# LONG TERM INTERNSHIP

Track - Cyber Security with IBM QRadar

Team ID - LTVIP2024TMID11398

Team Size - 4

Team Leader - Bhargava Sai Jetti

Team Member - Avala Jyotheeshwar Rao

Team Member - Bharani Siva Charan Chitti

Team Member - Chitrada Pavan

College - Dr. L.B. Degree & P.G. College

Project Title - Understanding Cyber Threats : Exploring Nessus & Beyond scanning tools.

# INTRODUCTION

Cybersecurity, within the realm of Artificial Intelligence (AI), embodies a critical frontier, aiming to fortify digital ecosystems by instilling intelligent defense mechanisms. AI in cybersecurity spans various technologies and methodologies, striving to emulate human cognitive abilities to detect, analyze and respond to evolving cyber threats.

Within this domain, AI leverages machine learning algorithms to discern patterns, anomalies and potential vulnerabilities within intricate datasets. This fusion of AI & cybersecurity fuels a diverse spectrum of applications.

# EXECUTIVE SUMMARY

The project "Understanding Cyber Threats: Exploring Nessus and Beyond Scanning Tools" serves several purposes and offers numerous benefits -

1) Vunerability Assessment - The primary purpose is to conduct thorough vulnerability assessments of network infrastructures and systems.

2) Risk Management - Through comprehensive scanning, organizations can access their security posture.

3) Security Compliance - Many industries and regulatory bodies require organizations to adhere to specific security standards.

4) Incident Poevention - By proactively identifying vulnerabilities organizations can take preventive measures to migate risks.

5) Resource Optimization - By automating the vulnerability assessment process, organizations can optimize resource utilization and reduce manual efforts required for security testing.
This frees up security personnel to focus on more strategic security initiatives.

# Suggested Pre-requisities

## → Basic Knowledge of Operating Systems

An operating system is the most important software that runs on a computer.
It manages the computers memory and processes, as well as all of its software & hardware.

## → Foundational Networking Concepts

These include the following

- IP address
- Computer network
- Protocol
- Ethernet
- Nodes
- Port
- Router
- Topology

→ Understanding of Common Cyber Threats -

- Phishing
- Ransomware
- DDOS attack
- Malware
- Exploits
- Spyware

→ Knowledge of Security Tools & Technologies -

- Firewalls
- Encryption
- Metasploit
- Sniffers
- WireShark
- Burp Suite
- Nessus
- Kali Linux

→ Comprehension of Risk Management -

Risk management is the identification, evaluation and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, & control the probability or impact of unfortunate events.

→ Python for hacking -

Python is a versatile programming language that offers a wide range of tools and libraries, making it well-suited for tasks such as penetration testing & network manipulation. Its simplicity and readability are particularly advantageous for ethical hackers. Python is a computer programming language often used to build websites and software, automate tasks, and conduct data analysis, Python is a general purpose language.

## ACTIVITY LOG FOR THE FIRST WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day – 1 | Introduction to Cyber Security Introduction security CIA Triad Implementation | This day covered fundamentals & basics of Cyber Security | |
| Day - 2 | Introduction to Networking OSI Model, TCP/IP Model, Ports, Protocols. | Understood OSI model, TCP/IP, Ports, Protocols | |
| Day – 3 | Python for hacking | Basics of the Python a versatile language. | |
| Day – 4 | Python packages | Essential concepts such as data types, loops, functions etc | |
| Day – 5 | Introduction to Linux Basic concepts & commands | Learnt essential Linux commands for file management | |
| Day – 6 | Key concepts of Python Assignment & Quiz-1 | Learn few other concepts of python & also got an assignment & wrote a quiz. | |

**WEEKLY REPORT**

**WEEK – 1 (From Dt.** 5/2/24 **to Dt.** 10/2/24 **)**

**Objective of the Activity Done:** To provide a understanding on Cyber Security

**Detailed Report:** On the first day we learnt about the basics of Cyber Security. These included fundamental security principles and implementation of CIA Triad.

On day two we learnt about Networking along with other concepts like OSI Model, TCP/IP Models, Ports, Protocols & mainly Network Configuration using Cisco Packet Tracer.

The third day was somewhat interesting cause we were taught about Python language; & we learned how to use it for hacking. On the fourth day we learnt about Linux commands & basic concepts which were enough to understand Linux Some extent.

The fifth day we learnt about file hierarchy and permissions.

Finaly on sixth day we learnt other key concepts of python language and also did an assignment related to the topics taught in this week and finally a quiz.

