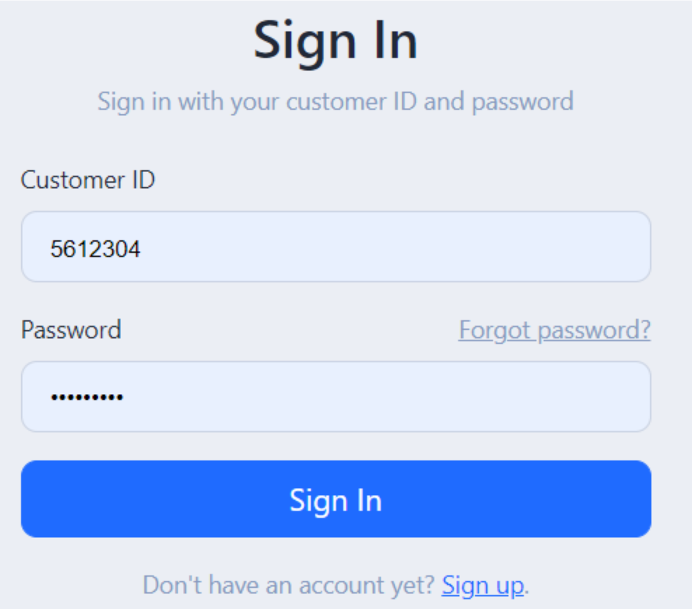
Chapter 3: Methodology

3.1 Format of Methodology to be adapted

3.1.1 Creation of the Website

In order to perform the security audit of the website of the banking, the first step is to form the website which involves development of whole server for the website. The website that has been formed is https://dayobanking.xyz/

In order to monitor the traffic, the customer has been allowed to sign in or sign up on the banking website.



Sign In

Sign in with your customer ID and password

Customer ID: 5612304

Password: •••••••••

Don't have an account yet? Sign up.

Figure 3.1 Account formation on https://dayobanking.xyz/

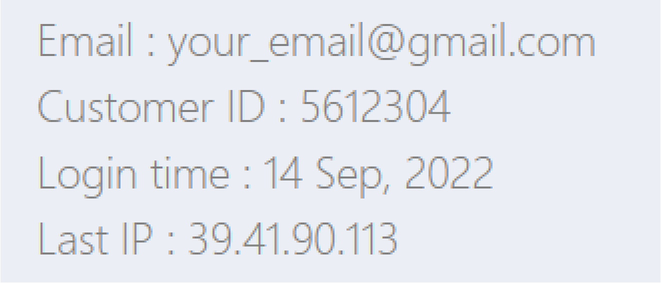
Now, different customer IDs and passwords have been formed for monitoring their activities. The sample IDs along with their sample passwords are provided below

Three users in the system: Customer ID's for login:

- **5612304**
- **1292220**
- **4067151**

Password is the same for all: **qwaszx123**

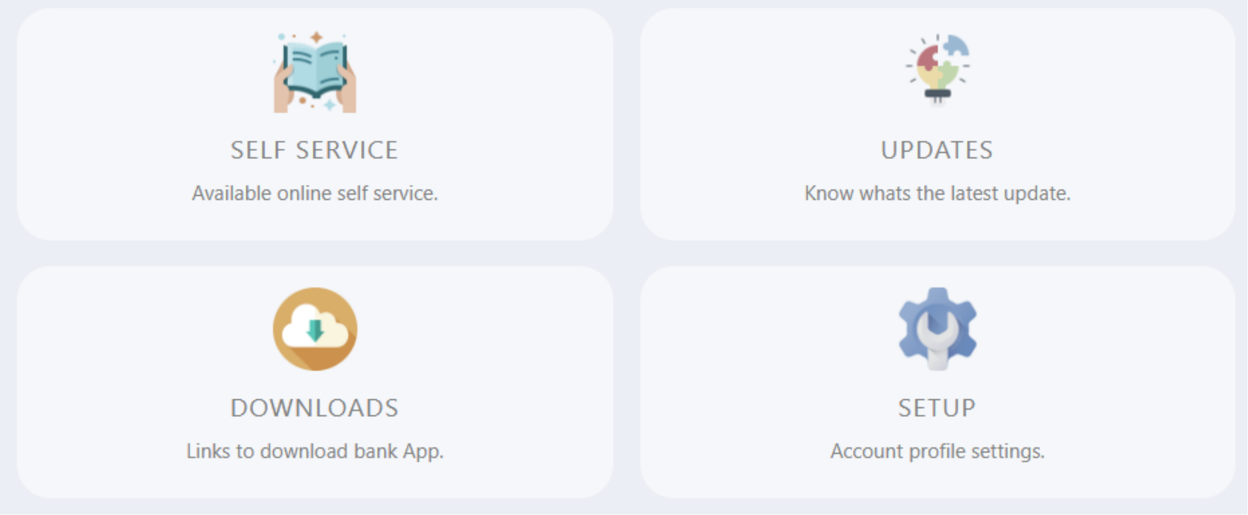
After the finalization of the account on that website, the customer will be logging the information containing different options of account settings, downloads, and other options. It is important to note that the administrator will be provided with the dashboard to access the information for any customer ID. The information will be provided to the administrator about the e-mail to see that the login has been made, the idea of the customer, the log in time and date, and the IP through which the customer had logged in. The illustration is given in figure 3.2.



Email : your_email@gmail.com
Customer ID : 5612304
Login time : 14 Sep, 2022
Last IP : 39.41.90.113

Figure 3.2 Customer's information appearing before the administrator

Now, the information that will appeared to the menu of the customer and will be accessible by the customer is provided in the figure 3.3.



SELF SERVICE
Available online self service.
UPDATES
Know whats the latest update.
DOWNLOADS
Links to download bank App.
SETUP
Account profile settings.

Figure 3.3 Dashboard illustration for the customer containing different menus

The dashboard provided to the customer will ensemble the self-services activities, the updates available on the application of the banks on the Android and other operating systems of cellular technologies, the download link of the banking application and the profile settings alerted to the account that will be incorporating information about the personal picture, login details, encrypted security codes, transaction history, availability of balance and so on. The dashboard illustration has been provided in figure 3.3. Lastly, the navigation panel for the customer has been formed which will displayed on the left corner, and has been depicted in figure 3.4

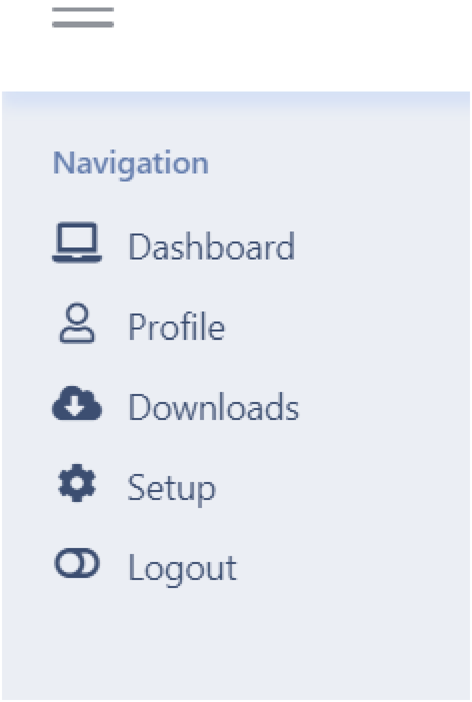


Figure 3.4 Navigation panel for the customer

3.1.2 Penetration Testing

Penetration testing (PenTest) is a form of security audit that entails a specific set of guidelines for how the test should be carried out. The established methods included in PenTest require careful handling in order to provide an accurate assessment of system security.

The phases of a penetration test are as follows: scoping the target, gathering information, discovering the target, enumerating the target, mapping the vulnerabilities, using social engineering to exploit the target, escalating privileges to gain access, maintaining access, documenting the test, and reporting the results. Target scoping, information collecting, and target discovery are all utilised in a black box approach, but the white-hat auditor may skip over them if they are familiar with the system under test (Menoski D., et al., 2014).

Discovering the resources that the dayobanking web server is using and the underlying technology that the dayobanking web server is running on is part of the process known as website enumeration. This information can be used to select vectors for an attack that are more likely to be successful, as well as to identify and exploit vulnerabilities in different versions of the day trading web server software (Santhosh, A. and Kurian, R., 2021)

In order to effectively test for vulnerabilities, a systematic method must be taken. Call it what you want, but without any sort of method in place, you're just making guesses and taking chances, which may yield short-term success but will inevitably lead to failure in the long run.

When it comes to enumerating websites, The access has been ade to a wide variety of tools, such as WHOIS, Nmap, Metasploit, dirbuster, burpsuite, nikto, and sqlmap etc. The detail of each tool is given in this chapter.

3.2 Information Gathering and Scanning

Gathering target information is the initial step in conducting a penetration testing. The process of obtaining information is looking for publicly available data on the system and determining how best to use that data (Al Shelbi., et al., 2018).

Collecting as much data as possible helps better in comprehending the application's or system's inner workings, which is essential for locating security holes that need fixing. There are two methods that can be used for this procedure.

3.2.1 Passive Information Gathering

Gathering information in a less evasive manner, known as "passive," can come before active methods. It relies solely on information about the target that has already been made public, and it attempts to collect as much data as possible without the pen tester ever making direct contact with the target. To do this, the advantage of publicly can be made for available resources like WHOIS domain lookups, social media platforms, email providers, and databases of websites sharing the same IP address, among other things.

3.2.1.1 WHOIS

WHOIS is a service and utility on the Internet that displays more data about a domain, its registrar, and its IP address. If you're attempting to think of a domain name for a new website, a WHOIS search is a great way to see if that name is already in use (Sinha S., 2018). By using the WHOIS online tool to gather information about the website "https://dayobanking.xyz" as shown in the figure below.

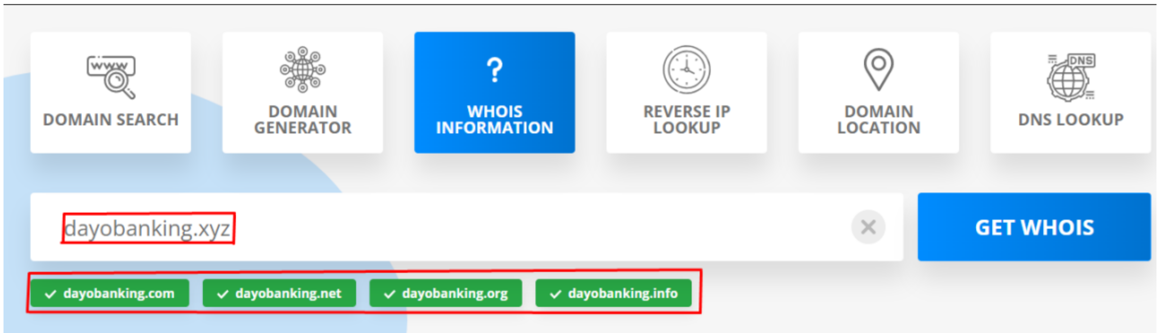
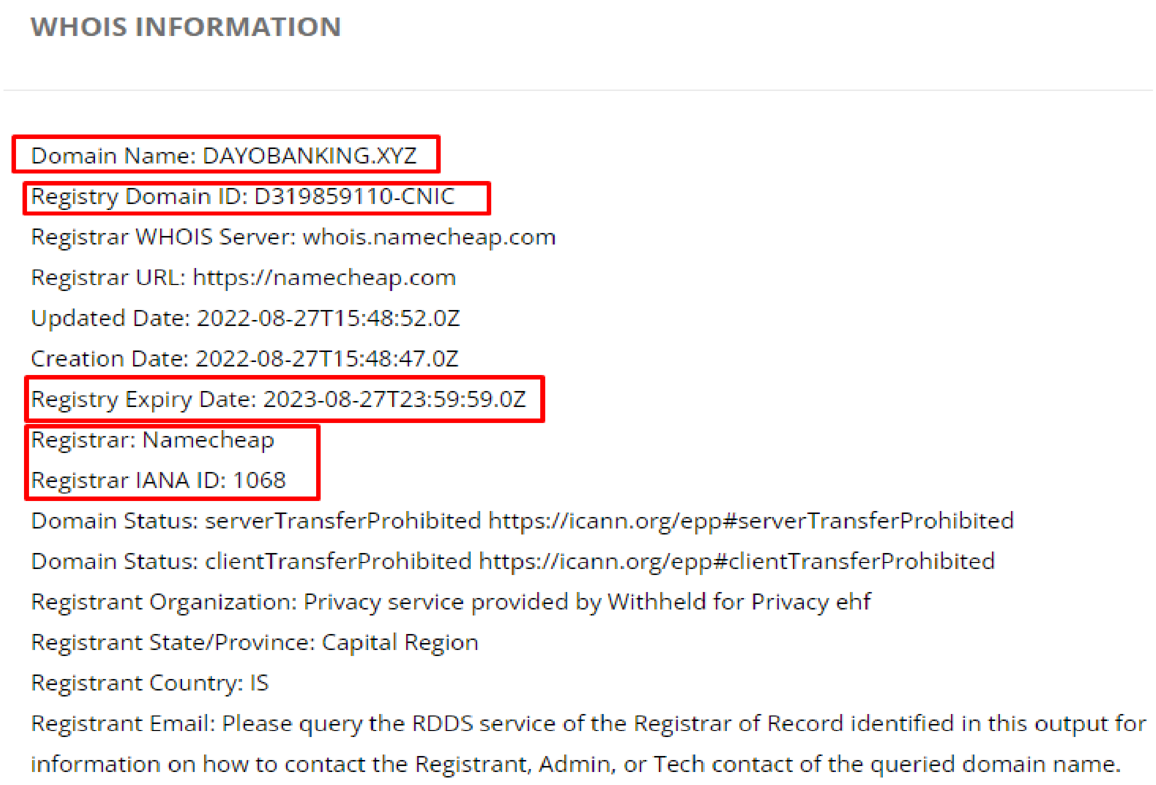


Figure 3.5 Illustration of "WHOIS"

It provides a lot of information such as; domain name, expiry date, registrar and registrar IANA ID as shown in the figure below.



WHOIS INFORMATION

Domain Name: DAYOBANKING.XYZ

Registry Domain ID: D319859110-CNIC

Registrar WHOIS Server: whois.namecheap.com

Registrar URL: https://namecheap.com

Updated Date: 2022-08-27T15:48:52.0Z

Creation Date: 2022-08-27T15:48:47.0Z

Registry Expiry Date: 2023-08-27T23:59:59.0Z

Registrar: Namecheap

Registrar IANA ID: 1068

Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Registrant Organization: Privacy service provided by Withheld for Privacy ehf

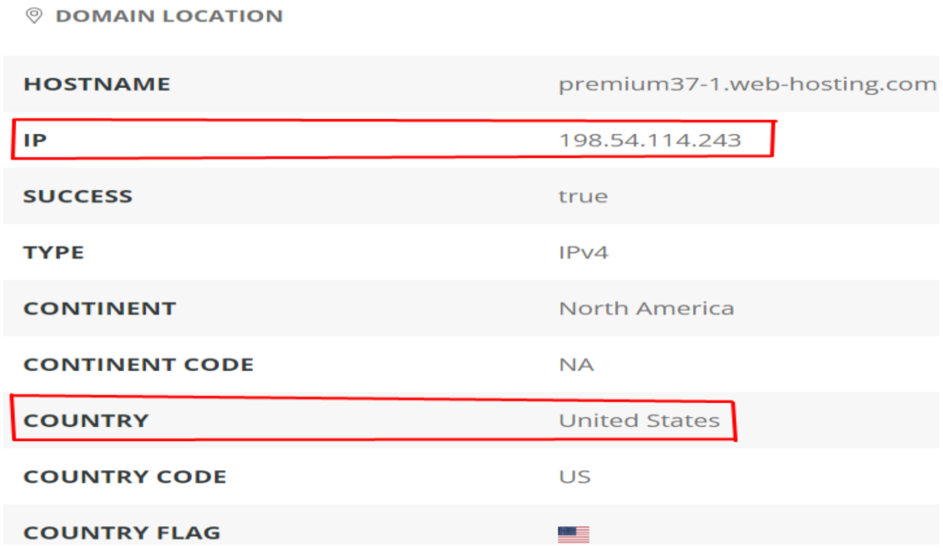
Registrant State/Province: Capital Region

Registrant Country: IS

Registrant Email: Please query the RDDS service of the Registrar of Record identified in this output for information on how to contact the Registrant, Admin, or Tech contact of the queried domain name.

Figure 3.6 Insertion and registration of a domain in "WHOIS"

It also provides the information about the location and IP address as shown in the figures below.

