LONG-TERM INTENSHIP

Track - cyber security with IBM Qradar

Team ID - LTVIP2024TMID11414

Team size - 5

Team leader - GORUSU LOKESH REDDY

Team member - GUMMALA HARI NAIDU

Team member - KAMBALA RAJ KUMAR.

Team member - SHAIK ABDUR RAAZIQ.

Team member - YERRAMASETTI MADHAN.

college :- Dr. L. B. Degree & P. G college

Project Title :- Understanding cyber threat Exploring Nessus & Beyond standing tools.

Introduction

Cyber Security within the realm of Artificial Intelligence (AI). Embodies a critical frontier, aiming to fortify digital ecosystems by instilling intelligent defense mechanisms. AI in Cyber Security 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 & Cyber security fuses a diverse spectrum of applications

Suggested Pre-requisites

→ Basic knowledge of operating Systems

An operating System is the most important software that runs on a Computer. It manages the Computer's 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
- Routers
- Topology

- 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 managment

Risk Managment is the identification Evaluation and Prioritization of risks followed by Co-ordinated and Economical application of resources to minimize monitor & Control the Probability of 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 to tasks such as Penetration testing & network manipulation. Its simplicity and readability and particularly advantages for Ethical hackers.

Summary

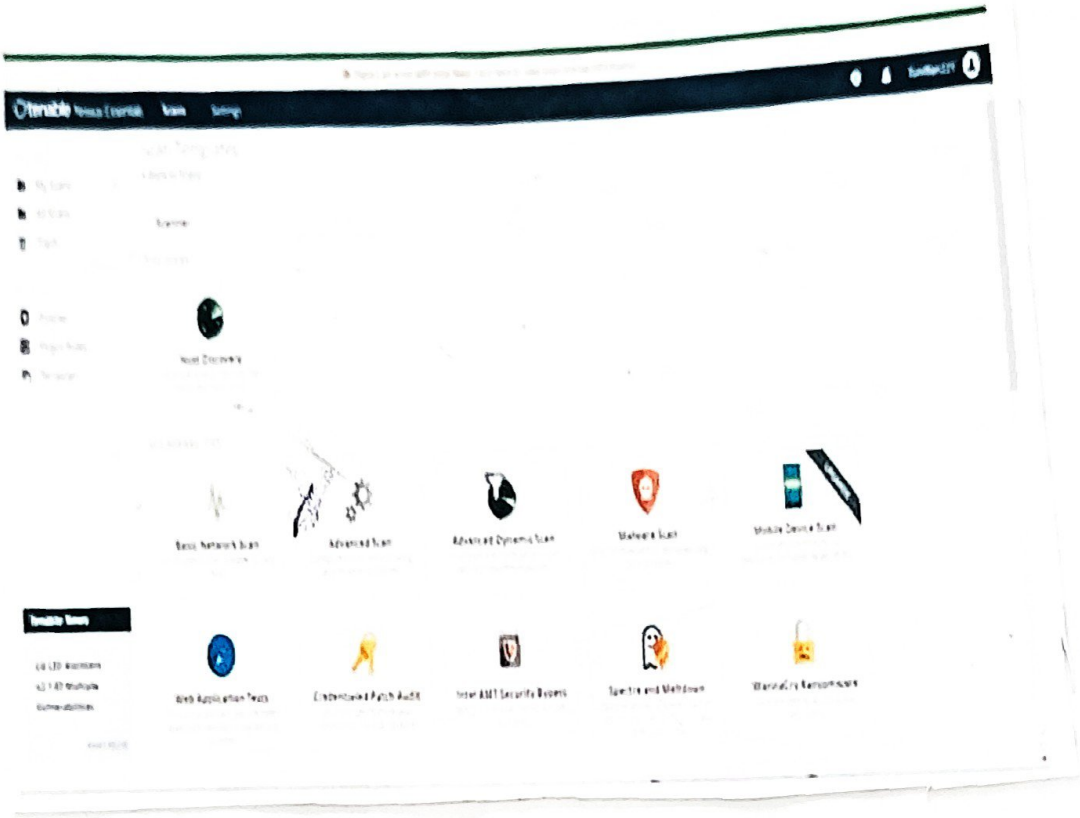
Our Relationship has successfully equipped participants with a comprehensive understanding of Cyber Security covering a range of Essential topics and Practical skills. We decided to the latest trends and Concepts in the field including ethical hacking setting up security operations Center (SOC) & Security Information & Event management (SIEM) Environments & Cyber Threat intelligence (CTI) Through a meticulously designed curriculum Interns gained insights into ethical hacking methodologies learning to identify vulnerabilities and propose effective strategies they also acquired Practical Experience in configuring & managing SOCs & SIEM Environment

Industry Profile

SmartBridge is an EdTech startup in Hyderabad, Telangana, India. It was founded in 2015 with the mission of bridging the gap between academics and industries. SmartBridge provides a platform to students, colleges, companies to connect and collaborate.

