PREFACE

Brief overview of the company’s history

- The Cyber security checking began in the 1970s when researcher **Bob Thomas** created a computer program called Creeper that could move across ARPANET's network.

- Cyber security began in the 1970s when researcher **Bob Thomas** created a computer programme called Creeper that could move across ARPANET’s network, leaving a breadcrumb trail wherever it went. Ray Tomlinson, the inventor of email, wrote the programme Reaper, which chased and deleted Creeper. Reaper was the very first example of antivirus software and the first self-replicating programme, making it the first-ever computer worm.

- Cyber security is the practice of **defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.** It's also known as information technology security or electronic information security.

- Cyber security is the art of **protecting networks, devices and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity and availability of information.**

Company’s Mission Statement

There are two primary versions of the mission statement for a cyber Program that we'll typically encounter: risk reduction and loss prevention.

Business Activities

- Cyber Security Specialist.

- Network Architect.

- Penetration Tester.

- Forensic Expert.

- Info Assurance Engineer.

- Information Security Analyst.

ACKNOWLEDGEMENTS

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. Mr.L.Suman, Assistant Professor, Computer Science and Engineering(Data Science),who has supported me with a lot and encouragement in every step of the internship work. I thank him 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 (CSD), Computer Science And Engineering(Data Science), for his kind support and for providing necessary facilities to carry out the work.

I wish to convey my special thanks to Dr. G. Balakrishna, 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 our gratitude to my family who fostered all the requirements and facilities that I need.

P.Bhargavi

204G1A3204

CONTENTS

Contents **Page No**

LIST OF FIGURES

LIST OF ABBREVIATIONS

DoS	Denial-of-Service
IDS	Intrusion Detection System
NIDS	Network Intrusion Detection System
HIDS	Host Intrusion Detection System
SaaS	Software as a service
RAT	Remote Access Trojans
APT	Advanced Persistent Threats
TCP/IP	Transmission Control Protocol/Internet Protocol
DNS	Open Systems Interconnection
IDS	Intrusion Detection Systems

CHAPTER 1

INTRODUCTION

In today's world, cyber security is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. This software protects the data. Cyber security is important because not only it helps to secure information but also our system from virus attack.

Cyber security means protecting data, networks, programs and other information from unauthorized or unattended access, destruction or change. In today’s world, cyber security is very important because of some security threats and cyber-attacks. For data protection, many companies develop software. This software protects the data. Cyber security is important because not only it helps to secure information but also our system from virus attack. After the U.S.A. and China, India has the highest number of internet users.

1.1 Cyber Threats

It can be further classified into 2 types. Cybercrime – against individuals, corporate, etc. and Cyber warfare – against a state.

1.2 Cyber Crime

Use of cyberspace, i.e computer, internet, cell-phone, other technical devices, etc., to commit a crime by an individual or organized group is called cyber-crime. Cyber attackers use numerous software and codes in cyberspace to commit cybercrime. They exploit the weaknesses in the software and hardware design through the use of malware. Hacking is a common way of piercing the defences of protected computer systems and interfering with their functioning. Identity theft is also common.

Cybercrimes may occur directly i.e., targeting the computers directly by spreading computer viruses. Other forms include DoS attack. It is an attempt to make a machine or network resource unavailable to its intended users. It suspends services of a host connected to the internet which may be temporary or permanent.

Malware is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It usually appears in the form of code, scripts, active content, and other software. ‘Malware’ refers to a variety of forms of hostile or intrusive software, for example, Trojan Horses, root kits, worms, adware, etc.

Another way of committing cybercrime is independent of the Computer Network or Device. It includes Economic frauds. It is done to destabilize the economy of a country, attack on banking security and transaction system, extract money through fraud, acquisition of credit/debit card data, financial theft, etc.

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.

1.3 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 cyberattack a six-month-long cyber-attack on the German parliament for which the sofacy group is suspected.Military computers.

CHAPTER-2

TECHNOLOGY

With the rapid growth in the Internet, cyber security has become a major concern to organizations throughout the world. The fact that the information and tools & technologies needed to penetrate the security of corporate organization networks are widely available has increased that security concern.

Today, the fundamental problem is that much of the security technology aims to keep the attacker out, and when that fails, the defences have failed. Every organization who uses internet needed security technologies to cover the three primary control types - preventive, detective, and corrective as well as provide auditing and reporting. Most security is based on one of these types of things: something we have (like a key or an ID card), something we know (like a PIN or a password), or something we are (like a fingerprint).