## ACTIVITY LOG FOR THE SECOND WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day - 1 | Setting up Virtualized Environment with Virtual Box | we learnt how to set up a virtual machine using virtual box. | |
| Day - 2 | Footprinting & Reconnaissance | Concepts like active & passive footprinting were taught & also learnt. | |
| Day - 3 | First tool for Networking | Learnt about wireshark tool & its uses. | |
| Day - 4 | Network scanning tools & concepts. | Learnt about Port scanning, Nmap utilization | |
| Day - 5 | Enumeration techniques & tools | Learnt that enumeration plays a vital role in network reconnaissance | |
| Day - 6 | Vulnerability assessment concepts along with an Assignment & Quiz - 2 | Learnt about the concept of vulnerability assessment & also wrote a quiz | |

**WEEKLY REPORT**

**WEEK – 2 (From Dt.12/2/24... to Dt.17/2/24...)**

**Objective of the Activity Done:** Engaging in Vulnerability Assessment

**Detailed Report:** On the first day we learnt how to install virtual box & use it to create an virtual machine. The second day focused mainly on management of virtual machines created in virtual box. This also includes installation. On third day we learnt about the first tool and most widely used tool for networking, it is non other than "WireShark" a packet analyzer. On fourth day we covered basic concepts of Networking, these include port scanning, vulnerability scanning concepts and tools. On fifth day we learnt about enumeration techniques and tools. Enumeration plays a crucial role in network reconnaissance; involving the systematic gathering of information about network resources. On the final day we learnt about vulnerability assessment and also did an assignment related to it. Finally we also wrote a quiz.

## ACTIVITY LOG FOR THE THIRD WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day - 1 | Techniques & tools for accessing systems | Learnt about password cracking and exploitation of vulnerabilities | |
| Day - 2 | Types of malware & their impacts. | Learnt about different malwares and ways to mitigate them. | |
| Day - 3 | Network sniffing concept | Explored packet analysis techniques & understood few protocols. | |
| Day - 4 | Types of social engineering attacks | Learnt about phishing, pretexting, tailgating. | |
| Day - 5 | Types of DoS attacks & their impact | Learnt about the DoS attacks & their impacts | |
| Day - 6 | Types of sessionhijacking attacks along with Assignment & Quiz - 3 | learnt about MITM attack, wrote a quiz & did an assignment | |

**WEEKLY REPORT**

**WEEK – 3 (From Dt.19/2/24... to Dt.24/2/24...)**

**Objective of the Activity Done:** Essential CyberSecurity Topics

**Detailed Report:** On the first day we learnt about password cracking and exploiting vulnerabilities; while also learning strategies for covering tracks and maintaining access to evade detection On second day we learnt about malware impacts on the systems and also acquired skills in malware analysis and removal techniques. Also explaration of malware. On third day: we learnt about the concepts of Network Sniffing and tools involved. Also explored packet analysis techniques and attacks associated with network. On fourth day we learnt about social engineering attacks like phishing, pretexting, & tailgating, while also exploring human behaviour & psychology. On fifth day we learnt about Dos attack tools and techniques and also countermeasures for DOS attacks. On last day we learnt about session hijacking attacks & ways to mitigate them along with an assignment & a quiz.

## ACTIVITY LOG FOR THE FORTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day - 1 | Web server vulnerabilities & attacks | Learnt about various vulnerabilities & attacks targetting web servers. | |
| Day - 2 | Web application vulnerabilities & attacks vectors | Learnt about SQL injection, cross-site scripting & CSRF | |
| Day - 3 | Cloud computing concepts & models | Learnt about IaaS, PaaS & SaaS. | |
| Day - 4 | Cryptographic concepts & algorithms | Learnt about symmetric & asymmetric encryption techniques | |
| Day - 5 | Overview of CTI & its impartance in Cyber security | Learnt about the significance in bolstering cyberSecurity defenses. | |
| Day - 6 | Basics of SIEM & IBM QRadar. Assignment & Quiz-4 | Learnt fundamental concepts of SIEM systems. | |

**WEEKLY REPORT**

**WEEK – 4 (From Dt...26/2/24... to Dt...2/3/24...)**

**Objective of the Activity Done:** Delve into various Aspects of Cybersecurity.

**Detailed Report:** On the first day we learnt about various vulnerabilities and attacks targeting web servers, including common exploits such as SQL injection etc.. On next day, we gained an insight into a range of web application vulnerabilities and attacks such as cross-site scripting (XSS) & Cross Site Request Forgery (CSRF) along with migitation strategies. On third day we learnt about cloud computing and models including Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). On fourth day we learnt about how encryption works, the difference between symmetric & asymmetric encryption. On fifth day, we learnt about various types of Cyber Threat Intelligence, including tactical operations. On ferial day we learnt and grasped few vital concepts of the SIEM, with a specific focus on IBM QRadar. We also did an assignment and wrote a quiz related to this week.

## ACTIVITY LOG FOR THE FIFTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day - 1 | Accessing & navigating the QRadar console. | Learnt about navigating the QRadar console, enabling effective interaction. | |
| Day - 2 | OSNIT framework. | Learnt about gathering, analyzing & leveraging OSNIT | |
| Day - 3 | Incident response & forensics in QRadar | Learnt about fundamentals of incident response, including the stages of incident handling. | |
| Day - 4 | Advanced rule creation & tuning techniques in QRadar | Learnt about the advanced techniques for crafting precise. | |
| Day - 5 | Overview of network security monitoring with QRadar | Learnt about the importance of the continuous monitoring for detecting threats. | |
| Day -6 | Overview of automation & orchestration in QRadar<br>Grand Assessment | Understood importance of streamlining.<br>Wrote the grand assessment. | |

**WEEKLY REPORT**

**WEEK – 5 (From Dt. 4/3/24 to Dt. 9/3/24)**

**Objective of the Activity Done:** To access & navigate the QRadar console.

**Detailed Report:**

On first day we learnt how to effectively access and navigate the QRadar console, gaining proficiency in interacting with the platform's user interface.