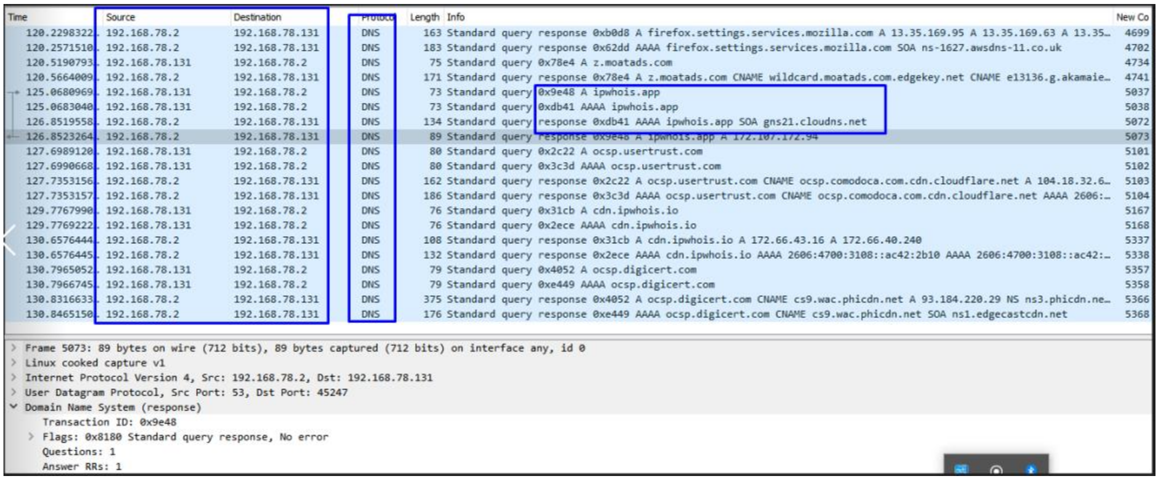


DOMAIN LOCATION

HOSTNAME	premium37-1.web-hosting.com
IP	198.54.114.243
SUCCESS	true
TYPE	IPv4
CONTINENT	North America
CONTINENT CODE	NA
COUNTRY	United States
COUNTRY CODE	US
COUNTRY FLAG	🇺🇸

Figure 3.7 Defining of a domain location in "WHOIS"

At the information gathering phase using WHOIS by capturing the traffic using Wireshark and the traffic is captured as shown in the figure below.



```
Time          Source            Destination       Protoco  Length Info                                                                                              New Co
 120.2298322. 192.168.78.2      192.168.78.131    DNS      163 Standard query response 0xb0d8 A firefox.settings.services.mozilla.com A 13.35.169.95 A 13.35.169.63 A 13.35…  4699
 120.2571510. 192.168.78.2      192.168.78.131    DNS      183 Standard query response 0x62dd AAAA firefox.settings.services.mozilla.com SOA ns-1627.awsdns-11.co.uk          4702
 120.5190793. 192.168.78.131    192.168.78.2      DNS       75 Standard query 0x78e4 A z.moatads.com                                                                         4734
 120.5664009. 192.168.78.2      192.168.78.131    DNS      171 Standard query response 0x78e4 A z.moatads.com CNAME wildcard.moatads.com.edgekey.net CNAME e13136.g.akamaie…  4741
 125.0680969. 192.168.78.131    192.168.78.2      DNS       73 Standard query 0x9e48 A ipwhois.app                                                                           5037
 125.0683040. 192.168.78.131    192.168.78.2      DNS       73 Standard query 0xdb41 AAAA ipwhois.app                                                                        5038
 126.8519558. 192.168.78.2      192.168.78.131    DNS      134 Standard query response 0xdb41 AAAA ipwhois.app SOA gns21.cloudns.net                                        5072
 126.8523264. 192.168.78.2      192.168.78.131    DNS       89 Standard query response 0x9e48 A ipwhois.app A 172.107.172.94                                                 5073
 127.6989120. 192.168.78.131    192.168.78.2      DNS       80 Standard query 0x2c22 A ocsp.usertrust.com                                                                    5101
 127.6990668. 192.168.78.131    192.168.78.2      DNS       80 Standard query 0x3c3d AAAA ocsp.usertrust.com                                                                 5102
 127.7353156. 192.168.78.2      192.168.78.131    DNS      162 Standard query response 0x2c22 A ocsp.usertrust.com CNAME ocsp.comodoca.com.cdn.cloudflare.net A 104.18.32.6…  5103
 127.7353157. 192.168.78.2      192.168.78.131    DNS      186 Standard query response 0x3c3d AAAA ocsp.usertrust.com CNAME ocsp.comodoca.com.cdn.cloudflare.net AAAA 2606:…  5104
 129.7767990. 192.168.78.131    192.168.78.2      DNS       76 Standard query 0x31cb A cdn.ipwhois.io                                                                        5167
 129.7769222. 192.168.78.131    192.168.78.2      DNS       76 Standard query 0x2ece AAAA cdn.ipwhois.io                                                                     5168
 130.6576444. 192.168.78.2      192.168.78.131    DNS      108 Standard query response 0x31cb A cdn.ipwhois.io A 172.66.43.16 A 172.66.40.240                               5337
 130.6576445. 192.168.78.2      192.168.78.131    DNS      132 Standard query response 0x2ece AAAA cdn.ipwhois.io AAAA 2606:4700:3108::ac42:2b10 AAAA 2606:4700:3108::ac42:…  5338
 130.7965052. 192.168.78.131    192.168.78.2      DNS       79 Standard query 0x4052 A ocsp.digicert.com                                                                     5357
 130.7966745. 192.168.78.131    192.168.78.2      DNS       79 Standard query 0xe449 AAAA ocsp.digicert.com                                                                  5358
 130.8316633. 192.168.78.2      192.168.78.131    DNS      375 Standard query response 0x4052 A ocsp.digicert.com CNAME cs9.wac.phicdn.net A 93.184.220.29 NS ns3.phicdn.ne…  5366
 130.8465150. 192.168.78.2      192.168.78.131    DNS      176 Standard query response 0xe449 AAAA ocsp.digicert.com CNAME cs9.wac.phicdn.net SOA ns1.edgecastcdn.net        5368

> Frame 5073: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.2, Dst: 192.168.78.131
> User Datagram Protocol, Src Port: 53, Dst Port: 45247
v Domain Name System (response)
    Transaction ID: 0x9e48
  > Flags: 0x8180 Standard query response, No error
    Questions: 1
    Answer RRs: 1
```

Figure 3.8 Capturing of a traffic of WHOIS using Wireshark

3.2.2 Active Information Gathering

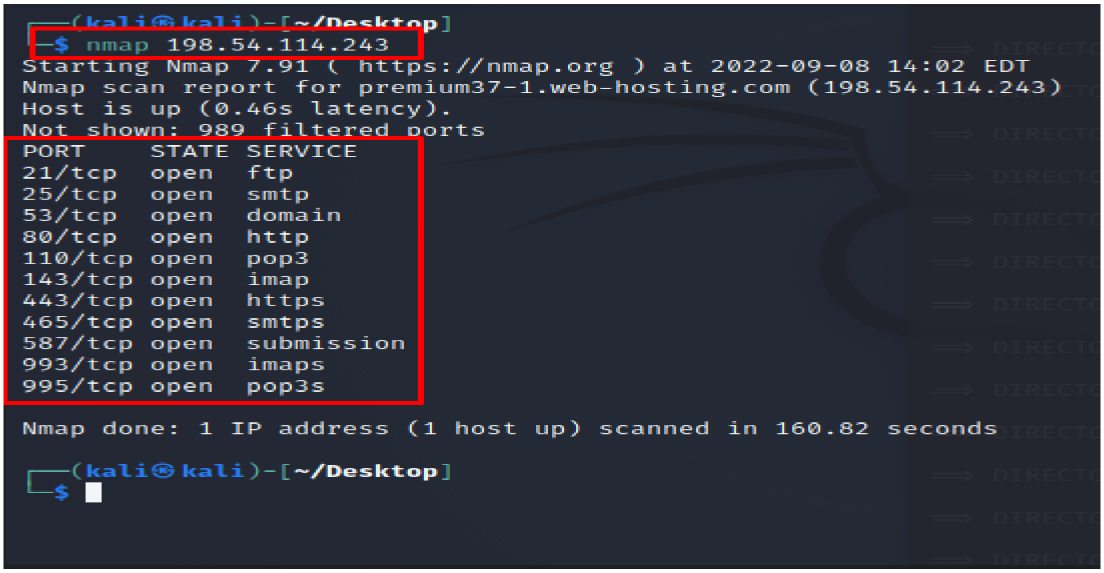
Active information gathering calls for more forethought on the part of the pen tester, as it leaves footprints that may set off alarms in the target system. In this approach, the target organization is actively engaged, increasing the likelihood that it will become aware of the process. At this point, the learning has been made about the available ports, services, program versions, OS version, etc (Shah M., et al., 2019)

3.3 Implementation of Methodology

To do so, the presented methodology for the system that can find website vulnerabilities and exploit these vulnerabilities. Using various tools such as; Dirbuster, Nikto, Nmap curl, ping and Whatweb and then the exploitation can be done using tools such as; burp suite, Wireshark, metasploitable framework and SQL map. Furthermore, the attacks that are performed on the bank website "DayoBanking" includes; Directory Traversal, stealing cookies using burp suite, exploiting FTP vulnerability, exploiting SMTP vulnerability, exploiting HTTP vulnerability, SQL injection attack and cross site scripting attack.

3.3.1 Nmap

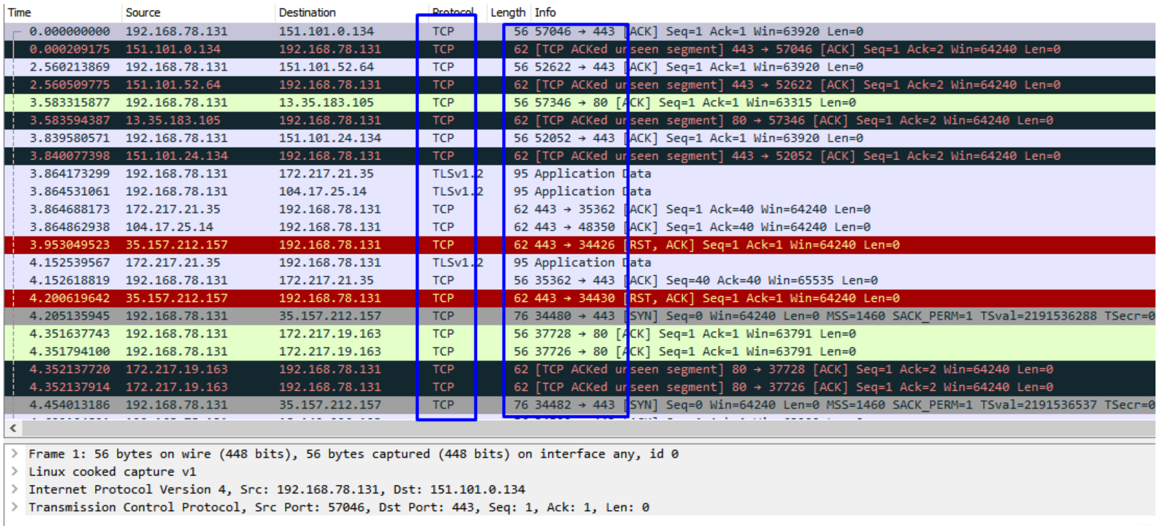
In this step nmap is used to scan for open ports and running services on the target website https://dayobanking.xyz using the IP address "198.54.114.243" as shown in the figure below.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ nmap 198.54.114.243
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-08 14:02 EDT
Nmap scan report for premium37-1.web-hosting.com (198.54.114.243)
Host is up (0.46s latency).
Not shown: 989 filtered ports
PORT     STATE SERVICE
21/tcp   open  ftp
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
110/tcp  open  pop3
143/tcp  open  imap
443/tcp  open  https
465/tcp  open  smtps
587/tcp  open  submission
993/tcp  open  imaps
995/tcp  open  pop3s

Nmap done: 1 IP address (1 host up) scanned in 160.82 seconds

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

Figure 3.9 Nmap a

At the same time the captured traffic is shown in the figure below.

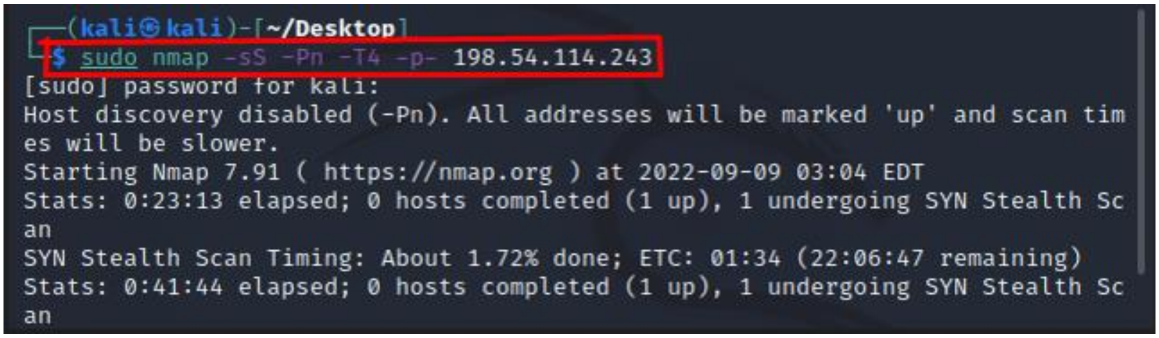


```
Time          Source           Destination      Protocol  Length Info
0.000000000   192.168.78.131   151.101.0.134    TCP       56 57046 → 443 [ACK] Seq=1 Ack=1 Win=63920 Len=0
0.000209175   151.101.0.134    192.168.78.131   TCP       62 [TCP ACKed unseen segment] 443 → 57046 [ACK] Seq=1 Ack=2 Win=64240 Len=0
2.560213869   192.168.78.131   151.101.52.64    TCP       56 52622 → 443 [ACK] Seq=1 Ack=1 Win=63920 Len=0
2.560509775   151.101.52.64    192.168.78.131   TCP       62 [TCP ACKed unseen segment] 443 → 52622 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3.583315877   192.168.78.131   13.35.183.105    TCP       56 57346 → 80 [ACK] Seq=1 Ack=1 Win=63315 Len=0
3.583594387   13.35.183.105    192.168.78.131   TCP       62 [TCP ACKed unseen segment] 80 → 57346 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3.839580571   192.168.78.131   151.101.24.134   TCP       56 52052 → 443 [ACK] Seq=1 Ack=1 Win=63920 Len=0
3.840077398   151.101.24.134   192.168.78.131   TCP       62 [TCP ACKed unseen segment] 443 → 52052 [ACK] Seq=1 Ack=2 Win=64240 Len=0
3.864173299   192.168.78.131   172.217.21.35    TLSv1.2   95 Application Data
3.864531061   192.168.78.131   104.17.25.14     TLSv1.2   95 Application Data
3.864688173   172.217.21.35    192.168.78.131   TCP       62 443 → 35362 [ACK] Seq=1 Ack=40 Win=64240 Len=0
3.864862938   104.17.25.14     192.168.78.131   TCP       62 443 → 48350 [ACK] Seq=1 Ack=40 Win=64240 Len=0
3.953049523   35.157.212.157   192.168.78.131   TCP       62 443 → 34426 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4.152539567   172.217.21.35    192.168.78.131   TLSv1.2   95 Application Data
4.152618819   192.168.78.131   172.217.21.35    TCP       56 35362 → 443 [ACK] Seq=40 Ack=40 Win=65535 Len=0
4.200619642   35.157.212.157   192.168.78.131   TCP       62 443 → 34430 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
4.205135945   192.168.78.131   35.157.212.157   TCP       76 34480 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2191536288 TSecr=0
4.351637743   192.168.78.131   172.217.19.163   TCP       56 37728 → 80 [ACK] Seq=1 Ack=1 Win=63791 Len=0
4.351794100   192.168.78.131   172.217.19.163   TCP       56 37726 → 80 [ACK] Seq=1 Ack=1 Win=63791 Len=0
4.352137720   172.217.19.163   192.168.78.131   TCP       62 [TCP ACKed unseen segment] 80 → 37728 [ACK] Seq=1 Ack=2 Win=64240 Len=0
4.352137914   172.217.19.163   192.168.78.131   TCP       62 [TCP ACKed unseen segment] 80 → 37726 [ACK] Seq=1 Ack=2 Win=64240 Len=0
4.454013186   192.168.78.131   35.157.212.157   TCP       76 34482 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2191536537 TSecr=0

> Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.131, Dst: 151.101.0.134
> Transmission Control Protocol, Src Port: 57046, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
```

Figure 3.10 Nmap Wireshark

3.3.2 TCP SYN Stealth Scan

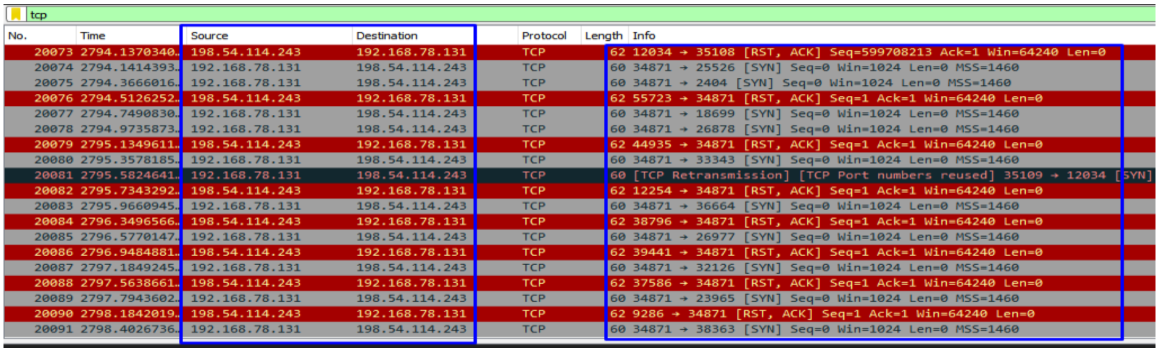
There is a good reason why SYN scan is the default and most preferred choice. Scanning thousands of ports per second is possible over a fast network without the interference of obtrusive firewalls. Since SYN scan never fully establishes TCP connections, it is covert and difficult to detect (Hwang J., et al., 2019). Performing TCP SYN stealth scan by using the command “sudo nmap –sS –Pn –T4 –p- 198.54.114.243” as shown below in the figure.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ sudo nmap -sS -Pn -T4 -p- 198.54.114.243
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan tim
es will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-09-09 03:04 EDT
Stats: 0:23:13 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
SYN Stealth Scan Timing: About 1.72% done; ETC: 01:34 (22:06:47 remaining)
Stats: 0:41:44 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Sc
an
```

Figure 3.11 TCP SYN Stealth Scan

The data captured successfully using Wireshark of the TCP SYN stealth scan. The TCP SYN stealth scan is represented in Wireshark by the [SYN] packet followed by [RST, ACK] as shown in the figure below.



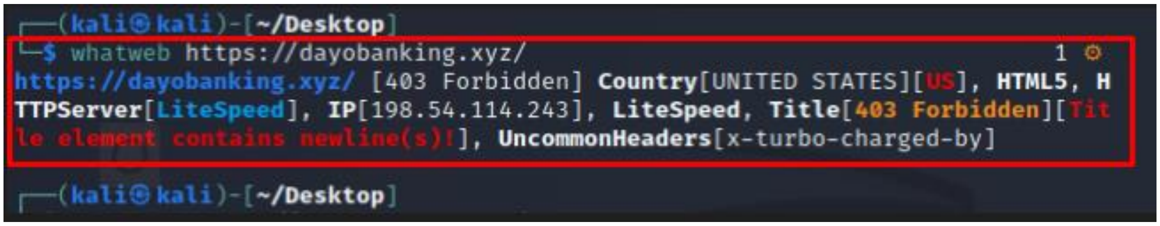
tcp

No.	Time	Source	Destination	Protocol	Length	Info
20073	2794.1370340…	198.54.114.243	192.168.78.131	TCP	62	12034 → 35108 [RST, ACK] Seq=599708213 Ack=1 Win=64240 Len=0
20074	2794.1414393…	192.168.78.131	198.54.114.243	TCP	60	34871 → 25526 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20075	2794.3666016…	192.168.78.131	198.54.114.243	TCP	60	34871 → 2404 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20076	2794.5126252…	198.54.114.243	192.168.78.131	TCP	62	55723 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20077	2794.7490830…	192.168.78.131	198.54.114.243	TCP	60	34871 → 18699 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20078	2794.9735873…	192.168.78.131	198.54.114.243	TCP	60	34871 → 26878 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20079	2795.1349611…	198.54.114.243	192.168.78.131	TCP	62	44935 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20080	2795.3578185…	192.168.78.131	198.54.114.243	TCP	60	34871 → 33343 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20081	2795.5824641…	192.168.78.131	198.54.114.243	TCP	60	[TCP Retransmission] [TCP Port numbers reused] 35109 → 12034 [SYN]
20082	2795.7343292…	198.54.114.243	192.168.78.131	TCP	62	12254 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20083	2795.9660945…	192.168.78.131	198.54.114.243	TCP	60	34871 → 36664 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20084	2796.3496566…	198.54.114.243	192.168.78.131	TCP	62	38796 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20085	2796.5770147…	192.168.78.131	198.54.114.243	TCP	60	34871 → 26977 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20086	2796.9484881…	198.54.114.243	192.168.78.131	TCP	62	39441 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20087	2797.1849245…	192.168.78.131	198.54.114.243	TCP	60	34871 → 32126 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20088	2797.5638661…	198.54.114.243	192.168.78.131	TCP	62	37586 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20089	2797.7943602…	192.168.78.131	198.54.114.243	TCP	60	34871 → 23965 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20090	2798.1842019…	198.54.114.243	192.168.78.131	TCP	62	9286 → 34871 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
20091	2798.4026736…	192.168.78.131	198.54.114.243	TCP	60	34871 → 38363 [SYN] Seq=0 Win=1024 Len=0 MSS=1460

Figure 3.12 TCP SYN Stealth Scan Wireshark

3.3.3 Whatweb

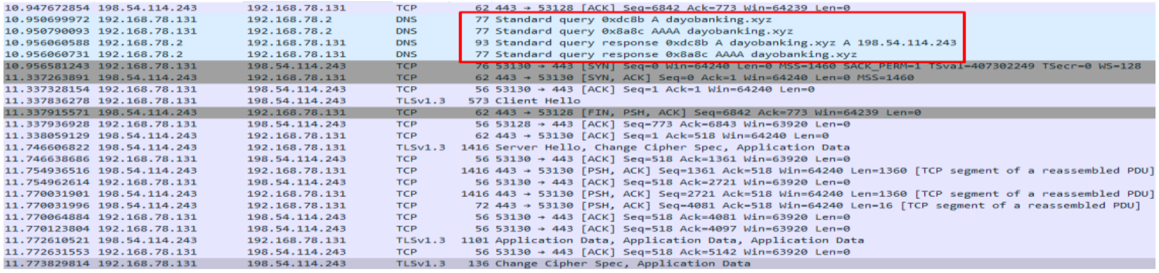
In this section whatweb will be used to find the running web server using the command "whatweb https://dayobanking.xyz/" and it return me the information of the website as shown below in the figure.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ whatweb https://dayobanking.xyz/                                        1
https://dayobanking.xyz/ [403 Forbidden] Country[UNITED STATES][US], HTML5, H
TTPServer[LiteSpeed], IP[198.54.114.243], LiteSpeed, Title[403 Forbidden][Tit
le element contains newline(s)!], UncommonHeaders[x-turbo-charged-by]

┌──(kali㉿kali)-[~/Desktop]
```

Figure 3.13 Illustration of Whatweb

The traffic is captured in Wireshark and it show that the host ask from the local DNS server to tell what is the IP address of https://dayobanking.xyz as shown the figure below.

