An Internship Report

on

PALOALTO CYBERSECURITY VIRTUAL INTERNSHIP

Submitted in partial fulfillment of the requirements for the award of the degree of

BACHELOR OF TECHNOLOGY

in

Computer Science and Engineering (AI & ML)

by

Shaik Mohammad Rafi (224G1A3353)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
(AI & ML) SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY (AUTONOMOUS)
(Affiliated to JNTUA, accredited by NAAC with ‘A’ Grade, Approved by AICTE, New Delhi & Accredited by NBA (EEE, ECE & CSE))
Rotarypuram village, B K Samudram Mandal, Ananthapuramu-515701.
2024 - 2025

SRINIVASA RAMANUJAN INSTITUTE OF TECHNOLOGY (AUTONOMOUS)

(Affiliated to JNTUA, accredited by NAAC with 'A' Grade, Approved by AICTE, New Delhi & Accredited by NBA (EEE, ECE & CSE)) Rotarypuram village, B K Samudram Mandal, Ananthapuramu-515701.

Department of Computer Science & Engineering (AI & ML)

Certificate

This is to certify that the internship report entitled "Cybersecurity Virtual Internship" is the bonafide work carried out by **SHAIK MOHAMMAD RAFI** bearing Roll Number 224G1A3353 in partial fulfilment of the requirements for the award of the degree of **Bachelor of Technology** in **Computer Science and Engineering (Artificial Intelligence & Machine Learning)** for 10 weeks from May – July 2024.

Internship Coordinator	**Head of the Department**
Dr. P. Chitralingappa M. Tech. Ph.D.	Dr. P. Chitralingappa M.Tech. Ph.D.
Associate Professor	Associate Professor

Date:

Place: Ananthapuramu

EXTERNAL EXAMINER

PREFACE

I completed a Virtual Internship in Cybersecurity during April to June 2024. This internship was organized by two important institutions. The first one is **Palo Alto Networks Inc.**, which is a well-known company in the field of cybersecurity. It is based in Santa Clara, California, and is recognized worldwide for providing security solutions. Palo Alto Networks is responsible for creating advanced firewalls that protect networks from threats and also offers cloud-based solutions that extend those protections to cover other areas of security. The company serves more than 70,000 organizations in over 150 countries, including many well-known businesses such as 85 of the Fortune 100 companies. It is also home to **Unit 42**, a threat research team that investigates security threats. Additionally, Palo Alto Networks hosts the annual **Ignite Conference**, which is an event where experts in cybersecurity gather to discuss new developments and trends in the field.

The second institution that helped organize the internship is **Eduskills**, a training institute that has been providing computer education to people from various sectors since 2012. Eduskills is an autonomous organization registered under the Government of Assam. It is also a member of several important organizations such as ALMA International, ITRC, NISD, and ATTEST. Eduskills focuses on providing modern and innovative training, and its goal is to help students become skilled in IT, which opens up job opportunities for them. One of Eduskills' strengths is that it provides placement drives, which are events where companies come to offer jobs to students.

This internship was part of my second-year B.Tech program at **Srinivasa Ramanujan Institute of Technology** in Anantapur. This program follows the **AICTE** (All India Council for Technical Education) model curriculum, which is designed by leading academicians in India to produce graduates who are ready for the job market and have the skills that industries require. Through this internship, I was able to gain important foundational knowledge in the field of cybersecurity. Specifically, I learned about the basics of cybersecurity and the architecture of cybersecurity systems, which helped me understand how to protect networks and systems from threats. The experience has helped me prepare for a future career in cybersecurity, and thanks to Eduskills, I was also exposed to several job opportunities through their placement drives, which could lead to employment in different companies.

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany the successful completion of any task would be incomplete without the mention of people who made it possible, whose constant guidance and encouragement crowned our efforts with success. It is a pleasant aspect that I have now the opportunity to express my gratitude for all of them.

It is with immense pleasure that I would like to express my indebted gratitude to my internship coordinator **Dr. P. Chitralingappa, Associate Professor, Department of Computer Science & Engineering (AI & ML)**, who has supported me a lot and encouraged me in every step of the internship work. I thank him/her for the stimulating support, constant encouragement and constructive criticism which have made possible to bring out this internship work.

I am very much thankful to **Dr. P. Chitralingappa, Associate Professor, & HOD Department of Computer Science & Engineering (AI & ML and Data Science),** for his kind support and for providing necessary facilities to carry out the internship.

I wish to convey my special thanks to **Dr. G. Bala Krishna, Principal** of **Srinivasa Ramanujan Institute of Technology** for giving the required information in doing my internship. Not to forget, I thank all other faculty and non-teaching staff, and my friends who had directly or indirectly helped and supported me in completing my internship in time.

I also express our sincere thanks to the Management for providing excellent facilities and support**.**

Finally, I wish to convey my gratitude to my family who fostered all the requirements and facilities that I need.

Shaik Mohammad Rafi

(224G1A3353)

INDEX

LIST OF FIGURES

CHAPTER 1 INTRODUCTION

In today's world, the importance of cybersecurity has grown immensely due to the increasing number of cyber-attacks and security threats faced by individuals, businesses, and governments. As technology advances, the need to protect sensitive data, systems, and networks from unauthorized access, theft, or damage has become paramount. Cybersecurity is essential not only to safeguard information but also to defend systems from various types of malicious attacks, such as viruses and malware.

