AI FOR CYBER SECURITY WITH IBM QRADER

UNDERSTANDING THE CYBER THREATS

TEAM ID: LTVIP2024TMID11382

TEAM SIZE: 2

TEAM LEADER : KAMBALA NAVIN

TEAM MEMBER : SAINI TIRUPATHI

COLLEGE: DR LANKAPALLI BULLAYYA COLLEGE,VISAKHAPATNAM

AI FOR CYBER SECURITY WITH IBM QRADER

UNDERSTING THE CYBER THREATS: EXPLORING THE NESSUS AND BEYOND SCANNING TOOLS

INTRODUCTION :-

Understanding cyber threats is crucial in today digital age where technology permeates nearly every aspect of our lives. Cyber security encompass a wide range of malcious activites conducted by individuals, groups or organizations with the intent to disrupt, steal manipulate digital assets. These threats can target various entities including individual business government and critical infrastructure.

Cyber threats can takes many forms such as

Malware :- Malcious Software designed to infect and damage computers or networks.

Social Enginerring:- Manipulating individuals into divulging confidental information or perforining actors that compromises Security.

Denial of Services (DoS) :- Overloading a System network, or website with Expensive traffic to distrupt network functionally and deny Services to legitimate Users.

OVERVIEW :-

Overview of Cyber Security in understanding the Cyber threats is an ongoing process that requires a multifacted approach. it involves implementing strong Security measures, Staying updated on Emerging threats Educating Users, and fastering a Culture of Security awarness. By adopting these Strategies, individuals and Organizations Can Enhance their resilience against cyber attacks and better protect their Sensitive information and System.

PURPOSE :-

Understanding Cyber threats Serves important purpose:-

1. Risk Mitigation :- By Understanding the various types of Cyber threats, individuals and organizations can identify Potential vulnerability in their System and network.

2. Protection of Assets :- Cyber threats pose a significants risk to digital assets, individuals sensitive information individual Property and critical infrastructure. Under standing those threats allows individuals and Organisation to Safeguard their assigns. Cyber threats can distrupt normal business operations, leading to financial loss and damage By understanding Cyber threats business can be improved.

- PROPSED SOLUTIONS & METHODS :-

To Understanding Cyber threats Effecticely, you Can utilize carious methods and resources.

Stay infsimed :- keep upto date with the latest news and trends and development in cyber threats. through reputable such as Cyber Security, news, websites industry publications, and Social Media Channels dedicated to Cyber Security