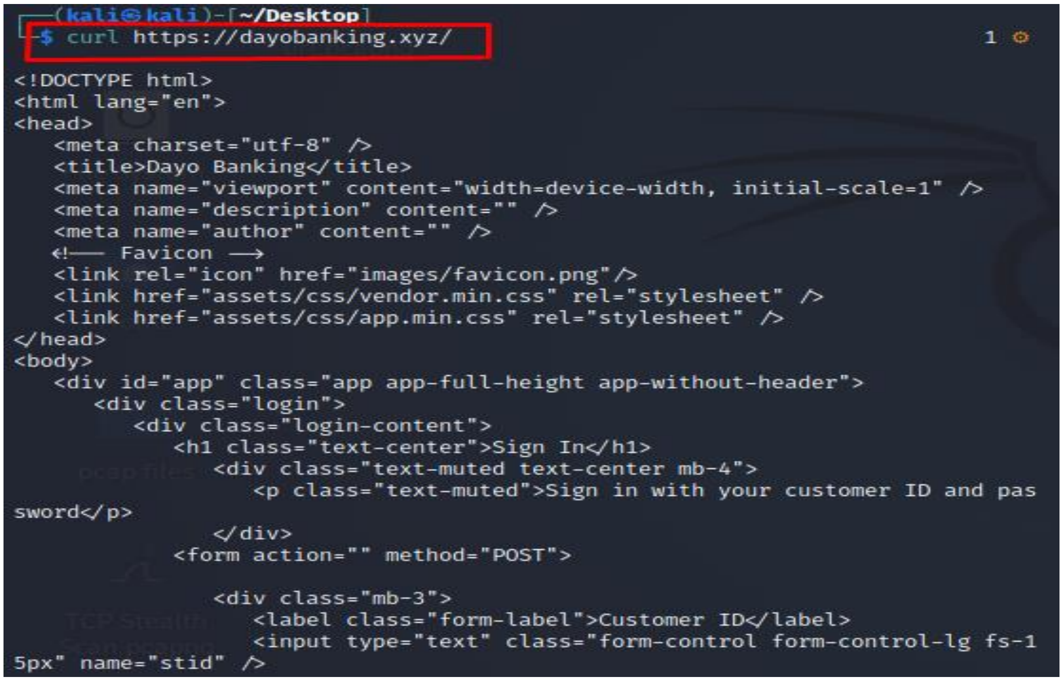


```
10.947672854 198.54.114.243  192.168.78.131  TCP        62 443 → 53128 [ACK] Seq=6842 Ack=773 Win=64239 Len=0
10.950699972 192.168.78.131  192.168.78.2    DNS        77 Standard query 0xdc8b A dayobanking.xyz
10.950790093 192.168.78.131  192.168.78.2    DNS        77 Standard query 0x8a8c AAAA dayobanking.xyz
10.956060588 192.168.78.2    192.168.78.131  DNS        93 Standard query response 0xdc8b A dayobanking.xyz A 198.54.114.243
10.956060731 192.168.78.2    192.168.78.131  DNS        77 Standard query response 0x8a8c AAAA dayobanking.xyz
10.956581243 192.168.78.131  198.54.114.243  TCP        76 53130 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=407302249 TSecr=0 WS=128
11.337263891 198.54.114.243  192.168.78.131  TCP        62 443 → 53130 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
11.337328154 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=1 Ack=1 Win=64240 Len=0
11.337836278 192.168.78.131  198.54.114.243  TLSv1.3   573 Client Hello
11.337915571 198.54.114.243  192.168.78.131  TCP        62 443 → 53128 [FIN, PSH, ACK] Seq=6842 Ack=773 Win=64239 Len=0
11.337936928 192.168.78.131  198.54.114.243  TCP        56 53128 → 443 [ACK] Seq=773 Ack=6843 Win=63920 Len=0
11.338059129 198.54.114.243  192.168.78.131  TCP        62 443 → 53130 [ACK] Seq=1 Ack=518 Win=64240 Len=0
11.746606822 198.54.114.243  192.168.78.131  TLSv1.3  1416 Server Hello, Change Cipher Spec, Application Data
11.746638686 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=518 Ack=1361 Win=63920 Len=0
11.754936516 198.54.114.243  192.168.78.131  TCP      1416 443 → 53130 [PSH, ACK] Seq=1361 Ack=518 Win=64240 Len=1360 [TCP segment of a reassembled PDU]
11.754962614 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=518 Ack=2721 Win=63920 Len=0
11.770031901 198.54.114.243  192.168.78.131  TCP      1416 443 → 53130 [PSH, ACK] Seq=2721 Ack=518 Win=64240 Len=1360 [TCP segment of a reassembled PDU]
11.770031996 198.54.114.243  192.168.78.131  TCP        72 443 → 53130 [PSH, ACK] Seq=4081 Ack=518 Win=64240 Len=16 [TCP segment of a reassembled PDU]
11.770064884 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=518 Ack=4081 Win=63920 Len=0
11.770123804 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=518 Ack=4097 Win=63920 Len=0
11.772610521 198.54.114.243  192.168.78.131  TLSv1.3  1101 Application Data, Application Data, Application Data
11.772631553 192.168.78.131  198.54.114.243  TCP        56 53130 → 443 [ACK] Seq=518 Ack=5142 Win=63920 Len=0
11.773829814 192.168.78.131  198.54.114.243  TLSv1.3   136 Change Cipher Spec, Application Data
```

Figure 3.14 Whatweb's traffic capture using Wireshark

3.3.4 Curl

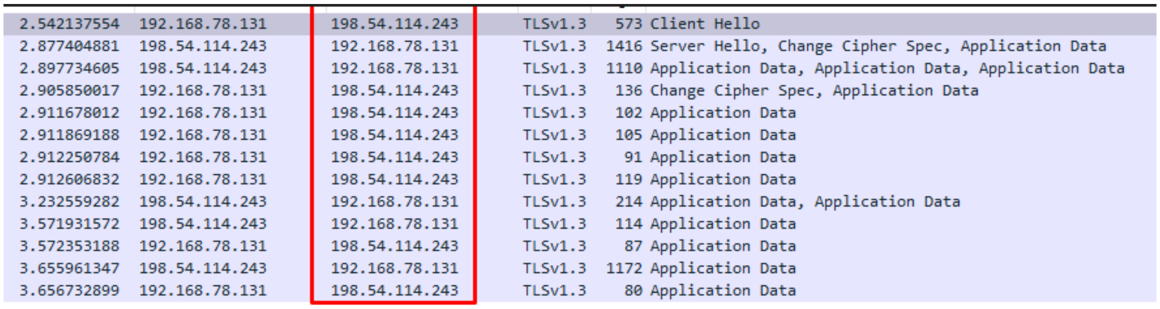
Using curl tool to show whether the website display the source code or not and it displays the source code as shown in the figure below.



```
┌──(kali㉿kali)-[~/Desktop]
└─$ curl https://dayobanking.xyz/                                    1 ⚙

<!DOCTYPE html>
<html lang="en">
<head>
   <meta charset="utf-8" />
   <title>Dayo Banking</title>
   <meta name="viewport" content="width=device-width, initial-scale=1" />
   <meta name="description" content="" />
   <meta name="author" content="" />
   <!-- Favicon -->
   <link rel="icon" href="images/favicon.png"/>
   <link href="assets/css/vendor.min.css" rel="stylesheet" />
   <link href="assets/css/app.min.css" rel="stylesheet" />
</head>
<body>
   <div id="app" class="app app-full-height app-without-header">
      <div class="login">
         <div class="login-content">
            <h1 class="text-center">Sign In</h1>
               <div class="text-muted text-center mb-4">
                  <p class="text-muted">Sign in with your customer ID and pas
sword</p>
               </div>
            <form action="" method="POST">

               <div class="mb-3">
                  <label class="form-label">Customer ID</label>
                  <input type="text" class="form-control form-control-lg fs-1
5px" name="stid" />
```

Figure 3.15 Illustration of Curl

The traffic is captured using Wireshark and all the data is tls encrypted because the website uses https as shown in the figure below.



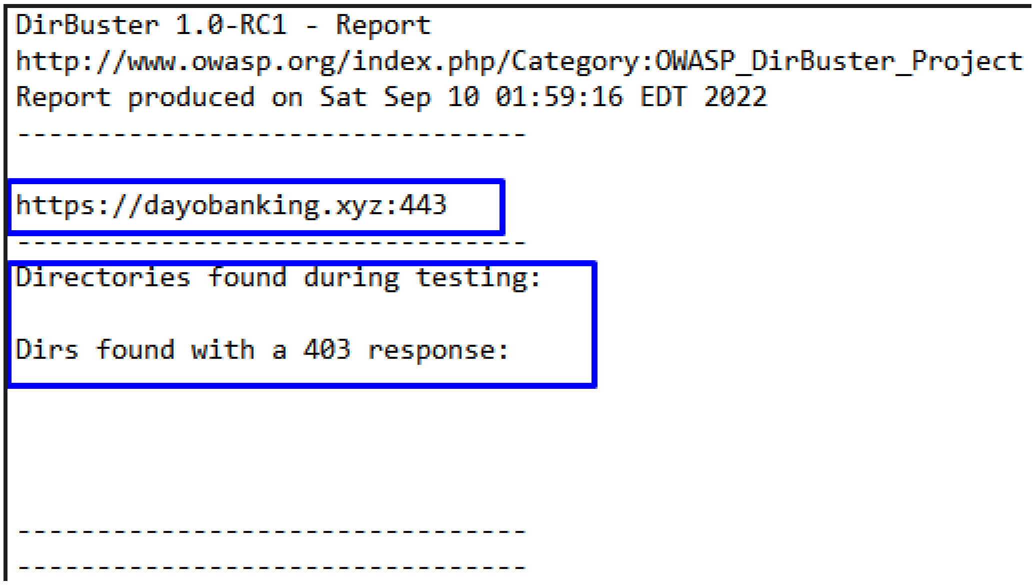
```
2.542137554  192.168.78.131  198.54.114.243  TLSv1.3   573 Client Hello
2.877404881  198.54.114.243  192.168.78.131  TLSv1.3  1416 Server Hello, Change Cipher Spec, Application Data
2.897734605  198.54.114.243  192.168.78.131  TLSv1.3  1110 Application Data, Application Data, Application Data
2.905850017  192.168.78.131  198.54.114.243  TLSv1.3   136 Change Cipher Spec, Application Data
2.911678012  192.168.78.131  198.54.114.243  TLSv1.3   102 Application Data
2.911869188  192.168.78.131  198.54.114.243  TLSv1.3   105 Application Data
2.912250784  192.168.78.131  198.54.114.243  TLSv1.3    91 Application Data
2.912606832  192.168.78.131  198.54.114.243  TLSv1.3   119 Application Data
3.232559282  198.54.114.243  192.168.78.131  TLSv1.3   214 Application Data, Application Data
3.571931572  198.54.114.243  192.168.78.131  TLSv1.3   114 Application Data
3.572353188  192.168.78.131  198.54.114.243  TLSv1.3    87 Application Data
3.655961347  198.54.114.243  192.168.78.131  TLSv1.3  1172 Application Data
3.656732899  192.168.78.131  198.54.114.243  TLSv1.3    80 Application Data
```

Figure 3.16 Curl's traffic capture using Wireshark

3.3.5 DirBuster

DirBuster is a multi-threaded Java program that can be used to try to guess the names of directories and files stored on web and application servers. Nowadays, it is not uncommon for a web server to appear to be in its default installation condition when, in fact, it hosts additional pages and apps

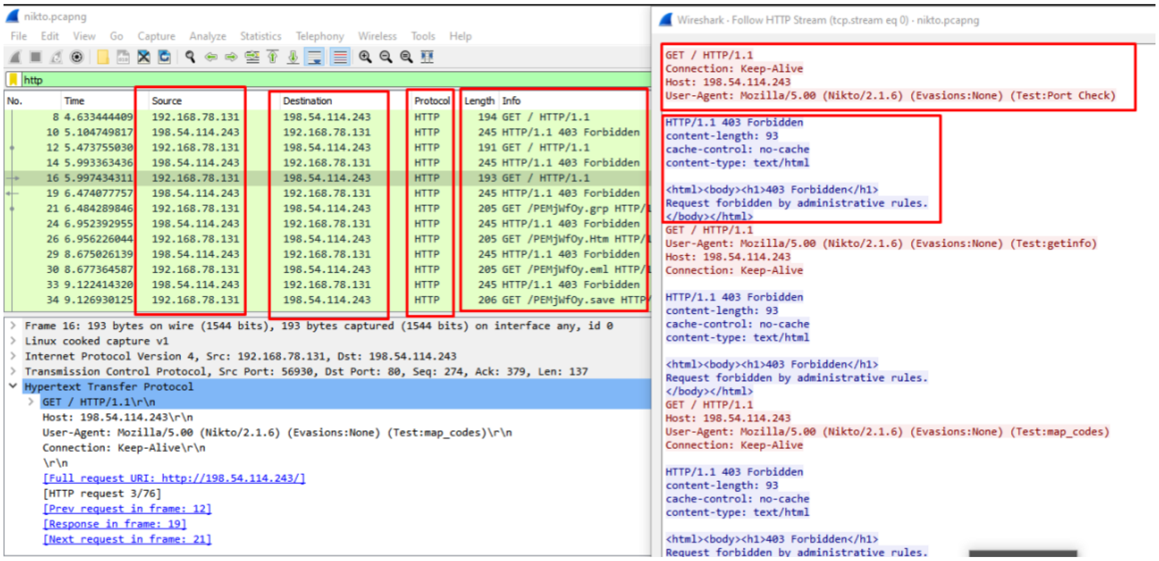
(Ijams C., 2021). With DirBuster, the task of locating the web server vulnerabilities has been made. By using the command “dirb https://dayobanking.xyz” in kali Linux and it show me the result as shown in the below figure.



```
DirBuster 1.0-RC1 - Report
http://www.owasp.org/index.php/Category:OWASP_DirBuster_Project
Report produced on Sat Sep 10 01:59:16 EDT 2022
--------------------------------

https://dayobanking.xyz:443
--------------------------------
Directories found during testing:

Dirs found with a 403 response:




--------------------------------
--------------------------------
```

Figure 3.17 Illustration of DirBuster’s results

The traffic is captured using Wireshark and all the directories respond with a http code 403 and 404 as shown in the figure below.



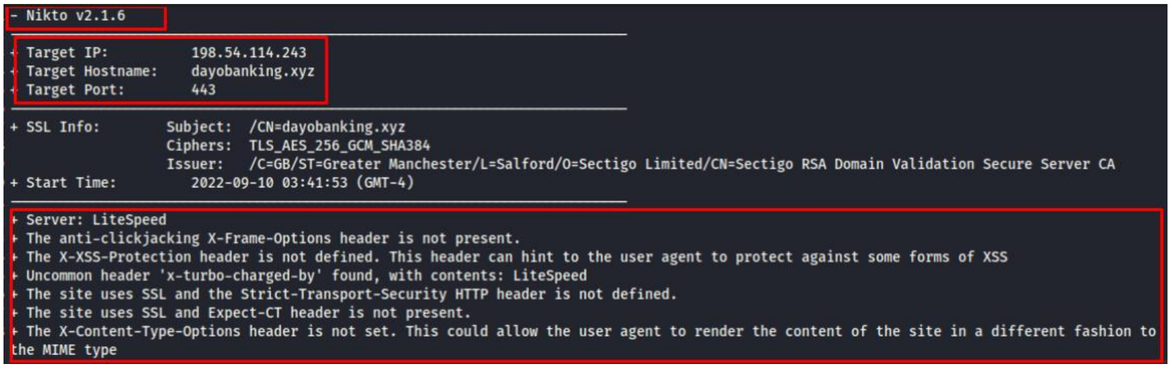
```
No.  Time         Source          Destination     Protocol Length Info
   8 4.633444409  192.168.78.131  198.54.114.243  HTTP      194 GET / HTTP/1.1
  10 5.104749817  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  12 5.473755030  192.168.78.131  198.54.114.243  HTTP      191 GET / HTTP/1.1
  14 5.993363436  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  16 5.997434311  192.168.78.131  198.54.114.243  HTTP      193 GET / HTTP/1.1
  19 6.474077757  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  21 6.484289846  192.168.78.131  198.54.114.243  HTTP      205 GET /PEMjWfOy.grp HTTP/1
  24 6.952392955  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  26 6.956226044  192.168.78.131  198.54.114.243  HTTP      205 GET /PEMjWfOy.Htm HTTP/1
  29 8.675026139  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  30 8.677364587  192.168.78.131  198.54.114.243  HTTP      205 GET /PEMjWfOy.eml HTTP/1
  33 9.122414320  198.54.114.243  192.168.78.131  HTTP      245 HTTP/1.1 403 Forbidden
  34 9.126930125  192.168.78.131  198.54.114.243  HTTP      206 GET /PEMjWfOy.save HTTP/

> Frame 16: 193 bytes on wire (1544 bits), 193 bytes captured (1544 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.131, Dst: 198.54.114.243
> Transmission Control Protocol, Src Port: 56930, Dst Port: 80, Seq: 274, Ack: 379, Len: 137
v Hypertext Transfer Protocol
  > GET / HTTP/1.1\r\n
    Host: 198.54.114.243\r\n
    User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)\r\n
    Connection: Keep-Alive\r\n
    \r\n
    [Full request URI: http://198.54.114.243/]
    [HTTP request 3/76]
    [Prev request in frame: 12]
    [Response in frame: 19]
    [Next request in frame: 21]
```

```
GET / HTTP/1.1
Connection: Keep-Alive
Host: 198.54.114.243
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:Port Check)

HTTP/1.1 403 Forbidden
content-length: 93
cache-control: no-cache
content-type: text/html

<html><body><h1>403 Forbidden</h1>
Request forbidden by administrative rules.
</body></html>
GET / HTTP/1.1
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:getinfo)
Host: 198.54.114.243
Connection: Keep-Alive

HTTP/1.1 403 Forbidden
content-length: 93
cache-control: no-cache
content-type: text/html

<html><body><h1>403 Forbidden</h1>
Request forbidden by administrative rules.
</body></html>
GET / HTTP/1.1
Host: 198.54.114.243
User-Agent: Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)
Connection: Keep-Alive

HTTP/1.1 403 Forbidden
content-length: 93
cache-control: no-cache
content-type: text/html

<html><body><h1>403 Forbidden</h1>
Request forbidden by administrative rules.
```

