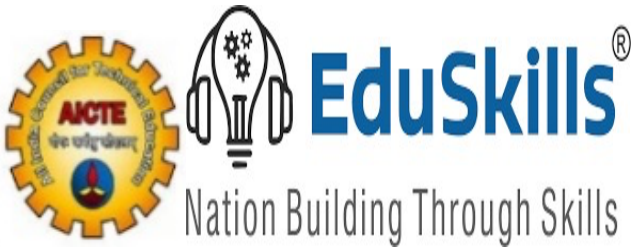
Palo Alto Cyber Security Virtual Internship

Sponsored By



Internship Report Submitted By

K.Swathi(22491A4722)
III B.Tech I semester
Computer Science and Cyber Security

DEPARTMENT OF COMPUTER SCIENCE - INTERNET OF THINGS & CYBER SECURITY WITH BLOCK CHAIN TECHNOLOGY

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY
(AUTONOMOUS)
Approved by AICTE | Permanent Affiliation: JNTU-Kakinada | UGC-Recognized | Accredited by NAAC A+ & NBA | ISO 9001:2015 Certified Vengamukkapalem (V), Ongole, Prakasam Dist., Andhra Pradesh – 523272

2024-2025

QIS COLLEGE OF ENGINEERING AND TECHNOLOGY

(AUTONOMOUS)

Approved by AICTE | Permanent Affiliation: JNTU-Kakinada | UGC-Recognized | Accredited by NAAC A+ & NBA|

ISO 9001:2015 Certified

Vengamukkapalem (V), Ongole, Prakasam Dist.,

Andhra Pradesh-523272

DEPARTMENT OF COMPUTER SCIENCE - INTERNET OF THINGS & CYBER SECURITY WITH BLOCK CHAIN TECHNOLOGY

BONAFIDE CERTIFICATE

This is to certify that the<**Embedded System Developer Virtual Internship**>

submitted by K.Swathi (22491A4722) during Academic Year 2024-2025 in

partial fulfilment of the requirements for the award of the degree of B. Tech,

QIS College of Engineering and Technology (Autonomous), Ongole.

Department Internship Coordinator **Head of the Department**

INDEX

ABSTRACT

The Palo Alto Cybersecurity Virtual Internship is a two-month program supported by Palo Alto Networks, designed to provide students with valuable experience in the field of cybersecurity. This opportunity is facilitated by EduSkills in collaboration with the All India Council for Technical Education (AICTE). It targets students currently pursuing degrees such as BE, BTech, ME, MTech, MCA, and related disciplines at Engineering and Polytechnic Institutions.

The program involves completing an online course via the Palo Alto Networks Cybersecurity Academy, which includes assessments. Upon successful completion, participants work on a project, guided by industry experts through mentoring sessions, aimed at enhancing their practical knowledge. Interns who finish the course and project will earn a course completion certificate, an internship certificate from AICTE, and a digital badge.

The internship is open to students from any branch or year of study, provided they are available for the full two-month duration. Successful interns may also gain hiring opportunities in global corporations.

Outline of the internship

S.no	Outline of the internship
1.	Introduction to Ethical hacking
2.	Foot printing and Reconnaissance
3.	Scanning Networks
4.	Enumeration
5.	Vulnerability Analysis
6.	System Hacking

1.Introduction to Palo Alto Cyber Security Virtual Internship

Introduction to Palo Alto Cyber Security Virtual Internship

What is Palo Alto Cyber Security Virtual Internship?

The Palo Alto Cybersecurity Virtual Internship is an 8-week online program designed to help students gain hands-on experience in cybersecurity. It is open to students pursuing engineering or related degrees at institutions partnered with EduSkills and AICTE. The program involves completing an online course on cybersecurity through Palo Alto Networks, followed by a project that students must submit with faculty assistance. Participants also benefit from mentoring sessions with industry experts. Those who successfully complete the program receive certificates and a digital badge, which may lead to potential job opportunities in cybersecurity.

Why is Palo Alto Cyber Security Virtual Internship Important?

The Palo Alto Cybersecurity Virtual Internship is important for several reasons. First, the cybersecurity field is experiencing a severe shortage of skilled professionals, with demand expected to grow significantly. According to reports, the cybersecurity workforce needs to increase by 145% to meet global market needs.This internship program helps bridge that gap by providing students with essential skills and knowledge, making them more competitive in the job market.

Additionally, the program offers hands-on experience through a structured learning path, including completing an online course, project work, and mentoring by industry experts. These components help students develop practical skills that are directly applicable to real-world cybersecurity challenges.

By offering certifications from recognized bodies like Palo Alto Networks and AICTE, the internship boosts the employability of participants, opening doors to career opportunities with leading companies in the cybersecurity sector.

The Palo Alto Cybersecurity Virtual Internship is crucial for several key reasons:

- **Bridging the Skills Gap:** The cybersecurity industry faces a significant shortage of professionals, and this internship helps address that by equipping students with essential, hands-on experience in the field. With the need for cybersecurity talent expected to grow by 145%, this program is vital for preparing the next generation of professionals.

