A

Virtual Internship Report on

Cyber Security

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

Bachelor of Technology

In

Computer Science & Engineering

By

P Anjaneyulu (20B81A05D3)

Under the Esteemed Supervision of

Mr. Sravanan Rajagopal, Training Partner Manager

Edu Skills, Hyderabad

(Duration: September 2022 to November 2022)

DEPARTMENT OF COMPUTR SCIENCE & ENGINEERING

SIR C R REDDY COLLEGE OF ENGINEERING

Approved by AICTE, Permanently affiliated to JNTU, Kakinada

Eluru, Andhra Pradesh

2020-2024

SIR C R REDDY COLLEGE OF ENGINEERING

CERTIFICATE

This is to certify that this Virtual Internship report entitled "**Cyber Security Internship"** submitted by **Pemmani Anjaneyulu (20B81A05D3),**in partial fulfillment for the award of degree of **BACHELOR OF TECHNOLOGY** in **COMPUTER SCIENCE AND ENGINEERING**, at **SIR C R REDDY College of Engineering**, Eluru affiliated to Jawaharlal Nehru Technological University, Kakinada.

Internship Internal Coordinator
K.B.Vara Prasad, M.Tech
Assistant Professor, CSE

Head of the Department
Dr. A Yesu Babu, M.Tech, Ph.D
Professor & Head, CSE

External Examiner

CERTIFICATE LINK:

https://drive.google.com/file/d/18xJpjYTletRVKvN6_7Phsj633D40F0Cw/view?usp=share_link

ACKNOWLEDGEMENT

First I would like to thank **Mr.SRAVANAN RAJAGOPAL**, TRAINING PARTNER MANAGER , Head, of , **Edu Skills,HYDERABAD** for giving me the opportunity to do an internship within the organization.

I also would like all the people that worked along with me **EDU SKILLS,HYDERABAD** to their patience and openness they created an enjoyable working environment.

It is indeed with a great sense of pleasure and immense sense of gratitude that I acknowledge the help of these individuals.

I am highly indebted to Principal **Dr. K. VENKATESWARA RAO,** for the facilities provided to accomplish this internship

I would like to thank my Head of the Department **Dr. A.YESU BABU** for his constructive criticism throughout my internship.

I would like to thank, **Mr. K.B. Vara Prasad** internship internal coordinator Department of CSE for their support and advices to get and complete internship in above Said organization.

I am extremely great full to my department staff members and friends who helped me in successful completion of this internship.

P. ANJANEYULU

20B81A05D3

ABSTRACT

.

Organization Information:

Palo Alto Cybersecurity Academy and Edu Skills have teamed up to create an outcome-driven skilling eff01t that will train 2000+ educators and 5000 students on Cybersecurity. This program has been recognized by APSCHE for delivery as a virtual internship program to all higher education students in India named up to create an outcome-driven skilling eff01t that will train 2000+ educators and 5000 students on Cybersecurity. This program has been recognized by APSCHE for delivery as a virtual internship program to all higher education students in India.

Learning Objectives/Internship Objectives

- Internships are generally thought of to be reserved for college students looking to gain experience in a particular field. However, a wide array of people can benefit from Training Internships in order to receive real world experience and develop their skills.

- An objective for this position should emphasize the skills you already possess in the area and your interest in learning more

- Internships are utilized in a number of different career fields, including architecture, engineering, healthcare, economics, advertising and many more.

- Some internship is used to allow individuals to perform scientific research while others are specifically designed to allow people to gain first-hand experience working.

- Utilizing internships is a great way to build your resume and develop skills that can be emphasized in your resume for future jobs. When you are applying for a Training Internship, make sure to highlight any special skills or talents that can make you stand apart from the rest of the applicants so that you have an improved chance of landing the position.

WEEKLY OVERVIEW OF INTERNSHIP ACTIVITIES

Week	NAME OF THE TOPIC/MODULE COMPLETED
Week – 1	Introduction to Cyber Security
Week – 2	Fundamentals to Network Security
Week – 3	Fundamentals to Cloud Security
Week – 4	Fundamentals to SOC (Security Operation Center)
Week – 5	Project Development
Week – 6	Project Development and Project Submission

INDEX

S.no **CONTENTS** **Page no**

1. INTRODUCTION

Cyber Security is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services.

It is a process that's designed to protect networks and devices from external threats. Businesses typically employ Cyber Security professionals to protect their confidential information, maintain employee productivity, and enhance customer confidence in products and services. The range of operations of cyber security involves protecting information and systems from major cyber threats.

These threats take many forms. As a result, keeping pace with cyber security strategy and operations can be a challenge, particularly in government and enterprise networks where, in their most innovative form, cyber threats often take aim at secret, political and military assets of a nation, or its people. The modern cybersecurity landscape is a rapidly evolving hostile environment with advanced threats and increasingly sophisticated threat actors. This lesson describes the current cybersecurity landscape, explains SaaS application challenges, describes various security and data protection regulations and standards, identify cybersecurity threats and attacker profiles, and explains the steps in the cyberattack lifecycle.

Modern cyberattack strategy has evolved from a direct attack against a high-value server or asset ("shock and awe") to a patient, multistep process that blends exploits, malware, stealth, and evasion in a coordinated network attack ("low and slow"). Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack 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.