Figure 3.18 DirBuster’s traffic capture using Wireshark

3.3.6 Nikto

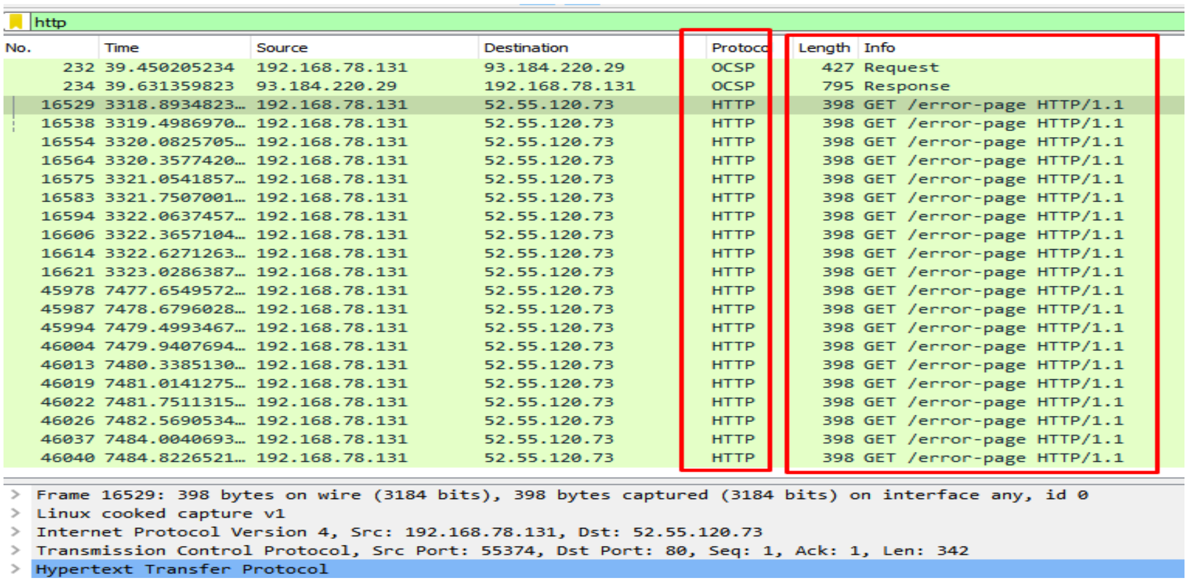
Nikto is a vulnerability scanner that scans web servers for exploitable software defects, such as malicious files/CGIs and out-of-date server software. Nikto is a free, open-source, command-line vulnerability scanner. It examines servers in both general and specific ways during the testing process. Every cookie that is accepted is recorded, and a copy of the log is also printed (Rawat S., et al., 2020). By using the command "nikto https://dayobanking.xyz" and it scan the website for vulnerabilities which include Anti-clickjacking and Cross site scripting etc. as shown in the figure below.



```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          198.54.114.243
+ Target Hostname:    dayobanking.xyz
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=dayobanking.xyz
                   Ciphers:  TLS_AES_256_GCM_SHA384
                   Issuer:   /C=GB/ST=Greater Manchester/L=Salford/O=Sectigo Limited/CN=Sectigo RSA Domain Validation Secure Server CA
+ Start Time:         2022-09-10 03:41:53 (GMT-4)
---------------------------------------------------------------------------
+ Server: LiteSpeed
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-turbo-charged-by' found, with contents: LiteSpeed
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to
the MIME type
```

Figure 3.19 Nikto operational board

In Wireshark by applying a filter "http" to filter all the http packets and it shows that each HTTP GET request has an error as shown in the figure below.



```
http
No.     Time             Source            Destination       Protoco  Length Info
    232 39.450205234     192.168.78.131    93.184.220.29     OCSP        427 Request
    234 39.631359823     93.184.220.29     192.168.78.131    OCSP        795 Response
  16529 3318.8934823…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16538 3319.4986970…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16554 3320.0825705…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16564 3320.3577420…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16575 3321.0541857…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16583 3321.7507001…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16594 3322.0637457…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16606 3322.3657104…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16614 3322.6271263…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  16621 3323.0286387…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  45978 7477.6549572…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  45987 7478.6796028…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  45994 7479.4993467…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46004 7479.9407694…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46013 7480.3385130…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46019 7481.0141275…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46022 7481.7511315…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46026 7482.5690534…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46037 7484.0040693…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1
  46040 7484.8226521…    192.168.78.131    52.55.120.73      HTTP        398 GET /error-page HTTP/1.1

> Frame 16529: 398 bytes on wire (3184 bits), 398 bytes captured (3184 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.131, Dst: 52.55.120.73
> Transmission Control Protocol, Src Port: 55374, Dst Port: 80, Seq: 1, Ack: 1, Len: 342
> Hypertext Transfer Protocol
```

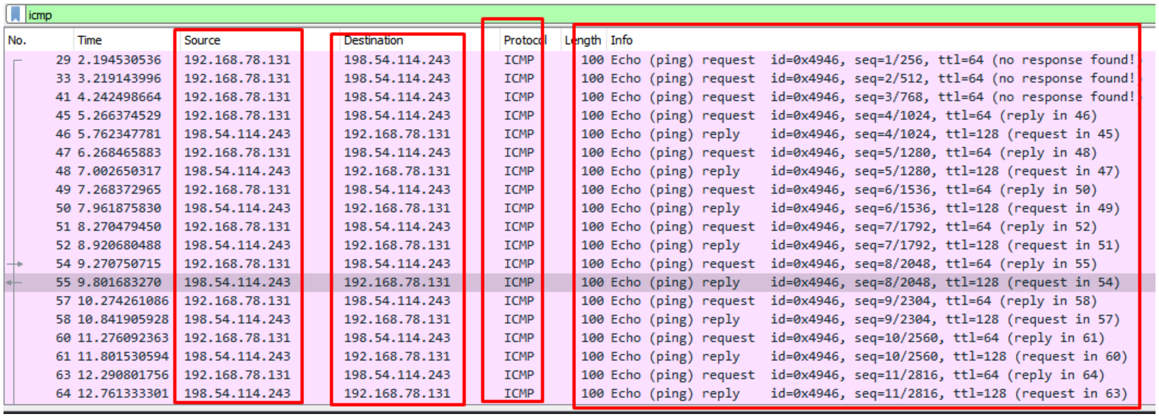
Figure 3.20 Wireshark usage in Nikto

3.3.7 Ping

Ping is a command-line application that serves as a test to determine whether or not a networked device is reachable. Ping is available on practically all operating systems that are capable of connecting to a network.

The ping command causes a query to be transmitted across the network to a certain device. A successful ping will result in a response being sent back to the computer that initiated the ping from the computer that was pinged (Saundatikar R., et al., 2021).

By using the command "ping 198.54.114.243" to send a ping request to the target and the target responded with a ping reply as shown the figure below.



```
icmp
No.   Time           Source           Destination      Protocol  Length  Info
   29 2.194530536    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=1/256, ttl=64 (no response found!
   33 3.219143996    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=2/512, ttl=64 (no response found!
   41 4.242498664    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=3/768, ttl=64 (no response found!
   45 5.266374529    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=4/1024, ttl=64 (reply in 46)
   46 5.762347781    198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=4/1024, ttl=128 (request in 45)
   47 6.268465883    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=5/1280, ttl=64 (reply in 48)
   48 7.002650317    198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=5/1280, ttl=128 (request in 47)
   49 7.268372965    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=6/1536, ttl=64 (reply in 50)
   50 7.961875830    198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=6/1536, ttl=128 (request in 49)
   51 8.270479450    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=7/1792, ttl=64 (reply in 52)
   52 8.920680488    198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=7/1792, ttl=128 (request in 51)
   54 9.270750715    192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=8/2048, ttl=64 (reply in 55)
   55 9.801683270    198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=8/2048, ttl=128 (request in 54)
   57 10.274261086   192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=9/2304, ttl=64 (reply in 58)
   58 10.841905928   198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=9/2304, ttl=128 (request in 57)
   60 11.276092363   192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=10/2560, ttl=64 (reply in 61)
   61 11.801530594   198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=10/2560, ttl=128 (request in 60)
   63 12.290801756   192.168.78.131   198.54.114.243   ICMP      100 Echo (ping) request  id=0x4946, seq=11/2816, ttl=64 (reply in 64)
   64 12.761333301   198.54.114.243   192.168.78.131   ICMP      100 Echo (ping) reply    id=0x4946, seq=11/2816, ttl=128 (request in 63)
```

Figure 3.21 Ping's testing through Wireshark

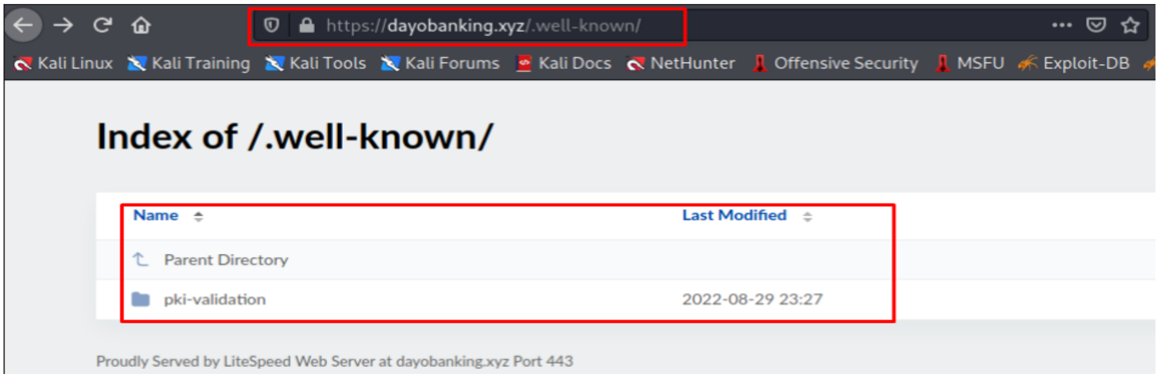
3.2 Vulnerable Exploitation

During this phase, the system will be broken into the essential steps or or access a resource by whatever means necessary. If the vulnerability analysis step came before, this one should go smoothly and with pinpoint accuracy. The primary objective is to pinpoint the primary point of entry and to pinpoint high-value target assets.

A high-value target list should have been compiled if the vulnerability analysis process had been carried out correctly. The assault vector should be chosen based on its likelihood of success and potential damage to the organization (Ge D., et al., 2022).

3.2.1 Directory Traversal

An attacker can access any file on the server the program is executing on by exploiting a web security flaw called directory traversal, or file path traversal. Possible examples include private operating system files, credentials for back-end systems, and application data. An attacker might potentially gain complete control of the server if he or she could alter application data or behavior via arbitrary file writing (Prasad K. S., et al., 2018). From the results of dirbuster it is clear that one directory is present and is not prevented as shown in the figures below.



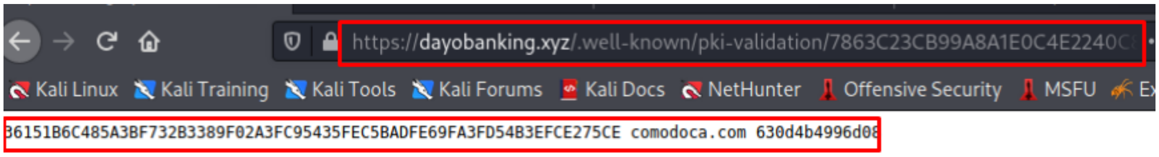
https://dayobanking.xyz/.well-known/

Index of /.well-known/

Name	Last Modified
Parent Directory	
pki-validation	2022-08-29 23:27

Proudly Served by LiteSpeed Web Server at dayobanking.xyz Port 443

Figure 3.22 Directory Traversal a

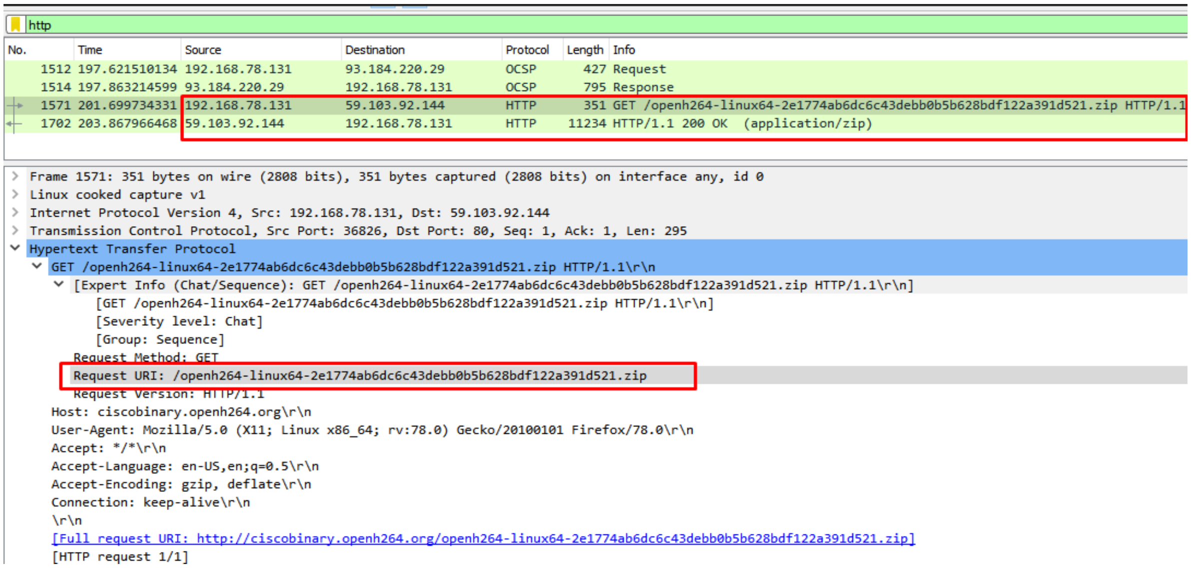


https://dayobanking.xyz/.well-known/pki-validation/7863C23CB99A8A1E0C4E2240C

```
36151B6C485A3BF732B3389F02A3FC95435FEC5BADFE69FA3FD54B3EFCE275CE comodoca.com 630d4b4996d08
```

Figure 3.23 Directory Traversal b

In Wireshark this attack is captured as shown in the below figure.



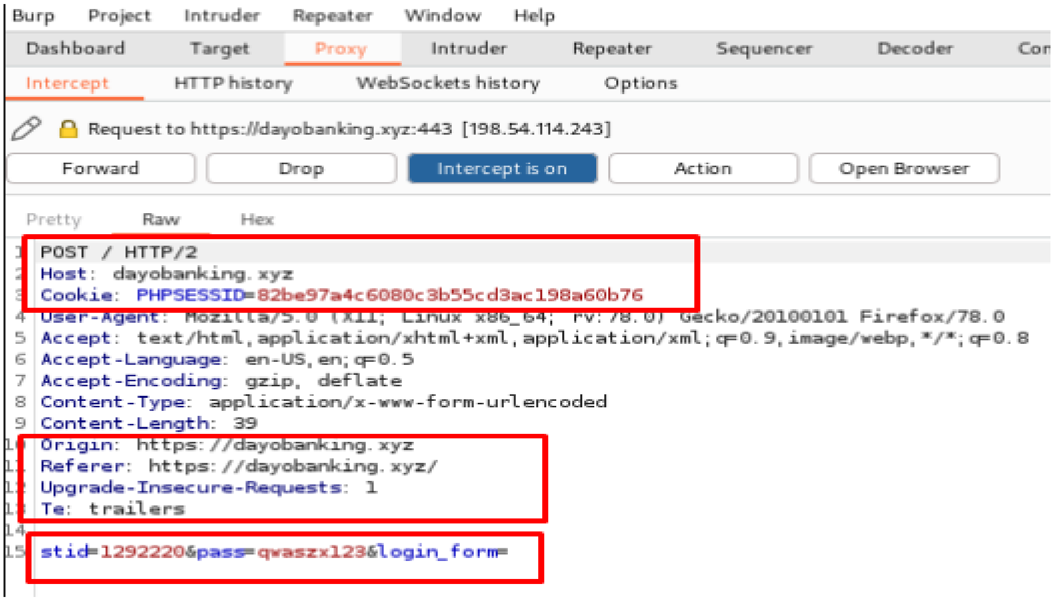
```
No.   Time          Source          Destination    Protocol Length Info
 1512 197.621510134 192.168.78.131  93.184.220.29  OCSP       427 Request
 1514 197.863214599 93.184.220.29   192.168.78.131 OCSP       795 Response
 1571 201.699734331 192.168.78.131  59.103.92.144  HTTP       351 GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1
 1702 203.867966468 59.103.92.144   192.168.78.131 HTTP     11234 HTTP/1.1 200 OK  (application/zip)
```

```
> Frame 1571: 351 bytes on wire (2808 bits), 351 bytes captured (2808 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.131, Dst: 59.103.92.144
> Transmission Control Protocol, Src Port: 36826, Dst Port: 80, Seq: 1, Ack: 1, Len: 295
v Hypertext Transfer Protocol
  v GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1\r\n
    v [Expert Info (Chat/Sequence): GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1\r\n]
        [GET /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip HTTP/1.1\r\n]
        [Severity level: Chat]
        [Group: Sequence]
      Request Method: GET
      Request URI: /openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip
      Request Version: HTTP/1.1
    Host: ciscobinary.openh264.org\r\n
    User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: */*\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    Connection: keep-alive\r\n
    \r\n
    [Full request URI: http://ciscobinary.openh264.org/openh264-linux64-2e1774ab6dc6c43debb0b5b628bdf122a391d521.zip]
    [HTTP request 1/1]
```

Figure 3.24 Directory Traversal Wireshark

3.2.2 Burpsuite

The Burp Suite is an integrated platform that may be used to verify the safety of web applications. Its many tools map and analyze an application's attack surface, detect, and exploit security flaws, and provide support for the full testing process thanks to their seamless integration with one another and their ability to work together to support it (Kim, J., 2020)



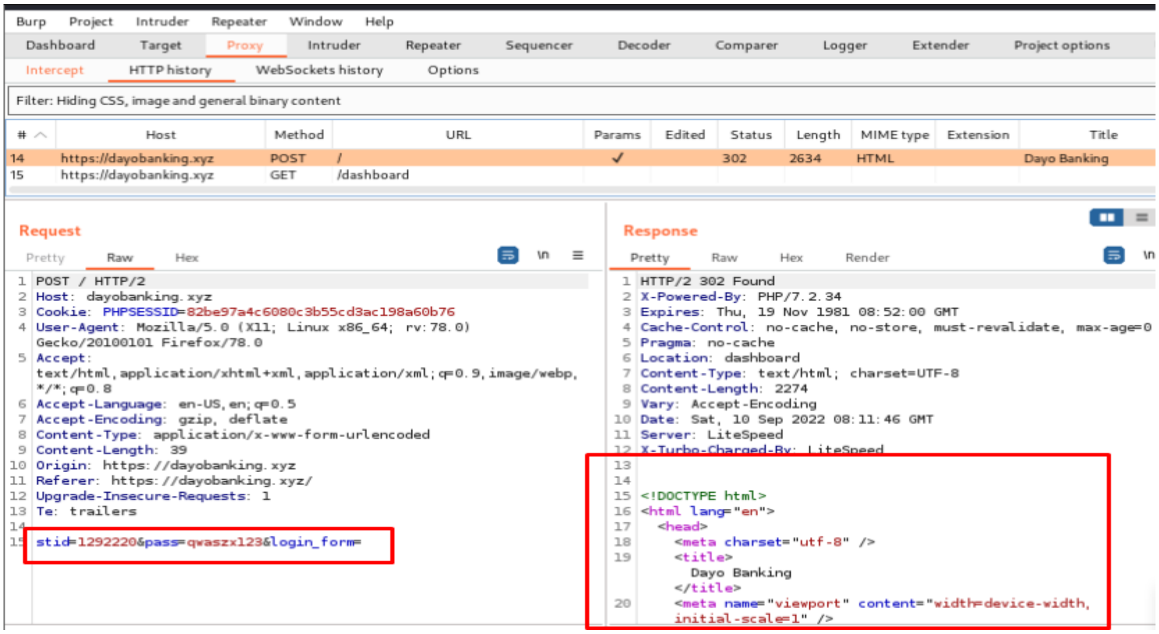
Request to https://dayobanking.xyz:443 [198.54.114.243]

```
POST / HTTP/2
Host: dayobanking.xyz
Cookie: PHPSESSID=82be97a4c6080c3b55cd3ac198a60b76
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: https://dayobanking.xyz
Referer: https://dayobanking.xyz/
Upgrade-Insecure-Requests: 1
Te: trailers

stid=1292220&pass=qwaszx123&login_form=
```

Figure 3.25 Burpsuite a

By using the proxy named “FoxyProxy” in the web browser and then configure FoxyProxy for burpsuite. On the intercept in burpsuite and then visit the website and capture the packets in burpsuite. It displays all the information such as; HTTP request type, host, cookie, user agent, referrer and origin as shown in the figure below.