Some of the important security technologies used in the cyber security are described below-

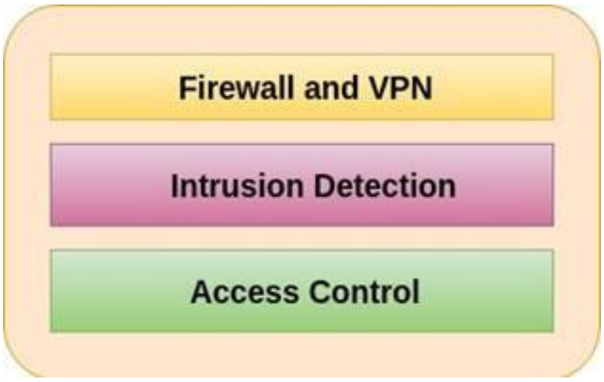


Fig.1-Security Technologies

2.1 Firewall

Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to prevent unauthorized Internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those that do not meet the specified security criteria.

2.2 Categories of Firewalls

Firewall can be categorized into the following types-

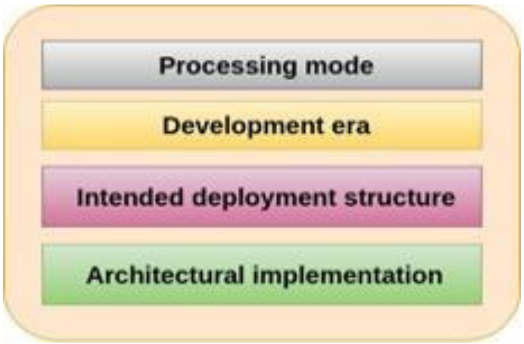


Fig.2-Categories of Firewalls

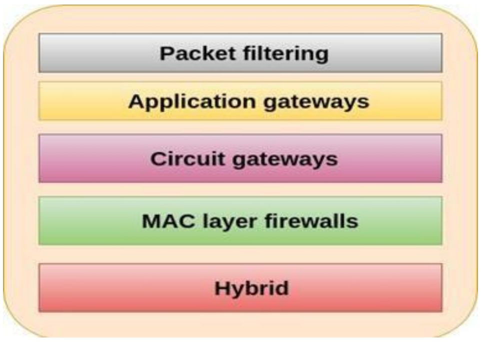


Fig.3-Processing mode

2.2.1 Processing mode

The five processing modes that firewalls can be categorized are-

- **Packet filtering**

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.
- Packet filtering firewalls can be categorized into two types-
    - **Static filtering:** The system administrator set a rule for the fire wall. These filtering rules governing how the firewall decides which packets are allowed and which are denied are developed and installed.
    - **Dynamic filtering:** It allows the firewall to set some rules for itself, such as dropping packets from an address that is sending many bad packets.

- **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 firewall that operates at the transport layer. It provides UDP and TCP connection security which means it can reassemble, examine or block all the packets in a TCP or UDP connection. It works between a transport layer and an application layers such as the session layer. Unlike application gateways, it monitors TCP data packet handshaking and session fulfilment of firewall rules and policies. It can also act as a Virtual Private Network (VPN) over the Internet by doing encryption from firewall to firewall.

- **MAC layer firewalls**

  This firewall is designed to operate at the media access control layer of the OSI network model. It is able to consider a specific host computer's identity in its filtering decisions. MAC addresses of specific host computers are linked to the access control list (ACL) entries. This entry identifies specific types of packets that can be sent to each host and all other traffic is blocked. It will also check the MAC address of a requester to determine whether the device being used are able to make the connection is authorized to access the data or not.

- **Hybrid firewalls**

  It is a type of firewalls which combine features of other four types of firewalls. These are elements of packet filtering and proxy services, or of packet filtering and circuit gateways.

2.2.2 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. A static packet filter is the simplest and least expensive forms of firewall protection. In this generation, each packet entering and leaving the network is checked and will be either passed or rejected depends on the user-defined rules. We can compare this security with the bouncer of the club who only allows people over 21 to enter and below 21 will be disallowed.

- **Second Generation**

Second-generation firewall comes with application-level or proxy servers. This generation of firewall increases the security level between trusted and untrusted networks. An application-level firewall uses software to intercept connections for each IP and to perform security inspection. 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**

The third-generation firewall comes with the stateful inspection firewalls. This generation of the firewall has evolved to meet the major requirements demanded by corporate networks of increased security while minimizing the impact on network performance. The needs of the third-generation firewalls will be even more demanding due to the growing support for VPNs, wireless communication, and enhanced virus protection. The most challenging element of this evolution is maintaining the firewall's simplicity (and hence its maintainability and security) without compromising flexibility.