Cyber Threats

Cyber threats can be divided into two main types:

1. **Cybercrime** – This refers to crimes committed by individuals or groups that target individuals, businesses, or organizations, often for financial gain or malicious intent.
2. **Cyber warfare** – This refers to politically motivated attacks on a nation's infrastructure, such as power grids, communication networks, or military systems. These types of attacks are often state-sponsored and can lead to significant national security threats. **Cybercrime**

Cybercrime involves the use of technology, such as computers, mobile devices, and the internet, to conduct illegal activities. Hackers and cyber attackers exploit vulnerabilities in systems to steal information, cause disruptions, or commit fraud. One of the most common forms of cybercrime is hacking, where attackers breach protected systems to gain unauthorized access. This often results in identity theft, data breaches, and financial theft.

Cybercrimes can also involve direct attacks on computers, such as spreading viruses. One example is a **DoS (Denial of Service) attack**, where attackers attempt to shut down a machine or network, making it unavailable to users. This attack can temporarily or permanently disrupt services.

Malware is software used to disrupt computer operations, steal sensitive information, or gain unauthorized access to private systems. Malware can appear in different forms, such as viruses, Trojan horses, worms, or adware, which interfere with a system's proper functioning.

Some cybercrimes happen outside of computer networks. This includes **economic fraud**, where criminals target banking systems, commit credit or debit card fraud, or steal money through online financial scams.

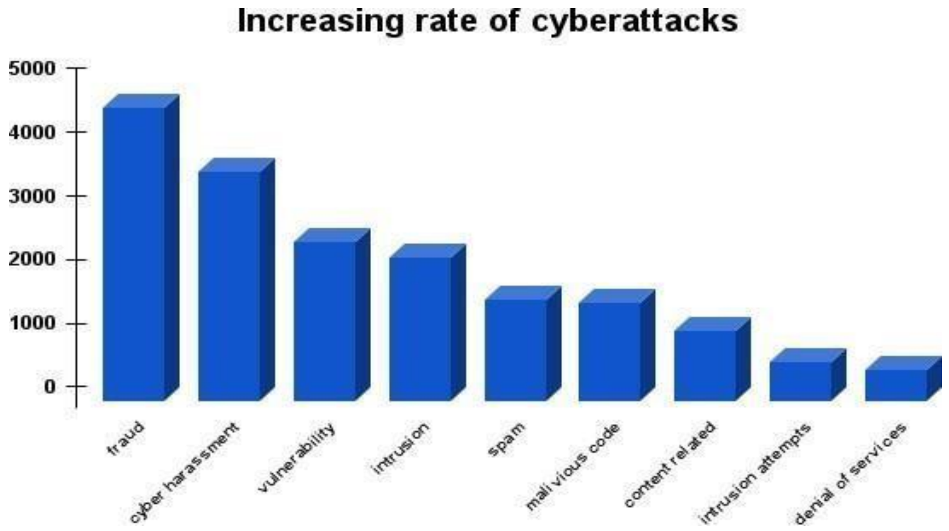


Fig.1.1 Cyber Attacks

Hinder the operations of a website or service through data alteration, data destruction. Others include using obscene content to humiliate girls and harm their reputation, Spreading pornography, threatening e-mail, assuming a fake identity, virtual impersonation. Nowadays misuse of social media in creating intolerance, instigating communal violence and inciting riots is happening a lot.

Cyber Warfare

Snowden revelations have shown that Cyberspace could become the theatre of warfare in the 21st century. Future wars will not be like traditional wars which are fought on land, water or air. When any state initiates the use of internet-based invisible force as an instrument of state policy to fight against another nation, it is called cyber war'.

It includes hacking of vital information, important webpage, strategic controls, and intelligence. In December 2014 the cyber-attack a six-month-long cyber-attack on the German parliament for which the Safety Group is suspected. Another example 2008 cyber- attack on US Military computers. Since these cyber-attacks, the issue of cyber warfare has assumed urgency in the global media.

CHAPTER 2 TECHNOLOGY

With the rapid growth of the internet, cybersecurity has become a major concern for organizations around the world. The fact that the tools and information needed to break through the security of corporate networks are easily available has increased this concern.

The main problem today is that most security technology focuses on keeping attackers out. When that fails, the entire defense system fails. Every organization that uses the internet needs security technologies to cover three main types of controls: **preventive**, **detective**, and **corrective**. These controls should also include proper auditing and reporting systems.

One key technology in cybersecurity is the **firewall**. A firewall is a network security system designed to stop unauthorized users from accessing a private network. It can be either hardware, software, or a combination of both. Firewalls prevent people on the internet from accessing private networks, such as company intranets. All messages that enter or leave the private network go through the firewall, which checks them and blocks any that don't meet the security rules.

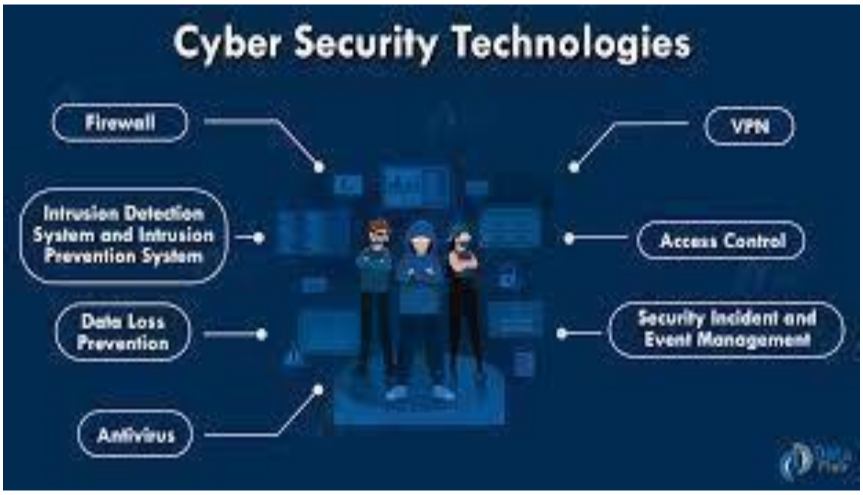

Cyber Security Technologies
Firewall
Intrusion Detection System and Intrusion Prevention System
Data Loss Prevention
Antivirus
VPN
Access Control
Security Incident and Event Management