On second day, we learnt how to create & manage user accounts, assign roles and permissions, and configure access controls to ensure security.

On third day we understood how to define reference sets, create detection rules & configure security policies to enforce compliance.

On fourth day we learnt about components and methodologies of the framework; and learnt how to effectively utilize it for enhancing network security.

On fifth day we learnt about the benefits & considerations of integration and also learnt basic practices for achieving interoperability.

On last day we learnt how to create custom scripts and workflows, integrating with QRadar with orchestration tools and also gave a grand assessment test to test the knowledge till now.

## ACTIVITY LOG FOR THE SIXTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day - 1 | Malware Detection Introduction | Understood various malware detection techniques | |
| Day - 2 | Converting Service Logs into Datasets. | Learnt converting unstructured service logs into structured datasets. | |
| Day - 3 | Databases in Cloud | Understood how scalable solutions help us. | |
| Day - 4 | Load Balancing Pattern | Learnt implementation of load balancing patterns | |
| Day - 5 | AWS Global Infrastructure | Learnt leveraging AWS Global Infrastructure. | |
| Day - 6 | Execution of Orchestrator Pattern for Microservices Architecture | Learnt techniques for implementing the Execution Orchestrator Pattern. | |

**WEEKLY REPORT**

**WEEK – 6 (From Dt..11/3/24.. to Dt16/3/24...)**

**Objective of the Activity Done:** Significance of Malware Detection

**Detailed Report:** On first day we understood the critical importance of malware detection in cybersecurity, recognizing its role in identifying and mitigating threats.

On second day we comprehended the process of converting unstructured service logs into structured datasets, including data extraction, parsing, normalization, & transformation techniques.

On third day, we got a proficiency in leveraging cloud based database services to store and retrieve data efficiently.

On fourth day, we learnt how to implement load balancing patterns to improve the reliability and performance of distributed systems.

On fifth day we learnt leveraging AWS Global Infrastructure to deploy, scale & optimize cloud based solutions, understanding its benefits.

On sixth day, we continued with the Grand Assessment test and also learnt about Orchestration techniques.

## ACTIVITY LOG FOR THE SEVENTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project Development | Overview about the project. | |
| Day-2 | Project Development | Illustration of demo Project | |
| Day-3 | Project Development | Topic / Titles of the Project | |
| Day-4 | Project Development | Titles of Project. | |
| Day-5 | Project Development | Titles of Project | |
| Day-6 | Project Development | Titles of Project. | |

WEEKLY REPORT

WEEK-7 (From Dt.18/3/24 to Dt.23/3/24..)

Objective of the Activity Done: Developing of Long Term Internship Project

Detailed Report

On the first day we are given a brief idea about the development process of the project. We had to login into the official SmartInternz site and get access to our projects.

On second day we are explained a demo project and we got an brief idea on how to develop the project based on the title which we choose.

On third day till the last day of the week we are explained various titles of the project and we had to choose any one of the title and develop the project for this internship based on the topic choosen by us.

There are almost more than a ten topics available for us to choose from.

## ACTIVITY LOG FOR THE EIGHTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project work | Explanation of Github | |
| Day-2 | Project work | Explanation of Github | |
| Day-3 | Project work | Explanation of Github | |
| Day-4 | Project work | Explanation of Github | |
| Day-5 | Project work | Explanation of Github | |
| Day-6 | Project work | Explanation of Github. | |

WEEKLY REPORT

week-8 (From Dt. 25/3/24 to Dt. 30/3/24)

**Objective of the Activity Done:** To complete the Project work

**Detailed Report:**

The whole 8th week was dedicated in explaining how to use Github and this included the following steps,

Step 1 - Creating a GitHub Account

Step 2 - Creating a repository on GitHub

Step 3 - Collaborating with teammates on GitHub.

Step 4 - Creating folders related to the project work on GitHub

Step 5 - Uploading essential files related to the project on GitHub.

## ACTIVITY LOG FOR THE NINTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project work | Clarified doubts | |
| Day-2 | Project work | Clarified doubts | |
| Day-3 | Project work | Clarified doubts | |
| Day-4 | Project work | Clarified doubts | |
| Day-5 | Project work | Clarified doubts | |
| Day-6 | Project work | Clarified doubts. | |

**WEEKLY REPORT**

**WEEK-9(From Dt.1/4/24 to Dt.6/4/24)**

**Objective of the Activity Done:** To complete the Project Work

**Detailed Report:**

After we learnt how to use GitHub, we were still left with some doubts regarding the project, so the Smart Internz team offered us a whole week to get our doubts clarified till a vast extent.

Some doubts which have arised during our project development were as follows,

-> Should all teammates do the project individually.?

-> Should each teammate assignments be included in the leader's GitHub repository.?

-> What files should the team leader give in his/her repository.?

-> Can two or more teams choose same project title, if yes can they present both their projects alike.?

-> Is there any reference for completing the project?

## ACTIVITY LOG FOR THE TENTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project Work | Created GitHub repository | |
| Day-2 | Project Work | Created GitHub folders | |
| Day-3 | Project Work | Created an access to teammates | |
| Day-4 | Project Work | Collaborated all teammates | |
| Day-5 | Project Work | Doubts Clarification | |
| Day-6 | Project Work | Doubts Clarification | |

WEEKLY REPORT

WEEK-10(From Dt. 8/4/24 to Dt. 13/4/24.)