2. DESCRIPTION OF INTERNSHIP

The PCCET certification is the first of its kind credential to cover foundational knowledge of industry recognized cybersecurity and network security concepts as well as various cutting-edge advancements across all Palo Alto Networks technologies. As the cybersecurity landscape becomes more complex, Palo Alto Networks Education Services has taken steps to align with industry standards following the NIST/NICE (National Institute of Standards and Technology/National Initiative for Cybersecurity Education) workforce framework

Target Audience: The PCCET certification is designed for students, technical professionals, as well as any non-technical individuals interested in validating comprehensive knowledge on current cybersecurity tenets.

TRAINING CURRICULUM

Introduction to Cyber Security

Fundamentals of Network Security

Fundamentals of Cloud Security

Fundamentals of SOC (Security Operation Center)

PROGRAM SCHEDULE:

Virtual Internship Starts on: September 2022

Virtual Internship Ends on: November 2022

Certificate Distribution by: 16 November 2022

3.MODULES

1.Introduction to Cyber Security

2.Fundamentals of Network Security

3.Fundamentals to Cloud Security

4.Fundamentals of SOC (Security Operation Center)

5.Technology

6.Internship Reflection

7.Conclusion

Introduction to Cyber Security

This course introduces the fundamentals of cybersecurity, including the concepts needed to recognize and potentially mitigate attacks against home networks and mission-critical infrastructure.

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

- Describe the current cybersecurity landscape
- Identify cybersecurity threats
- Evaluate different malware types and cyberattack 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

Lesson Topics:

This course comprises five lessons and takes about two hours to complete.

- Lesson 1: Cyber Security Landscape
- Lesson 2: Cyberattack Types
- Lesson 3: Cyberattack Techniques
- Lesson 4: APTs and Wi-Fi Vulnerabilities
- Lesson 5: Security Models

Lesson 1: Cyber Security Landscape:

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

Modern Computing Trends:

The nature of enterprise computing has changed dramatically over the past decade.

Introduction to Web 2.0 and Web 2.0 Applications

Core business applications are now commonly installed alongside Web 2.0 apps on a variety of endpoints. Networks that were originally designed to share files and printers are now used to collect massive volumes of data, exchange real-time information, transact online business, and enable global collaboration. Many Web 2.0 apps are available as software-as-a-service (SaaS), web-based, or mobile apps that can be easily installed by end users or that can be run without installing any local programs or services on the endpoint

Web 3.0

The vision of Web 3.0 is to return the power of the internet to individual users, in much the same way that the original Web 1.0 was envisioned. To some extent, Web 2.0 has become shaped and characterized, if not controlled, by governments and large corporations dictating the content that is made available to individuals and raising many concerns about individual security, privacy, and liberty. AI and Machine Learning

New Application Threat Vectors

Exploiting vulnerabilities in core business applications has long been a predominant attack vector, but threat actors are constantly developing new tactics, techniques, and procedures (TTPs).

Protect Networks and Cloud Environments

To effectively protect their networks and cloud environments, enterprise security teams must manage the risks associated with a relatively limited, known set of core applications, as well as the risks associated with an ever-increasing number of known and unknown cloud-based applications. The cloud-based application consumption model has revolutionized the way organizations do business, and applications such as Microsoft Office 365 and Salesforce are being consumed and updated entirely in the cloud.

Lesson 2: Cyberattack Types:

Attackers use a variety of techniques and attack types to achieve their objectives. Malware and exploits are integral to the modern cyberattack 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 a vulnerability.

Malware Types:

Logic Bombs

A logic bomb is malware that is triggered by a specified condition, such as a given date or a particular user account being disabled.

Spyware and adware

Spyware and adware are types of malwares that collect information, such as internet surfing behavior, login credentials, and financial account information, on an infected endpoint. Spyware often changes browser and other software settings and slows computer and internet speeds on an infected endpoint. Adware is spyware that displays annoying advertisements on an infected endpoint, often as pop-up banners.

Rootkits

A rootkit is malware that provides privileged (root-level) access to a computer. Rootkits

are installed in the BIOS of a machine, which means operating system-level security tools cannot detect them.

Backdoors

A backdoor is malware that allows an attacker to bypass authentication to gain access to a compromised system.

Trojan Horses

A Trojan horse is malware that is disguised as a harmless program but actually gives an attacker full control and elevated privileges of an endpoint when installed. Unlike other types of malware, Trojan horses are typically not self-replicating.

Worms

A worm is malware that typically targets a computer network by replicating itself to spread rapidly. Unlike viruses, worms do not need to infect other programs and do not need to be executed by a user or process.

Virus

A virus is malware that is self-replicating but must first infect a host program and be executed by a user or process.

Ransomware Types:

Ransomware is malware that locks a computer or device (locker ransomware) or encrypts data (crypto ransomware) on an infected endpoint with an encryption key that only the attacker knows, thereby making the data unusable until the victim pays a ransom (usually in cryptocurrency such as Bitcoin).

Lesson 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.

Business Email Compromise (BEC)

Business email compromise (BEC) is one of the most prevalent types of cyberattacks that

organizations face today. The FBI Internet Crime Complaint Center (IC3) estimates that "in aggregate" BEC attacks cost organizations three times more than any other cybercrime and BEC incidents represented nearly a third of the incidents investigated by Palo Alto Networks Unit 42 Incident Response Team in 2021. According to the Verizon 2021 Data Breach Investigations Report (DBIR), BEC is the second most common form of social engineering today.