Fig 2.1 Security Technologies 2.1 Firewall

A firewall is a security system for computer networks that blocks unauthorized access to or from a private network. It can be set up as hardware, software, or both. Firewalls are used to stop unauthorized internet users from getting into private networks that are connected to the internet.

All messages that go in or out of a private network must pass through the firewall. The firewall checks each message and blocks any that don’t meet the security rules.

Categories of Firewall Fire wall can be categorized into the

following types:

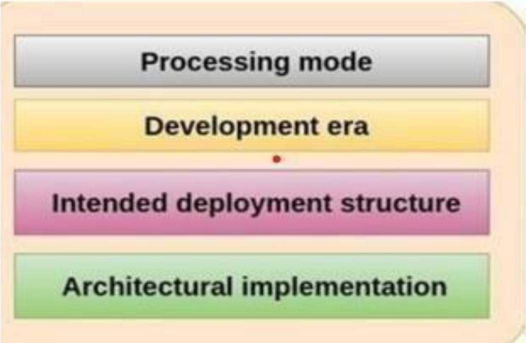


Fig 2.2 Categories of Firewalls 2.1.1 Processing mode

The five processing modes that firewalls can be categorized are

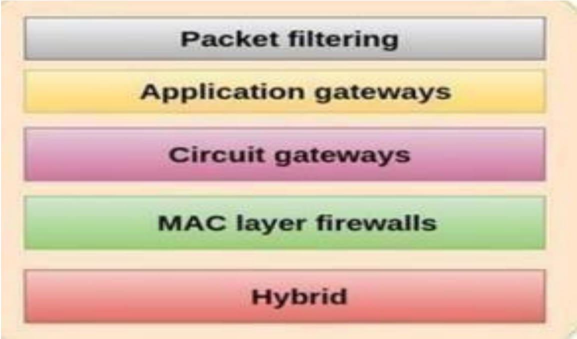


Fig.2.3 Processing mode

Packet Filtering

Packet filtering firewalls check the header information of data packets that enter a network. This firewall is installed on TCP/IP networks (Transmission Control Protocol/Internet Protocol networks) and decides whether to forward the packet to the next network connection or drop it, based on the rules programmed into the firewall. Packet filtering firewalls examine header information of a data packets that come into a network. This firewall installed on TCP/IP network and determine whether to forward it to the next network connection or drop a packet based on the rules programmed in the firewall.

It scans network data packets looking for a violation of the rules of the firewalls database. Most firewall often based on a combination of: Internet Protocol (IP) source and destination address. Direction (inbound or outbound). Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests.

Application Gateways

It is a firewall proxy which frequently installed on a dedicated computer to provides network security. This proxy firewall acts as an intermediary between the requester and the protected device. This firewall proxy filters incoming node traffic to certain specifications that mean only transmitted network application data is filtered. Such network applications include FTP, Telnet, Real Time Streaming Protocol (RTSP), Bit Torrent, etc.

Circuit Gateways

A Circuit-Level Gateway is a type of firewall that works at the transport layer of a network, providing security for TCP and UDP connections. This means it can reassemble, examine, or block all the data packets within a connection. It operates between the transport layer and the application layer (like the session layer).

Unlike Application Gateways, which only filter certain types of application data, Circuit Gateways monitor the process of TCP handshaking (the process where two devices communicate to establish a connection) and ensure that the connection follows the firewall rules. It can also function as a VPN (Virtual Private Network) by encrypting data between two firewalls, ensuring secure communication over the internet.

MAC Layer Firewalls

MAC Layer Firewalls operate at the Media Access Control (MAC) layer of the OSI (Open Systems Interconnection) network model. These firewalls filter network traffic based on the MAC addresses of specific host computers. Each MAC address is associated with an Access Control List (ACL), which defines the types of data packets that can be sent to each host. Any traffic that does not meet these criteria is blocked.

When a device tries to connect to the network, the firewall checks its MAC address to determine whether it is authorized to access the data. This ensures that only approved devices can communicate with the network, enhancing security.

Hybrid Firewalls

Hybrid Firewalls combine features from multiple types of firewalls, integrating aspects of packet filtering, proxy services, and circuit gateways. This type of firewall offers flexibility and can adapt to various security needs by utilizing the strengths of different firewall technologies.

2.1.2 Development Era

Firewall can be categorized on the basis of the generation type. These are:

First Generation

Second Generation

Third Generation

Fourth Generation

Fifth Generation

First Generation

The first-generation firewall comes with static packet filtering firewall. In this generation, the firewall examines each packet of data that enters or leaves the network. Each packet is either allowed to pass through or is blocked, based on specific rules set by the user. For example, just like a bouncer at a club who checks IDs, allowing only people over the age of 21 to enter while turning away those who are younger, the firewall uses these user-defined rules to control access to the network.