- **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, session layer information, 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.

2.2.3. Intended deployment structure

Firewall can also be categorized based on the structure. These are-

Commercial Appliences
Small Office
Residential Software

Fig.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.

- **Small Office Home Office**

  The SOHO firewall is designed for small office or home office Networks who need protection from Internet security threats.

- **Residential Software**

  Residential-grade firewall software is installed directly on a user system. Some of these applications combine firewall services with other protections such as antivirus or intrusion detection.

2.2.4. 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.

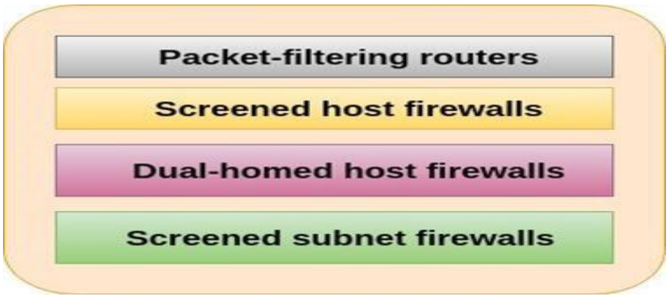


Fig.5-Architectural Implementation

- **Packet-filtering routers**

  Packet filtering firewall is used to control the network access by monitoring the outgoing and incoming packets. It allows them to pass or halt based on the source and destination IP addresses protocols and ports. During communication, a node transmits a packet; this packet is filtered and matched with the predefined rules and policies. Once it is matched, a packet is considered secure and verified and are able to be accepted otherwise blocked them. 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**

  This architecture adds an extra layer (perimeter network) of security to the screened host architecture by adding a perimeter network that further isolates the internal network from the Internet. In this architecture, there are two screening routers and both connected to the perimeter net. One router sits between the perimeter net and the internal network, and the other router sits between the perimeter net and the external network. To break into the internal network, an attacker would have to get past both routers. There is no single vulnerable point that will compromise the internal network.

- **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.

  A VPN works same as firewall like firewall protects data local to a device wherever VPNs protects data online. To ensure safe communication on the internet, data travel through secure tunnels, and VPNs user used an authentication method to gain access over the VPNs server. 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 analyses that traffic for possible hostile 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 compliments the firewall security. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, 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. HIDS may also identify malicious traffic that arises from the host itself.

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 as byte 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. In this terminology, it is impossible to detect new attacks, for which no pattern is available.

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. In this, users are granted access permission and certain privileges to a system and resources. 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.

2.4.2. Logical access control

This type of access control limits connection to computer networks,system files.

The more secure method for access control involves two factor authentication. The first factor is that a user who desires access to a system must show credential and the second factor could be an access code, password, and a biometric reading.

The access control consists of two main components:

Authorization and Authentication. Authentication is a process which verifies that someone claims to be granted access whereas an authorization provides that whether a user should be allowed to gain access to a system or denied it.

CHAPTER-3

APPLICATIONS

Cyber security threats change over time and it is important for organizations to counter these threats. Intruders adjust by creating new tools and tactics to undermine security when new protections are developed to counter more recent attacks. Your organization's cyber security is only as strong as its weakest link. To safeguard your data and systems, it's crucial to have a collection of cyber security tools and techniques at your disposal. Below are a few important applications of cyber security -

3.1. Network Security Surveillance

Continuous network monitoring is the practice of looking for indications of harmful or intrusive behaviour. 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 (IAC)

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 (RBAC) to limit access to certain system components.

Managers can manage who has access to what, when they can access it, and for how long, thanks to solution providers like Okta.

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 multi-factor authentication. With the application of AI in cyber security, software security is bound to increase.

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 enables organizations to continue working in the event of data loss, assaults, or calamities. By regularly data backup and spending money on a system that will enable corporate activities to continue, this application offers models or techniques that may help firms manage with severe data loss. Thus, this application of cyber security ensures business continuity.

3.6. Physical Security

System locks, intrusion detection systems, alarms, surveillance systems, and data destruction systems are a few examples of physical security measures. These allow organizations to secure their IT infrastructure.

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 being developed and 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

4.1.1. 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 cyberattack lifecycle.

4.1.2. Cyberattack 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.

4.1.3. Cyberattack Techniques

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 botnets 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.

4.1.4. 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

4.2.1. 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.