Phishing Attacks

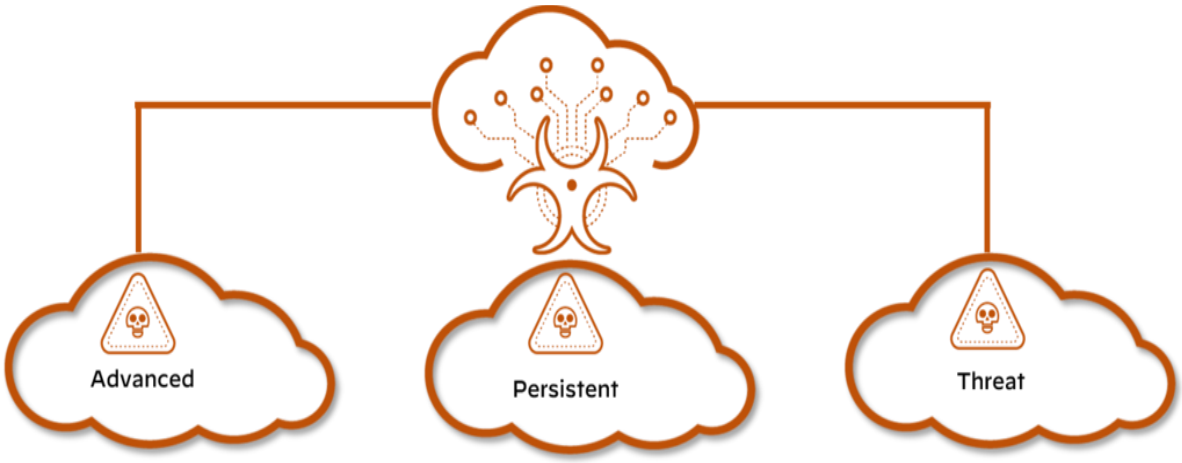
We often think of spamming and phishing as the same thing, but they are actually separate processes, and they each require their own mitigations and defenses. Phishing attacks, in contrast to spam, are becoming more sophisticated and difficult to identify and many more types of attacks

Lesson 4: 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 APTs.

Advanced Persistent Threats

Advanced persistent threats, or APTs, are a class of threats that are far more deliberate and potentially devastating than other types of cyberattacks. APTs are generally coordinated events that are associated with cybercriminal groups.



Lazarus

Attacks against nation-states and corporations are common, and the group of cybercriminals that may have done the most damage is Lazarus. The Lazarus group is known as an APT. The Lazarus group has been known to operate under different names, including Bluenoroff and Hidden Cobra. They were initially known for launching numerous attacks against government and financial

institutions in South Korea and Asia. In more recent years, the Lazarus group has been targeting banks, casinos, financial investment software developers, and crypto-currency businesses. The malware attributed to this group recently has been found in 18 countries around the world.

Lesson 5:Security

Models

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.

Perimeter-Based Security Model

Perimeter-based network security models date back to the early mainframe era (circa late 1950s), when large mainframe computers were located in physically secure "machine rooms." These rooms could be accessed by a limited number of remote job entry (RJE) terminals directly connected to the mainframe in physically secure areas.

Relies on Physical Security

Today's data centers are the modern equivalent of machine rooms, but perimeter-based physical security is no longer sufficient. Click the arrows for more information about several obvious but important reasons for the security issues associated with perimeter-based security.

Fundamentals of Network Security

This training introduces someone with no prior knowledge to the fundamentals of network security including concepts they must understand to recognize and potentially defend home networks and mission-critical infrastructure.

After completing this training, you should be able to:

- 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 WildFire® subscription services

Lesson Topics

This training comprises five lessons and takes about two hours to complete.

- Lesson 1: The Connected Globe

- Lesson 2: Addressing and Encapsulation
- Lesson 3: Network Security Technologies
- Lesson 4: Endpoint Security and Protection
- Lesson 5: Secure the Enterprise