Second Generation

Second-generation firewalls are known as application-level firewalls or proxy servers. They provide better security between trusted networks (like your home or office) and untrusted networks (like the internet).

These firewalls use software to check and monitor the connections for each device on the network. They act as a middleman, known as a proxy, between users on the trusted network and the internet. It involves proxy services which act as an interface between the user on the internal trusted network and the Internet. Each computer communicates with each other by passing network traffic through the proxy program. This program evaluates data sent from the client and decides which to move on and which to drop.

Third Generation

Third-generation firewalls use a method called stateful inspection. These firewalls have been developed to meet the growing security needs of corporate networks while ensuring that the network performance remains fast.

As businesses rely more on features like VPNs (Virtual Private Networks), wireless communication, and better virus protection, the demands on third-generation firewalls continue to increase.

One of the biggest challenges in creating these firewalls is keeping them simple to use and maintain. This simplicity is important for security, but it must not come at the cost of flexibility and performance.

Fourth Generation

The fourth-generation firewall comes with dynamic packet filtering firewall. This firewall monitors the state of active connections, and on the basis of this information, it determines which network packets are allowed to pass through the firewall. By recording session information such as IP addresses and port numbers, a dynamic packet filter can implement a much tighter security posture than a static packet filter.

Fifth Generation

The fifth-generation firewall comes with kernel proxy firewall. This firewall works under the kernel of Windows NT Executive. This firewall proxy operates at the application layer. In this, when a packet arrives, a new virtual stack table is created which contains only the protocol proxies needed to examine the specific packet. These packets investigated at each layer of the stack, which involves evaluating the data link header along with the network header, transport header and application layer data.

This firewall works faster than all the application-level firewalls because all evaluation takes place at the kernel layer and not at the higher layers of the operating system.

2.1.3 Intended Deployment Structure Firewall can also be categorized based on the structure. These are –

Commercial Appliences
Small Office
Residential Software

Fig.2.4 Intended Deployment Structure Commercial Appliances It runs on a custom operating system. This firewall system consists of firewall application software running on a general-purpose computer. It is designed to provide protection for a medium-tolarge business network. Most of the commercial firewalls are quite complex and often require specialized training and certification to take full advantage of their features.

Small Office Home Office

The SOHO (Small Office/Home Office) firewall is a critical component for safeguarding small business and home office networks against a variety of Internet security threats. As these environments often lack the extensive IT resources of larger organizations, the SOHO firewall is tailored to meet the specific needs of smaller setups while maintaining a high level of security. Here's a more detailed exploration of the SOHO firewall and its functionalities. In an increasingly digital world, SOHO firewalls play a crucial role in protecting small office and home office networks from a wide array of cyber threats. They are designed to be user-friendly, cost-effective, and efficient, catering to the specific security needs of smaller environments. Whether through dedicated hardware firewalls or residential software options, implementing robust firewall solutions is essential for maintaining the security and integrity of sensitive data in small networks. As technology continues to evolve, SOHO firewalls will remain a vital part of an effective security strategy for individuals and small businesses alike.

2.1.4 Architectural Implementation

The firewall configuration that works best for a particular organization depends on three factors: the objectives of the network, the organization's ability to develop and implement the architectures, and the budget available for the function. There are four common architectural implementations of firewalls:

Fig.2.5 Architectural Implementation

Packet-Filtering Routers

A packet filtering firewall is a fundamental security mechanism that helps regulate network access by inspecting and controlling the flow of data packets traveling in and out of a network. It operates at the network layer of the OSI model, making it essential for protecting against unauthorized access and potential cyber threats. Here's a more detailed overview of how packet filtering firewalls work, their functionalities, advantages, and limitations.

Screened Host Firewalls

This firewall architecture combines the packet-filtering router with a separate and dedicated firewall. The application gateway needs only one network interface. It is allowing the router to pre-screen packets to minimize the network traffic and load on the internal proxy. The packet-filtering router filters dangerous protocols from reaching the application gateway and site systems.

Dual-Homed Host Firewalls

The network architecture for the dual-homed host firewall is simple. Its architecture is built around the dual-homed host computer, a computer that has at least two NICs. One NIC is to be connected with the external network, and other is connected to the internal network which provides an additional layer of protection. With these NICs, all traffic must go through the firewall in order to move between the internal and external networks. The Implementation of this architecture often makes use of NAT. NAT is a method of mapping assigned IP addresses to special ranges of no routable internal IP addresses, thereby creating another barrier to intrusion from external attackers.

Screened Subnet Firewalls

Screened subnet firewalls, also known as screened subnet architecture or DMZ (Demilitarized Zone) firewalls, are a more advanced network security configuration that provides enhanced protection for internal networks by creating a buffer zone between the internal network and the external Internet. This architecture is particularly effective for organizations that host servers accessible from the Internet, such as web servers, email servers, or application servers. Here's a detailed overview of screened subnet firewalls, their architecture, benefits, and limitations.

2.2 VPNs

A VPN stands for virtual private network. It is a technology which creates a safe and an encrypted connection on the Internet from a device to a network. This type of connection helps to ensure our sensitive data is transmitted safely. It prevents our connection from eavesdropping on the network traffic and allows the user to access a private network securely. This technology is widely used in the corporate environments.

