

LONG-TERM INTERNSHIP

Track - Cyber Security with IBM Qudar

Team ID - LTVIP2024TMID1114

Team size - 5

Team leader - GOAVSU LOKESH REDDY

Team member - GUMMALA HARI NAIDU

Team member - KAMBALA RAJ KUMAR.

Team member - SHAIK ABDUR RAHMAN.

Team member - YERRAMSETTI MADHAN.

College :- Dr. L. B. Deyeu & P. G college

Project Title :- Understanding cyber threat
Exploring issues & beyond studying 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, seeking to emulate human cognitive abilities to detect, analyze, and respond to evolving cyber threats. Within this domain, AI leverages machine learning algorithms to discern actions, anomalies, and potential vulnerabilities within intricate datasets. This fusion of AI and Cyber Security fuels a diverse spectrum of applications, ranging from advanced threat detection and response systems to automated incident management and proactive security measures. The integration of AI into traditional cybersecurity paradigms promises to revolutionize how organizations protect their digital assets and maintain operational resilience in the face of日益复杂的 cyber threats.

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 other software and hardware.

→ Foundational Networking Concepts

These include the following

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

- Phishing
- Ransomware
- DDoS attack
- Malware
- Exploit
- 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 & impact of uncertain 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 are particularly advantages for ethical hackers.