Burpsuite also show the username, password and the source code of the visited page as shown in the figure below.


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options
Intercept HTTP history WebSockets history Options
Pretty Raw Hex
Pretty Raw Hex Render

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title
14	https://dayobanking.xyz	POST	/	✓		302	2634	HTML		Dayo Banking
15	https://dayobanking.xyz	GET	/dashboard							

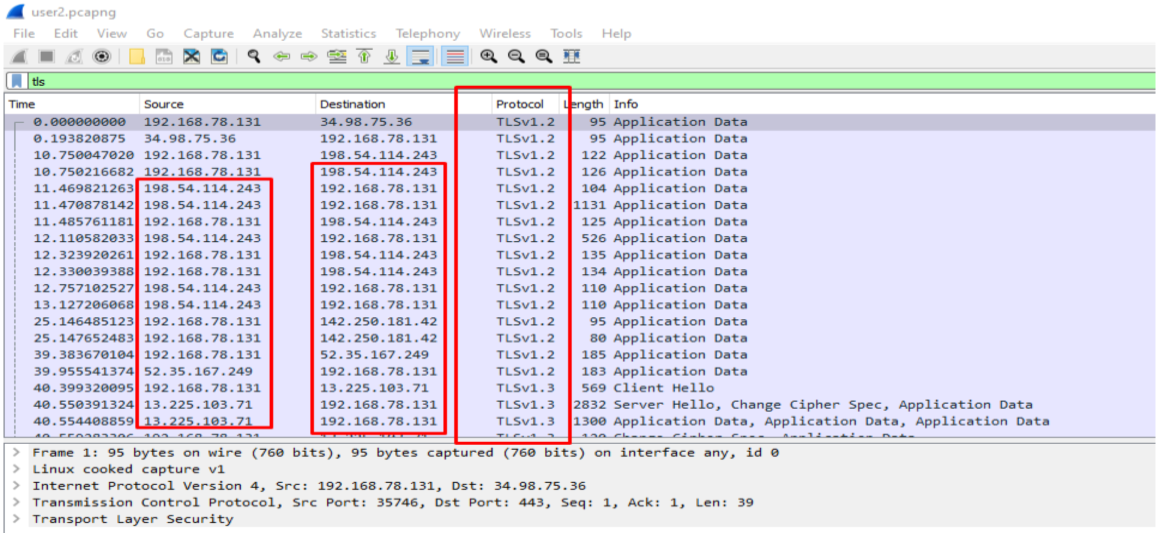
Request

```
POST / HTTP/2
Host: dayobanking.xyz
Cookie: PHPSESSID=82be97a4c6080c3b55cd3ac198a60b76
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,
*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 39
Origin: https://dayobanking.xyz
Referer: https://dayobanking.xyz/
Upgrade-Insecure-Requests: 1
Te: trailers

stid=1292220&pass=qwaszx123&login_form=
```

Response

```
HTTP/2 302 Found
X-Powered-By: PHP/7.2.34
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-cache, no-store, must-revalidate, max-age=0
Pragma: no-cache
Location: dashboard
Content-Type: text/html; charset=UTF-8
Content-Length: 2274
Vary: Accept-Encoding
Date: Sat, 10 Sep 2022 08:11:46 GMT
Server: LiteSpeed
X-Turbo-Charged-By: LiteSpeed


<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="utf-8" />
    <title>
      Dayo Banking
    </title>
    <meta name="viewport" content="width=device-width,
    initial-scale=1" />
```

Figure 3.26 Burpsuite b


user2.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tls
Time          Source          Destination     Protocol Length Info
0.000000000   192.168.78.131  34.98.75.36     TLSv1.2    95 Application Data
0.193820875   34.98.75.36     192.168.78.131  TLSv1.2    95 Application Data
10.750047020  192.168.78.131  198.54.114.243  TLSv1.2   122 Application Data
10.750216682  192.168.78.131  198.54.114.243  TLSv1.2   126 Application Data
11.469821263  198.54.114.243  192.168.78.131  TLSv1.2   104 Application Data
11.470878142  198.54.114.243  192.168.78.131  TLSv1.2  1131 Application Data
11.485761181  192.168.78.131  198.54.114.243  TLSv1.2   125 Application Data
12.110582033  198.54.114.243  192.168.78.131  TLSv1.2   526 Application Data
12.323920261  192.168.78.131  198.54.114.243  TLSv1.2   135 Application Data
12.330039388  192.168.78.131  198.54.114.243  TLSv1.2   134 Application Data
12.757102527  198.54.114.243  192.168.78.131  TLSv1.2   110 Application Data
13.127206068  198.54.114.243  192.168.78.131  TLSv1.2   110 Application Data
25.146485123  192.168.78.131  142.250.181.42  TLSv1.2    95 Application Data
25.147652483  192.168.78.131  142.250.181.42  TLSv1.2    80 Application Data
39.383670104  192.168.78.131  52.35.167.249   TLSv1.2   185 Application Data
39.955541374  52.35.167.249   192.168.78.131  TLSv1.2   183 Application Data
40.399320095  192.168.78.131  13.225.103.71   TLSv1.3   569 Client Hello
40.550391324  13.225.103.71   192.168.78.131  TLSv1.3  2832 Server Hello, Change Cipher Spec, Application Data
40.554408859  13.225.103.71   192.168.78.131  TLSv1.3  1300 Application Data, Application Data, Application Data

> Frame 1: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface any, id 0
> Linux cooked capture v1
> Internet Protocol Version 4, Src: 192.168.78.131, Dst: 34.98.75.36
> Transmission Control Protocol, Src Port: 35746, Dst Port: 443, Seq: 1, Ack: 1, Len: 39
> Transport Layer Security
```

Figure 3.27 Burpsuite's illustration using Wireshark

At the same time, the traffic is captured using Wireshark and it is noticed from figure 3.25 that all the traffic uses tlsv1.2 because the website uses https, so it is not possible to display any useful information because all the data is encrypted as shown in the figure below.

3.3 Metasploit Framework

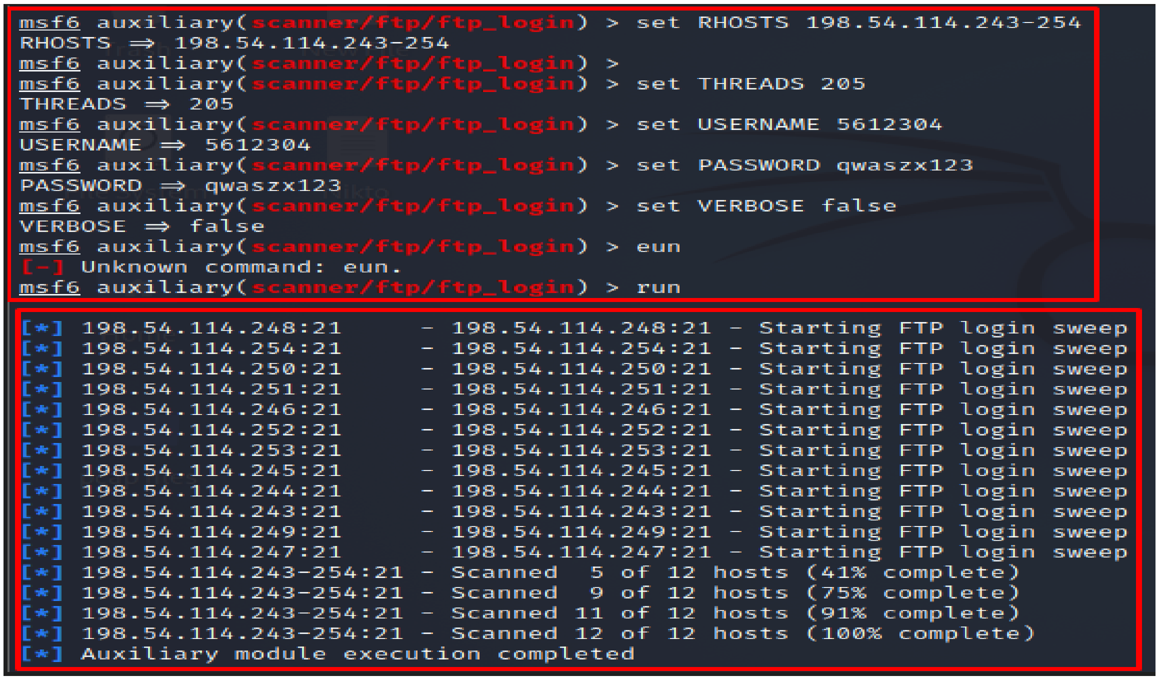
You may create, verify, and run exploit code with the help of the Metasploit Framework, a Ruby-based, modular penetration testing platform. You can use the tools in the Metasploit Framework to scan for security flaws, discover open networks, launch attacks, and stay undetected. The Metasploit Framework is, at its core, a set of widely used tools that together form a comprehensive environment for penetration testing and exploit creation (Raj S., et al., 2020)(Raj, and Walia, 2020).

3.3.1 Using Metasploit Framework

The Metasploit Framework can be accessed and managed through MSFconsole, a command line interface. As the most popular entry point into the Metasploit Framework, MSFconsole is often the first port of call for penetration testers. Using the control panel, you may do actions like scanning targets, exploiting vulnerabilities, and data collection. By using the command "msfconsole" in a new terminal of kali Linux and it open the msfconsole window.

3.3.2 Exploiting FTP Vulnerability

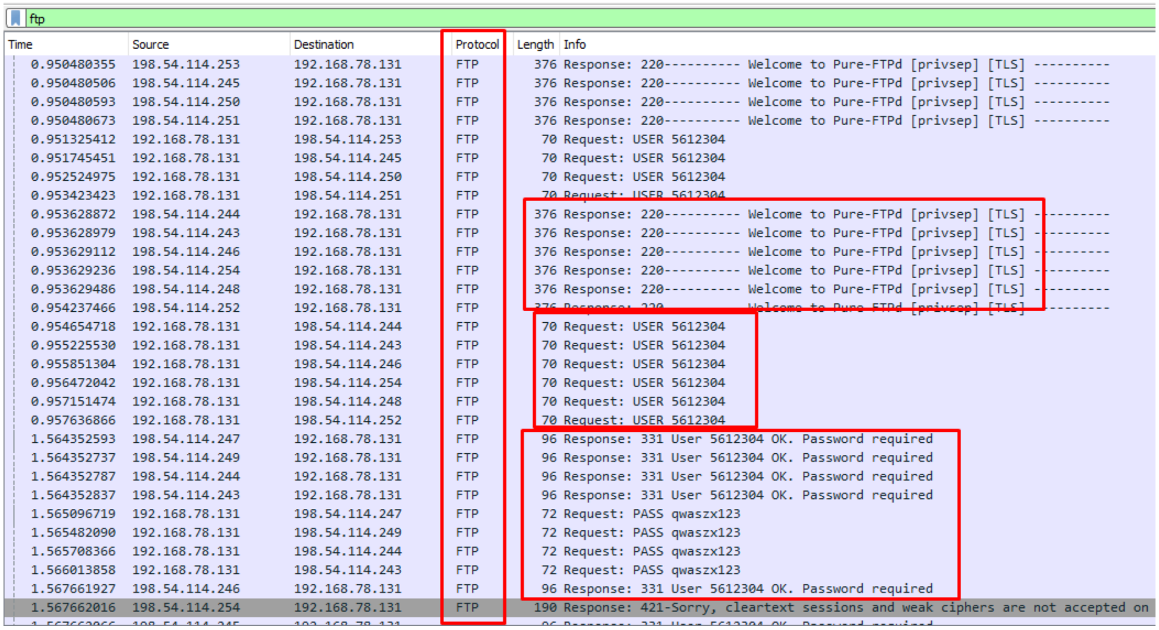
Search the keyword "ftp" in msfconole and it display a lot of information then search the vulnerability "auxiliary/scanner/ftp/ftp_login" and msfconsole display the targeted vulnerability. The use the vulnerability by using the command "use auxiliary/scanner/ftp/ftp_login". Then set the RHOSTS to 198.54.114.243-254. Also set other fields such as; username and password then run the payload and it completed successfully as shown in the figure below.



```
msf6 auxiliary(scanner/ftp/ftp_login) > set RHOSTS 198.54.114.243-254
RHOSTS => 198.54.114.243-254
msf6 auxiliary(scanner/ftp/ftp_login) >
msf6 auxiliary(scanner/ftp/ftp_login) > set THREADS 205
THREADS => 205
msf6 auxiliary(scanner/ftp/ftp_login) > set USERNAME 5612304
USERNAME => 5612304
msf6 auxiliary(scanner/ftp/ftp_login) > set PASSWORD qwaszx123
PASSWORD => qwaszx123
msf6 auxiliary(scanner/ftp/ftp_login) > set VERBOSE false
VERBOSE => false
msf6 auxiliary(scanner/ftp/ftp_login) > eun
[-] Unknown command: eun.
msf6 auxiliary(scanner/ftp/ftp_login) > run

[*] 198.54.114.248:21      - 198.54.114.248:21 - Starting FTP login sweep
[*] 198.54.114.254:21      - 198.54.114.254:21 - Starting FTP login sweep
[*] 198.54.114.250:21      - 198.54.114.250:21 - Starting FTP login sweep
[*] 198.54.114.251:21      - 198.54.114.251:21 - Starting FTP login sweep
[*] 198.54.114.246:21      - 198.54.114.246:21 - Starting FTP login sweep
[*] 198.54.114.252:21      - 198.54.114.252:21 - Starting FTP login sweep
[*] 198.54.114.253:21      - 198.54.114.253:21 - Starting FTP login sweep
[*] 198.54.114.245:21      - 198.54.114.245:21 - Starting FTP login sweep
[*] 198.54.114.244:21      - 198.54.114.244:21 - Starting FTP login sweep
[*] 198.54.114.243:21      - 198.54.114.243:21 - Starting FTP login sweep
[*] 198.54.114.249:21      - 198.54.114.249:21 - Starting FTP login sweep
[*] 198.54.114.247:21      - 198.54.114.247:21 - Starting FTP login sweep
[*] 198.54.114.243-254:21 - Scanned  5 of 12 hosts (41% complete)
[*] 198.54.114.243-254:21 - Scanned  9 of 12 hosts (75% complete)
[*] 198.54.114.243-254:21 - Scanned 11 of 12 hosts (91% complete)
[*] 198.54.114.243-254:21 - Scanned 12 of 12 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 3.28 Exploiting FTP Vulnerability

The traffic is captured using Wireshark and Wireshark captured the attack successfully as shown in the figure below.