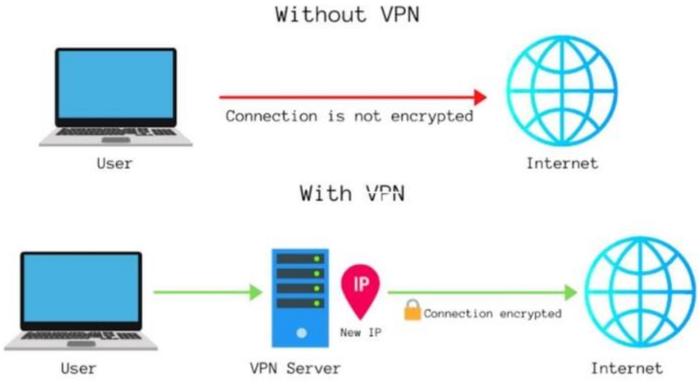


Fig 2.6 Virtual Private Network

VPNs are used by remote users who need to access corporate resources, consumers who want to download files and business travelers want to access a site that is geographically restricted.

2.3 Intrusion Detection System (IDS)

An IDS is a security system which monitors the computer systems and network traffic. It attacks originating from the outsider and also for system misuse or attacks originating from the insider. A firewall does a job of filtering the incoming traffic from the internet, the IDS in a similar way compliment the firewall security.

The Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.

Intrusion Detection System have different types to detects the suspicious activities.

2.3.1 NIDS

It is a Network Intrusion Detection System which monitors the inbound and outbound traffic to and from all the devices over the network.

2.3.2 HIDS

It is a Host Intrusion Detection System which runs on all devices in the network with direct access to both internet and enterprise internal network. It can detect anomalous network packets that originate from inside the organization or malicious traffic that a NIDS has failed to catch.

2.3.3 Signature-based Intrusion Detection System

It is a detection system which refers to the detection of an attack by looking for the specific patterns, such sequences in network traffic, or known malicious instruction sequences used by malware. This IDS originates from anti-virus software which can easily detect known attacks malware. This IDS originates from anti-virus software which can easily detect known attacks. In this terminology, it is impossible to detect new attacks, for which no pattern is available.

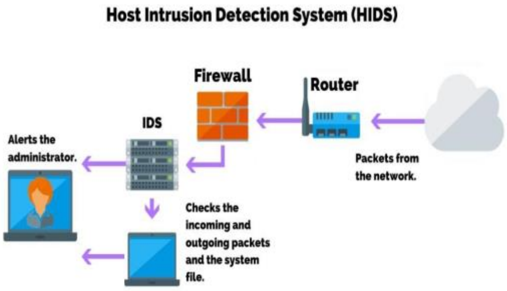

Host Intrusion Detection System (HIDS)
Firewall
Router
IDS
Alerts the administrator.
Packets from the network.
Checks the incoming and outgoing packets and the system file.

Fig 2.7 Intrusion Detection System

2.3.4 Anomaly-based Intrusion Detection System

This detection system primarily introduced to detect unknown attacks due to the rapid development of malware. It alerts administrators against the potentially malicious activity. It monitors the network traffic and compares it against an established baseline. It determines what is considered to be normal for the network with concern to bandwidth, protocols, ports and other devices. **2.4 Access Control**

Access control is a process of selecting restrictive access to a system. It is a concept in security to minimize the risk of unauthorized access to the business or organization. Here, users must provide the credential to be granted access to a system. These credentials come in many forms such as password, key card, the biometric reading, etc. Access control ensures security technology and access control policies to protect confidential information like customer data.

The access control can be categories into two types –

Physical access control

Logical access control

2.4.1 Physical Access Control

This type of access control limits access to buildings, rooms, campuses, and physical IT assets.

CHAPTER 3 APPLICATIONS

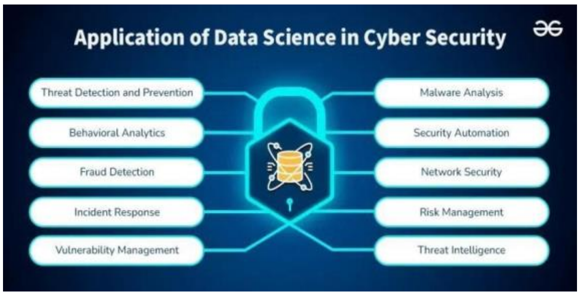


Fig 3.1 Applications of Cybersecurity

Cybersecurity threats evolve constantly, so organizations must adapt to these changes. Intruders often develop new tools and tactics to bypass security measures that are put in place to counter recent attacks.

The cybersecurity of your organization is only as strong as its weakest point. To protect your data and systems, it’s essential to have a range of cybersecurity tools and techniques available. Here are a few important applications of cybersecurity:

3.1 Network Security Surveillance

Continuous network monitoring is the practice of looking for indications of harmful or intrusive behavior. It is often used in conjunction with other security tools like firewalls, antivirus software, and IDPs. Monitoring for network security may be done manually or automatically using the software.

3.2 Identification and Access Control (IAM)

The management has control over which individual can access which sections of the data. Usually, the management regulates who has access to data, networks, and computer systems. Here is where cyber security comes into the picture by identifying users and executing an access control. Various cyber security applications ensure IAM across an organization. IAM may be implemented in both software and hardware, and it often makes use of role-based access control.

3.3 Software Security Applications that are crucial to company operations are protected by application security. It contains controls like code signing and application white listing and may assist unify your security rules with things like file-sharing rights and multifactor authentication.

3.4 Risk Management

Risk management, data integrity, security awareness training, and risk analysis are all covered by cyber security. The evaluation of risks and the control of the harm that may be done as a result of these risks are important components of risk management. The security of sensitive information is another issue covered by data security.