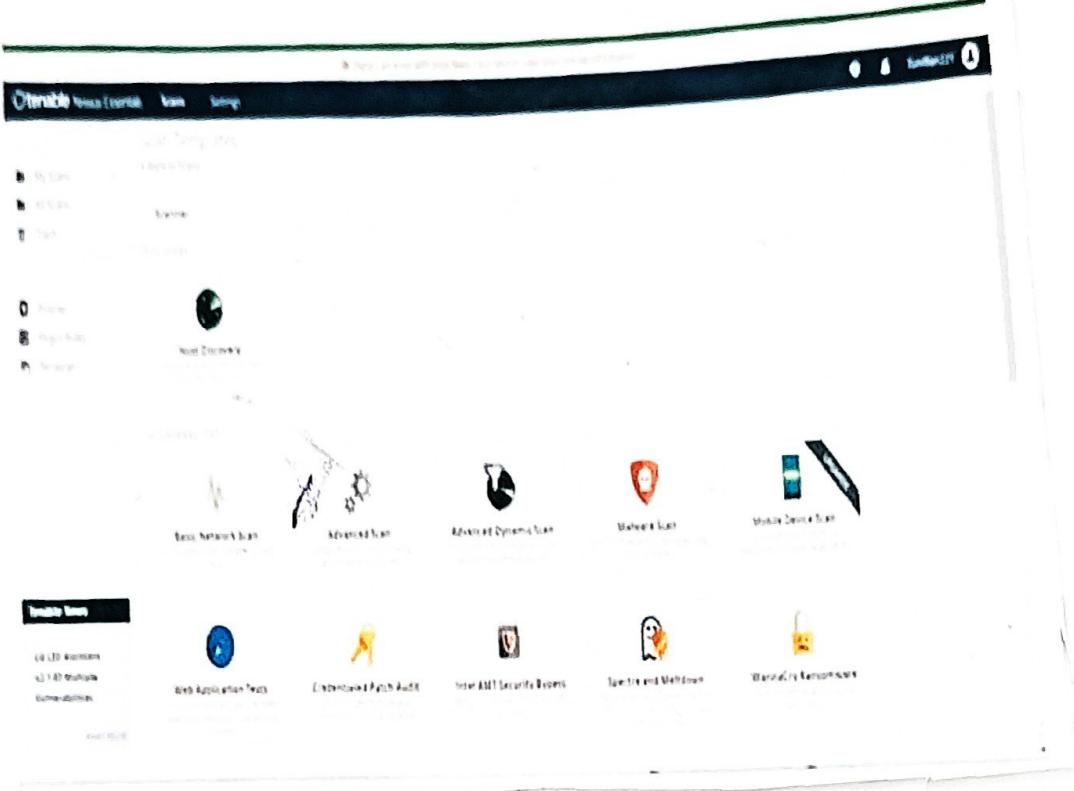
Session Summary

our relationship has successfully equipped participants with a comprehensive understanding of Cyber Security. Covering a range of essential topics and practical skills, we delved into the latest trends and concepts in the field, including ethical hacking, setting up security operations, Center (CSOC) & Security Information & Event management (SIEM). Participants gained insights into ethical hacking methodologies, learning to identify vulnerabilities and create effective strategies. They also acquired practical experience in configuring & managing SOC's & SIEM environments.

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 for Student Colleges, Companies, to connect and collaborate. At SmartBridge, we offer Cutting-Edge EdTech platforms Smart Putting Project-Based Learning and Remote Internship Platform. Serves as a catalyst for forging collaboration between academia and industry. By weaving projects closely woven 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 tool, which scans a computer and raises alerts if it discovers any vulnerability or collects. If it finds any use, for that malicious hackers could use. It gains access to any computer you have connected to a network.

- Nessus was founded by René Pfeifer in the year 1998 to provision to the community of free remote security.

Analysis of the Results

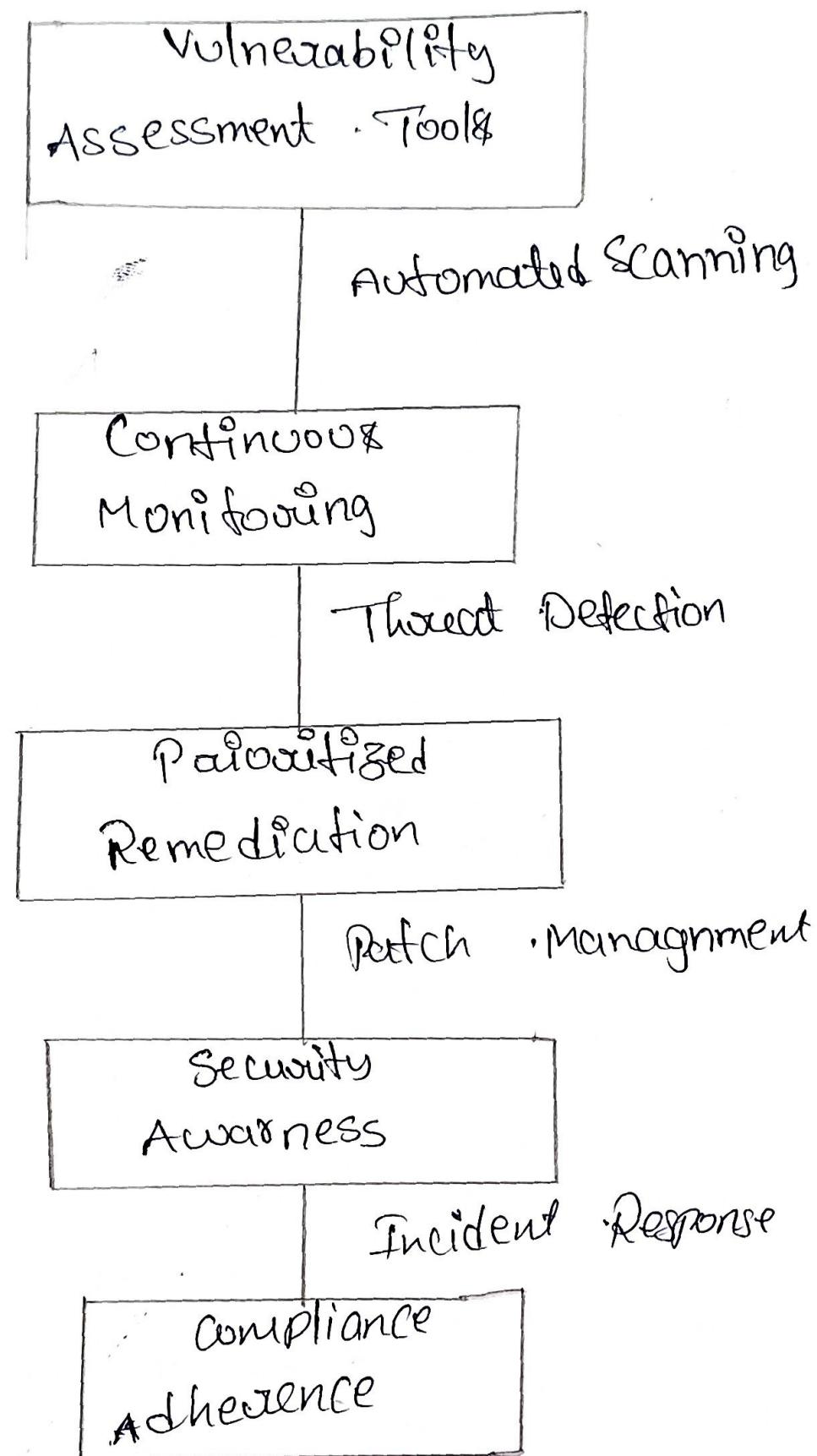
The screenshot shows the Tenable Nessus interface. At the top, there are tabs for 'Dashboard', 'Vulnerabilities', 'Scans', and 'Settings'. Below this, it says 'New Scan / Basic Network Scan' and 'Targets to scan: 192.168.43.1'. On the left, there's a sidebar with options: 'My Scans' (selected), 'All Scans', 'Targets', 'Practices' (selected), 'Plugin Lists', and 'Report Types'. The main area has tabs for 'General', 'Scanning Options', and 'Advanced Options'. Under 'General', 'Targets' is set to '192.168.43.1'. Under 'Scanning Options', 'Type' is set to 'Basic'. Under 'Advanced Options', 'Targets' is set to '192.168.43.1'. At the bottom, there are buttons for 'Scan' and 'Cancel'.