4.2.2. 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.

4.2.3. 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.

4.2.4. 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 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.

4.2.5. Secure the Enterprise

In this lesson, we will explore endpoint security challenges and solutions, including malware protection, anti-malware software, personal firewalls, host-based 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.

Module-3: Fundamentals of cloud security

4.3.1. 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.

4.3.2. 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.

4.3.3. 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.

4.3.4. Hybrid Data center 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.

4.3.5. 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.

4.3.6. 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.

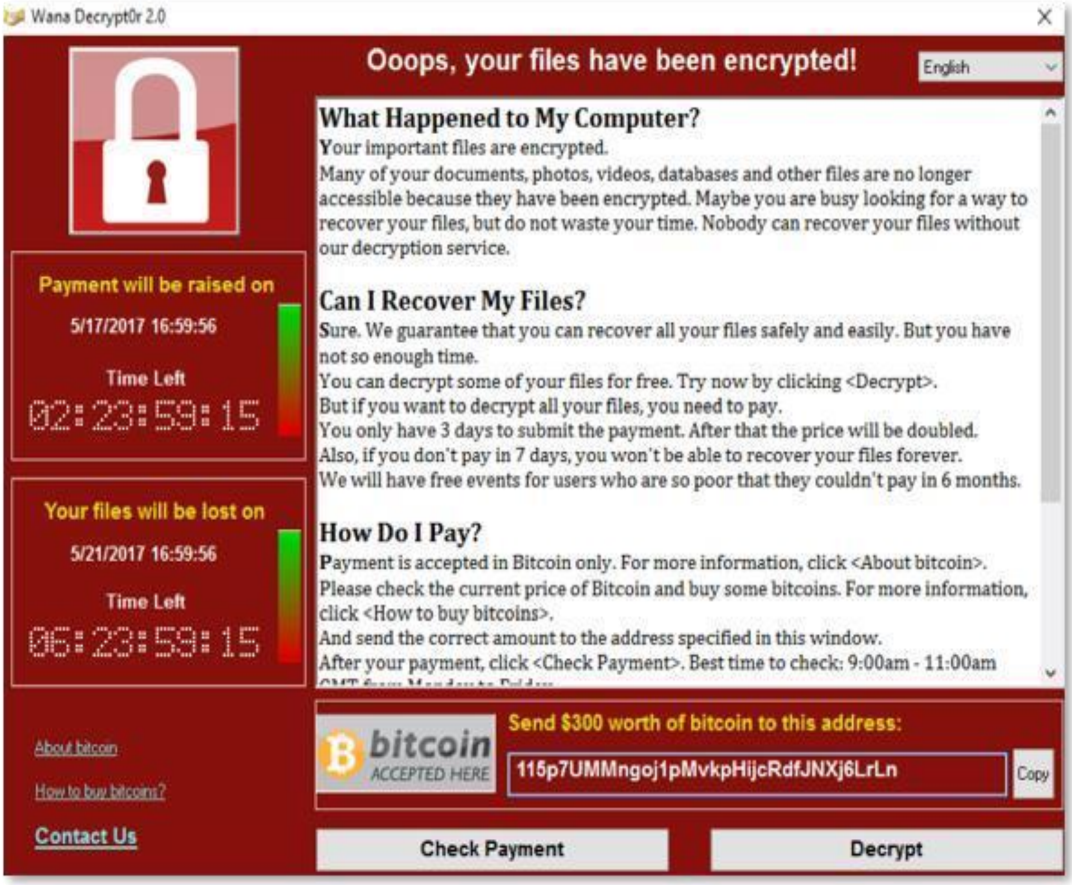
Module-4: Fundamentals of SOC (Security operations center)

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

Ransomware specific type of malware that gains control of your system and blocks access to your files. It can infect your computer from an email attachment or through a bad website. Upon infection, a ‘ransom note’ pops up, offering to restore your system back to normal in exchange for compensation. With ransomware, we always recommend to never pay the ransom! Why? There is absolutely no guarantee that you’ll get your files back. You simply cannot trust a criminal to adhere to their promises. Secondly, you’ll be putting a target on your back. If you pay the ransom once, you’ll be flagged as a user who pays the ransom, and the criminals will be back to take advantage of you again.