3.5 Planning for Disaster Recovery and Business Continuity

Data recovery helps organizations keep operating even when they experience data loss, attacks, or disasters. By regularly backing up data and investing in systems that allow business activities to continue, organizations can effectively manage severe data loss. This aspect of cybersecurity is crucial for ensuring business continuity.

3.6 Physical Security

Physical security includes measures such as system locks, intrusion detection systems, alarms, surveillance systems, and data destruction systems. These tools help organizations protect their IT infrastructure from unauthorized access and physical threats.

3.7 Compliance and Investigations

Cyber security is helpful during the examination of suspicious situations.

Additionally, it helps to upkeep and adheres to regulations.

3.8 Security During Software Development

The software aids in detecting software flaws when they are developed ensuring that regulations and standards are followed. Cyber security tools thoroughly test, scan, and analyze the software to identify any bugs, openings, or weaknesses that hackers or competing businesses might exploit. **3.9 Security against DDoS**

Cyber security aids in providing a mitigation solution to deal with DDoS. It redirects traffic to other cloud-based servers and resolves the issue.

3.10 Protecting Critical Systems

Cyber security aids in preventing assaults on huge servers linked to wide-area networks. It upholds industry-standard, strict safety standards for users to abide by cyber security precautions to secure the devices. It keeps track of all apps in real time and routinely evaluates the network security, servers, and users themselves.

CHAPTER 4 MODULES

Module-1: Introduction to Cyber security Cyber security Landscape

The modern cyber security landscape is a rapidly evolving hostile environment with advanced threats and increasingly sophisticated threat actors. This lesson describes the current cyber security landscape, explains SaaS application challenges, describes various security and data protection regulations and standards, identify cyber security threats and attacker profiles, and explains the steps in the cyber-attack lifecycle.

Cyber Attack Types

Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyber-attack strategy. This lesson describes the different malware types and properties, the relationship between vulnerabilities and exploits, and how modern malware plays a central role in a coordinated attack against a target. This lesson also explains the timeline of eliminating vulnerability.

Cyber Attack Technique

Attackers use a variety of techniques and attack types to achieve their objectives. Spamming and phishing are commonly employed techniques to deliver malware and exploits to an endpoint via an email executable or a web link to a malicious website. Once an endpoint is compromised, an attacker typically installs back doors, Remote Access Trojans (RATs), and other malware to ensure persistence. This lesson describes spamming and phishing techniques, how bots and botnet's

function, and the different types of botnets.

Advanced Persistent Threats and Wi-Fi Vulnerabilities With the explosive growth in fixed and mobile devices over the past decade, wireless (Wi-Fi) networks are growing exponentially—and so is the attack surface for Advanced Persistent Threats (ATP). This lesson describes Wi-Fi vulnerabilities and attacks and APT's. **Security Modules** The goal of a security model is to provide measurable threat prevention through trusted and untrusted entities. This can be a complicated process, as every security model will have its own customizations and many variables need to be identified. This lesson describes the core concepts of a security model and why the model is important, the functions of a perimeter-based security model, the Zero Trust security model design principles, and how the principle of least privilege applies to the Zero Trust security model.

Module-2: Fundamentals of Network Security The Connected Globe

In this lesson, we will discuss how hundreds of millions of routers deliver Transmission Control Protocol/Internet Protocol (TCP/IP) packets using various routing protocols across local-area networks and wide-area networks. We also will discuss how the Domain Name System (DNS) enables internet addresses, such as www.paloaltonetworks.com, to be translated into routable IP addresses.

Addressing and Encapsulation

This lesson describes the functions of physical, logical, and virtual addressing in networking, IP addressing basics, sub netting fundamentals, OSI and the TCP/IP models, and the packet lifecycle.

Network Security Technologies

In this lesson, we will discuss the basics of network security technologies such as firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), web content filters, virtual private networks (VPNs), data loss prevention (DLP), and unified threat management (UTM), which are deployed across the industry.

Endpoint and Security Protection

In this lesson, we will explore endpoint security challenges and solutions, including malware protection, anti-malware software, personal firewalls, host-based and intrusion prevention systems (HIPSs), and mobile device management (MDM) software. We will also introduce network operations concepts, including server and systems administration, directory services, and structured host and network troubleshooting. **Secure the Enterprise**

Module-3: Fundamentals of Cloud Security Cloud Computing

The move toward cloud computing not only brings cost and operational benefits but also technology benefits. Data and applications are easily accessed by users no matter where they reside, projects can scale easily, and consumption can be tracked effectively.

Cloud Native Technologies

Like a new universe, the cloud native ecosystem has many technologies and projects quickly spinning off and expanding from the initial core of containers.

Cloud Native Security

The speed and flexibility that are so desirable in today's business world have led companies to adopt cloud technologies that require not just more security but new security approaches. In the cloud, you can have hundreds or even thousands of instances of an application, presenting exponentially greater opportunities for attack and data theft.

Hybrid Data Centre Security

Data centers are rapidly evolving from a traditional, closed environment with static, hardware-based computing resources to an environment in which traditional and cloud computing technologies are mixed.

Prisma Access SASE Security

With increasing numbers of mobile users, branch offices, data, and services located outside the protections of traditional network security appliances, organizations are struggling to keep pace and ensure the security, privacy, and integrity of their networks and customers' data.