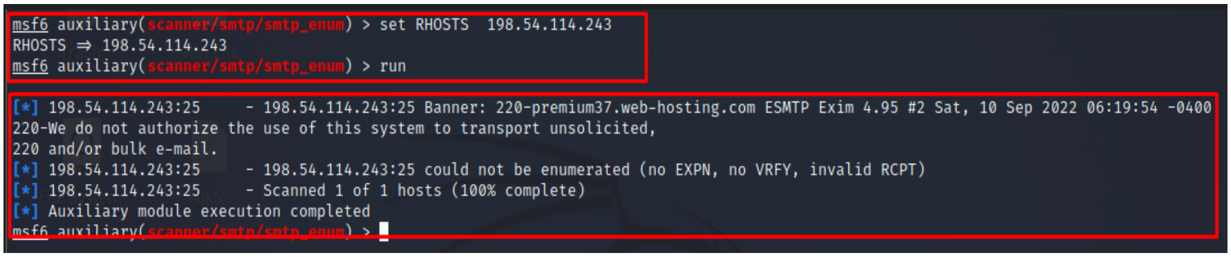
ftp

Time	Source	Destination	Protocol	Length	Info
0.950480355	198.54.114.253	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.950480506	198.54.114.245	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.950480593	198.54.114.250	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.950480673	198.54.114.251	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.951325412	192.168.78.131	198.54.114.253	FTP	70	Request: USER 5612304
0.951745451	192.168.78.131	198.54.114.245	FTP	70	Request: USER 5612304
0.952524975	192.168.78.131	198.54.114.250	FTP	70	Request: USER 5612304
0.953423423	192.168.78.131	198.54.114.251	FTP	70	Request: USER 5612304
0.953628872	198.54.114.244	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.953628979	198.54.114.243	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.953629112	198.54.114.246	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.953629236	198.54.114.254	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.953629486	198.54.114.248	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.954237466	198.54.114.252	192.168.78.131	FTP	376	Response: 220---------- Welcome to Pure-FTPd [privsep] [TLS] ----------
0.954654718	192.168.78.131	198.54.114.244	FTP	70	Request: USER 5612304
0.955225530	192.168.78.131	198.54.114.243	FTP	70	Request: USER 5612304
0.955851304	192.168.78.131	198.54.114.246	FTP	70	Request: USER 5612304
0.956472042	192.168.78.131	198.54.114.254	FTP	70	Request: USER 5612304
0.957151474	192.168.78.131	198.54.114.248	FTP	70	Request: USER 5612304
0.957636866	192.168.78.131	198.54.114.252	FTP	70	Request: USER 5612304
1.564352593	198.54.114.247	192.168.78.131	FTP	96	Response: 331 User 5612304 OK. Password required
1.564352737	198.54.114.249	192.168.78.131	FTP	96	Response: 331 User 5612304 OK. Password required
1.564352787	198.54.114.244	192.168.78.131	FTP	96	Response: 331 User 5612304 OK. Password required
1.564352837	198.54.114.243	192.168.78.131	FTP	96	Response: 331 User 5612304 OK. Password required
1.565096719	192.168.78.131	198.54.114.247	FTP	72	Request: PASS qwaszx123
1.565482090	192.168.78.131	198.54.114.249	FTP	72	Request: PASS qwaszx123
1.565708366	192.168.78.131	198.54.114.244	FTP	72	Request: PASS qwaszx123
1.566013858	192.168.78.131	198.54.114.243	FTP	72	Request: PASS qwaszx123
1.567661927	198.54.114.246	192.168.78.131	FTP	96	Response: 331 User 5612304 OK. Password required
1.567662016	198.54.114.254	192.168.78.131	FTP	190	Response: 421-Sorry, cleartext sessions and weak ciphers are not accepted on

Figure 3.29 Exploiting FTP Vulnerability Wireshark

3.3.3 Exploiting SMTP Vulnerability

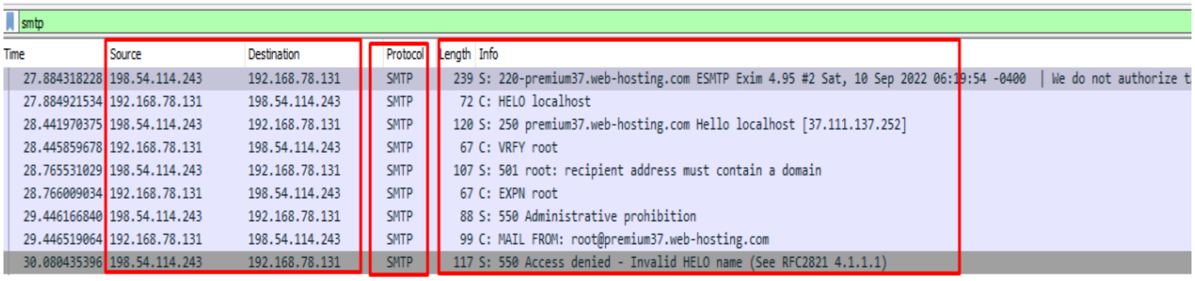
Search smtp in msfconole and it display a lot of information after that search the vulnerability "auxiliary/scanner/smtp/smtp_enum" and msfconsole display the targeted vulnerability. The use the vulnerability by using the command "use auxiliary/scanner/smtp/smtp_enum". Then set the RHOSTS to 198.54.114.243-254. Then run the payload and it completed successfully as shown in the figure below.



```
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS  198.54.114.243
RHOSTS ⇒ 198.54.114.243
msf6 auxiliary(scanner/smtp/smtp_enum) > run

[*] 198.54.114.243:25     - 198.54.114.243:25 Banner: 220-premium37.web-hosting.com ESMTP Exim 4.95 #2 Sat, 10 Sep 2022 06:19:54 -0400
220-We do not authorize the use of this system to transport unsolicited,
220 and/or bulk e-mail.
[*] 198.54.114.243:25     - 198.54.114.243:25 could not be enumerated (no EXPN, no VRFY, invalid RCPT)
[*] 198.54.114.243:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) > 
```

Figure 3.30 Exploiting SMTP Vulnerability

The traffic is captured using Wireshark and Wireshark captured the attack successfully as shown in the figure below.



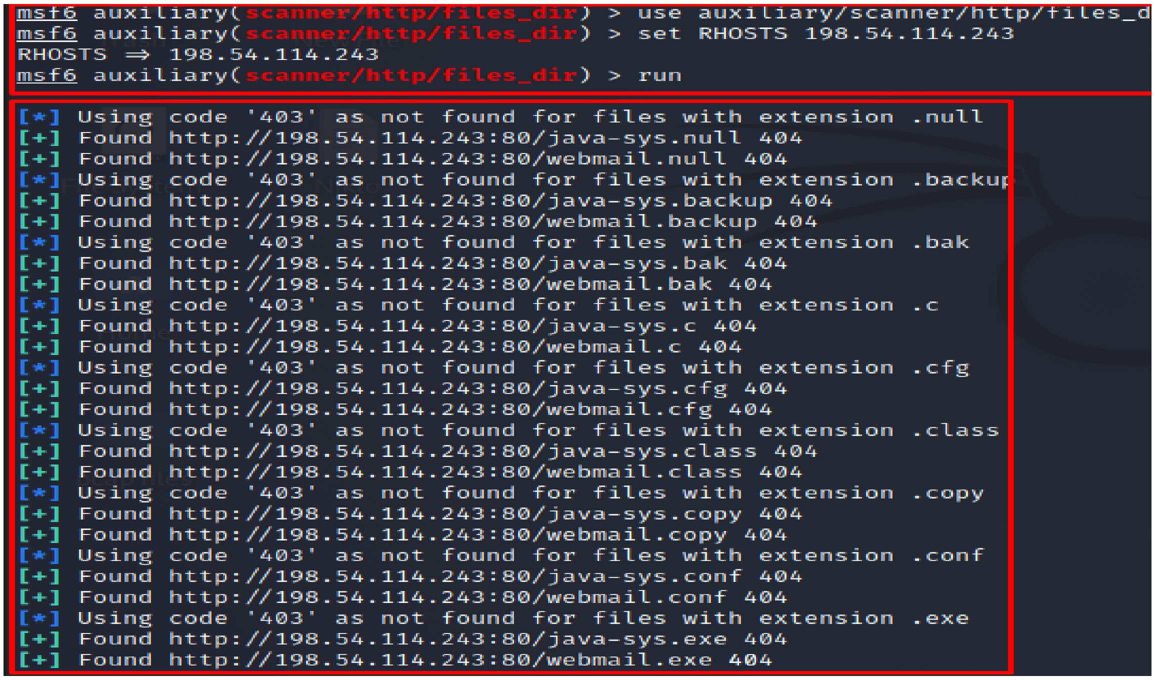
smtp

Time	Source	Destination	Protocol	Length	Info
27.884318228	198.54.114.243	192.168.78.131	SMTP	239	S: 220-premium37.web-hosting.com ESMTP Exim 4.95 #2 Sat, 10 Sep 2022 06:19:54 -0400 | We do not authorize t
27.884921534	192.168.78.131	198.54.114.243	SMTP	72	C: HELO localhost
28.441970375	198.54.114.243	192.168.78.131	SMTP	120	S: 250 premium37.web-hosting.com Hello localhost [37.111.137.252]
28.445859678	192.168.78.131	198.54.114.243	SMTP	67	C: VRFY root
28.765531029	198.54.114.243	192.168.78.131	SMTP	107	S: 501 root: recipient address must contain a domain
28.766009034	192.168.78.131	198.54.114.243	SMTP	67	C: EXPN root
29.446166840	198.54.114.243	192.168.78.131	SMTP	88	S: 550 Administrative prohibition
29.446519064	192.168.78.131	198.54.114.243	SMTP	99	C: MAIL FROM: root@premium37.web-hosting.com
30.080435396	198.54.114.243	192.168.78.131	SMTP	117	S: 550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Figure 3.31 Exploiting SMTP Vulnerability Wireshark

3.3.4 Exploiting HTTP Vulnerability

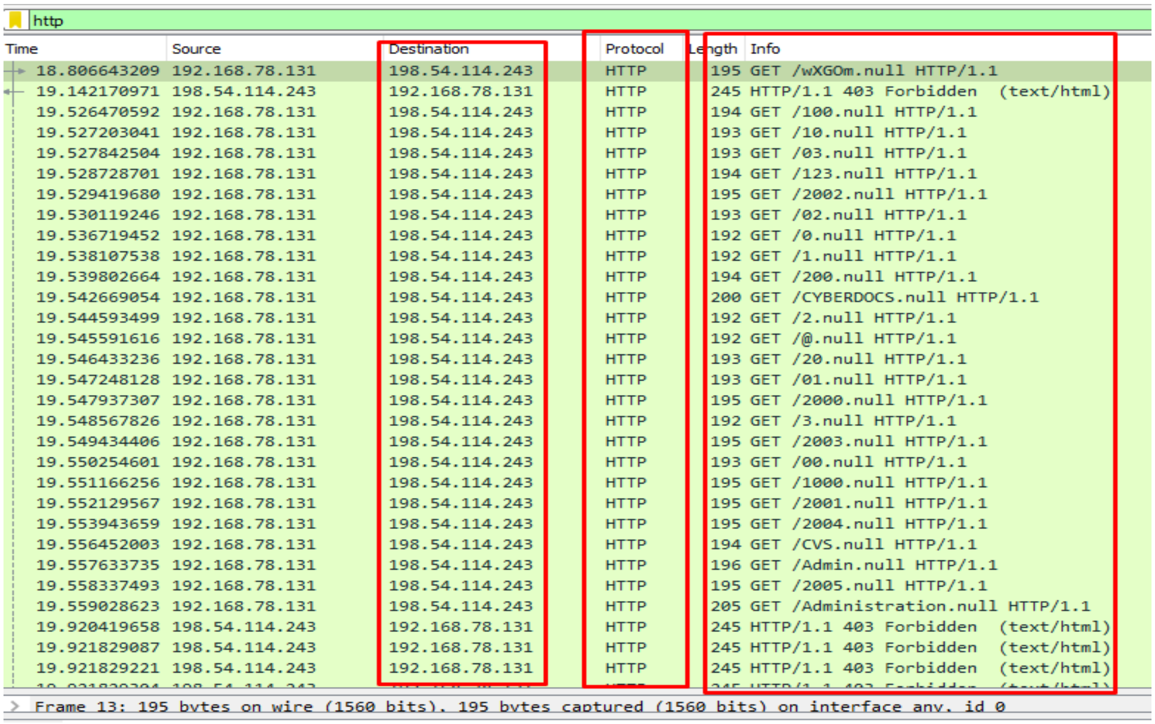
Search http in msfconole and it display a lot of information after that search the vulnerability "auxiliary/scanner/http/files_dir" and msfconsole display the targeted vulnerability. The use the vulnerability by using the command "use auxiliary/scanner/http/files_dir". Then set the RHOSTS to 198.54.114.243-254. Also set other fields such as; username and password then run the payload and it completed successfully as shown in the figure below.



```
msf6 auxiliary(scanner/http/files_dir) > use auxiliary/scanner/http/files_d
msf6 auxiliary(scanner/http/files_dir) > set RHOSTS 198.54.114.243
RHOSTS ⇒ 198.54.114.243
msf6 auxiliary(scanner/http/files_dir) > run

[*] Using code '403' as not found for files with extension .null
[+] Found http://198.54.114.243:80/java-sys.null 404
[+] Found http://198.54.114.243:80/webmail.null 404
[*] Using code '403' as not found for files with extension .backup
[+] Found http://198.54.114.243:80/java-sys.backup 404
[+] Found http://198.54.114.243:80/webmail.backup 404
[*] Using code '403' as not found for files with extension .bak
[+] Found http://198.54.114.243:80/java-sys.bak 404
[+] Found http://198.54.114.243:80/webmail.bak 404
[*] Using code '403' as not found for files with extension .c
[+] Found http://198.54.114.243:80/java-sys.c 404
[+] Found http://198.54.114.243:80/webmail.c 404
[*] Using code '403' as not found for files with extension .cfg
[+] Found http://198.54.114.243:80/java-sys.cfg 404
[+] Found http://198.54.114.243:80/webmail.cfg 404
[*] Using code '403' as not found for files with extension .class
[+] Found http://198.54.114.243:80/java-sys.class 404
[+] Found http://198.54.114.243:80/webmail.class 404
[*] Using code '403' as not found for files with extension .copy
[+] Found http://198.54.114.243:80/java-sys.copy 404
[+] Found http://198.54.114.243:80/webmail.copy 404
[*] Using code '403' as not found for files with extension .conf
[+] Found http://198.54.114.243:80/java-sys.conf 404
[+] Found http://198.54.114.243:80/webmail.conf 404
[*] Using code '403' as not found for files with extension .exe
[+] Found http://198.54.114.243:80/java-sys.exe 404
[+] Found http://198.54.114.243:80/webmail.exe 404
```

Figure 3.32 Exploiting HTTP Vulnerability

The traffic is captured using Wireshark and Wireshark captured the attack successfully as shown in the figure below.



http

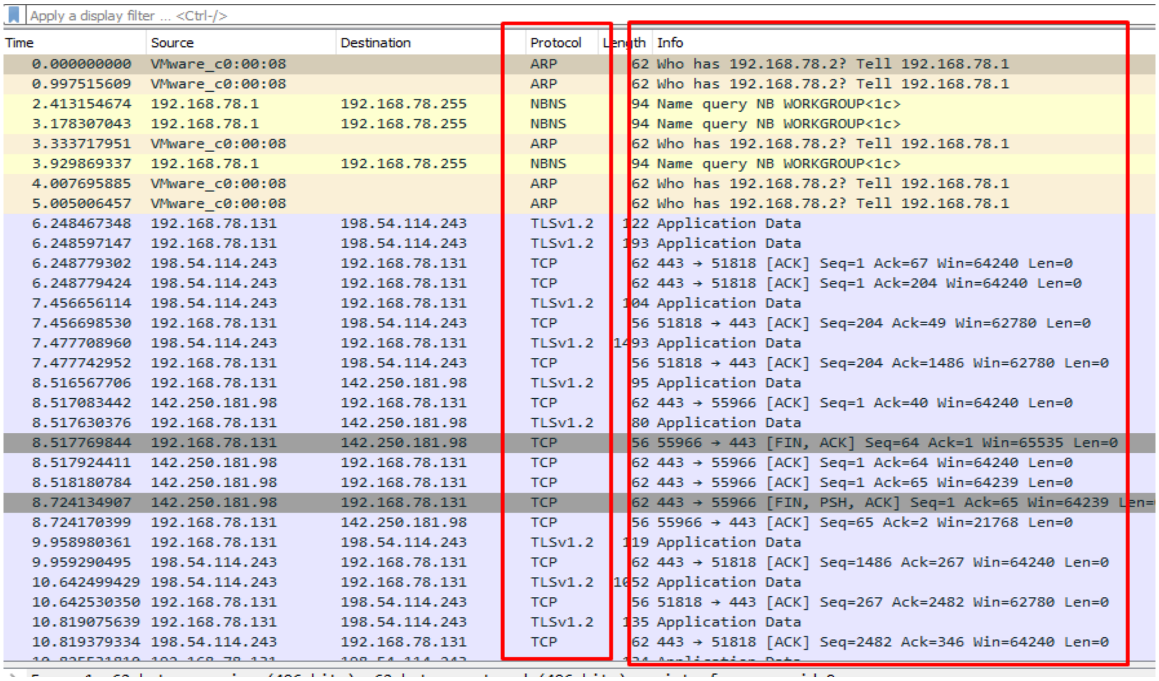
Time	Source	Destination	Protocol	Length	Info
18.806643209	192.168.78.131	198.54.114.243	HTTP	195	GET /wXGOm.null HTTP/1.1
19.142170971	198.54.114.243	192.168.78.131	HTTP	245	HTTP/1.1 403 Forbidden (text/html)
19.526470592	192.168.78.131	198.54.114.243	HTTP	194	GET /100.null HTTP/1.1
19.527203041	192.168.78.131	198.54.114.243	HTTP	193	GET /10.null HTTP/1.1
19.527842504	192.168.78.131	198.54.114.243	HTTP	193	GET /03.null HTTP/1.1
19.528728701	192.168.78.131	198.54.114.243	HTTP	194	GET /123.null HTTP/1.1
19.529419680	192.168.78.131	198.54.114.243	HTTP	195	GET /2002.null HTTP/1.1
19.530119246	192.168.78.131	198.54.114.243	HTTP	193	GET /02.null HTTP/1.1
19.536719452	192.168.78.131	198.54.114.243	HTTP	192	GET /0.null HTTP/1.1
19.538107538	192.168.78.131	198.54.114.243	HTTP	192	GET /1.null HTTP/1.1
19.539802664	192.168.78.131	198.54.114.243	HTTP	194	GET /200.null HTTP/1.1
19.542669054	192.168.78.131	198.54.114.243	HTTP	200	GET /CYBERDOCS.null HTTP/1.1
19.544593499	192.168.78.131	198.54.114.243	HTTP	192	GET /2.null HTTP/1.1
19.545591616	192.168.78.131	198.54.114.243	HTTP	192	GET /@.null HTTP/1.1
19.546433236	192.168.78.131	198.54.114.243	HTTP	193	GET /20.null HTTP/1.1
19.547248128	192.168.78.131	198.54.114.243	HTTP	193	GET /01.null HTTP/1.1
19.547937307	192.168.78.131	198.54.114.243	HTTP	195	GET /2000.null HTTP/1.1
19.548567826	192.168.78.131	198.54.114.243	HTTP	192	GET /3.null HTTP/1.1
19.549434406	192.168.78.131	198.54.114.243	HTTP	195	GET /2003.null HTTP/1.1
19.550254601	192.168.78.131	198.54.114.243	HTTP	193	GET /00.null HTTP/1.1
19.551166256	192.168.78.131	198.54.114.243	HTTP	195	GET /1000.null HTTP/1.1
19.552129567	192.168.78.131	198.54.114.243	HTTP	195	GET /2001.null HTTP/1.1
19.553943659	192.168.78.131	198.54.114.243	HTTP	195	GET /2004.null HTTP/1.1
19.556452003	192.168.78.131	198.54.114.243	HTTP	194	GET /CVS.null HTTP/1.1
19.557633735	192.168.78.131	198.54.114.243	HTTP	196	GET /Admin.null HTTP/1.1
19.558337493	192.168.78.131	198.54.114.243	HTTP	195	GET /2005.null HTTP/1.1
19.559028623	192.168.78.131	198.54.114.243	HTTP	205	GET /Administration.null HTTP/1.1
19.920419658	198.54.114.243	192.168.78.131	HTTP	245	HTTP/1.1 403 Forbidden (text/html)
19.921829087	198.54.114.243	192.168.78.131	HTTP	245	HTTP/1.1 403 Forbidden (text/html)
19.921829221	198.54.114.243	192.168.78.131	HTTP	245	HTTP/1.1 403 Forbidden (text/html)

```
> Frame 13: 195 bytes on wire (1560 bits), 195 bytes captured (1560 bits) on interface any, id 0
```

Figure 3.33 Exploiting HTTP Vulnerability Wireshark

3.3.5 SQL Injection Attack

The SQL injection is not performed successfully because the website doesn't have any sql injection vulnerably. As shown in the figure below.