What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

Fig.6-Example of Ransomware

CHAPTER-6

OUTCOMES

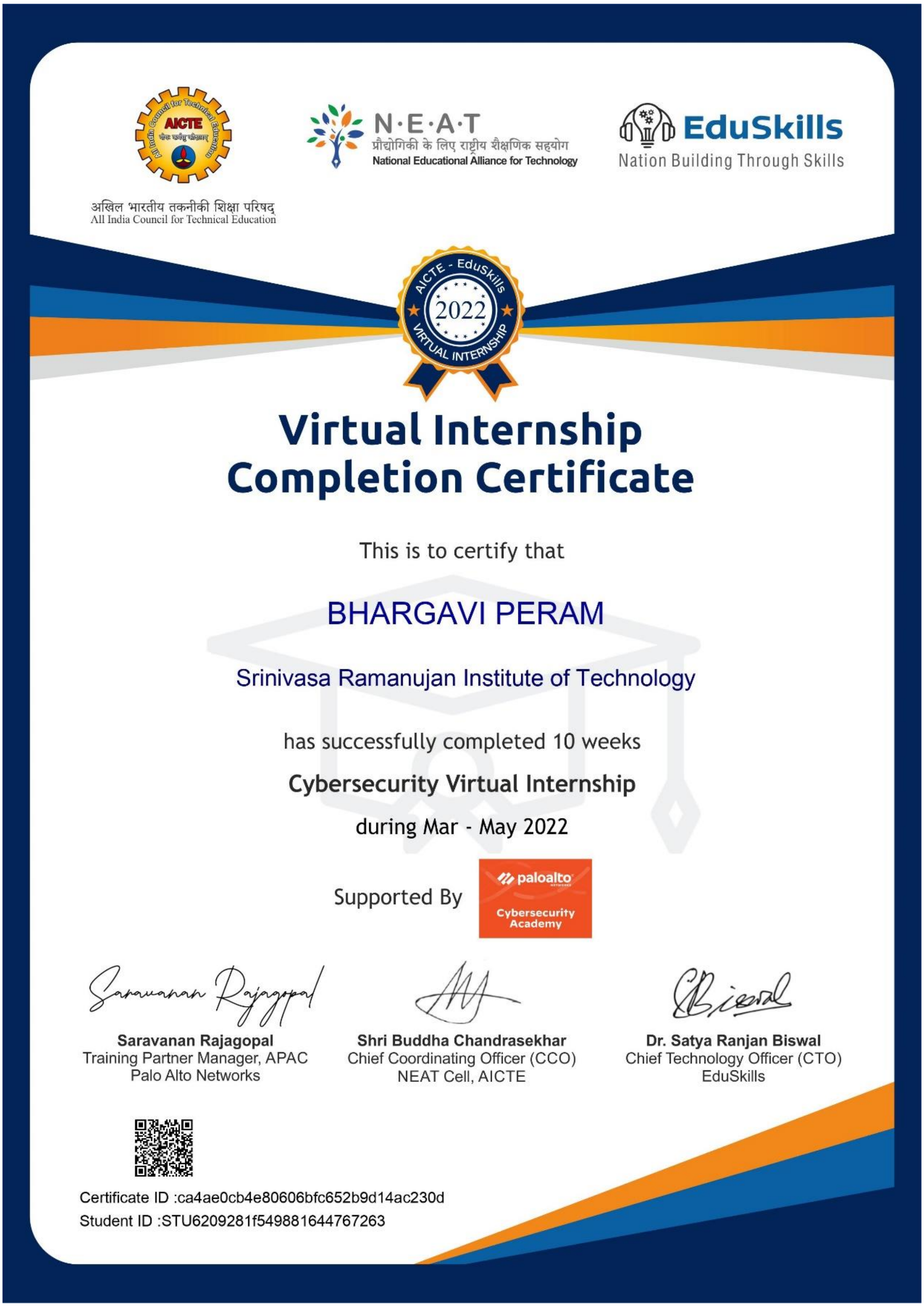
After you complete this training, you should be able to:

- Describe the current cyber security landscape. o Identify cyber security threats. o Evaluate different malware types and cyberattack techniques. o Describe the relationship between vulnerabilities and exploits. o Identify how spamming and phishing attacks are performed. o Describe Wi-Fi vulnerabilities, attacks, and advanced persistent threats. o Explain perimeter- based Zero Trust security models. o Identify capabilities of the Palo Alto Networks prevention-first architecture.
- Explain IP addressing, subnetting, and packet encapsulation based on the Open Systems Interconnection (OSI) model. o 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 center through mixed traditional and cloud computing technologies.

CONCLUSION

Today due to high internet penetration, cyber security is one of the biggest-need of the world as cyber security threats are very dangerous to the country’s security. Not only the government but also the citizens should spread awareness among the people to always update your system and network security settings and to the use proper anti-virus so that your system and network security settings stay virus and malware-free.