Prisma SaaS

Prisma SaaS builds on the existing SaaS visibility and granular control capabilities of Palo Alto Networks prevention-based architecture provided through App-ID, with detailed SaaS-based reporting and granular control of SaaS usage.

Module-4: Fundamentals of SOC (Security Operations Centre)

The Fundamentals of Security Operations Center training is a high-level introduction to the general concepts of SOC and SecOps. This lesson provides an overview of the Security Operations framework.

CHAPTER 5 REAL TIME EXAMPLES

This can be described as any attack designed to steal a user’s passwords or credentials. There are basic techniques that even non-hackers can use like manual guessing. This is where a bad actor can guess your password based on the information they learn from your social media. Or even basic shoulder surfing, where someone literally watches you as you type in your password, or even if you have a sticky note of your password on your desk.

Fig 5.1 Password Attack

Advanced techniques such as brute force attacks illustrate the dangers of weak passwords. In a brute force attack, hackers utilize software capable of generating millions of password guesses in a short time. This highlights why using a weak password can be as ineffective as having no password at all.

A password attack encompasses various methods employed to unlawfully access password-protected accounts. These attacks are often supported by software that accelerates the process of cracking or guessing passwords. The most prevalent methods include brute force attacks, dictionary attacks, password spraying, and credential stuffing.

In brute force attacks, hackers systematically attempt every possible combination of allowed characters to find the correct password. Dictionary attacks, on the other hand, involve guessing passwords by cycling through commonly used words and their simple variations, much like those found in a dictionary.

Password spraying differs from other methods by focusing on a limited set of common passwords and attempting them across multiple accounts, rather than bombarding a single account with numerous guesses. This approach reduces the likelihood of triggering account lockout mechanisms and is harder to detect. Cyber threat actors exploit end users' tendency to reuse passwords through credential stuffing. This involves utilizing breached usernames and passwords to attempt (or "stuff") a large number of login requests into a different website in hopes that some users have reused the breached usernames and passwords.

They can even use programs that have key logging. This is when you're on a malicious website or even if you've accidentally installed a key logging program, and now the hacker can see anything you type. They're basically waiting till you go to your banking website or social media and type in your credentials.

Back in August of 2021, the Canada Revenue Agency was a victim of a password cyber-attack, whereas their online systems were shut down for several days, and over 5000 accounts were compromised! This was due to the technique called credential stuffing. This is where the hackers buy or steal users' passwords from other sources and data breaches, and they use those passwords to try to log into the CRA account.

CHAPTER 6 LEARNING OUTCOMES

After you complete this training, you should be able to:

Describe the current cyber security landscape.

Identify cyber security threats.

Evaluate different malware types and cyber-attack techniques.

Describe the relationship between vulnerabilities and exploits.

Identify how spamming and phishing attacks are performed.

Describe Wi-Fi vulnerabilities, attacks, and advanced persistent threats.

Explain perimeter-based Zero Trust security models. Identify capabilities of the Palo Alto Networks prevention-first architecture.

Describe basic operations of enterprise networks, common networking devices, routed and routing protocols, network types and topologies, and services such as DNS.

Explain IP addressing, subnetting, and packet encapsulation based on the Open Systems Interconnection (OSI) model.

Describe network security technologies such as packet filtering, stateful inspection, application firewalls, and IDS and IPS and web content filters.

Explain how to explore endpoint and mobile device security using technology such as personal firewalls, host-based IPS, and management features.

Describe how to properly secure enterprise networks through PAN-OS deployment templates and migration options and DNS, URL Filtering, Threat Prevention, and Wild Fire subscription services.

Describe cloud computing models, virtualization, hypervisors, public cloud service provider options, and private deployment options.

Explain the development operations (DevOps) strategy that unites teams to discover and remediate issues, automate deployment, and reduce time to market.