Lesson 1: The Connected Globe

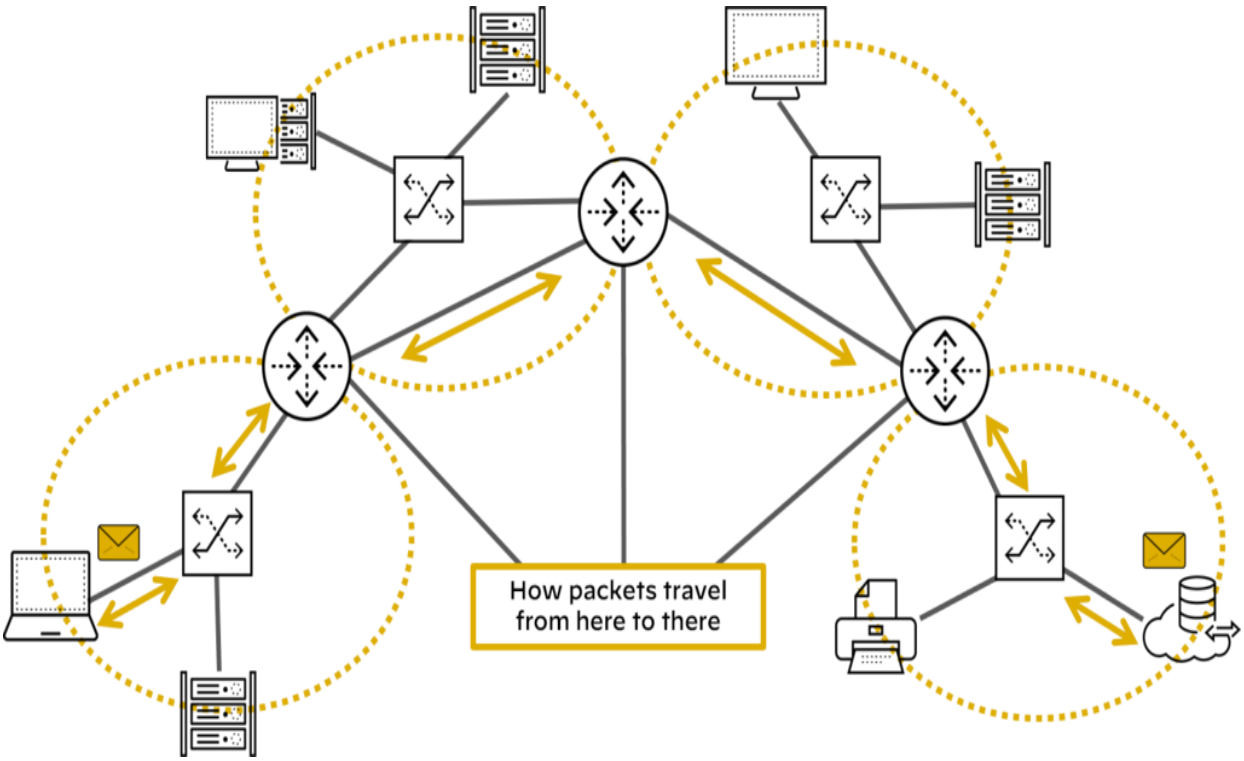
In this lesson, we will discuss how hundreds of millions of routers deliver Transmission Control Protocol/Internet Protocol (TCP/IP) packets using various routing protocols across local-area networks and wide-area networks. We also will discuss how the Domain Name System (DNS) enables internet addresses,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

The Net

In the 1960s, the U.S. Defense Advanced Research Projects Agency (DARPA) created ARPANET, the precursor to the modern internet. ARPANET was the first packet-switched network. A packet-switched network breaks data into small blocks (packets), transmits each individual packet from node to node toward its destination, and then reassembles the individual packets in the correct order at the destination.

How Things Connect

The ARPANET evolved into the internet (often referred to as the network of networks) because the internet connects multiple local area networks (LAN) to a worldwide wide area network (WAN) backbone.



Today billions of devices worldwide are connected to the Internet and use the transport communications protocol/internet protocol (TCP/IP) to communicate with each over packet-switched networks. Specialized devices and technologies such as routers, routing protocols, SD-WAN, the domain name system (DNS) and the world wide web (WWW) facilitate communications between connected devices.

Lesson 2: Addressing and Encapsulation

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

TCP/IP Overview

In cybersecurity, you must understand that applications sending data from one host computer to another host computer will first segment the data into blocks and will then forward these data blocks to the TCP/IP stack for transmission.

TCP/IP Protocol Stack

The TCP stack places the block of data into an output buffer on the server and determines the maximum segment size of individual TCP blocks permitted by the server operating system. The TCP stack then divides the data blocks into appropriately sized segments, adds a TCP header, and sends the segment to the IP stack on the server.

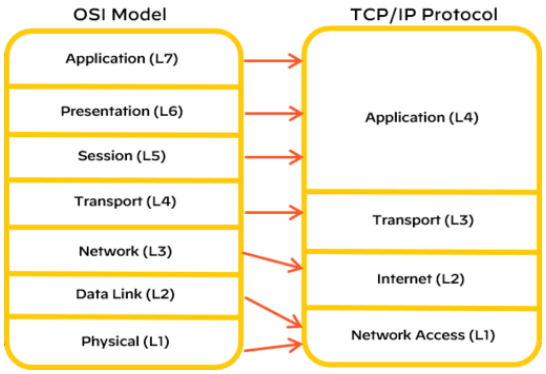
The IP stack adds source and destination IP addresses to the TCP segment and notifies the server operating system that it has an outgoing message that is ready to be sent across the network. When the server operating system is ready, the IP packet is sent to the network adapter

Introduction to Subnetting

Subnetting is a technique used to divide a large network into smaller, multiple subnetworks by segmenting an IP address into two parts: the network portion of the address and the host portion of the address.

OSI Model and TCP/IP Protocol Layers

The OSI model is defined by the International Organization for Standardization and consists of seven layers. This model is a theoretical model used to logically describe networking processes



Lesson 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.

Legacy Firewalls

Firewalls have been central to network security since the early days of the internet. A firewall is a hardware platform or software platform or both that controls the flow of traffic between a trusted network (such as a corporate LAN) and an untrusted network (such as the internet).

