LONG TERM INTERNISHIP

Track - Cyber Security with IBM ORador

Team 10 - LTVIP2024 TMID 11398

Team Size - 4

Team Leader - Bhargava Sai Jetti

Team Member - Avala Jyotheeshwar Rao

Team Member - Bharani Siva Charan Chitto

Team Member - Chitrada Pavan

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

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

INTRODUCTION

Cybersecurity, within the realm of Artificial Intelligence (AI), embodies a withcal prontier, curring to fortify crosystems by instilling intelligent defense mechanisms. AI in cybersecurity yours various technologies and methodologies, string to emulate human cognitive abilities to detect, analyze and orespond to enduring cypes thoucuts domain. AI leverages machine algorithms to discorn patterns; anatrolies and potential vulnerabilities within intricate This Jusian of AI & cybersecurity Juels a diverse spectrum of applications.

Suggested Pou-requisties

Basic knowledge of Operating Systems

An operating system is the most important software that owns on a computer.

If manages the computers memory and processes; as well as all of its software a hardware processes; as well as all of its software a hardware

- These include the following
 - · IP address
 - · (omputer network
 - Ponotocol
 - . Ethernet
 - · Nodes
 - · Post
 - Router
 - · Topology

- -> Understanding of Common Cyber Throat -
 - · Phishing
 - · Ransomware
 - · DDOS attack
 - · Malware
 - · Exploits
 - · Spyware
- -> Knowledge of Security Tools & Technologies -
 - · Fiarwalls
 - · Encryption
 - Metasploit
 - · Snifters
 - · Wiou Shark
 - · Burp Suite
 - · Nessus
 - · Kali Linux

-> Compachension of Risk Management -

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

-> Python for hacking -

Python is a versatile programming language that offers a wide stange of tools and libraries, making it well-swited for tasks libraries, making it well-swited for tasks buch as peretration testing & network manipulation-such as peretration and readability are particularly Its simplicity and readability are particularly advantageous for ethical hackens

EXECUTIVE SUMMARY

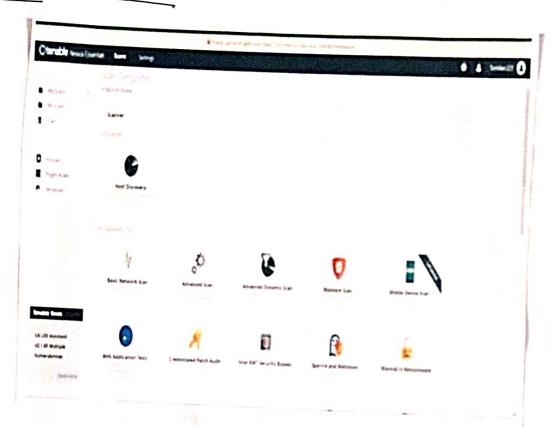
Our internship has successfully equiped participants with a comprehensive understanding of cybersecurity, ravering a viarge of essential topics and practical skills. We decided to the latest trends and concepts in the field, including ethical hacking setting up Socialty operations Onler (500) E security Intoarration & Event management (SIETY). environments, & Cyper Threat intelligence ((T1). Thaough a meticulously designed curriculum, interns gained insights into ethical hacking methodologies; learning to identify rulnerabilities and propose effective snakgies. They also acquired practical experience in configuring & managing SO(s & SIEM enviorements.

INDUSTRY Profile

Smartboidge is an EdTech Startup in Hyderakad. Telangana, Inclia. It was founded in 2015 with the mission of bouidging the gap between araclemics and inclustries. SmootBridge provides a platform la students, collèges, companies to connect and collaborate. At Smoot-Bridge our cutting-edge ad-tech platform, "Smart Interny", Poroject Based Learning & Remote Intourship Platform somes as a catalyst for forstering collaboration between academia and industry. By providing project based, collaborative learning solutions intricately wowen into the curriculum, it empowers students to cultivate the exertical skills required to become job ready candidates.

Analyzing Scan Vukerability Assessment Tools Automated Scanning Continuous Monitoring Detection Thread Porjositized Remediction Patch Monogement Security Awareness Incident Response compliance Adherence

About Nessus -



Nessus is one of the most wickly used vulnerability assessment tools, known for its comprehensive scanning capabilities. It performs network unbrability scanning to identify security issues, misconfigurations, and potential threats within a network infrastructure. The tool provides detailed supports on discovered vulnerabilities, prioritizing them based on severity levels and offering exercitation succommendations.