**Objective of the Activity Done:** To complete the Project work

**Detailed Report:**

During this week we decided to start our project work.

For that first we as a team created accounts personally on GitHub.

Then we created a folder in name of assignments and uploaded all the assignments given during our term in long term internship.

After that all the team members were made to be collaborated to the leader's repository and were given push access to the team leaders repository so that they could upload their assignments individually into the folder created by the team leader in name of "Assignments".

Last two days we clarified few other doubts which we were unable to configure.

ACTIVITY LOG FOR THE ELEVENTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project work | Understanding the title. | |
| Day-2 | Project work | Gathering required materials. | |
| Day-3 | Project work | Updating the software. | |
| Day-4 | Project work | Installation of required applications | |
| Day-5 | Project work | Doubts Clarification | |
| Day-6 | Project work | Doubts Clarification | |

WEEKLY REPORT

week-11 (From Dt:15/4/24 to Dt:20/4/24.)

**Objective of the Activity Done:** To complete the Project Work

**Detailed Report**

During this week we started our project. The title which we took is, "Understanding Cyber Threats : Exploring Nessus & Beyond Scanning Tools".

On the first day we understood our project title. Our project was based on exploring Nessus tools for vulnerability scanning and also exploring various other tools rather than Nessus.

On second day we gathered all the materials required for the project, these include laptops, wifi connection, reference books etc. On third day we updated our systems so that we don't lag in the project development phase.

On fourth day, we installed the applications & other software for our project. These include Nessus application and kali Linux to use other scanning tools.

Last two days we used to clarify our doubts in the installation process.

## ACTIVITY LOG FOR THE TWELTH WEEK

| Day & Date | Brief description of the daily activity | Learning Outcome | Person In-Charge Signature |
|---|---|---|---|
| Day-1 | Project Work | Signed into APSCHE SmartInternz site | |
| Day-2 | Project Work | Understood the project milestones | |
| Day-3 | Project Work | Assigning tasks to team members | |
| Day-4 | Project Work | Evaluated the whole output presented by team members | |
| Day-5 | Project Work | Combining all gatherings and completing project | |
| Day-6 | Project Work | Creating a project demonstration video | |

**WEEKLY REPORT**

**week-12 (From Dt. 22/4/24 to Dt. 27/4/24.)**

**Objective of the Activity Done:** To complete the Project work

**Detailed Report**

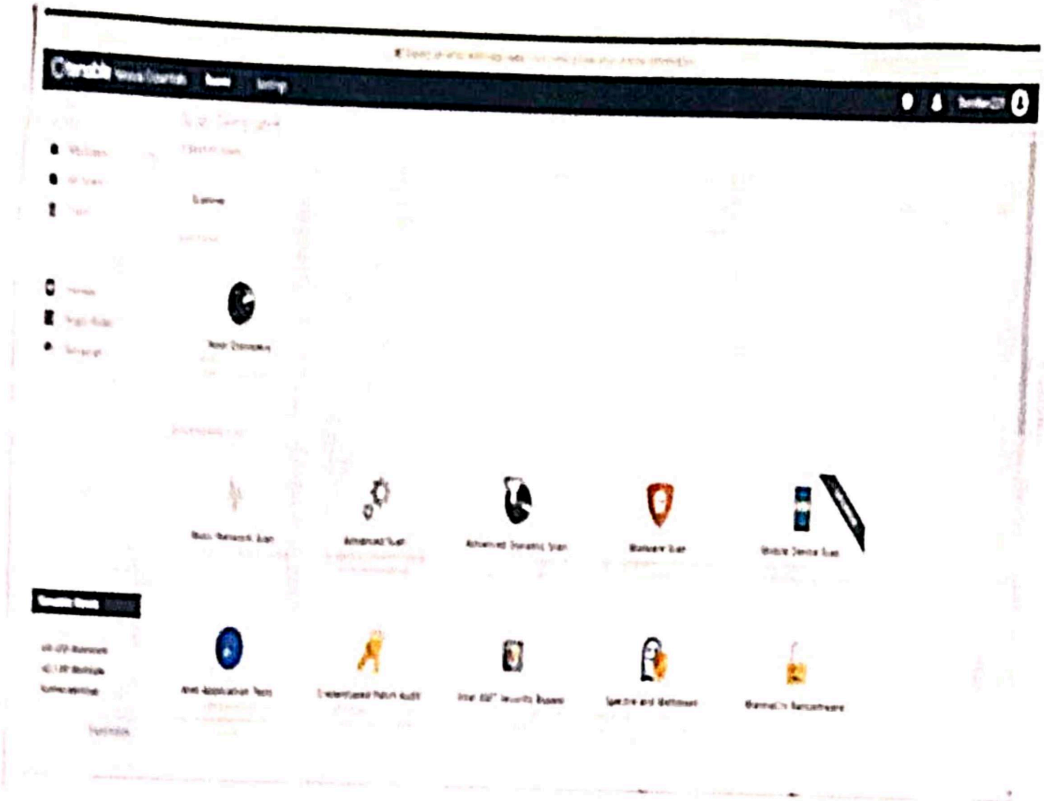
On the first day we logged into the APSCHE SmartInternz website using our credentials and then went into the project workspace to get access for our project.