INTERNSHIP CERTIFICATE



AICTE

अखिल भारतीय तकनीकी शिक्षा परिषद्
All India Council for Technical Education

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

EduSkills
Nation Building Through Skills

AICTE - EduSkills
2022
VIRTUAL INTERNSHIP

Virtual Internship Completion Certificate

This is to certify that

BHARGAVI PERAM

Srinivasa Ramanujan Institute of Technology

has successfully completed 10 weeks

Cybersecurity Virtual Internship

during Mar - May 2022

Supported By paloalto Cybersecurity Academy

Saravanan Rajagopal

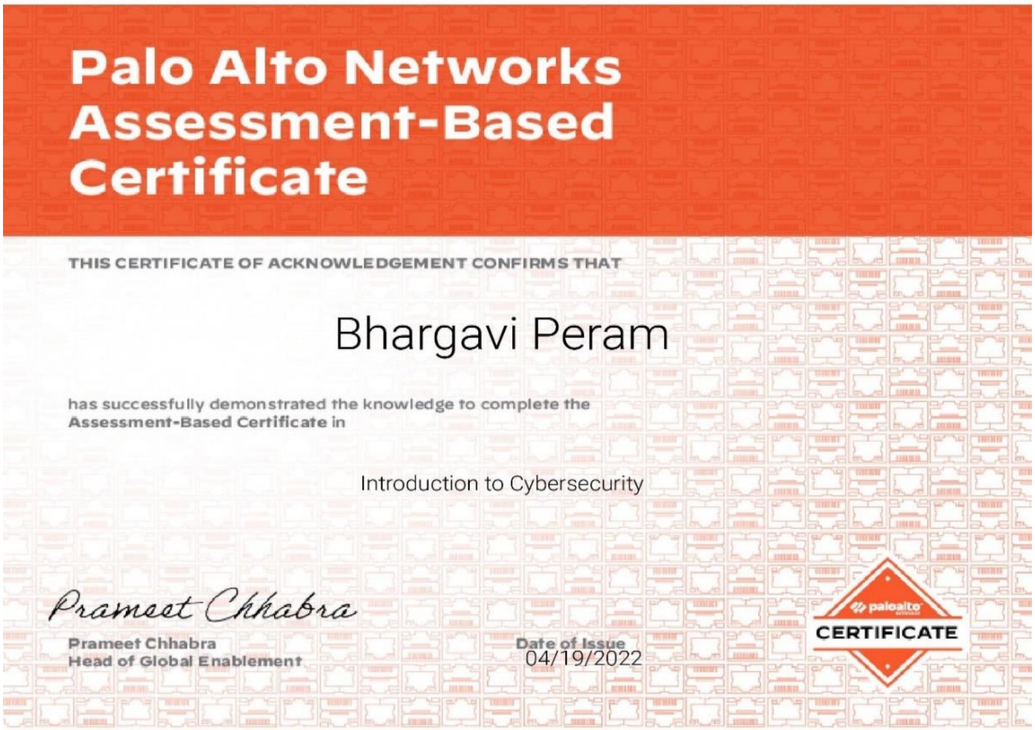
Saravanan Rajagopal
Training Partner Manager, APAC
Palo Alto Networks

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

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

Certificate ID :ca4ae0cb4e80606bfc652b9d14ac230d
Student ID :STU6209281f549881644767263

INTRODUCTION TO CYBERSECURITY



Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Bhargavi Peram

has successfully demonstrated the knowledge to complete the Assessment-Based Certificate in