Packet Filtering Firewalls

First-generation packet filtering (also known as port-based) firewalls have the following characteristics:

Operation

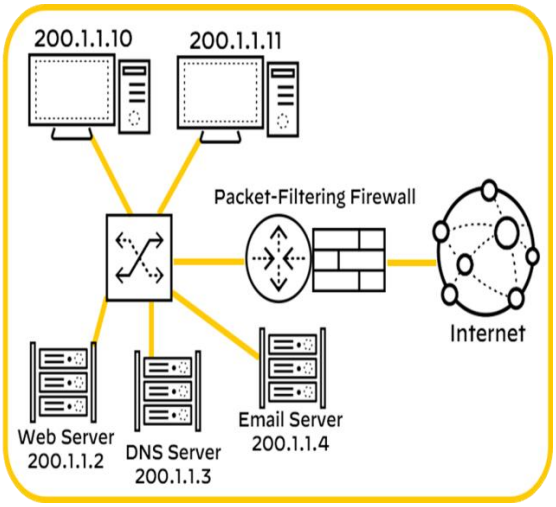
Packet filtering firewalls operate up to Layer 4 (Transport layer) of the OSI model and inspect individual packet headers to determine source and destination IP address, protocol (TCP, UDP, ICMP), and port number.

Match

Packet filtering firewalls match source and destination IP address, protocol, and port number information contained within each packet header to a corresponding rule on the firewall that designates whether the packet should be allowed, blocked, or dropped.

Inspection

Packet filtering firewalls inspect and handle each packet individually, with no information about context or session.



Lesson 4: Endpoint Security and Protection

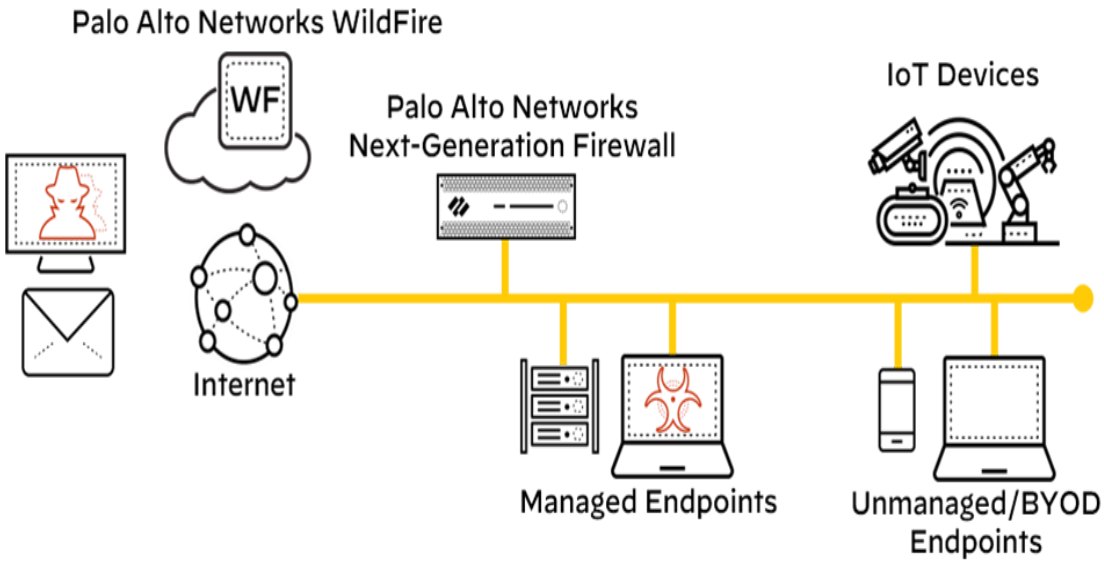
In this lesson, we will explore endpoint security challenges and solutions, including malware protection, anti-malware software, personal firewalls, host-based intrusion prevention systems (HIPSs), and mobile device management (MDM) software. We will also introduce network operations concepts, including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

Endpoint Security

In 2022, there were more than 11.5 billion internet of things (IoT) devices worldwide, including machine-to-machine (M2M), wide-area IoT, short-range IoT, massive-and-critical IoT, and multi-access edge computing (MEC) devices. Traditional endpoint security encompasses numerous security tools

Endpoint Protection

Advanced malware and script-based attacks can bypass traditional antivirus solutions with ease and potentially wreak havoc on your business.



Lesson 5: Secure the Enterprise

The networking infrastructure of an enterprise can be extraordinarily complex. The Palo Alto Networks prevention-first security architecture secures enterprises' perimeter networks

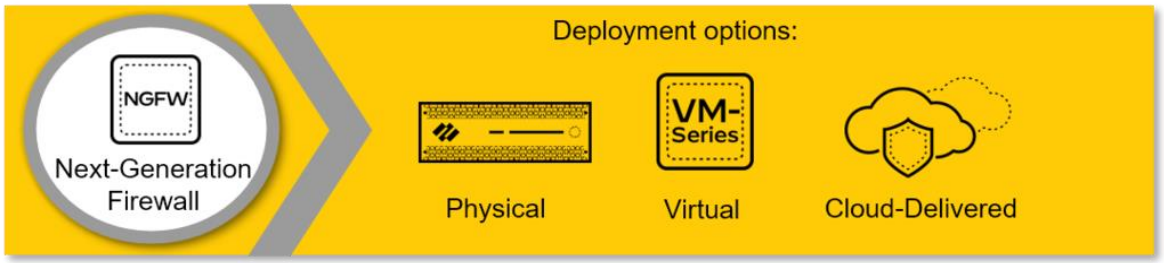
Prevention-First Architecture

Simplifying your security posture allows you to reduce operational costs and infrastructure while increasing your ability to prevent threats to your organization.