At SmartBridge, our cutting edge edtech platform SmartInternz, Project Based learning & Remote Internship platform serves as a catalyst for fostering collaboration between academia and industry. By braiding industry-driven content into the curriculum, it empowers students to cultivate the essential skills required to become job ready candidates.

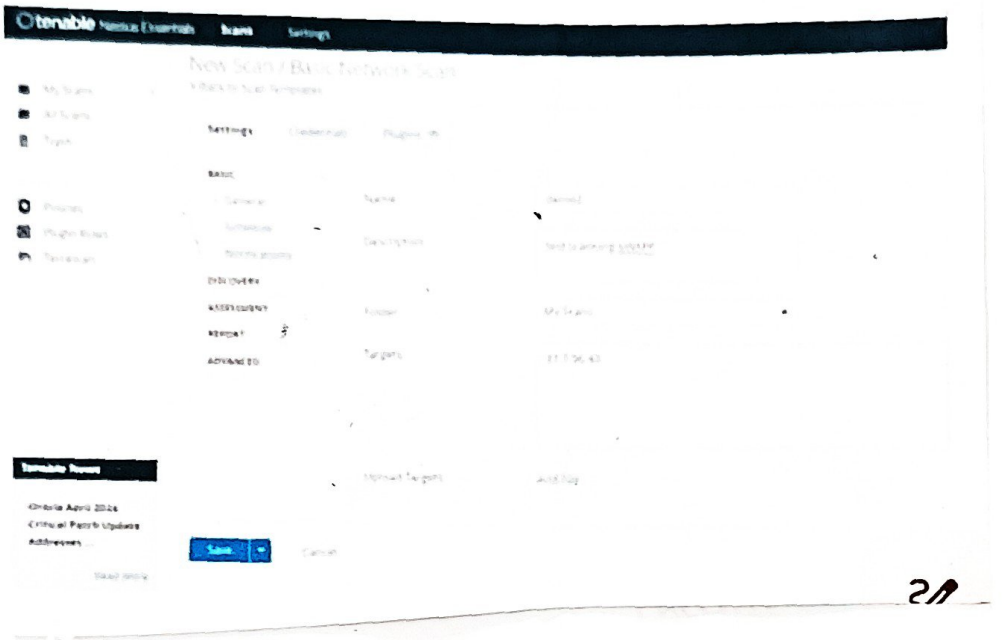
About Nessus:



Nessus is a remote security scanning tools, which scans a Computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any Computer you have Connected to a network.

- Nessus was founded by Renaud Deraison in the year 1998 to provision to the Community a free remote security.