Analysis of the Results -

	ties or less			
My Brains	A Water fit brief Serrelassi			
And Services	bertings commit	races Mogres e		
	•			
Property.	- Almohay	Nations	many (
Trape Same	Antiquesting)	Compression	THE IS ALTONIA STREET	
Pindhawa	Assistate esticate		south billing	
	euto Wellige			
	MISSING SERVICE	Brokelger	May 11 min	•
	Administration	· Cargara	EL 5 NO 30	
		liphosa Lauger	467554	
re tort mee				
Trainer				
	Epiloo	n.		

For this project we choose two sites one as the tanget & the other as proctice site. The Scan which we performed on them is 'Basic Network Scan' & this is about in Nessus.

The practice site is Acuretix.

The tanget site is bloapp.

Report on Practice Site -



The paactice sto used is Acurchix.

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

Then we found that the IP address:

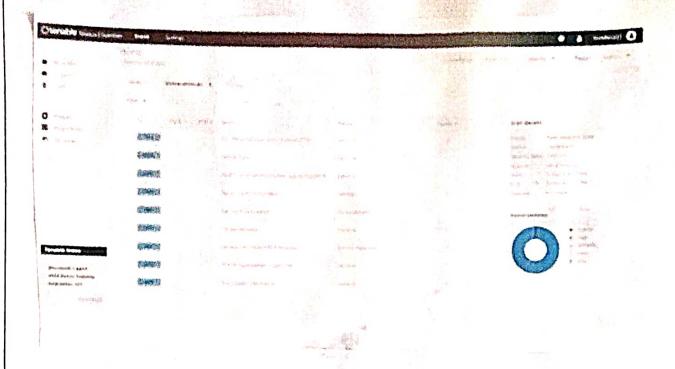
13 44-228.249.3.

Now use this IP address on NESSUS

Now use this IP address on the Scan .

and choose Bosic Network Scan .

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



After som is completed the first supposed is as follows, total nine vulnerabilitées aux encountered,

- ·) (ommon Platform Enumeration
- 2) Device Type
- 3) Host Fully Qualified Pomain Name Resolution
- 4) Nessus Scan information
- o) Messus SYN scanner
- 6) OS Identification
- 7) Service Detection
- 8) TCP/IP
- 9) Toucestoute Information

Report Tanget Site

ort extremely buyly web opp



Downsond Take L Travery

/ Home /

a bulgger area amphication in a hose mill spice was the exclusive experiences in development and exchange to plantical and to previous and extremationists market present which tensing and effects hope so; governing

ethus nusion schools as usugue's read in team to this web videorishelders

It convers bit major branch west things, excluding all make from the Catholic Top 10 project

Editable is a stopp accomplise that uses a failful advances it can be handed on Levis Montaines with Apparents ment there 2. I was now for remarked and exclude or a nature.

heather passables in to manneal the medium a common color VM pre-mented with brighting

Deservoired and White is SWARPS improduction fater or malacing from exercising

Contract in you were attentioned markets control must environment brooklesses that

became that work this from which should minurise probests

Chemical Shalp Stimulars

target site for this project is bWAPP. The

NSLOOKUP and get the IP address Use

like before.

IP addones which we got is 31-3-96.40.

Metwork Scan on this IP address Basic Use

save the scan. After that hit

lowner button and weit for a while the

it completed the priocess. toll



After the scan we encountered total 20 vulnerabilities,

- 1) Openbsd
- 2) Opensih
- HTTP (Multiple issues)
- 4) SSH (Multiple issues)
- lueb Server (Multiple 155 cles)
- Scrike Detection
- 7) Messus SYN Sounner
- 8) Apacho HTTP Server Version
- 9) Common Platform Enumeration
- 10) Device Type
- 11) Drupal Software Detection
- 13) Host Fully Qualified Domain Name Resolution
- 13) Nessus Sian infoormation
- 14) Open Pool Re-check
- 15) Os identification
- OS security Patch Assessment Not Available 16)
- 17) Patch Report
- Solar winds server & Application Monitor Detection. 18)
- Target Credential Status
- Toraceroute Information 20)

CONCLUSION:

In consciousion the project Understanding threats and heyond scanning tools has provided valuable insights into the nealm of cyheoremity of the vulneanability project aimed to enhance own understanding of cyheor security threats and he went are Berond and the methodolgis used to he heigate them

Throught the Moint neveral key and Outcomy

- onthe in identifying Vulheaghility a coucid order
- 2. Comprehensive Scanning Capability Work one comments
 Scanning Capability unhibits and slay large

& security awarmers and incident onessor.