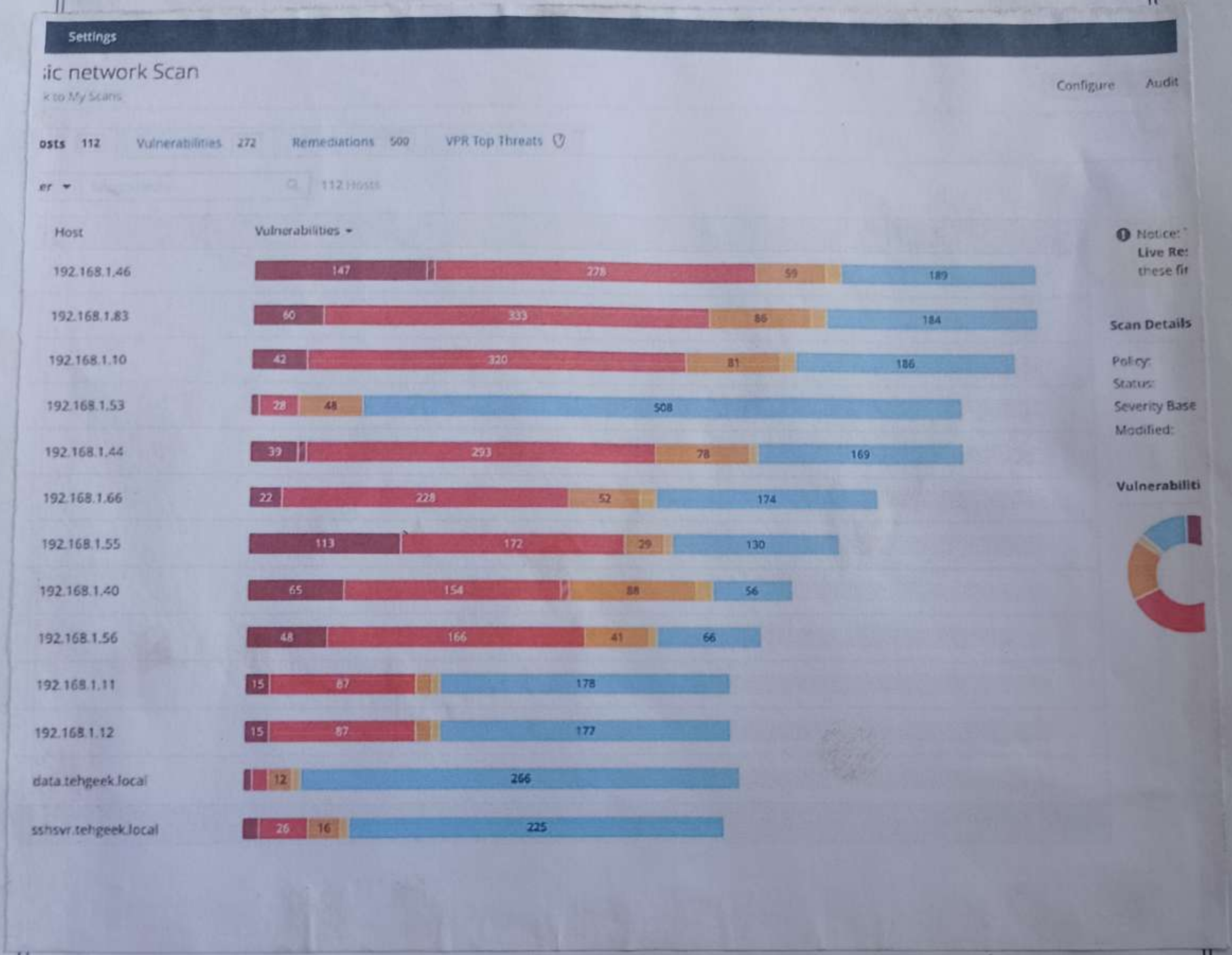
Toyning and Education :- Take Adcuantage online Courage wоrkshopes and Certifications affsits by cyber Security Organizations University and trineeing procciders. these resources cover a widerange of topices fsim basics of Cyber Security principals to advanced through repsits Published leading cyber Security frames. government agenices and resources Organizations thesis repsrt Into Emergencies Cyber threats Provide cvariable insides. Attack threats, recommanded mitigations.

Participate in Cyber Security Communications :-

Professional associations focussed on Cyber Security injections with other Cyber Security Professional with share insights Exchanges best practises & Collaberation