Then next day we understood the milestones to complete our project and the other day each team member was assigned a specific milestone to reach by himself to complete the whole project.

After that on fourth day, all the work done individually by the teammates was reviewed together to check if it reaches the requirement to complete the project and few errors were rectified on this day.

On day five we combined all the final outputs and have completed our project successfully. We also had to do a demonstration video regarding our project. So, on sixth day we successfully completed it too and submitted everything to the GitHub repository of the team leader.

# About Nessus -

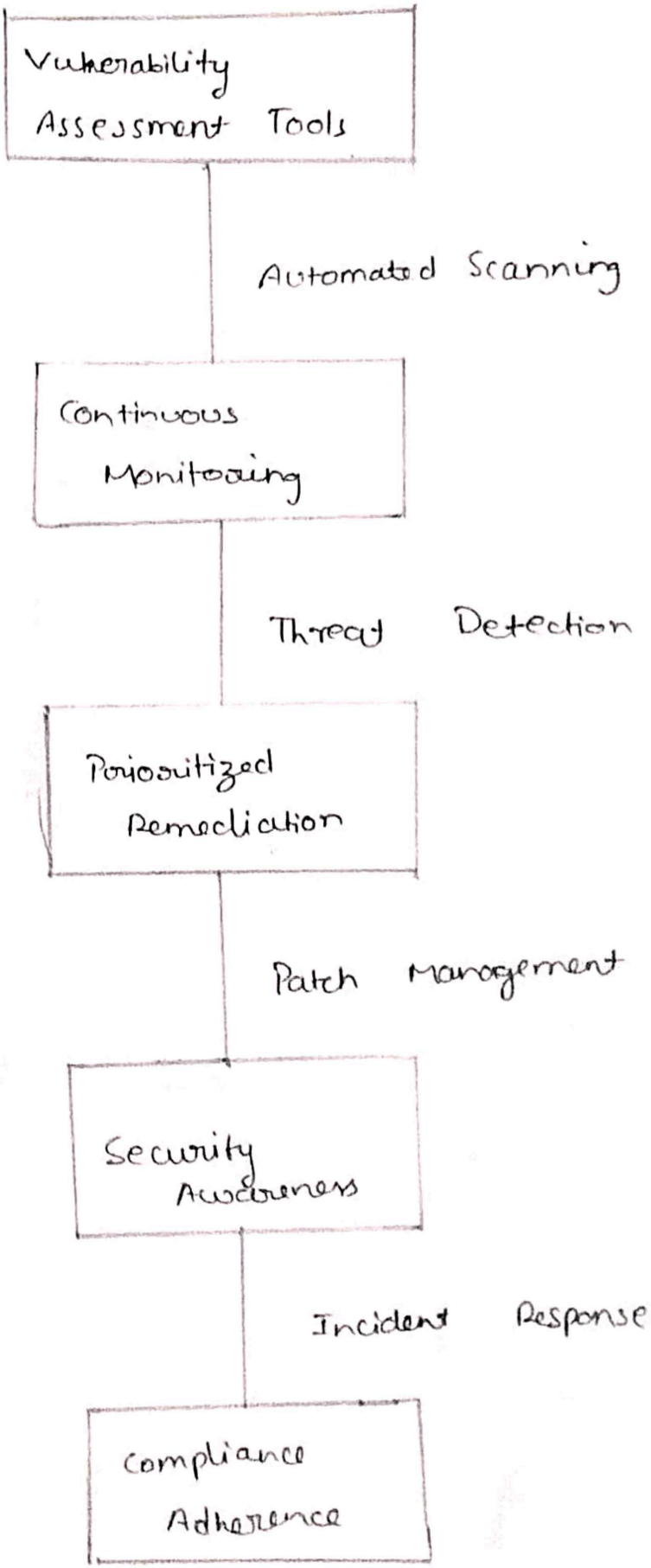


Nessus is one of the most widely used vulnerability assessment tools, known for its comprehensive scanning capabilities.

It performs network vulnerability scanning to identify security issues, misconfigurations, and potential threats within a network infrastructure.

The tool provides detailed reports on discovered vulnerabilities, prioritizing them based on severity levels and offering remediation recommendations.

## Analyzing Scan –



## PROCESS OF THE PROJECT –

All we have to do in this project is scan for the vulnerabilities and give effective mitigation strategies for them. We could also follow the milestones given on APSCHE SmartInternz site for reference, these milestones include the following,

⇒ Introduction to Cyber Threats and Vulnerability Scanning –

This includes the following;

- Understanding Cyber Threats
- Introduction to Nessus
- Beyond Nessus: Overview of Other Scanning Tools
- Importance of vulnerability Management
- Understanding Nessus Reports.

⇒ Planning And Preparation –

This includes the following,

- Preparing the Environment
- Scoping the Scan
- Compliance & Regulatory Requirements
- Resource Allocation & Scheduling
- Stakeholder Communication.