Introduction to Cybersecurity

Prameet Chhabra

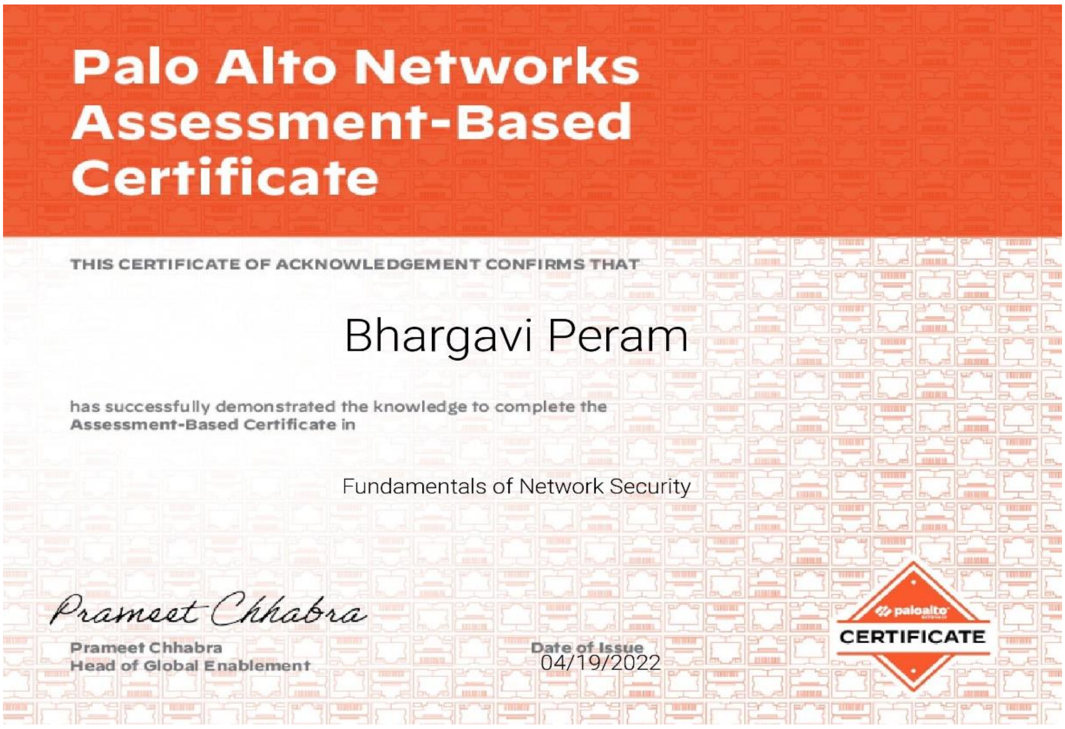
Prameet Chhabra
Head of Global Enablement

Date of Issue
04/19/2022

paloalto

CERTIFICATE

FUNDAMENTALS OF NETWORK SECURITY



Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Bhargavi Peram

has successfully demonstrated the knowledge to complete the Assessment-Based Certificate in

Fundamentals of Network Security

Prameet Chhabra

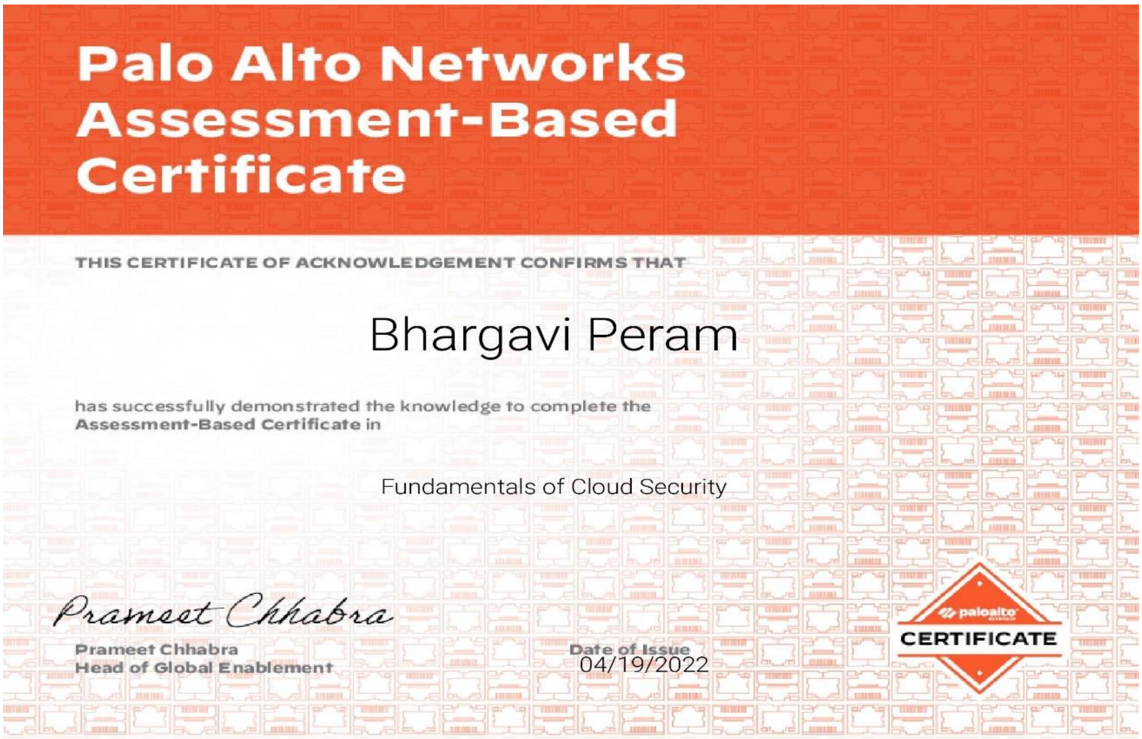
Prameet Chhabra
Head of Global Enablement