– THEORITICAL ANALYSIS

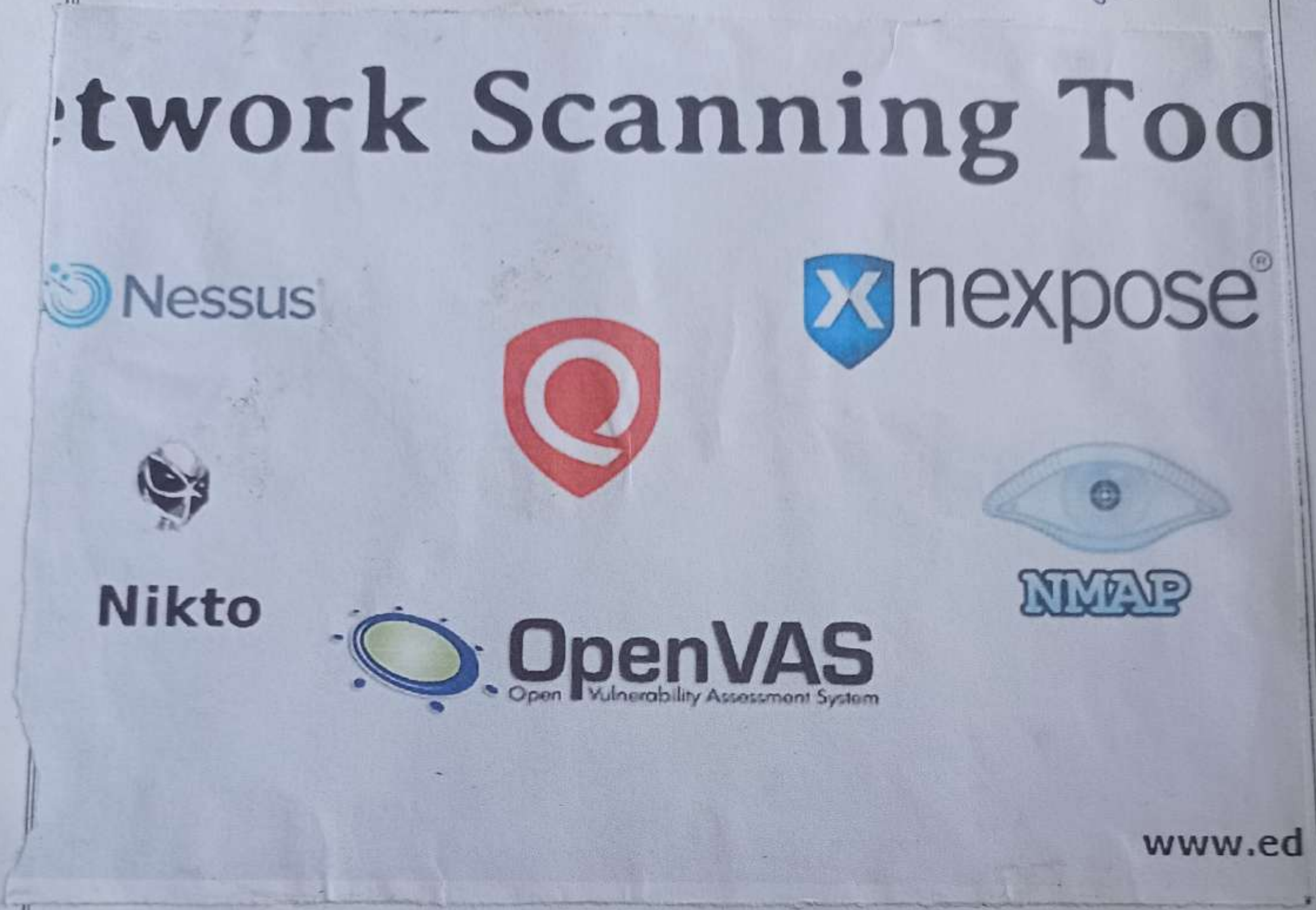
DIAGRAMMATIC OVERVIEW OF THE PROJECT



The Above Represented picture is An Nessus Report. The above mentioned are the Scanned Internet Protocol Address Vulnerabilities from Nessus tool. Here, Nessus is an highly Configurable and a good fit for more technical users. & Consistently detects the most recent CVEs while still keeping on track of legacy.

- Netwoɤking Scanning Tools & Techniques:-

These are several Scanning tools and Methodologies.



Thes let's Examine Some well-known Example.

1. Nessus:-

A well known Commercial vulnerability detection tool Called Nessus provides Number of functions.