Next-Generation Firewall

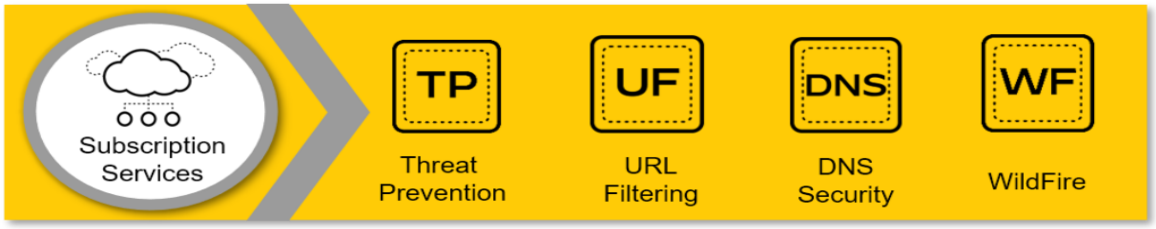
The Palo Alto Networks Next-Generation Firewall is the foundation of our product portfolio. The

firewall is available in physical, virtual, and cloud-delivered deployment options



Subscription Services

Subscription services add enhanced threat services and next-generation firewall capabilities, including DNS Security, URL Filtering, Threat Prevention, and WildFire malware prevention.



Panorama

Panorama provides centralized network security management. It simplifies administration while delivering comprehensive controls and deep visibility into network-wide traffic and security threats.

Fundamentals of Cloud Security

This training introduces the viewer to the fundamentals of cloud security, including concepts they must understand to recognize threats and potentially defend data centres, public/private clouds, enterprise networks, and small office/home office (SOHO) networks from cloud-based attacks.

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

- 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 centres through mixed traditional and cloud computing technologies
- Detail how Secure Access Service Edge (SASE) solutions help organizations embrace the concepts of cloud and mobility
- Describe how SaaS solutions provide data classification, sharing and permission visibility, and threat detection within the application
- Describe how the Prisma Cloud security platform detects and prevents security risks

Lesson Topics

This training comprises 7 lessons and takes about 2 hours and 30 minutes to complete.

- Lesson 1: Cloud Computing
- Lesson 2: Cloud Native Technologies
- Lesson 3: Cloud Native Security
- Lesson 4: Hybrid Data Centre Security
- Lesson 5: Prisma Access SASE Security
- Lesson 6: Prisma SaaS
- Lesson 7: Prisma Cloud Security

Lesson 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.

Definition

Cloud computing is not a location but rather a pool of resources that can be rapidly provisioned in an automated, on-demand manner. Read the quote below for the definition of cloud computing according to the U.S. National Institute of Standards and Technology.

Cloud Computing Ecosystem

The cloud computing ecosystem consists of service models, deployment models, responsibilities, and security challenges.

Service Models, Deployment Models, and Responsibilities

Virtualization is a critical component of a cloud computing architecture that, when combined with software orchestration and management tools that are covered in this course, allows you to integrate disparate processes so that they can be automated, easily replicated, and offered on an as-needed basis.

Shared Responsibility Model

The security risks that threaten your network today do not change when you move from on-premises to the cloud. The shared responsibility model defines who (customer and/or provider) is responsible for what (related to security) in the public cloud.

Cloud Security Responsibilities

In general terms, the cloud provider is responsible for security of the cloud, including the physical security of the cloud data centres, and foundational networking, storage, compute, and

virtualization services.

Lesson 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.

Cloud Native Technology Properties

A useful way to think of cloud native technologies is as a continuum spanning from virtual machines (VMs) to containers to serverless. On one end are traditional VMs operated as stateful entities, as we've done for over a decade now. On the other are completely stateless, serverless apps that are effectively just bundles of app code without any packaged accompanying operating system (OS) dependencies.

Virtualization

Virtualization is the foundation of cloud computing. You can use virtualization to create multiple virtual machines to run on one physical host computer.

Overview

You can think of virtual machines as separate computers running various operating systems on a physical host computer. Virtual machines and their associated operating systems often are referred to as "virtual guest operating systems." These virtual guest operating systems all share the physical compute resources: processors, dynamic memory (RAM), and permanent storage media of a physical host machine.

Hypervisor

Hypervisor software allows multiple, virtual guest operating systems to run concurrently on a single physical host computer. The hypervisor functions between the computer operating system and the hardware kernel.

Lesson 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.

The Four Cs of Cloud Native Security

The CNCF defines a container security model for Kubernetes in the context of cloud native security. Each layer provides a security foundation for the next layer.

Cloud

The cloud (and data centres) provide the trusted computing base for a Kubernetes cluster. If the

cluster is built on a foundation that is inherently vulnerable or configured with poor security controls, then the other layers cannot be properly secured.

Clusters

Securing Kubernetes clusters requires securing both the configurable cluster components and the applications that run in the cluster.

Containers

Securing the container layer includes container vulnerability scanning and OS dependency scanning, container image signing and enforcement, and implementing least privilege access.

Code

The application code itself must be secured. Security best practices for securing code include requiring TLS for access, limiting communication port ranges, scanning third-party libraries for known security vulnerabilities, and performing static and dynamic code analysis.

Fundamentals of SOC(Security Operation Center)

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

The Fundamentals of Security Operations Centre training is a high-level introduction to the general concepts of SOC and SecOps. It will introduce the Security Operations framework, people, processes, and technology aspects required to support the business, the visibility that is required to defend the business, and the interfaces needed with other organizations outside of the SOC.