⇒ Conducting Vulnerability Scans –

This includes the following:

- Executing Nessus Scans
- Interpreting Scan Results.
- Analyzing Scan Findings
- Addressing False Positives & False Negatives
- Repeating of Scans

⇒ Remediation & Mitigation –

This includes the following,

- Prioritizing Remediation Efforts
- Implementing Security Controls
- Testing & Validation
- Incident Response and Contingency Planning
- Continuous monitoring & Improvement.

⇒ Integration And Automation –

- Integrating with Security Information & Event Management Systems.
- Automating Scanning Workflows
- Leveraging Threat Intelligence
- Scalability & Flexibility
- Monitoring and Reporting Automation

⇒ Best Practices & Future Trends -

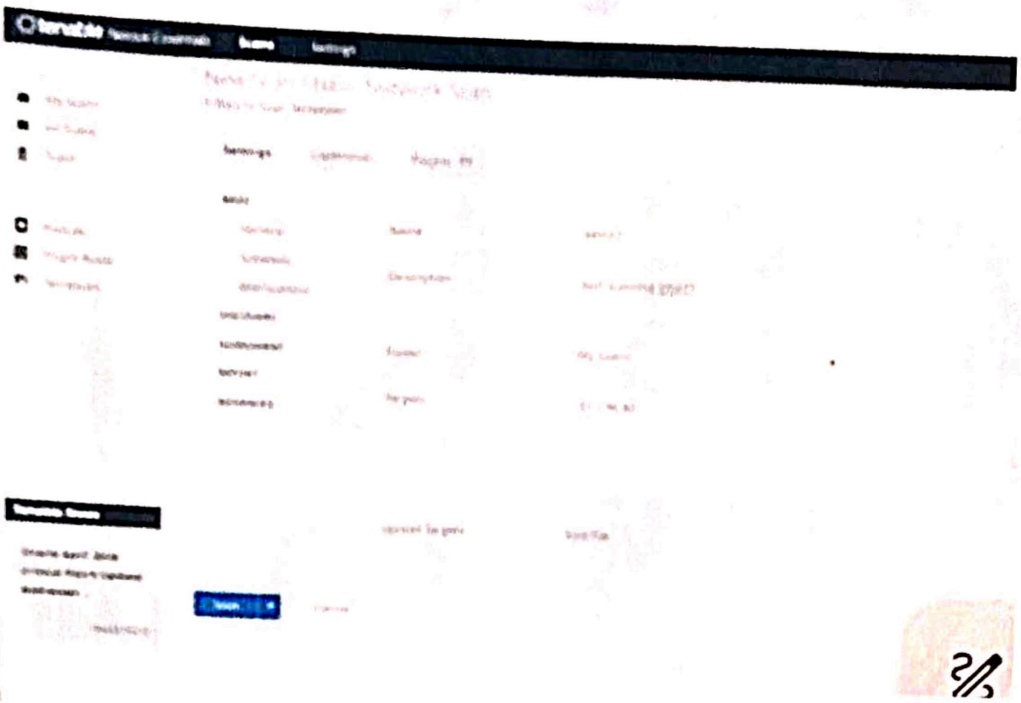
- Best Practices in Vulnerability Management
- Emerging Trends in Vulnerability Management
- Case Studies & Use Cases
- Continuous Learning & Professional Development
- Conclusion And Recommendations

By following all these milestones we could complete the project. So each team member was assigned with a specific milestone to do a research on and the all the results were combined together into a singal project.

Along with "Nessus Scanning Tool" we have also used "Nmap" on Kali Linux and have compared both the results obtained and made our conclusion.

To use Nessus you first need the IP address of the target, so for that cause we used "NSLOOKUP" to find the IP address and with the help of that we were able scan the whole website fully and identify the vulnerabilities causing threat to it.

# Analysis of the Results -



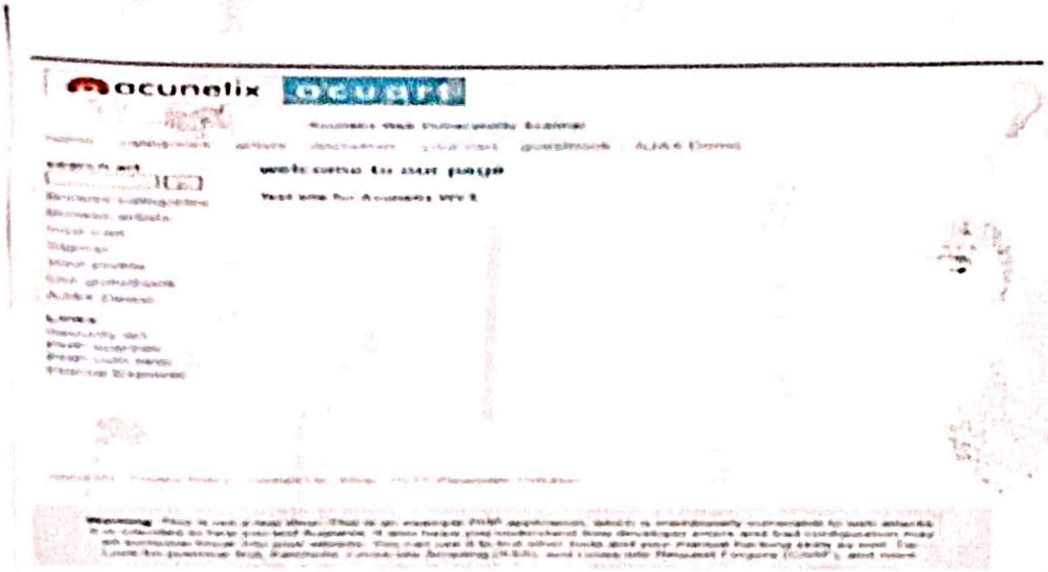
For this project we choose two sites one as the target & the other as practice site.