2. Open VAS:-

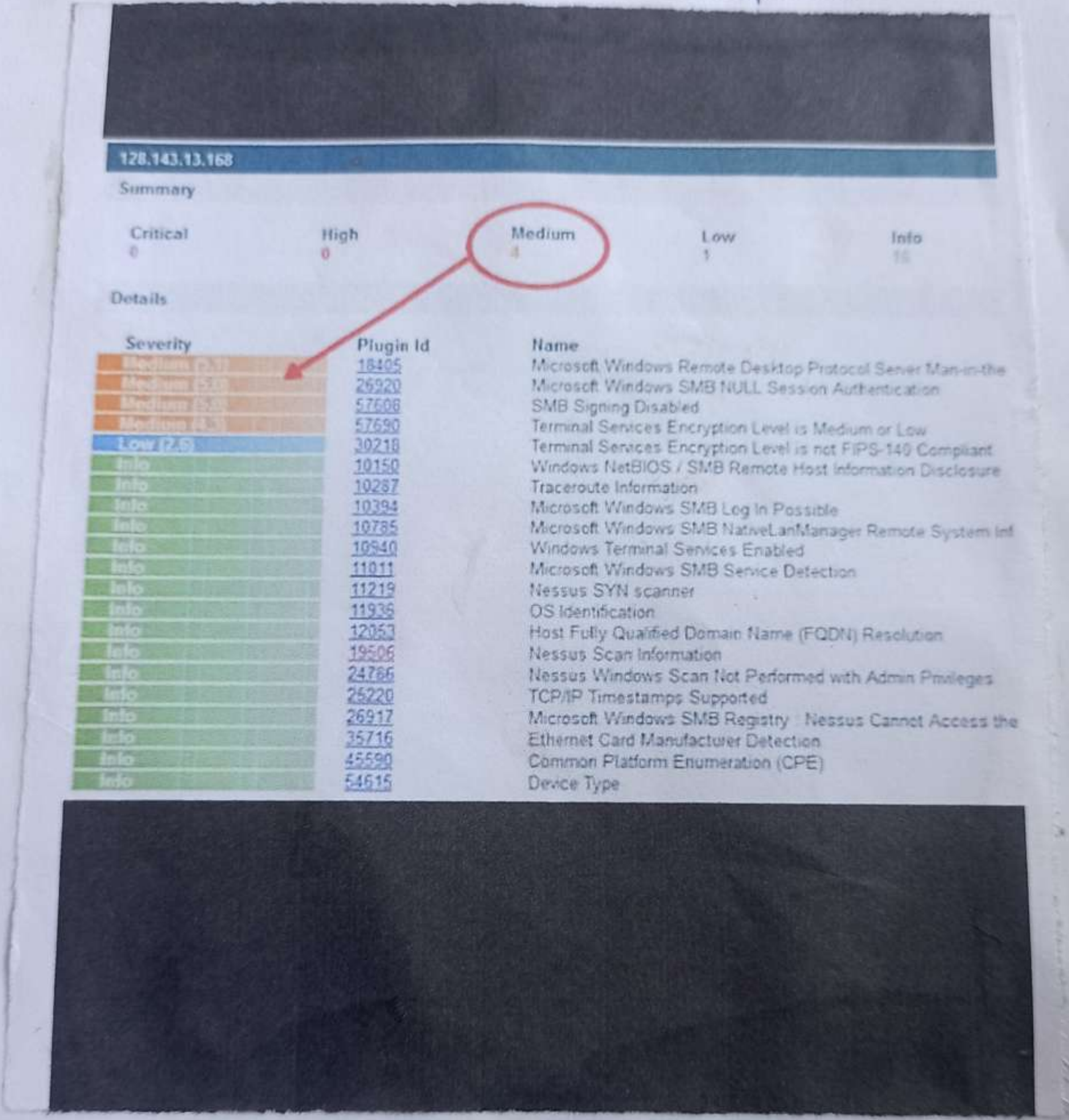
An Effective open-Source vulnerability Scanner Called openVAS (open vulnerability Assessment System).

3. NMap:-

The Netwoɤik Scanning tool Nmap is flexible and relliable. on their Netwoɤiks. It Enables find hosts, Services and open ports NMap provides Command lines.

- What is plugin?

A plugin is an analogous to the Virus definition that are added and updated regulasly to a Virus protection Program on a personal Computers.



[redacted]

128.143.13.168

Summary

Critical	High	Medium	Low	Info
0	0	4	1	16

Details

Severity	Plugin Id	Name
Medium (5.1)	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the
Medium (5.0)	26920	Microsoft Windows SMB NULL Session Authentication
Medium (5.0)	57608	SMB Signing Disabled
Medium (4.3)	57690	Terminal Services Encryption Level is Medium or Low
Low (2.6)	30218	Terminal Services Encryption Level is not FIPS-140 Compliant
Info	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
Info	10287	Traceroute Information
Info	10394	Microsoft Windows SMB Log In Possible
Info	10785	Microsoft Windows SMB NativeLanManager Remote System Inf
Info	10940	Windows Terminal Services Enabled
Info	11011	Microsoft Windows SMB Service Detection
Info	11219	Nessus SYN scanner
Info	11936	OS Identification
Info	12053	Host Fully Qualified Domain Name (FQDN) Resolution
Info	19506	Nessus Scan Information
Info	24786	Nessus Windows Scan Not Performed with Admin Privileges
Info	25220	TCP/IP Timestamps Supported
Info	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the
Info	35716	Ethernet Card Manufacturer Detection
Info	45590	Common Platform Enumeration (CPE)
Info	54615	Device Type

[redacted]

The result will be indicated the hacking has taken place. A System adminstrator would need to investigate furthur to find Evidence of an actual breach. The result will be indicated whether their could be weakness to hacking activities.