21

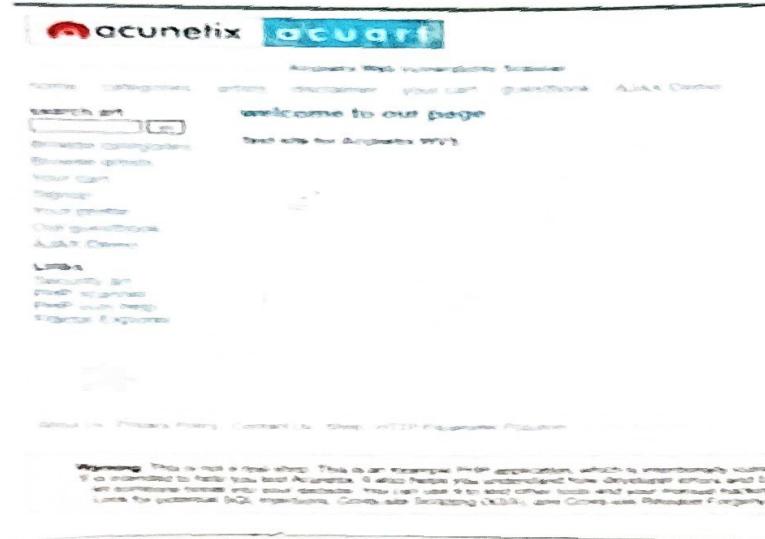
for this Project we choose two sites one as the target & the other as Practice site. The Scan which we performed on them is Basic Network Scan & this is done in Nessus. The Practice site is Acunetix. The target site is bWAPP.