The Scan which we performed on them is 'Basic Network Scan' & this is done in Nessus Scanning Tool.

The practice site is Acunetix.

The target site is bWAPP.

Report on Practice Site -



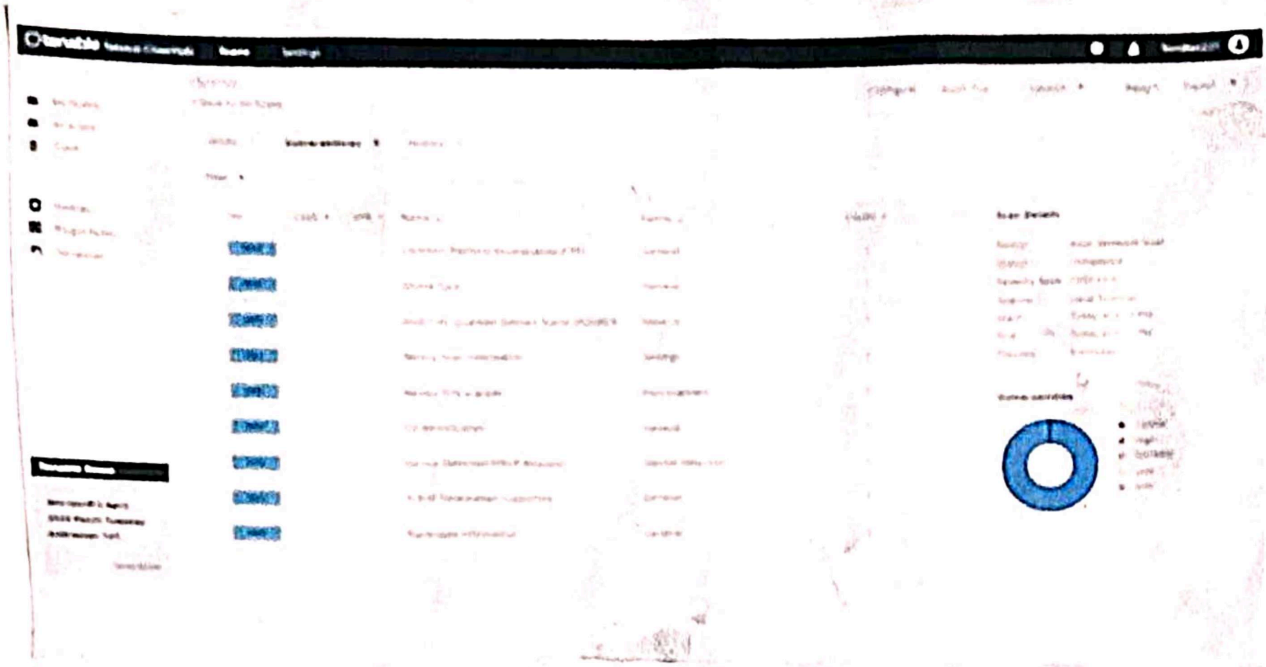

The practice site used is Acunetix.

First we use NSLOOKUP on this site to find the IP address.

Then we found that the IP address is 44.228.249.3.

Now use this IP address on Nessus and choose Basic Network Scan.