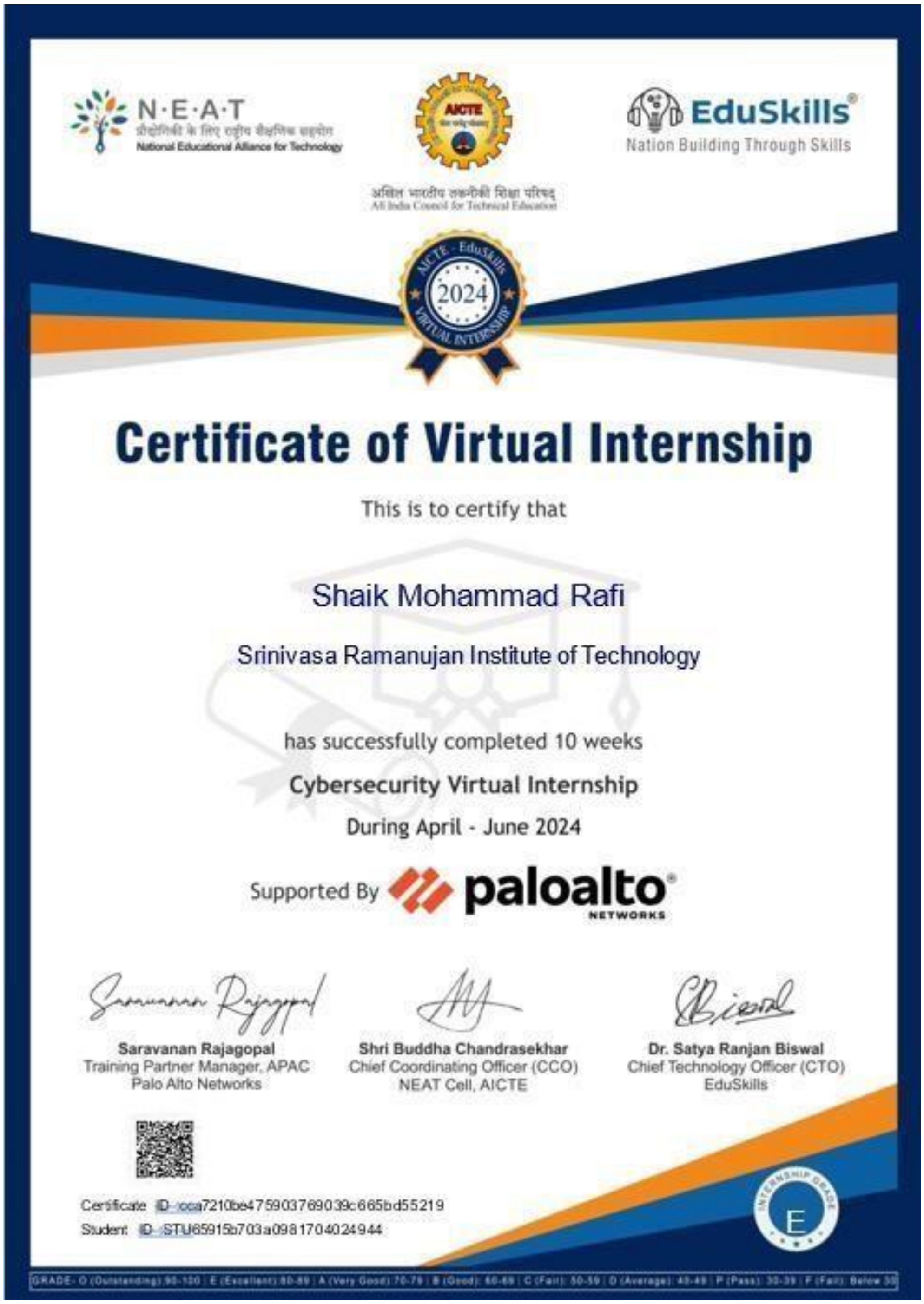
Describe the evolution of data centers through mixed traditional and cloud computing technologies.

Detail how Secure Access Service Edge (SASE) solutions help organizations embrace the concepts of cloud and mobility.

CHAPTER 7 CONCLUSION

In today's world, where the internet is ubiquitous and integral to daily life, cybersecurity plays a vital role in safeguarding a country's security. The increasing reliance on digital platforms for communication, commerce, and information sharing exposes both individuals and organizations to significant risks. To address these vulnerabilities, it is essential for both the government and citizens to collaborate in raising awareness about the importance of cybersecurity. This includes emphasizing the need for regular updates to software systems, which are crucial for closing security gaps that cybercriminals can exploit. Additionally, using effective antivirus software is paramount for protecting devices from viruses and malware that can compromise sensitive information. By fostering a culture of cybersecurity awareness and proactive measures, we can enhance our collective defenses against cyber threats and ensure a safer digital environment for everyone.

INTERNSHIP CERTIFICATE



N·E·A·T
प्रौद्योगिकी के लिए राष्ट्रीय शैक्षणिक गठबंधन
National Educational Alliance for Technology

AICTE
अखिल भारतीय तकनीकी शिक्षा परिषद्
All India Council for Technical Education

EduSkills®
Nation Building Through Skills

AICTE - EduSkills 2024 VIRTUAL INTERNSHIP

Certificate of Virtual Internship

This is to certify that

Shaik Mohammad Rafi

Srinivasa Ramanujan Institute of Technology

has successfully completed 10 weeks

Cybersecurity Virtual Internship

During April - June 2024

Supported By paloalto® NETWORKS

Saravanan Rajagopal
Training Partner Manager, APAC
Palo Alto Networks

Shri Buddha Chandrasekhar
Chief Coordinating Officer (CCO)
NEAT Cell, AICTE

Dr. Satya Ranjan Biswal
Chief Technology Officer (CTO)
EduSkills

Certificate ID cca7210be4759037690 39c665bd55219
Student ID STU65915b703a0981704024944

INTERNSHIP GRADE E

GRADE- O (Outstanding):90-100 | E (Excellent):80-89 | A (Very Good):70-79 | B (Good): 60-69 | C (Fair): 50-59 | D (Average): 40-49 | P (Pass): 30-39 | F (Fail): Below 30

REFERENCES

[1]. https://beacon.paloaltonetworks.com/student/collection/737796-palo-alto-networks certified cybersecurity-entry-level-technician-packet.

[2].A Cybersecurity Agenda for the 45th President. (2017, January 5). Retrieved from https://www.csis.org/news/cybersecurity-agenda-45th-president

[3]. An Examination of the Cybersecurity Labor Market. (n.d.). Retrieved from http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RA ND_RR430.pdf

[4]. Applications Now Available for City Colleges of Chicago's New Cyber Security "Boot Camp". (2017, March 18). Retrieved from http://www.ccc.edu/news/Pages/Applications-Now-Available-for-City-Colleges- of-Chicagos-New-Cyber-Security-Boot-Camp-.aspx

[5].Apprenticeship USA Investments. (2017, June 22). Retrieved from https://www.dol.gov/featured/apprenticeship/grants

[6].Assessment Act. Retrieved from https://www.congress.gov/bill/114th-congress/senate-bill/2007/text

[7].ATE Centers. (n.d.). Retrieved from http://www.atecenters.org/