Theoretical Analysis

Block Diagram:

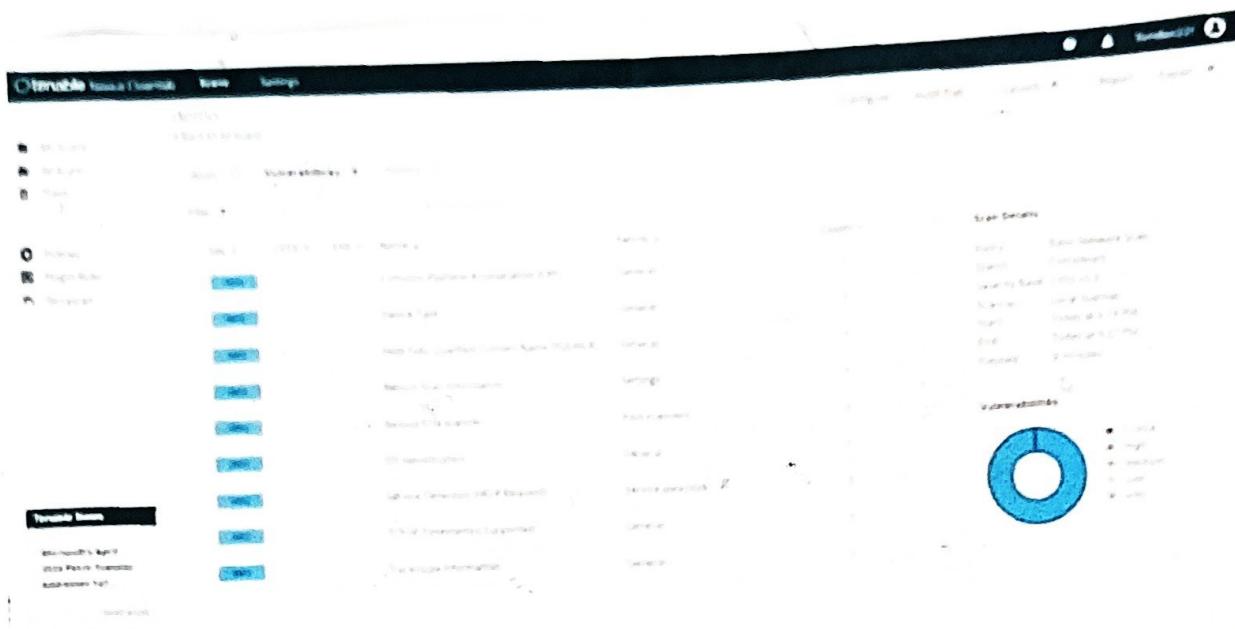


Report on Practice . Site



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 List . launch . button
and wait for sometime . till it gets
Completed.



After Scan is Completed. the final report as follows. total nine vulnerabilities

1) Exp - Counter

2) Common - Platform - Enumeration

3) Device type

4) Host Fully Qualified Domain Name Resolution

5) Nessus - Scan - Information

6) Nessus - Scan information

7) OS - Identification

8) Service - Detection

9) TCP / IP

10) Traceroute - Information.

Report on Target site:

The screenshot shows the homepage of the bWAPP website. At the top, there's a yellow header with the text "bWAPP" and a bee icon, followed by "an extremely buggy web app!". To the right of the header are two logos: "MME" with a shield icon and another logo with a blue circle and a white arrow. Below the header is a black navigation bar with links: Home, Bugs, Download, Tutorials & Training, and Blog. On the left, there's a breadcrumb trail: / Home /. The main content area has several sections of text and links. On the right side, there are four social media icons: Twitter, LinkedIn, Facebook, and YouTube.

bWAPP, or a buggy web application, is a free and open source deliberately insecure web application to help security enthusiasts, developers and students to discover and to prevent web vulnerabilities. bWAPP prepares one to conduct successful penetration testing and ethical hacking projects.

What makes bWAPP so unique? Well, it has over 100 web vulnerabilities! It covers all major known web bugs, including all used from the OWASP Top 10 project.