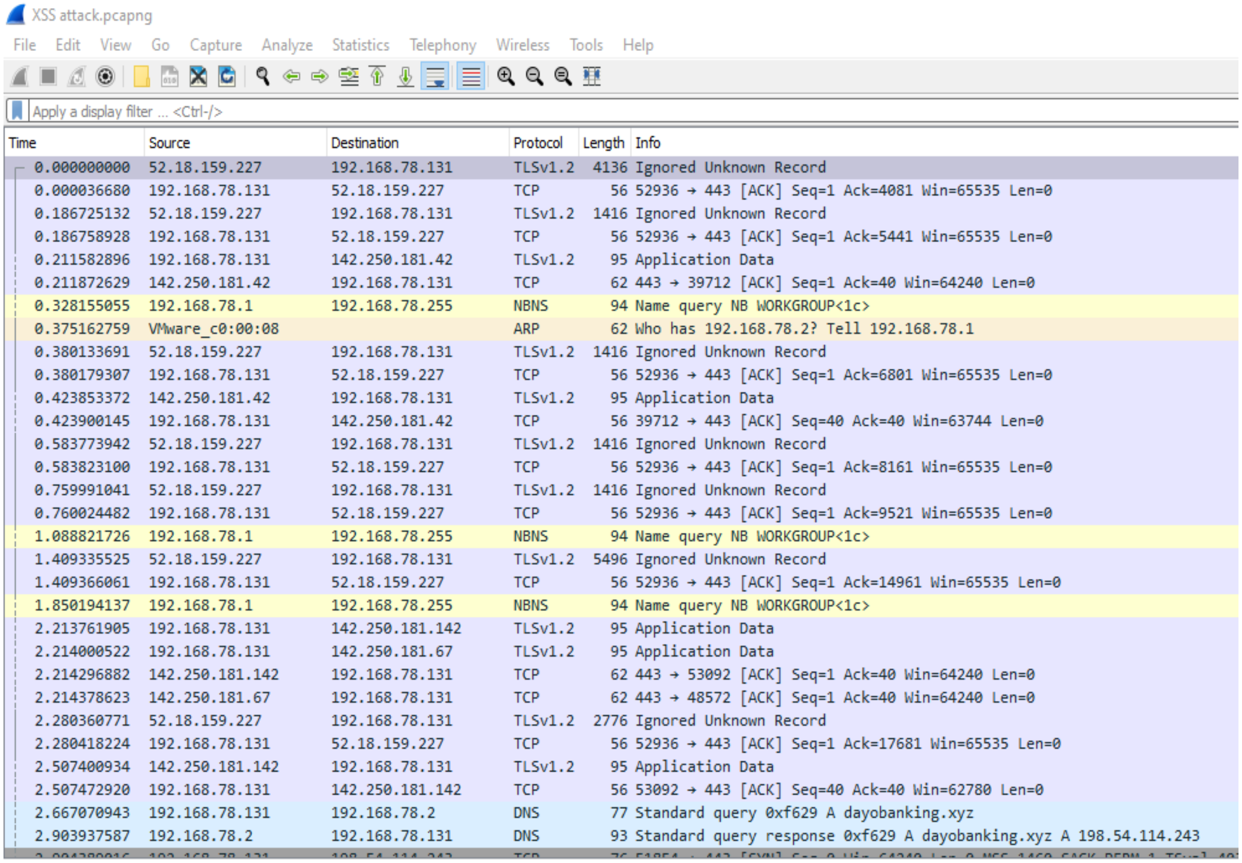


Time	Source	Destination	Protocol	Length	Info
0.000000000	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
0.997515609	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
2.413154674	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
3.178307043	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
3.333717951	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
3.929869337	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
4.007695885	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
5.005006457	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
6.248467348	192.168.78.131	198.54.114.243	TLSv1.2	122	Application Data
6.248597147	192.168.78.131	198.54.114.243	TLSv1.2	193	Application Data
6.248779302	198.54.114.243	192.168.78.131	TCP	62	443 → 51818 [ACK] Seq=1 Ack=67 Win=64240 Len=0
6.248779424	198.54.114.243	192.168.78.131	TCP	62	443 → 51818 [ACK] Seq=1 Ack=204 Win=64240 Len=0
7.456656114	198.54.114.243	192.168.78.131	TLSv1.2	104	Application Data
7.456698530	192.168.78.131	198.54.114.243	TCP	56	51818 → 443 [ACK] Seq=204 Ack=49 Win=62780 Len=0
7.477708960	198.54.114.243	192.168.78.131	TLSv1.2	1493	Application Data
7.477742952	192.168.78.131	198.54.114.243	TCP	56	51818 → 443 [ACK] Seq=204 Ack=1486 Win=62780 Len=0
8.516567706	192.168.78.131	142.250.181.98	TLSv1.2	95	Application Data
8.517083442	142.250.181.98	192.168.78.131	TCP	62	443 → 55966 [ACK] Seq=1 Ack=40 Win=64240 Len=0
8.517630376	192.168.78.131	142.250.181.98	TLSv1.2	80	Application Data
8.517769844	192.168.78.131	142.250.181.98	TCP	56	55966 → 443 [FIN, ACK] Seq=64 Ack=1 Win=65535 Len=0
8.517924411	142.250.181.98	192.168.78.131	TCP	62	443 → 55966 [ACK] Seq=1 Ack=64 Win=64240 Len=0
8.518180784	142.250.181.98	192.168.78.131	TCP	62	443 → 55966 [ACK] Seq=1 Ack=65 Win=64239 Len=0
8.724134907	142.250.181.98	192.168.78.131	TCP	62	443 → 55966 [FIN, PSH, ACK] Seq=1 Ack=65 Win=64239 Len=
8.724170399	192.168.78.131	142.250.181.98	TCP	56	55966 → 443 [ACK] Seq=65 Ack=2 Win=21768 Len=0
9.958980361	192.168.78.131	198.54.114.243	TLSv1.2	119	Application Data
9.959290495	198.54.114.243	192.168.78.131	TCP	62	443 → 51818 [ACK] Seq=1486 Ack=267 Win=64240 Len=0
10.642499429	198.54.114.243	192.168.78.131	TLSv1.2	1052	Application Data
10.642530350	192.168.78.131	198.54.114.243	TCP	56	51818 → 443 [ACK] Seq=267 Ack=2482 Win=62780 Len=0
10.819075639	192.168.78.131	198.54.114.243	TLSv1.2	135	Application Data
10.819379334	198.54.114.243	192.168.78.131	TCP	62	443 → 51818 [ACK] Seq=2482 Ack=346 Win=64240 Len=0

Figure 3.34 SQL Injection Attack Wireshark

3.3.6 Cross Site Scraping Attack

Perform cross site scripting network and it doesn’t work it was neutral as shown in the figure 3.31.


XSS attack.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

Time	Source	Destination	Protocol	Length	Info
0.000000000	52.18.159.227	192.168.78.131	TLSv1.2	4136	Ignored Unknown Record
0.000036680	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=4081 Win=65535 Len=0
0.186725132	52.18.159.227	192.168.78.131	TLSv1.2	1416	Ignored Unknown Record
0.186758928	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=5441 Win=65535 Len=0
0.211582896	192.168.78.131	142.250.181.42	TLSv1.2	95	Application Data
0.211872629	142.250.181.42	192.168.78.131	TCP	62	443 → 39712 [ACK] Seq=1 Ack=40 Win=64240 Len=0
0.328155055	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
0.375162759	VMware_c0:00:08		ARP	62	Who has 192.168.78.2? Tell 192.168.78.1
0.380133691	52.18.159.227	192.168.78.131	TLSv1.2	1416	Ignored Unknown Record
0.380179307	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=6801 Win=65535 Len=0
0.423853372	142.250.181.42	192.168.78.131	TLSv1.2	95	Application Data
0.423900145	192.168.78.131	142.250.181.42	TCP	56	39712 → 443 [ACK] Seq=40 Ack=40 Win=63744 Len=0
0.583773942	52.18.159.227	192.168.78.131	TLSv1.2	1416	Ignored Unknown Record
0.583823100	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=8161 Win=65535 Len=0
0.759991041	52.18.159.227	192.168.78.131	TLSv1.2	1416	Ignored Unknown Record
0.760024482	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=9521 Win=65535 Len=0
1.088821726	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
1.409335525	52.18.159.227	192.168.78.131	TLSv1.2	5496	Ignored Unknown Record
1.409366061	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=14961 Win=65535 Len=0
1.850194137	192.168.78.1	192.168.78.255	NBNS	94	Name query NB WORKGROUP<1c>
2.213761905	192.168.78.131	142.250.181.142	TLSv1.2	95	Application Data
2.214000522	192.168.78.131	142.250.181.67	TLSv1.2	95	Application Data
2.214296882	142.250.181.142	192.168.78.131	TCP	62	443 → 53092 [ACK] Seq=1 Ack=40 Win=64240 Len=0
2.214378623	142.250.181.67	192.168.78.131	TCP	62	443 → 48572 [ACK] Seq=1 Ack=40 Win=64240 Len=0
2.280360771	52.18.159.227	192.168.78.131	TLSv1.2	2776	Ignored Unknown Record
2.280418224	192.168.78.131	52.18.159.227	TCP	56	52936 → 443 [ACK] Seq=1 Ack=17681 Win=65535 Len=0
2.507400934	142.250.181.142	192.168.78.131	TLSv1.2	95	Application Data
2.507472920	192.168.78.131	142.250.181.142	TCP	56	53092 → 443 [ACK] Seq=40 Ack=40 Win=62780 Len=0
2.667070943	192.168.78.131	192.168.78.2	DNS	77	Standard query 0xf629 A dayobanking.xyz
2.903937587	192.168.78.2	192.168.78.131	DNS	93	Standard query response 0xf629 A dayobanking.xyz A 198.54.114.243

Figure 3.35 Cross Site Scraping Attack Wireshark

Chapter 4 – Results

4.1 Results of the Tests using Security Audits

By using WHOIS various information can be gather such as IP address, Location, domain, and subdomains etc. and it works about 5 percent of the total enumeration. Then the usage of Nmap for open ports and running services scanning and it also works about 3 percent of total enumeration. After that use NMap for TCP SYN Stealth Scan and it works about 2 percent of the total task. Then use Whatweb to find the web server information and its contribution to the total work is about 2 percent. Using Curl display the source code of the target web page by using this it contributes it about 3 percent of the total tack. Then use DirBuster to scan for useful information about the directories and it work successfully but many of the directories are hidden and cannot be accessed only one directory is accessible so its contribution s about 5 percent to the task. Also scanning of the website using Nikto to find the vulnerabilities on the website provide a result of various vulnerabilities such as XSS, clickjacking its contribution to the task is about 10 percent. Also use ping utility to check that the target responds and by using this it is conclude that the target website is active its contribution s about 5 percent of the total task. Using Directory Traversal, open a directory which has some information it contributes is about 10 percent of the total tack. Using Burpsuite capture the http messages both query and response and also capture the session cookies and other useful information its contribution is about 10 percent to the task. Then use msfconsole to exploit the FTP Vulnerability and it successfully exploit the vulnerability and its contribution is about 15 percent to the task. After that also use msfconsole to exploit the SMTP Vulnerability the vulnerability is exploited successfully, and its contribution is about 15 percent to the task. Finally, by using msfconsole to exploit the HTTP Vulnerability it exploits the vulnerability successfully and its contribution is about 15 percent to the task.

This information can be best understanding by the following bar chart.

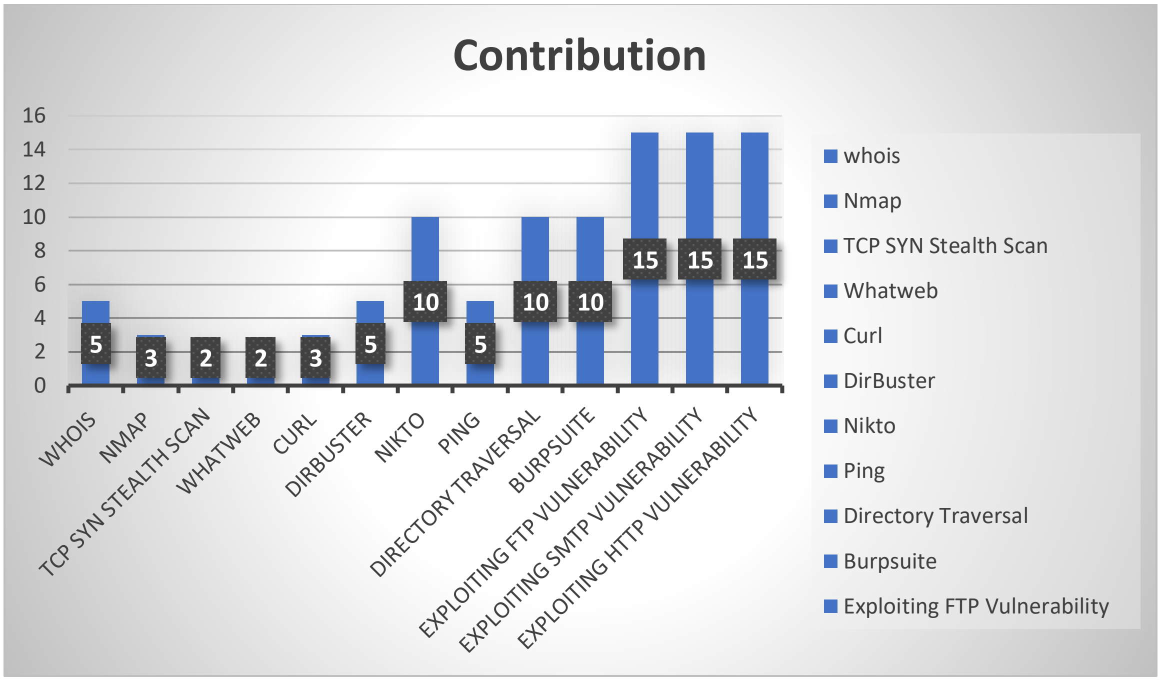


Figure 4.1 Bar chart for comparative analysis of Vulnerability though Audit

Furthermore, the detail about the attacks is also given in the bar chart below.

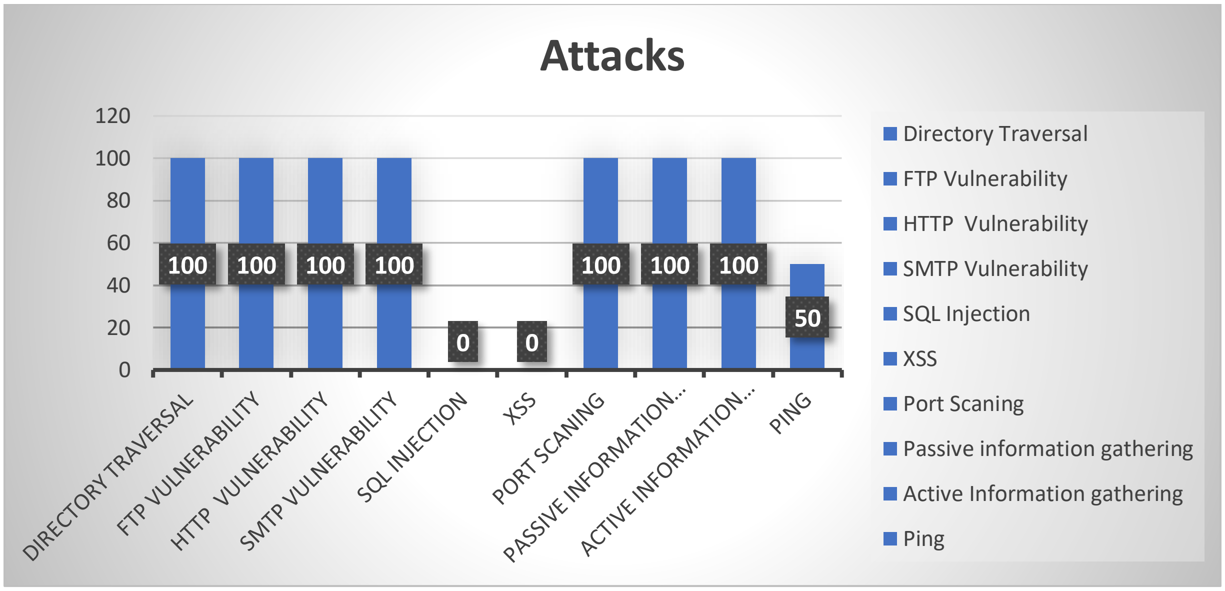


Figure 4.2 Results of Attacks

The results shows that different vulnerability assessments have been carried out. Different attacks on different components were being detected. However, the assessments shown that the contribution was 0 percent for both XSS and SQL Injection. Also, for Ping it was 50 percent. For the rest, it was total 100% contribution to the audit.

4.2 Recommendation for Audits and Policies

As already discussed in chapter 3, the website security order will be carried out which is a procedure of examination of the files, plugins, core of the website, and server for identification of potential vulnerabilities and loopholes. The security audit will be including dynamic code analysis and include configuration and penetration tests. Therefore, as cybersecurity auditor it will be necessary to make a checklist that will be continuing an auditory checklist involving core files of the websites, the traffic of website, extensions, SSL renewals and planning, teams, use notices and settings, plugins, third party items and site as well as server settings.

4.2.1 Development of Organizational Framework

This section provides the details about the framework development at three different levels which will ensure that the organization will be having the knowledge about the domain and will be communicating that knowledge among the applications and humans by utilization of different systems. Before implementation of the framework, it is necessary to understand essential terminologies like an asset which is something having some value being owned by an individual or an organization, and that asset has to be secured from any threats. Also, the vulnerabilities as well as threats to the assets increases if the value of an acid gets increased. Therefore, the asset will be prone to substantial risk in case of more occurrence of attacks. similarly, the mitigation risks and preventive controls have to be carried out by adaption of the framework at three different levels for securing the assets

1. The first level of the framework will be illustrating the security objective and assets of the organization for which the auditor will be responsible for identification of an asset and the categorization. This level will not include the cyber security experts for identification of the assets as well as securing the objectives of an organization
2. The second level will be illustrating the made amendments that are necessary for dealing with attacks and abilities that have been stated in previous chapters. The analysis of the risks as well as vulnerabilities will be tackled by the cyber security experts, trained personnel, and auditors of an organization

3. The third level will be involving the utilization of preventive measures and controls to logical controls and physical administration for which step by step audit will be carried out and the security objective through that ordered will be achieved