- **Practical Training:** The internship offers structured learning through an online course and project work, allowing students to develop real-world skills. Participants receive mentoring from industry experts, enhancing their practical understanding and problem-solving abilities in cybersecurity scenarios.

- **Career Advancement:** Upon successful completion, interns earn certificates from Palo Alto Networks and AICTE, making them more competitive in the job market. This certification, coupled with the hands-on experience, can open doors to job opportunities in top global companies.

These elements make the Palo Alto Cybersecurity Virtual Internship a key tool for empowering students and meeting the growing global demand for cybersecurity experts.

2. Footprinting and Reconnaissance

The **"Footprinting and Reconnaissance"** phase in cybersecurity typically involves gathering as much information as possible about a target system or network. In the context of the Palo Alto Cybersecurity Virtual Internship, this stage is part of a broader educational experience where interns learn to identify potential vulnerabilities and threats. Footprinting involves mapping the target system's network, identifying its structure, technologies, and security weaknesses. This process includes activities like DNS interrogation, IP address scanning, and searching for exposed ports. Reconnaissance is often done in two forms: active (direct interaction with the target) and passive (gathering data from public resources).

Through the internship, participants learn the importance of these techniques for understanding the attack surface of a system before an actual cyberattack occurs. The hands-on experience allows students to develop practical skills while gaining exposure to Palo Alto's security tools and methodologies. This phase also helps interns understand how attackers leverage information to design successful intrusion strategies. The insights gained during footprinting and reconnaissance are critical for developing robust defense strategies to prevent cyber threats and mitigate potential security breaches.

Conclusion:

Footprinting and Reconnaissance as part of the Palo Alto Cybersecurity Virtual Internship are essential steps in the cybersecurity learning process. These techniques provide interns with the critical ability to gather intelligence about potential security weaknesses in systems and networks. By mastering tools like DNS interrogation, port scanning, and network mapping, interns gain insights into the attack surface of a target, enhancing their skills in both offensive and defensive cybersecurity strategies. The internship equips students with practical, hands-on experience, enabling them to understand how attackers operate and how to defend against such tactics. Ultimately, these skills contribute significantly to developing robust cybersecurity strategies, and through mentorship and industry guidance, interns are better prepared for future roles in the growing cybersecurity field

3. Scanning Networks

Scanning Networks is a crucial technique covered in the Palo Alto Cybersecurity Virtual Internship. This phase involves using various tools and methods to identify active devices, open ports, and services on a network, which are potential vulnerabilities that could be exploited by attackers.

Key techniques involved in network scanning include:

- **Port Scanning:** Tools like Nmap are used to detect open ports on a target system. Open ports can provide entry points for attacks, so identifying them helps in strengthening network defenses.
- **Vulnerability Scanning:** This involves scanning systems for known vulnerabilities that could be exploited. Tools like Nessus and OpenVAS are commonly used for identifying vulnerabilities in network devices and software.
- **Network Mapping:** Mapping out a network's structure helps in understanding how systems are connected, which is essential for identifying weak points. This can include identifying devices, operating systems, and the relationships between systems.
- **Ping Sweeping:** This is a method of discovering which hosts are alive on a network. A ping sweep involves sending ICMP echo requests to a range of IP addresses to see which respond.
- **Banner Grabbing:** Banner grabbing involves connecting to open ports and capturing service banners that reveal information about the software version and other details that could help in exploitation.

During the Palo Alto internship, students learn these scanning techniques in the context of real-world scenarios, preparing them for roles where identifying and securing network vulnerabilities is a key responsibility. By conducting these scans, interns understand how attackers probe networks and, more importantly, how to secure them effectively

4. Enumeration

The **Palo Alto Cybersecurity Virtual Internship** is a comprehensive program designed to equip students with the skills needed in the growing field of cybersecurity. The internship involves various stages, including learning, hands-on experience, and mentoring. Here is an enumeration of key components of the program:

- **Registration and Enrollment:**
  - Students must register through the AICTE Internship Portal to begin the program. Once selected, they are enrolled in the Palo Alto Networks Cybersecurity Academy.

- **Coursework:**
  - Interns complete an online cybersecurity course provided by Palo Alto Networks. This course covers fundamental topics like network security, threat detection, and defense strategies. It includes assessments to evaluate the intern's understanding.

- **Project Work:**
  - After completing the course, interns are assigned a practical project. This allows them to apply the theoretical knowledge gained during the course in real-world scenarios.

- **Mentoring:**
  - Interns attend mentoring sessions with industry experts for hands-on guidance. These sessions help interns gain practical insights into cybersecurity practices and industry expectations.

- **Career Advancement:**
  - Participants also receive a career development session, where corporate mentors provide guidance on resume building, interview preparation, and job search strategies.