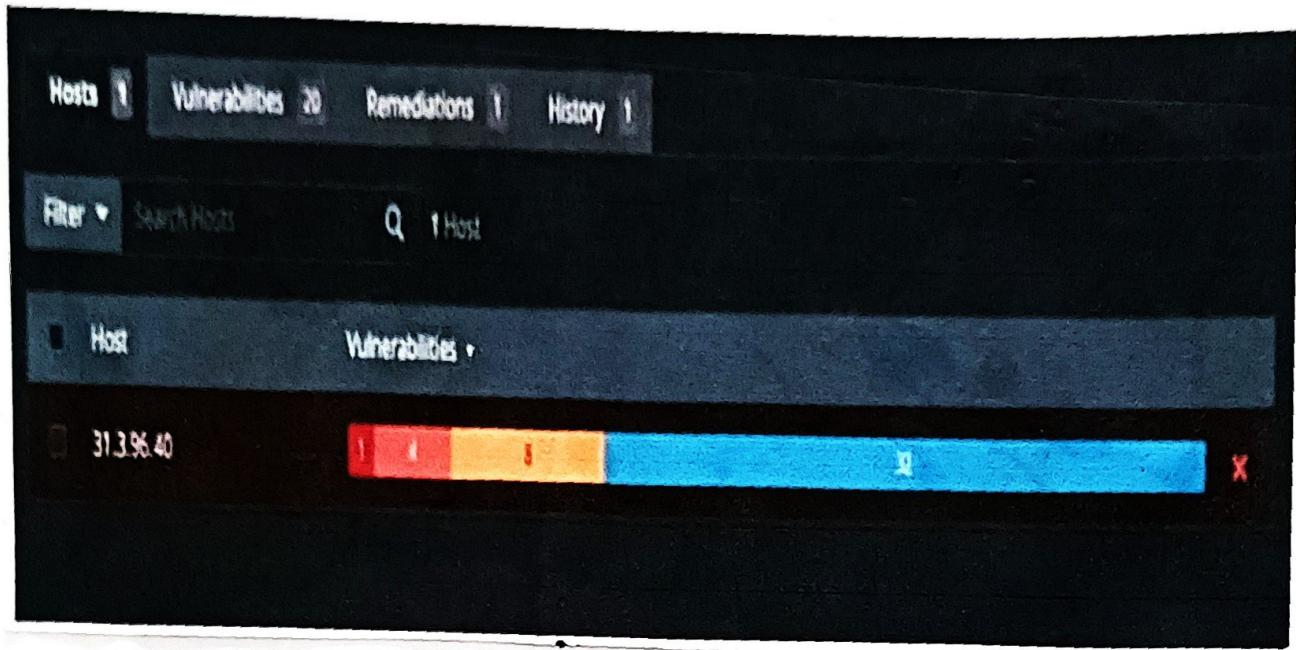
bWAPP is a PHP application that uses a MySQL database. It can be hosted on Linux Webshells with Apache 2.2 and MySQL. It can also be installed with WAMP or XAMPP. Another possibility is to download the Deb-Bin, a custom Linux VM pre-installed with bWAPP.

Download our What is bWAPP? introduction tutorial including two exercises.

bWAPP is for web application security testing and educational purposes only. Have fun with this free and open source project!

Authors: Mele Mansurhan

The Target - site for the Project is
bWAPP . us . 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 see the scan . After that hit
the . Launch . button . and wait for
a while . till . if 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 fingerprint
- 11) Drupal software detection
- 12) Host fully qualified domain name (FQDN) resolved

13. Nessus Scan Information
14. Open Port Re check
15. OS identification
16. OS security Patch Assessment • Not Available
17. Patch Report
18. Solarwinds - Server & Application Monitor
SAM) detection
19. Target Credential Status • by Authentication
Protocol - No Credential Provider
20. Trace route information

Conclusion:

In conclusion, the Project Understanding Cyber Threats, Exploring the Nessus, and Beyond Scanning Tools, has provided valuable insights into the realm of Cyber Security 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.

Throughout the Project, several key findings and outcomes have emerged

1. The importance of vulnerability assessment plays a crucial role in identifying and mitigating security vulnerabilities across networking infrastructure. The first way to conduct a comprehensive vulnerability and assessment