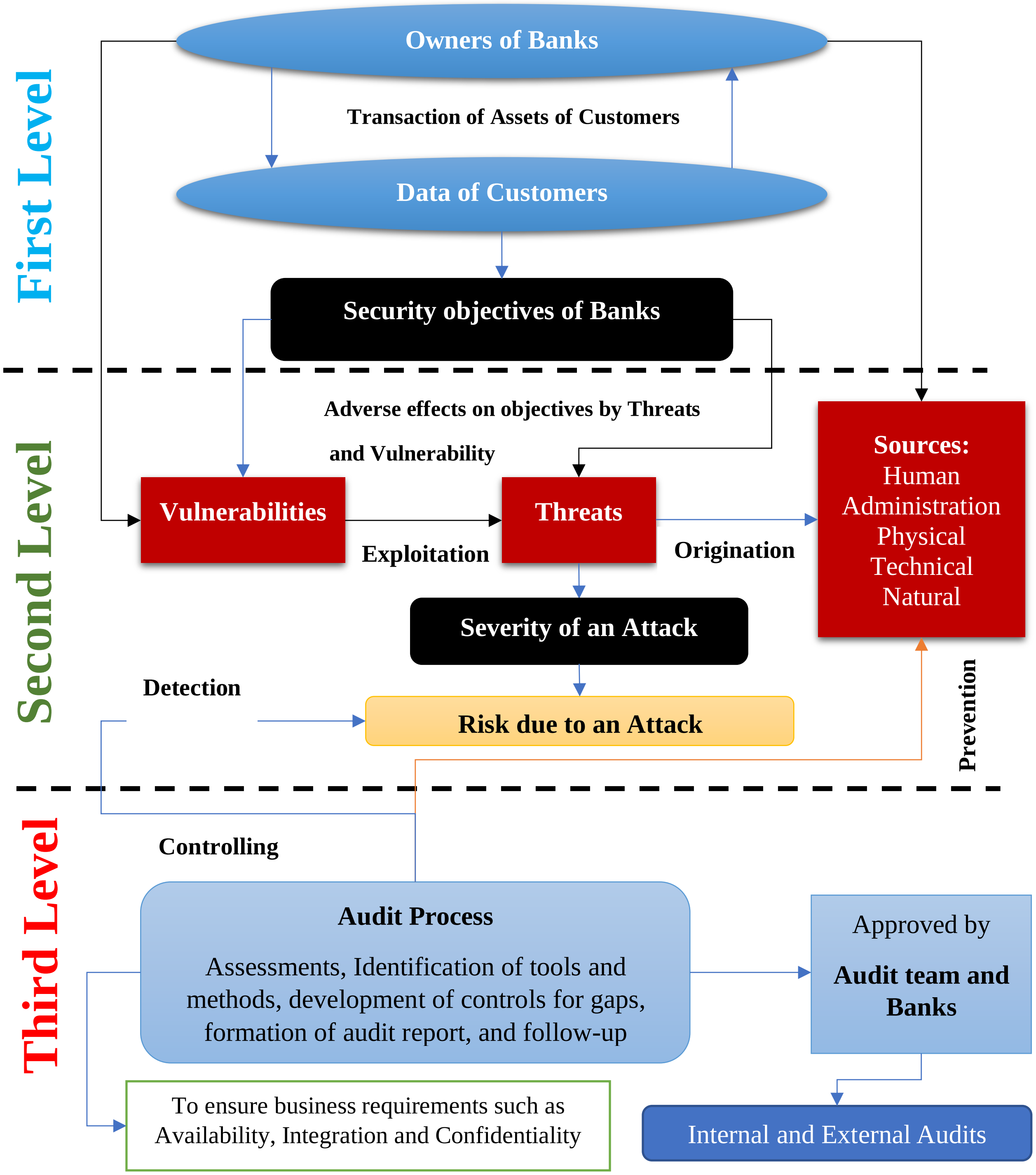

First Level
Owners of Banks
Transaction of Assets of Customers
Data of Customers
Security objectives of Banks
Second Level
Adverse effects on objectives by Threats
and Vulnerability
Vulnerabilities
Exploitation
Threats
Origination
Sources:
Human
Administration
Physical
Technical
Natural
Severity of an Attack
Detection
Risk due to an Attack
Prevention
Third Level
Controlling
Audit Process
Assessments, Identification of tools and methods, development of controls for gaps, formation of audit report, and follow-up
Approved by
Audit team and Banks
To ensure business requirements such as Availability, Integration and Confidentiality
Internal and External Audits

Figure 4.3 Proposed Framework for a Bank to ensure Cybersecurity and Protection of Customers' Assets

4.2.2 Implementation of the Security Measures by Cyber Security Expert/Engineer/Manager

The details about the security audit that has to be implemented by the cyber security engineer has been provided in steps below

1. The security scan will be carried out that will be verifying the website, and check whether it is blacklisted or not, and will be checking outdated software, malware, or any other type of errors.
2. The next step will be reviewing the settings of the site by utilization of content management system that will provide an access to the dashboard of the site (which has already been provided in chapter 3 for the website dayobanking.xyz). From here the verification of the website will be carried out by identification of configuration settings as well as potential vulnerabilities. So, the comments settings, visible information, and input validation methods will be taken into account that have to be verified by the cyber security expert
3. The third step will be utilization of web server for verifying the privileges of the users and the observation will be made about what changes have been made by the customers in their portals. In other words, the user accounts and permissions will be verified. Here, the user roles as well as permissions will be organized for management purposes, and the categorization as well as roles will be defined according to the levels. Six different roles that are really available include super administrator, administrator, author, editor, contributor, and subscribers. According to the roles, the permissions will be assigned which may include publishing of information, writing a content or details, management, and configuration of the website
4. The fourth step that has to be followed involves performance of regular updates since the outdated components of the website will be containing vulnerabilities that could have adverse impact on the website leading to the hacking. Therefore, the plugins, extensions, content management system, and software will be updated. Updating all those components will reduce the cyber-attack risk. Therefore, the important elements of the website and software have to be continuously updated as they are listed, and have to be checked after specified intervals

5. The fifth step will be making sure that the IP as well as domain have been kept secure and those addresses or domains will be blacklisted that would have found involved in performance of malicious activities which may include sending of spam emails from a distribution of malwares, phishing activities, and botnets.
6. The last suggested step is renewal of SSL and checking of the plans or related to the website. it also involves checking the expiry date of the domain, SSL certificate and hosting plan. It will allow the expert to check the website before it gets expired. based on their dependence of the registrar, the domain registry is applicable for 10 years, and the SSL validity its only for the duration of 13 months

Chapter 5: Conclusions

5.1 Conclusions

The focus of the dissertation work was to identify the cyber security risks of the banking sector. Therefore, the dissertation work involved research in two phases of pilot project and final dissertation work. In the pilot project, the literature work was completed that focused on different aspects of cyber security, policies, and asset management. For this purpose, the stakeholders were being analyzed and the network NIS drivers were monitored to have oversighting on their assets. In addition to that, the cyber security policies involving different regulations were studied, and the diversion was made towards Cyber Security Acts of United Kingdom. Lastly, the networking and security tools were observed, and the selection had been made for Wireshark tool for performance of analysis.

In the section of problem definition, the reliable banking operations and Lack of frameworks were discussed for which the research objectives had been defined. Those objectives were concerned with identification of cyber-attacks, security risks associated with banking sector, defining of policies by the Government of United Kingdom, development of network policies and framework, and implementation of technical practices. So, the research issues were raised, and the research question was developed that was associated with introduction of network policies to mitigate the cyber-attacks. Therefore, the banking sector and the cybersecurity perspective was discussed and different types of intrusions involving malware, DoS, and spoofing were reviewed. After that, multiple malware detection methods involving signature-based techniques and behavior-based techniques were analyzed.

The literature review involved study about information and communication technologies and the software defined network was analyzed using all the three layers. Moreover, different cyber threat domains including attacks sponsored by states, extremism, organized crimes, and crimes being carried out by individuals were analyzed that helps in identifying the security threats and challenges being post on the assets of people and government of UK for which the national risk register has been already formed. Before the implementation of strategy, for different techniques and detection approaches were analyzed which involved computer vision techniques, Hammer model, AI approaches, determination of DoS attack on Microsoft server and other related approaches were analyzed.

The methodology involved formation of the website that involved different customers having particular IDs and passwords. The administrator of the website has authority to make changes and monitor the activities of the consumers by their IP addresses and emails. The detection of any malicious activity can be observed from that IP address, the e-mail address, the customer ID and the login duration. The penetration testing had been carried out in the form of security audit for which the active and passive information gathering was performed. different tools work analyze for identification of the vulnerabilities and the traffic was captured using Wireshark software. The results shown that different types of attacks were 100% identified except SQL injection and XSS

From the above analysis it is conclude that the bank website “dayobanking” uses https that is a secure protocol using TLSv1.2 transport layer protocol. It is an encrypted protocol. Most of the attacks re prevented using this protocol. But many vulnerabilities are found in this website too. First of all, NMap is used to find the open ports and running services on each port and also to run TCP SYN stealth scan. There is not any prevention to prevent NMap scanning. Next all the directories are prevented using two types of response code (403 and 404) but one directory is found that can accessed. The directory is found using tool “dirbuster”. Burp suite is also used to capture cookies and other related information. Website vulnerability tool Nikto is used to find the vulnerabilities in the “dayobanking” and there are various vulnerabilities present on the website.

After the acquirement of the results, the recommendation in policy section has been devised which involved development of organizational framework for the banking sector in the form of three layers to deal with security objectives, make amendments and utilize the preventive measures. In addition to that framework that security audit steps have been defined that are to be implemented by the cyber security expert on regular basis to prevent any type of attacks

5.2 Recommendations for the Future

The research work provided the basis of securing the banking sector from cyberattacks. From the analysis, it can be observed that the team along with cybersecurity experts have to secure the network from cyber attackers to ensure that the assets of the customers are safe. The security measures will not only safeguard the assets of the government, public and organisations but also ensures the integrity, availability and safety of the data as well as information at national and international level. As a future work, the vulnerability tests on other types of organizations and different types of cyber-attacks have to be performed to identify the nature of those attacks and the damage that could be caused by the attacks.

References

Al Shelbi., et al., 2018. *A study on penetration testing process and tools.* Farmingdale, NY, USA, IEEE.

Al-Ghamdi M., 2021. Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings,* April.

Barnett T., 2014. *Cisco Visual Networking Index: Global mobile data traffic forecast update, 2013-2018,* San Jose, CA, USA: CISCO.

Barno D. W., 2006. Challenges in Fighting a Global Insurgency. *The US Army War College Quarterly: Parameters,* 36(2).

Bashar A. K., et al., 2019. *Comprehensive Review of Artificial Intelligence and Statistical Approaches in Distributed Denial of Service Attack and Defense Methods.* s.l., IEEE, pp. 51619-51713.

Bilal M. et al., September 2011. *Trust & Security issues in Mobile banking and its effect on Costomers,* Karlskrona, Sweden: BIT.

Bilim A. et al., 2021. Electronic Banking (e-Banking) Fraud with Phishing Attack Methods. *European Journal of Science and Technology,* Volume 31, pp. 982-985.

Chen T. M. et al., 2004. *The Evolution of Viruses and Worms,* s.l.: s.n.

Corera G., 2008. *The world's most wanted cyber-jihadist,* s.l.: BBC News.

Cornish P., et al., 2009. *Cyberspace and the National Security,* London, UK: A Chatham House Report.

Craigen D., et al., 2014. Defining Cybersecurity. *Technology Innovation Management Review,* pp. 13-21.

Cummings R. H., 2010. Cyberjamming, Wall Street Journal. In: *Cold War Radio: The Dangerous History of American Broadcasting in Europe.* s.l.:s.n., pp. 3-4.

Cyber Security Organization, n.d. *Cyber Security Challenge UK.* [Online]
Available at: http://www.cybersecuritychallenge.org.uk/
[Accessed 8 7 2022].

Damico, T. M., 2009. Cyber Attack Prevention for the Home User: How to Prevent a Cyber Attack. *Inquiries Journal,* , 1(11), p. .

DARPA, 2001. *Denial of Service (DOS_ Attack Assessment Anlaysis Report,* New York: s.n.

Dr. Umamaheswari K., 2021. Impacts of Cyber Crime on Internet Banking. *International Journal of Engineering Technologu and Management Sciences,* 6(5), pp. 25-31.

Dupré L., et al., 2014. *Network and Information Security in the Finance Sector - Regulatory landscape and Industry priorities,* s.l.: ENISA report.

Elleithy K., et al., 2006. Denial of Service Attack Techniques: Analysis, Implementation and Comparison. *Systemics, Cybernetics and Informatics,* 3(1), pp. 66-71.

Elsinger, H., Lehar, A. & Summer, M., 2006. Risk Assessment for Banking Systems. *Management Science, ,* 52(9), pp. 1301-1314.

Etaher N. et al., 2014. *Understanding the Threat of Banking Malware.* s.l., Cyberforensics Organization, pp. 73-80.

Ge D., et al., 2022. Estimation of rapid chloride permeability of SCC using hyperparameters optimized random forest models. *Hourbal of Sustainable Cement-Based Materials,* pp. 1-19.

Ghazi-Tehrani et al., 2021. Phishing Evolves: Analyzing the Enduring. *Victims & Offenders - An International Journal of Evidence-based Research, Policy, and,* 16(3), pp. 316-342.

GOV.UK, 2022. *2022 cyber security incentives and regulation review,* s.l.: GOV.UK.

Harb H. et al., 2008. *SecureSMSPay: Secure SMS Mobile Payment model.* Guiyang, China, IEEE.

Hassani H. et al., 2019. Digitalisation and Big Data Mining in Banking. *Big data and congnitive computing,* 2(3).

HM Government, 2016. *National Cyber Security Strategy 2016,* s.l.: National Cyber Security Centre.

HM Government, 2020. *National Risk Register - 2020 Edition,* s.l.: s.n.

HMG, 2021. *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Dvelopment and Foreign Policu,* s.l.: HM Government.

HMG, 2021. *National Cyber Security Strategy,* s.l.: HM Government.

Hwang J., et al., 2019. Effective Detecting Method of Nmap Idle Scan. *Journal of JAITC,* 9(1), pp. 1-10.

IBM Security, 2021. *Cost of a Data Breach,* s.l.: IBM.

ICICI Bank, n.d. *Personal Banking, Online Banking Services - ICICI Bank.* [Online]
Available at: https://www.icicibank.com/
[Accessed 8 7 2022].

Ijams C., 2021. *Ethical Penetration Test for E Corp,* s.l.: s.n.

Intruder Systems Ltd., 2022. *About Intruder.* [Online]
Available at: https://www.intruder.io/

IOLO, n.d. *System Mechanic Ultimate Defense.* [Online]
Available at: https://www.iolo.com/products/system-mechanic-ultimate-defense/

ITU, 2006. *Overview of Cybersecurity. Recommendation ITU-X1205.,* Geneva: International Telecommunication Unit.

Kemmerer, 2003. *Cybersecurity.* Portland, OR, USA, IEEE.

Kim, J., 2020. *Burp Suite: Automating Web Vulnerability Scanning,* s.l.: ProQuest.

Lewis J. A., 2006. *Cybersecurity and critical infrastrucutre protection,* NW Washignton, DC: Center for Strategic & International Studies.

Li Y., et al., 2021. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. *Energy Reports*, July, 7(2021), pp. 8176-8186.

Liu, W., Ren, P., Liu, K. & Duan, H., 2011. *Behavior-Based Malware Analysis and Detection.* [Online]
Available at: https://dl.acm.org/citation.cfm?id=2120624
[Accessed 10 6 2022].

Menoski D., et al., 2014. *Evaluating Website Security with Penetration Testing Methodology.* Zrenjanin, Serbia, AIIT.

Mishra R., et al., August, 2020. *Behavioral Study of Malware Affecting Financial Institutions and Clients.* Calgary, AB, Canada, IEEE.

Mohd. Khairul Affendy Ahmed et al., 2010. Security Issues on Banking Systems. *International Journal of Computer Science and Infromation Technologies,* 1(4), pp. 268-272.

Narendiran C. et al., 2008. *Performance evaluation on end-to-end security architecture for mobile banking system.* Dubai, UAE, IEEE.

Natalius, S., 2018. *Assessing the Role of Online Banking Characteristics in the Target Selection of Banking Malware.* [Online]
Available at: https://repository.tudelft.nl/islandora/object/uuid:c0308b34-f6f4-46b1-9a23-14a12ef2ae38/datastream/obj/download
[Accessed 10 6 2022].

NCSC, 2021. *NCSC Annual Review,* s.l.: National Cyber Security Centre.

Norton, 2022. *LifeLock.* [Online]
Available at: https://www.lifelock.com/

Open Network Foundation, 2012. *"Software-defined networking: The new norm for networks,* CA, USA: ONF.

Patrikakis, C., Masikos, M. & Zouraraki, O., . Distributed Denial of Service Attacks. *The Internet Protocol Journal,* , 7(4), p. 13–35.

Paul Williams, 2021. *CBEST Threat Intelligence-Led Assessments,* s.l.: Prudental Regulation Authority.

Pemble, M., 2005. Malware Trends: Evolutionary trends in bank customer-targeted malware. *Network Security archive,* , 2005(10), pp. 4-7.

Perimeter 81, 2018. *We are Perimeter 81.* [Online]
Available at: https://www.perimeter81.com/about-us?accountid=2597329217&utm_source=google&utm_medium=cpc&utm_campaign=17072827859&utm_adgroup=135575893109&utm_target=kwd-415398361840&utm_matchtype=e&utm_network=g&utm_device=c&utm_creative=594979949403&utm_term=perimete

Prasad K. S., et al., 2018. An Integrated Approach Towards Vulnerability Assessment & Penetration Testing for a Web Application. *International Journal of Engineering & Technology,* 7(2.32).

Raj S., et al., 2020. *A Study on Metasploit Framework: A Pen-Testing Tool.* Shillong, India, IEEE.

Ramesh P. B. et al., 2011. A Comprehensive Analysis of Spoofing. *International Journal of Advanced Computer Science and Applications,* January, 1(6), pp. 157-162.

Rawat S., et al., 2020. Web Application Vulnerability Exploitation using Penetration Testing scripts. *International Journal of Scientific Research and Engineering Trends,* 6(1), pp. 311-317.

Santhosh, A. and Kurian, R., 2021. *Identifying Subdomains of the Website Using SUBLIST3R and Comparing SUBLIST3R AMASS,.* s.l., s.n.

Saundatikar R., et al., 2021. Web Penetrator – Web App Penetration Testing Tool. *IITM Journal of Management and IT,* 12(1), pp. 59-61.

Sethi A., et al., 2008. *Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks.* Chicago, IL, USA, IEEE.

Shah M., et al., 2019. *Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool.* Sukkur, Pakistan, IEEE.

Sharma, A., 2012. Data Management and Deployment of Cloud Applications in Financial Institutions and its Adoption Challenges. *International Journal of Scientific & Technology Research,* , 1(1), pp. 25-31.

Shulha O. et al., 2022. Banking Information Resource Cybersecurity System Modeling. *Journal of Open Innovatio: Technology, Market and Complexity,* 8(80).

Sinha S., 2018. Beginning Ethical Hacking with Kali Linux. In: *Computational Techniques for Resolving Security Issues.* s.l.:Apress Berkeley, CA.

Sipior, J. C., Ward, B. T. & Roselli, G. R., 2005. The Ethical and Legal Concerns of Spyware. *Information Systems Management,* , 22(2), pp. 39-49.

Software Testing, 2022. *Top 11 Most Powerful CyberSecurity Software Tools In 2022.* [Online]
Available at: https://www.softwaretestinghelp.com/cybersecurity-software-tools/

Soni P., July 2010. *M-Payment Between Banks Using SMS [Point of View].* s.l., IEEE, pp. 903-905.

Stytz, M. R., Lichtblau, D. E. & Banks, S. B., 2005. *Toward Using Intelligent Agents to Detect, Assess, and Counter Cyberattacks in a Network-Centric Environment.* [Online]
Available at: https://apps.dtic.mil/docs/citations/ada464134
[Accessed 10 6 2022].

Tan Z., et al., 2014. Detection of Denial-of-Service Attacks Based on Computer Vision Techniques. *IEEE Transactions on Computers*, 64(9), pp. 1-14.

The Economist, 2007. *World wide web of terror,* s.l.: s.n.

Varga et al., 2021. Cyber-threat perception and risk management in the Swedish financial sector. *Computers & Security,* 105(201), pp. 1-18.

Wireshark, n.d. *About Wireshark.* [Online]
Available at: https://www.wireshark.org/index.html#aboutWS

World Bank, 2019. *Financial Sector's Cybersecurity,* s.l.: s.n.

Xia W., et al., 2015. A Survey on Software-Defined Networking. *IEEE Communication Survey & Tutorials,* 17(1), pp. 27-51.

Yang D. et al., 13-15 June 2010. *Mobile Payment Pattern Based on Multiple Trusted Platforms - China Case.* Athens, Greece, IEEE.

Zhang Y. et al., 2007. *CANTINA: A content-based approach to detecting phishing web sites.* Banff, Alberta, Canada, s.n.

Zolkipli M. et al., March 2011. *An approach for malware behavior identification and classification.* Shanghai, China, IEEE.