Certification:
- Upon successful completion of the course and project, interns receive certifications from Palo Alto Networks and AICTE, as well as a digital badge. These certificates are valuable for enhancing their employability in cybersecurity.

Job Opportunities:
- Students who complete the internship may also be eligible for hiring opportunities with global corporations, thanks to the partnership between Palo Alto Networks and EduSkills.

This internship provides a solid foundation for students to build expertise in cybersecurity, bridging the skills gap in the field and offering practical exposure to the tools and techniques used by professionals.

5. Vulnerability Analysis

Vulnerability Analysis of Palo Alto Cyber Security Virtual Internship

In the **Palo Alto Cybersecurity Virtual Internship**, **Vulnerability Analysis** is a key component, providing interns with hands-on skills in identifying and analyzing security weaknesses in systems and networks. Here are some focal points of this stage:

- **Identifying Vulnerabilities:**
  - Interns are trained to use vulnerability assessment tools like Nessus or OpenVAS, which scan for common vulnerabilities, misconfigurations, outdated software, and weak points that attackers could exploit.

- **Assessing Risks:**
  - A core aspect of the analysis is understanding the severity of each vulnerability. Interns learn to prioritize vulnerabilities based on factors like exploitability, potential damage, and how they align with current security standards.

- **Patch Management and Remediation:**
  - As part of the process, students explore remediation steps, including patching, configuration adjustments, or implementing additional security controls to minimize the risks associated with identified vulnerabilities.

- **Reporting and Documentation:**
  - Interns practice creating detailed vulnerability reports that outline the findings, risk levels, and recommended mitigation strategies. Reporting is crucial for communicating risks to stakeholders and guiding security improvements.

- **Continuous Monitoring:**
  - Vulnerability analysis is reinforced as a continuous process. Interns learn the importance of regular scans and updates to stay ahead of evolving threats and vulnerabilities.

Through vulnerability analysis, the Palo Alto Cybersecurity Virtual Internship prepares students to assess, document, and address security risks, contributing to a proactive approach in cybersecurity management. This experience is essential for interns to become adept in real-world cybersecurity roles.

6. System Hacking

The **System Hacking** phase in the Palo Alto Cybersecurity Virtual Internship is designed to teach interns how hackers exploit vulnerabilities within a system, as well as methods to detect and defend against such attacks. This phase introduces students to common hacking techniques and corresponding countermeasures, enabling them to understand both offensive and defensive aspects of cybersecurity. Here are some key components of system hacking covered in the program:

- **Password Cracking:** Interns learn methods hackers use to crack passwords, such as brute force, dictionary attacks, and rainbow tables. They also explore defensive strategies like implementing strong password policies and using multi-factor authentication to prevent unauthorized access.

- **Privilege Escalation:** This involves gaining higher access levels within a system. Interns learn how attackers might exploit system vulnerabilities to increase their privileges, and they also explore ways to secure privileged accounts and monitor unusual access patterns.

- **Spyware and Keyloggers:** The internship covers the use of spyware and keyloggers, which are used by attackers to gather sensitive information covertly. Students learn to recognize and prevent these attacks by securing endpoints and using anti-malware tools.

- **Rootkits:** A focus on rootkits helps students understand how attackers hide malicious processes within a system to avoid detection. Interns learn detection techniques, such as signature-based and heuristic analysis, and methods to remove rootkits from infected systems.

- **Steganography and Covering Tracks:** Interns are introduced to steganography (hiding information within files) and log manipulation, which attackers use to cover their tracks. They learn how to monitor system logs effectively and use forensic tools to detect tampering attempts.

The system hacking phase of the internship aims to provide interns with a solid understanding of the tools, techniques, and strategies used by attackers. This practical experience helps them build skills in detecting and preventing malicious activities, an essential aspect of a cybersecurity professional's responsibilities. Through hands-on exercises and guided mentorship, interns gain insights into how to protect systems and networks from sophisticated attacks.

Conclusion

The Palo Alto Cybersecurity Virtual Internship is a valuable program that empowers students with foundational and advanced skills in cybersecurity. Through a blend of online coursework, practical projects, and mentorship from industry experts, interns gain hands-on experience in essential cybersecurity techniques, including threat detection, network scanning, and vulnerability assessment. The structured learning path, certification, and networking opportunities offered by the program make it highly beneficial for students aiming to enter the cybersecurity field. Furthermore, the collaboration with AICTE and EduSkills broadens access, helping to close the skills gap in the cybersecurity industry and prepare a new generation of professionals to meet global security needs.


NATIONAL INTERNSHIP PORTAL
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
SWATHI KUPPIREDDY
QIS College of Engineering and Technology
has successfully completed 10 weeks
Cybersecurity Virtual Internship
During July - September 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 :8c9c86df8cc789525c465432a20f1c4c
Student ID :STU662bbcd0e990e1714142416
INTERNSHIP GRADE
B
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