The training consists of nine lessons and will take approximately 3 hrs to complete. This training is intended for learners who want to enter the field of cybersecurity - whether a student entering the workforce or an established professional transitioning from another field - and will help them demonstrate knowledge about SOC. It is recommended that the lessons be taken in order, but the menu below can be used to access any lesson, should you wish to determine your own learning path.

Lesson 1 - Day in the Life of a SOC Analyst

This lesson provides an overview of the Security Operations framework.

Duration 20 minutes

Lesson 2 - Business

The Business pillar defines the purpose of the Security Operations team to the business.

Duration 20 minutes

Lesson 3 - People

The People pillar defines the humans that will be accomplishing the goals of the Security Operations team.

Duration 20 minutes

Lesson 4 - Processes

The Processes pillar defines the processes and procedures executed by the Security Operations organization.

Duration 20 minutes

Lesson 5 - Interfaces

The Interfaces pillar defines what functions need to be involved to achieve the stated goals.

Duration 20 minutes

Lesson 6 - Visibility

The Visibility pillar defines what information the SecOps function needs.

Duration 20 minutes

Lesson 7 - Technology

The Technology pillar increases the capabilities for Security Operations to complete its core mission.

Duration 20 minutes

Lesson 8 - SOAR

SOAR is the automation of the orchestration of all the elements of Security Operations.

Duration 20 minutes

Lesson 9 - SOAR Solution

Cortex XSOAR is a Security Orchestration, Automation, and Response (SOAR) platform.

Lesson 1: Day in the Life of a SOC Analyst

a SOC analyst on the Security Operations team and it is his job to triage alerts to determine if there is a security threat. Before Erik starts his job, he will need to understand the general concepts of SOC and SecOps, and the business goals. Erik will need training and support from the people he interacts with on a daily basis. While mitigating threats, Erik will need to know the processes to follow, the teams he will be interacting with, and the technology he will be using to gain visibility into the network.

Lesson 2: Business

Both Erik and the SOC team are responsible for protecting the business. The reason for Security Operations, for all of the equipment, for everything SOC does is ultimately to service one main goal, protect the business. Without the Business pillar, there would be no need for Erik or the SOC team.

The Business pillar defines the purpose of the Security Operations team to the business and how it will be managed. The Business pillar helps to provide Erik and the rest of the SOC team with answers to questions such as "Who do we need to help protect the business?"; "How will we protect the business?"; "Where are we going to do this from?"; and "How do we know if what we have in place is working effectively?"

Lesson 3: People

The People pillar defines who will be accomplishing the goals of the Security Operations team and how they will be managed. As a part of the People pillar, Erik received training necessary for him to be able to triage the alerts in addition to the other processes and functions within the SOC.

This training provides Erik with the skills necessary to become efficient at detecting and prioritizing alerts. As Erik's knowledge increases, he will have opportunities to grow on the SOC team. He will also have the skills to advance in his career to other areas.

Employee Utilization

Methods should be developed to maximize the efficiency of a Security Operations team specific to the existing staff. Security Operations staff are prone to burnout due to console burn out and extreme workloads. To avoid this, team members should be assigned different tasks throughout the day. These tasks should be structured and may include:

• Shift turnover stand-up meeting (beginning of shift)
• Event triage
• Incident response
• Project work
• Training
• Reporting
• Shift turnover stand-up meeting (end of shift)

Another tactic to avoid burnout is to schedule shifts to avoid high-traffic commute times. Depending on the area, 8am-5pm may line up with peak (vehicle) traffic patterns. Shifting the schedule by two hours could reduce stress on the staff.

Training

Proper training of staff will create consistency within an organization. Consistency drives effectiveness and reduces risk. Use of a formal training program will also enable the organization to bring on new staff quickly. Some organizations resort to on-the-job or shadow training for new hires, which is not recommended on its own. While shadowing other analysts during initial employment in the SOC is important, it should not be the only means of training.

Lesson 4: Processes

While monitoring the ticketing queue, Erik notices a new set of alerts that has been sent to the SOC team by one of the network devices. Based on the alert messages, Erik needs to determine whether the alert message is a security incident, so he opens an incident ticket. Erik starts by doing his initial research in the log files on the network device to determine if the threat is real. After reviewing the log files, Erik determines that the alert is a real threat. Based on the Severity Triangle, Erik has determined that the severity level for this alert is currently High.

The Processes pillar defines the step-by-step instructions and functions that are to be carried out by the SOC team for the necessary security policies to be followed. Processes are a series of actions or steps taken to achieve an end goal. As part of the Processes pillar, Erik will need to determine the other teams that should be involved, the scope of the work for each team, and what each team will be responsible for.

Lesson 5: Interfaces

The alert generated by the network device; he partners with the Threat Intelligence Team

to identify the potential risks this threat may pose to the organization. Erik also interfaces with the Help Desk, Network Security Team, and Endpoint Security Teams to determine the extent the threat has infiltrated the network.

Security operations is not a silo and needs to work with many other functions or teams. Each interaction with another team is described as an interface. The Interfaces pillar defines which functions need to take place to help achieve the stated goals, and how the SOC will interface with other teams within the organization by identifying the scope of each team's responsibilities and the separation of each team's duties.