Analysis of the Results



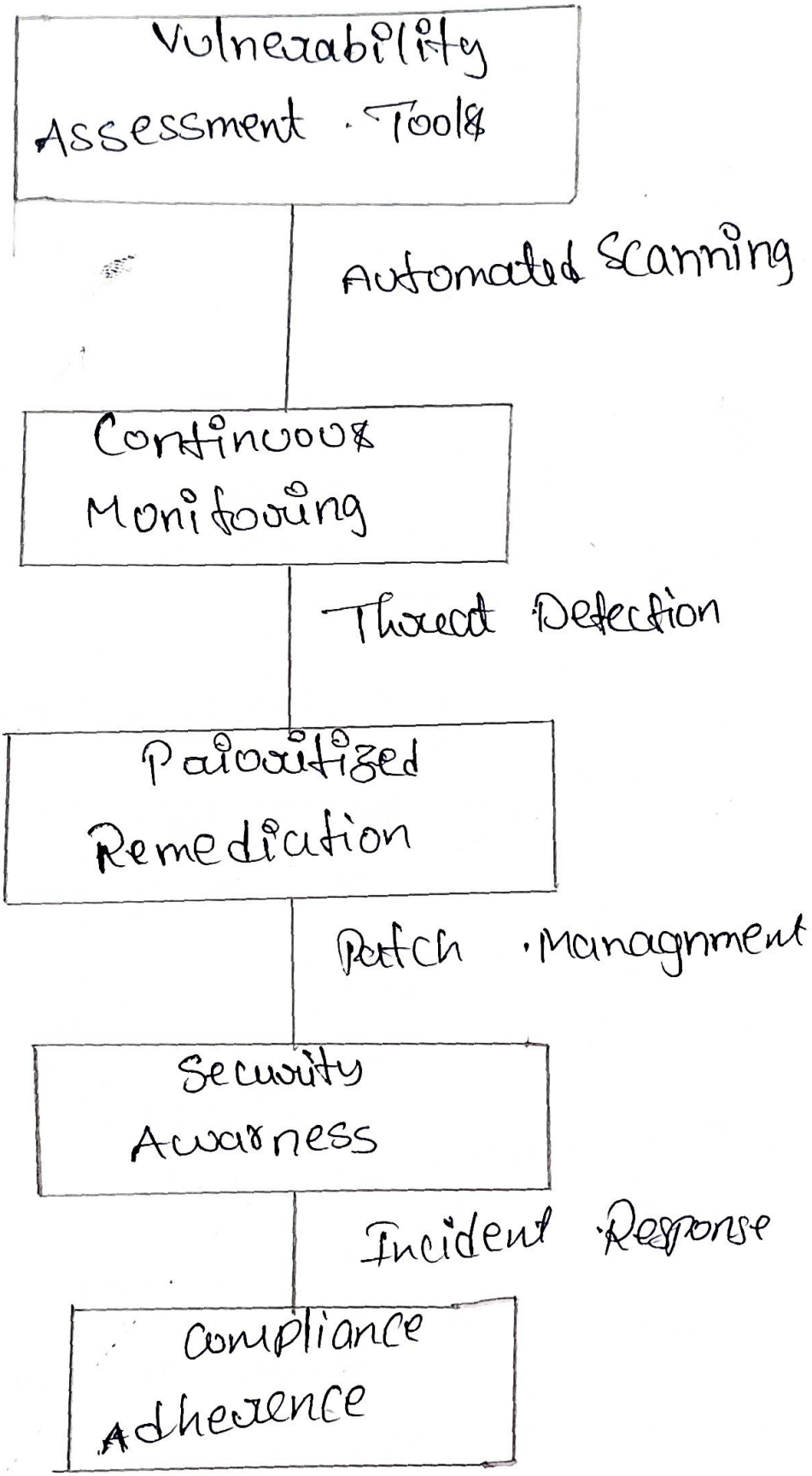
For this Project we choose two sites one as the target & the other as Practice site. The scan which we performed on them is Basic Network Scan & this is done in Nessus

The Practice Site is Acunetix

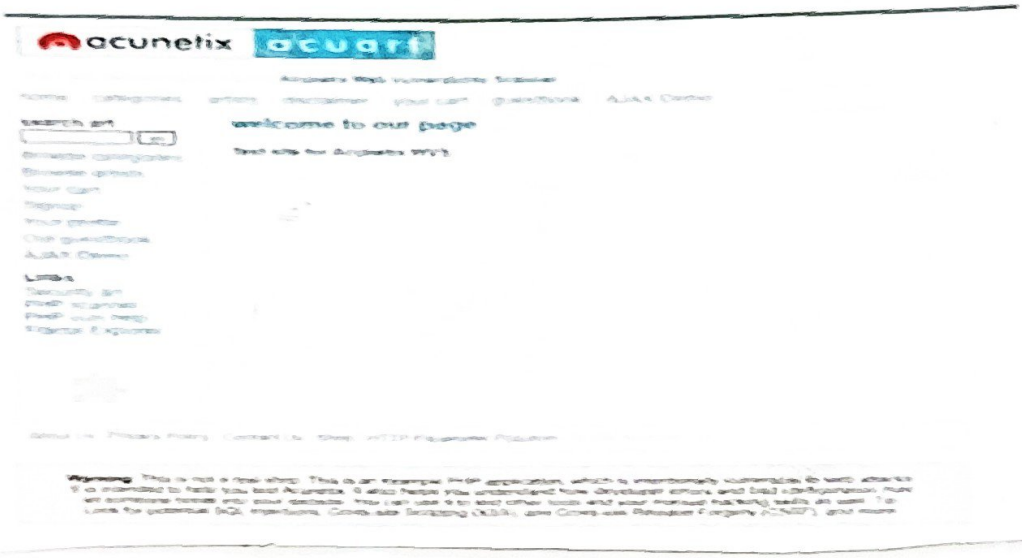
The target site is bwAPP

Theoretical Analysis

Block diagram:



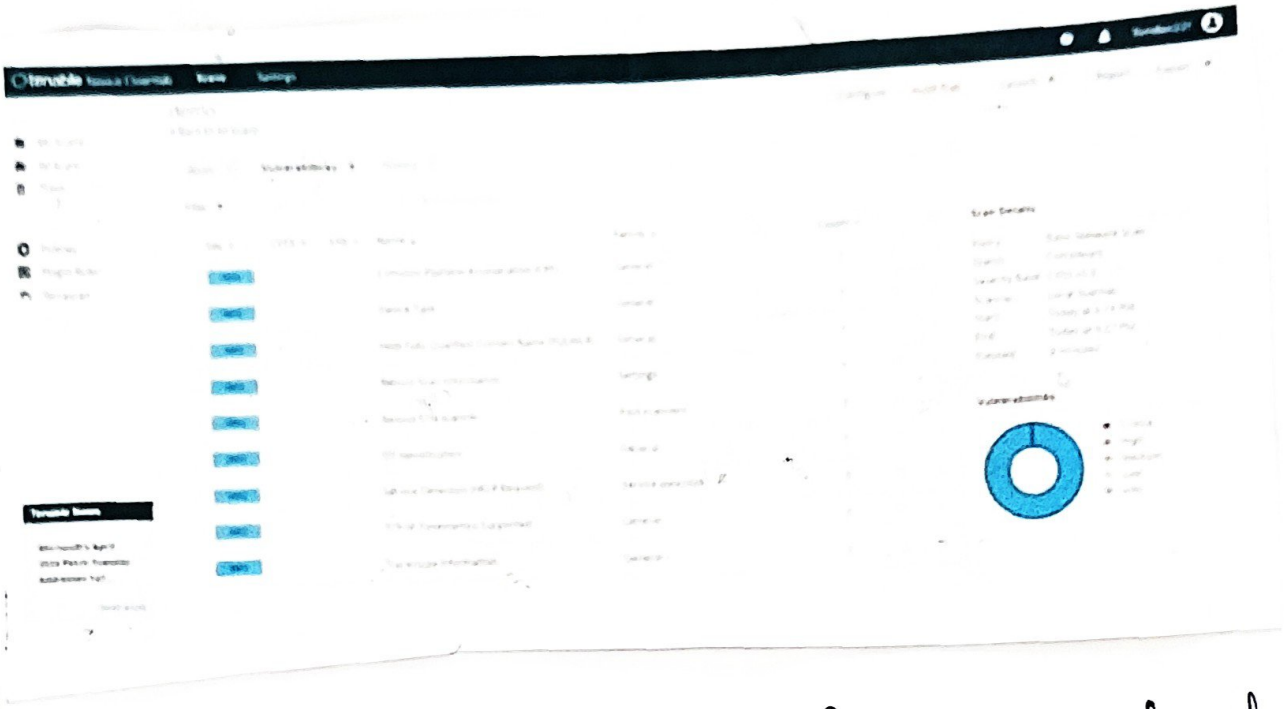
Report on Practice site



The Practice site used in 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 as follows. total nine . vulnerabilites

1) IP . countoral.
1) Common . Platform . Enumeration
2) Device type
3) . Host Fully Qualified Domain name Resolution
4) Nessus . scan . information
5) Nessus . scan information
6) OS . Indentification
7) Service . Detection
8) TCP / IP
9) Traceroute . Information.

Report on Target site:

The target site for this Project is bwapp or 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 addres and save the scan states that hit the launch button and wait for a while till it completed the process

After the scan we encountered total 20 vulnaribilites

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 (FQDN) Resolut

13. Nessus Scan Information

14. Open Port Re-check

15. OS identification

16. OS security Patch Assesment - Not Available

17. Patch Report

18. Solarwinds - server & Application Monitor

SAM) - detection

19. Target - Credential Status - by Authentication Protocol - No Credential Provided

20 - Traceroute information

Conclusion:

In conclusion the Project understanding Cyber threats. Exploring the Nessus and Beyound scanning tools has Provided valuable insights into the realm of Cyber security vulnerability assessment. Through an Exploration of prominent scanning tools like Nessus and Beyound the Project aimed to Enhance our understanding of cyber threats and the methodologies used to mitigate them.

Throughout the Project several key findings and outcomes have Emerged

1. Importance of vulnerability Assessment plays a crucial role in identifying and mitigating security vulnerability across networking infrastructure... Effective way to conduct Acomprehensive valunerability and assessments