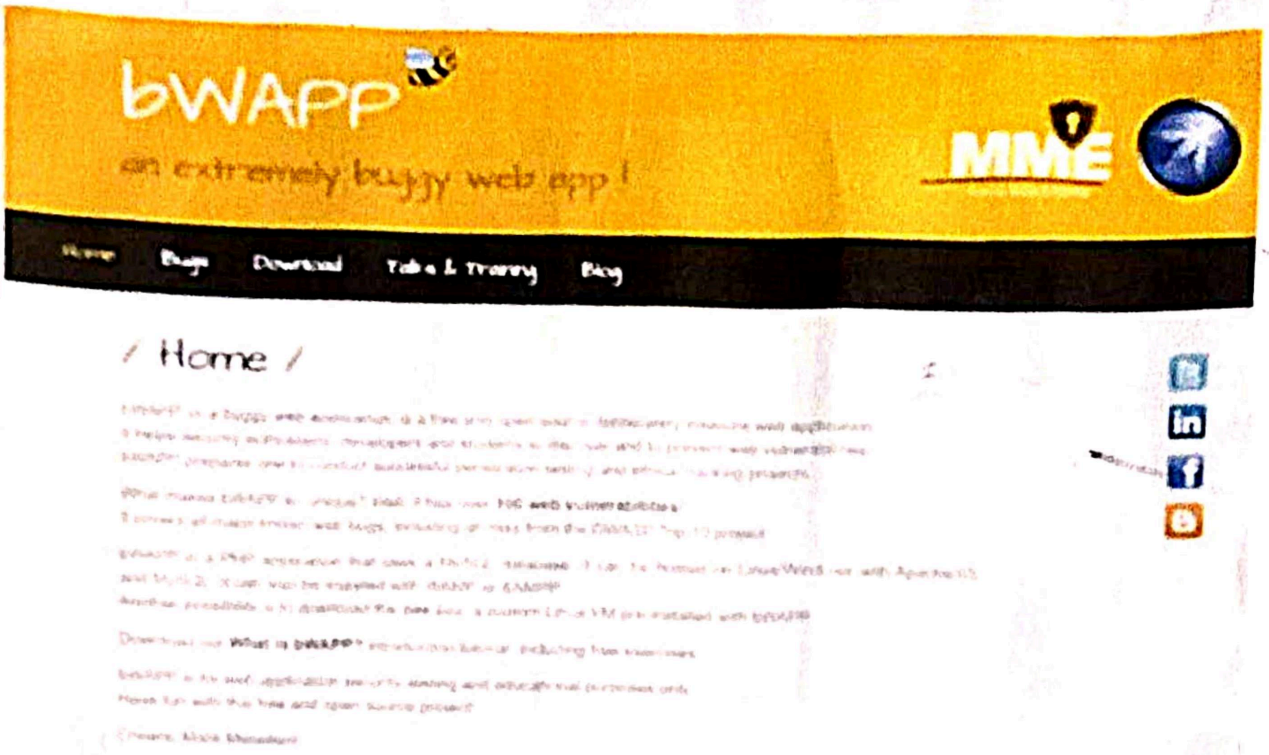
Click on save and hit launch button and wait for sometime till it gets completed.



After scan is completed the final report is as follows, total nine vulnerabilities are encountered.

1) Common Platform Enumeration
2) Device Type
3) Host Fully Qualified Domain Name Resolution
4) Nessus Scan information
5) Nessus SYN scanner
6) OS Identification
7) Service Detection
8) TCP / IP
9) Traceroute Information

Report on Target Site -




The target site for this project is bWAPP.

Use NSLOOKUP and get the IP address same like before.

The IP address which we got is 31.3.96.40.

Use Basic Network Scan on this Ip address and save the scan. After that hit the launch button and wait for a while till it completed the process.


After the scan we encountered total 20 vulnerabilities,

1) Openbsd
2) Openssh
3) HTTP (Multiple issues)
4) SSH (Multiple issues)
5) Web Server (Multiple issues)
6) Service Detection
7) Nessus SYN Scanner
8) Apache HTTP Server Version
9) Common Platform Enumeration
10) Device Type
11) Drupal Software Detection
12) Host Fully Qualified Domain Name Resolution
13) Nessus Scan information
14) Open Port Re-check
15) OS identification
16) OS Security Patch Assessment Not Available
17) patch Report
18) Solar winds Server & Application Monitor Detection.
19) Target Credential Status
20) Traceroute Information

# Remediation & Mitigation Strategies

We have to take the following precautions to avoid the vulnerabilities encountered in scanning process, this applies for both the target site & the practice site,

1) Patch Management - Regularly update and patch software, frameworks, & plugins to address known vulnerabilities.

2) Web Application Firewall - Implement a WAF to filter & monitor HTTP traffic, blocking malicious requests & known attack patterns.

3) Secure Coding Practices - Train developers in secure coding practices to prevent common vulnerabilities like XSS & CSRF.

4) Input Validation - Validate and sanitize all user input to prevent injection attacks & data manipulation.

5) Least Privilege Principle - Limit user access and permissions to only what is necessary for their roles to minimize the potential impact of a breach.

6) Security Heders - Utilize security headers such as CSP, HTTP Strict Transport Security & X-Content-Type-Options to enhance browser security.

7) Encryption - Use SSL / TLS encryption to secure data in transit & implement strong encryption for sensitive data at rest.

# Uploading Project on GitHub

There are few steps left finally to upload the whole project onto the GitHub platform;

The steps involved are as follows -

Step 1 - Normally create a GitHub account of our personal.

Step2 - We then created the repository in name of our InstituteId number, our name & domain of internship & then made the repository "public" so that anyone with the link could view it.

Step3 - After that all the team members have been collaborated and given push access to the team leader's repository.

Step4 - Then we created folder as "Assignments" & again in that individual folders for all the teammates have been created and their respective assignments were submitted over there.

Step5 - In the final step we created folder named "Project" and submitted all the project related files in it & we also created a "readme.md" file & gave our project demonstration video link in it.

This way by following the above easy steps we have successfully uploaded our project work onto GitHub.

# CONCLUSION

In conclusion, vulnerability management is a critical aspect of maintaining a robust cybersecurity posture. By leveraging tools like Nessus & following best practices, organizations can effectively identify, prioritize, & mitigate security risks associated with various threats.

The project "Understanding Cyber Threats: Exploring Nessus & Beyond Scanning Tools", has provided valuable insights into the realm of cybersecurity vulnerability assessment.

Through an exploration of prominent scanning tools like Nessus and Beyond, the project aimed to enhance our understanding of cyber threats and the methodologies used to mitigate them. Nessus provides comprehensive scanning capabilities, enabling organizations to identify a wide range of security issues, misconfigurations, and potential threats within their IT environments.