- ADVANTAGES AND DISADVATAGES

- ADVANTAGES :-

Pro Active Defense (PAD) :- Understanding Cyber Threats allows individulas and Organisations to anticipate potential attacks, Enabling then to implement protective defence mitigate risk before they Materializing.

Risk Mitigations :- Understanding Cyber Threats helps Organisation Identify and prioritize Cyber Security risk, allowing them to allocate resource Effecientely to address most Significant threats and Vulneabilityes.

Affective Incident Response :- cyber threats Organizations can develop robust incident response plans and procedure Enabling Effecively to Security incident minimizing damage & downtime.

- DISADVANTAGES :- Disadvantages in understanding Cyber threats is the rapid Evolution of technology and Used by Cybercriminals. The landscape is contantly changing, with new Vulnerabilitces.

Aditionally, the complexity of cyber threats can be dauting. Many attacks involve Sophisticated techniques that may requires Specialized Knowledge to Comprehend fully. these threats Can be participating particulating difficult.

APPLICATIONS:-

Understanding Cyber Threats finds application in Various domines cyber Security. Analist to monitor detect and respond to cyber threats in real time. understand the techniques and produces of threats actors helps Security team develop Effective defense Stragies.

Risk Management :-

Organisation leverage knowledge of cyber threats to acess and proize risk to Their System network and data This information informs decision. Making process related to allocated resources for cyber Security Major messurements. Implementing risk mitigations.

Incident Response:- during Security incident understanding cyber threats Enable and Effective respons Efforts incident response teams using intelligence identifying incident, Contains the incidents, The nature of the attack, Eradicate the threats.

Threat Encyclopedia :- A comprehensive database of common Cyber Threats Such as malware, phishing, ransomware, DDos attacks, Etc, Each threat Entry includes:

- Descriptions: Explanating of the Threats; how it Operates and its impacts.
- Examples: Real-world of the Threats, how it operates, and its potential action.

CONCLUSION:-

Understanding Cyber threats is Essential in today interconnected world to protect against malcious activites and mitigate potential risk.

By Comphensively Understanding the techniques, and procedure Employed by threats activityes by staying informed, implemented robust Security measures and fostering a Culture of Cyber-Security, individuals and Organizations can miligate the risks posed by Cyber threats

Cyber Security is an ongoing process that require a multifacted approach. it involves implementing Strong Security measures, staying updated on Emerging threats, Educating users, and fastering a culture of Security awarness. By adopting these strategies, individuals and Organizations can Enhance their resilence against Cyber attacks and better protect their Sensitives information and System. Understanding cyber threats is a critical Endeavor in today's digital age. It's not merely about recongnizing the Existence of threats but Comprehending their nature, motivation, and potential impact.

Here's a Summary of key Conclusion.

- FUTURE SCOPE :-

The future Scope of Understanding Cyber Threats is Expansive and Evolving. it involves advancements in technology, Such as artificial intelligence and gauntum Computing, which both pose new opportunities and Challenges for Cybersecurity.

Additionally as Society becomes increasingly interconnected through the internet of Think (IOT) and other Emerging technology, the attack Surface for cyber threats Expands.

Understanding These future trends requires ongoing research, collaborates between industry and academia, and a proactive approach to staying ahead of Evolving Cyber threats.

Cybersecurity is an Ongoing process that requires a mutifacted approach. it involves implementing strong Security measures, Staying updates on Emerging threats, Educating Users, and fostering a culture of Security awarness. By recognizing The diverse nature of threats, Understanding their motivations, and implementing Effective defense Strategies, individuals and Organizations can better protect themselves in the digital landscape.