Lesson 6: Visibility

A detailed analysis of the threat, he will need to gather all of the necessary information to make a well-informed decision. Network visibility is needed for Erik to gather information about the network's status, the traffic passing through the network, and the conditions on which traffic is allowed to pass through. Without network visibility, Erik may miss important data that could lead to a real threat being treated as a false positive or missed altogether. The better visibility Erik has into every aspect of the company's network, the better he and the SOC team can make an informed decision.

The Visibility pillar enables the SOC team to use tools and technology to capture network traffic, limit access to certain URL's determine which applications are being used by end users, and to detect and prevent the accidental or malicious release of proprietary or sensitive information.

Lesson 7: Technology

The beginning of our scenario has been mitigated. Erik now needs to work with SOC team members and other teams to determine if the current network technology can be used to automate a process or response to automatically remediate this issue, or similar issues that may arise.

The Technology pillar includes tools and technology to increase our capabilities to prevent or greatly minimize attempts to infiltrate your network. In the context of IT Security Operations, technology increases our capabilities to securely handle, transport, present, and process information beyond what we can do manually. By using technology, you amplify and extend your abilities to work with Information in a secure manner.

Lesson 8: SOAR

Scale is one of the biggest challenges for SOCs. We stepped through each pillar to mitigate a threat, but while Erik was working on one threat, alerts and incidents continued to pour in. The number of incidents that each member of the SOC team must respond to is greater than what can be managed through human intervention.

The only reasonable long-term solution is to empower existing resources with a combination of innovative orchestration, artificial intelligence, and machine learning technologies to automate many of the manual processes that a SOC team faces each day. By automating processes, the SOC team can focus its attention on what is truly critical: identifying, investigating, and mitigating emerging cyberthreats.

Lesson 9: SOAR Solution

Cortex by Palo Alto Networks offers solutions that improve SOC efficiency. Cortex XDR and Cortex XSOAR in particular allow SOC analysts like Erik to do in minutes what would take them hours to resolve otherwise. It is tools such as these that will allow SOCs to scale into the future.

4.Technology

AI and Machine Learning

AI and machine learning are two related technologies that enable systems to understand and act on information in much the same way that a human might use information. AI acquires and applies knowledge to find the most optimal solution, decision, or course of action. Machine learning is a subset of AI that applies algorithms to large datasets to discover common patterns in the data that can then be used to improve the performance of the system.

Blockchain

Blockchain is essentially a data structure containing transactional records (stored as blocks) that ensures security and transparency through a vast, decentralized peer-to-peer network with no single controlling authority. Cryptocurrency, such as Bitcoin, is an example of a blockchain application.

Data Mining

Data mining enables patterns to be discovered in large datasets by using machine learning, statistical analysis, and database technologies.

Mixed Reality

Mixed reality includes technologies, such as virtual reality (VR), augmented reality (AR), and extended reality (XR), that deliver an immersive and interactive physical and digital sensory experience in real time.

Natural Language Search

Natural language search is the ability to understand human spoken language and context (rather than a Boolean search, for example) to find information.

5.Internship Reflection

My internship experience was great. I took part in the "Palo Alto Cyber Security supported virtual internship" program through Edu Skills and learned about the Cyber Security. I now can understand about information security and information warfare, how hackers exploit vulnerabilities to access systems. I've learnt how to identify threats, minimize risk, and learn strategies on when to play offense or defense with your information and communication technologies **..**

We experienced a great deal of self-directed learning during the course of the 60-day internship. Because of our mentor, Mr. Sravanan Rajagopal, who everyday discussed the learning objectives and assisted us in achieving them, learning was a very simple process for us. We had weekly mentor and doubt sessions to get our questions about the course and internship answered.

During the internship, I assigned a few problems. I encountered several difficulties because Cyber Security is a new topic and because I am new to protecting systems, servers, networks, data and devices connected to the internet from malicious attacks intended towards illegally accessing, altering and exploiting data.

However, our mentors and support staff were incredibly attentive and helpful.

In order for us to connect with one another and support one another during the process, all of the intern applicants were added to a group in the security for our environment.

In conclusion I can say that this internship exposed me to a lot of the industry. I developed my problem-solving skills and my ability to deal with a variety of issues and people. It was a significant life-changing event for me. I'm confident that this will allow me to take a step closer to achieving my objective.

6.Conclusion

Organizations are finding themselves under the pressure of being forced to react quickly to the dynamically increasing number of cybersecurity threats. Since the attackers have been using an attack life cycle, organizations have also been forced to come up with a vulnerability management life cycle. The vulnerability management life cycle is designed to counter the efforts made by the attackers in the quickest and most effective way. This chapter has discussed the vulnerability management life cycle in terms of the vulnerability management strategy. It has gone through the steps of asset inventory creation, the management of information flow, the assessment of risks, assessment of vulnerabilities, reporting and remediation, and many more….

Cybersecurity is crucial because it safeguards all types of data against theft and loss. Sensitive data, protected health information (PHI), personally identifiable information (PII), intellectual property, personal information, data, and government and business information systems are all included

Cyber security elements can include:

- Application Security
- Cloud Security
- Data Security
- Identity Management
- Mobile Security
- Network Security
- Operational Security
- Endpoint Security

Through the knowledge and expertise I gained through this internship I can contribute to the development of crucial technologies and help in providing data security and communication to the users.