Date of Issue
04/19/2022

paloalto

CERTIFICATE

FUNDAMENTALS OF CLOUD SECURITY



Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Bhargavi Peram

has successfully demonstrated the knowledge to complete the Assessment-Based Certificate in

Fundamentals of Cloud Security

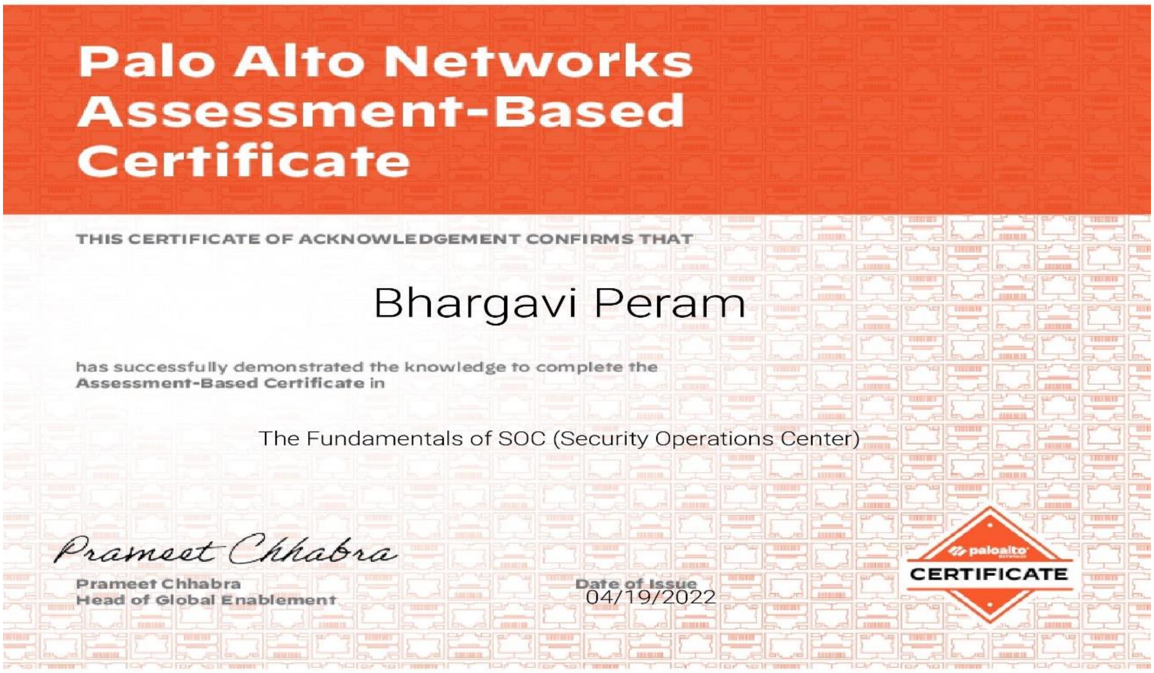
Prameet Chhabra

Prameet Chhabra
Head of Global Enablement

Date of Issue
04/19/2022

paloalto
CERTIFICATE

THE FUNDAMENTALS OF SOC (SECURITY OPERATIONS CENTER)



Palo Alto Networks Assessment-Based Certificate

THIS CERTIFICATE OF ACKNOWLEDGEMENT CONFIRMS THAT

Bhargavi Peram

has successfully demonstrated the knowledge to complete the Assessment-Based Certificate in

The Fundamentals of SOC (Security Operations Center)

Prameet Chhabra

Prameet Chhabra
Head of Global Enablement

Date of Issue
04/19/2022

paloalto
CERTIFICATE

References

- https://www.etechcomputing.com/7-types-of-cyber-security-attacks-with-real-lifeexamples/#:~:text=Drive%2DBy%20Download%20Attacks&text=A%20common%20ex ample%20of%20this,being%20downloaded%20onto%20your%20computer.
- https://beacon.paloaltonetworks.com/student/collection/737796/path/831806