PROJECT REPORT

Understanding Cyber Threats: Exploring The Nessus And Beyond Scanning Tools

TEAM ID : LTVIP2024TMID05719

COLLEGE NAME : GIET ENGINEERING COLLEGE

SUBMITTED BY

A.HEMA LAXMI	**20T91A0502**
M.G.SIVA	**20S01A0503**
CH.SAI TEJA	**20T91A0514**
G.VINAY ROHITH	**20T91A0524**
M.HARINI	**20T91A0559**

ABSTRACT

The escalating landscape of cyber threats necessitates a comprehensive understanding of these adversaries and the tools to combat them. This work delves into the world of cyber threats, unpacking their mechanisms and how they capitalize on vulnerabilities. It then focuses on Nessus, a well-regarded vulnerability scanner, emphasizing its role in detecting weaknesses within systems and networks. The discussion extends beyond Nessus, acknowledging the existence of a diverse range of vulnerability scanning tools, each offering unique advantages. Finally, it explores the potential benefits of employing a combination of these tools to establish a more fortified security posture. The digital age thrives on interconnectedness, but this exposes us to a relentless barrage of cyber threats. This project explores the ever-shifting landscape of cyberattacks and how vulnerability scanning tools can bolster our defenses.

INTRODUCTION

Understanding Cyber Threats

In today's interconnected world, cybersecurity is paramount. Organizations and individuals alike face an ever-evolving landscape of cyber threats, ranging from simple malware to sophisticated attacks on critical infrastructure. To safeguard against these threats, security professionals rely on powerful tools and techniques.

The Role of Vulnerability Scanners

Vulnerability scanners play a crucial role in identifying and assessing potential security weaknesses within systems, networks, and applications. These tools help security teams proactively discover vulnerabilities before they can be exploited by malicious actors. In this context, we'll explore two notable vulnerability scanning tools: Nessus and Beyond Scanning.

Nessus Vulnerability Scanner

Overview

Nessus is a widely used vulnerability scanner developed by Tenable. It provides comprehensive security assessments by scanning networks, servers, and applications for known vulnerabilities.

Nessus employs a vast database of vulnerability checks, which it compares against the target environment.

The scanner identifies weaknesses such as outdated software, misconfigurations, and insecure protocols.

Nessus offers both agent-based and agentless scanning options, making it versatile for different scenarios.

Key Features

Scalability: Nessus can scan large networks efficiently, making it suitable for enterprises.

Customizable Policies: Users can create custom scan policies based on their specific requirements.

Reporting: Nessus generates detailed reports, highlighting vulnerabilities and suggesting remediation steps.

Integration: It integrates with other security tools and platforms.

Beyond Scanning

Overview

Beyond Scanning represents a paradigm shift in vulnerability assessment. It extends beyond traditional scanning by integrating security testing into the software development lifecycle.

Rather than treating security as an afterthought, Beyond Scanning emphasizes proactive security measures during development.

It leverages existing testing frameworks and tools to create security testing templates and bespoke tests.

My Basic Network Scan

Report generated by Nessus™ Sat, 20 Apr 2024 10:43:29 India Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.103..... 4

Vulnerabilities by Host

192.168.0.103

Vulnerabilities Total: 43

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
MEDIUM	6.5	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	57582	SSL Self-Signed Certificate
MEDIUM	5.3	-	57608	SMB Signing not required
MEDIUM	5.3	-	45411	SSL Certificate with Wrong Hostname
INFO	N/A	-	46180	Additional DNS Hostnames
INFO	N/A	-	12634	Authenticated Check : OS Name and Installed Package Enumeration
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	46215	Inconsistent Hostname and IP Address
INFO	N/A	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	100871	Microsoft Windows SMB Versions Supported (remote check)

INFO	N/A	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	-	10719	MySQL Server Detection
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	10147	Nessus Server Detection
INFO	N/A	-	64582	Netstat Connection Information
INFO	N/A	-	14272	Netstat Portscanner (SSH)
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	97993	OS Identification and Installed Software Enumeration over SSH v2 (Using New SSH Library)
INFO	N/A	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	35297	SSL Service Requests Client Certificate
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	91263	SSL/TLS Service Requires Client Certificate
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	11154	Unknown Service Detection: Banner Retrieval

INFO	N/A	-	135860	WMI Not Available
INFO	N/A	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

youtube

Report generated by Nessus™

Sat, 20 Apr 2024 11:26:47 India Standard Time

Vulnerabilities by Host

- youtube.com 4

Vulnerabilities by Host

youtube.com

0	1	2	0	31
CRITICAL	HIGH	MEDIUM	LOW	INFO

Vulnerabilities Total: 34

SEVERITY	CVSS V3.0	VPR SCORE	PLUGIN	NAME
HIGH	7.5	6.1	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	54615	Device Type
INFO	N/A	-	10107	HTTP Server Type and Version
INFO	N/A	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	-	11219	Nessus SYN scanner
INFO	N/A	-	19506	Nessus Scan Information
INFO	N/A	-	11936	OS Identification
INFO	N/A	-	50845	OpenSSL Detection
INFO	N/A	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	83298	SSL Certificate Chain Contains Certificates Expiring Soon
INFO	N/A	-	42981	SSL Certificate Expiry - Future Expiry
INFO	N/A	-	10863	SSL Certificate Information
INFO	N/A	-	95631	SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
INFO	N/A	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	21643	SSL Cipher Suites Supported

INFO	N/A	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	94761	SSL Root Certification Authority Certificate Information
INFO	N/A	-	156899	SSL/TLS Recommended Cipher Suites
INFO	N/A	-	22964	Service Detection
INFO	N/A	-	42822	Strict Transport Security (STS) Detection
INFO	N/A	-	25220	TCP/IP Timestamps Supported
INFO	N/A	-	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	-	87242	TLS NPN Supported Protocol Enumeration
INFO	N/A	-	62564	TLS Next Protocols Supported
INFO	N/A	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	-	10287	Traceroute Information
INFO	N/A	-	100669	Web Application Cookies Are Expired
INFO	N/A	-	10386	Web Server No 404 Error Code Check

* indicates the v3.0 score was not available; the v2.0 score is shown

CONCLUSION

In the realm of cybersecurity, vulnerability scanners play a pivotal role in safeguarding digital environments. Nessus, a widely used vulnerability scanner developed by Tenable, meticulously scans networks, servers, and applications for known vulnerabilities. Its scalability, customizable policies, and detailed reporting make it indispensable for proactive security. Beyond Scanning, on the other hand, represents a paradigm shift. It integrates security testing into the software development lifecycle, emphasizing automation, DevSecOps principles, continuous testing, and “security as code.” By understanding these tools, organizations can fortify their defenses against cyber threats and build a safer digital world.

FUTURE SCOPE

Machine Learning Integration: Incorporating machine learning techniques into vulnerability scanning tools like Nessus can enhance accuracy and adaptability. ML models can learn from historical data to identify emerging vulnerabilities.

Automated Remediation: Going beyond detection, vulnerability scanners could automatically remediate identified vulnerabilities. Scripts or playbooks could apply patches, reconfigure settings, or isolate affected systems.

Cloud-Native Security: Adapting scanning tools for cloud-native environments is crucial. Addressing dynamic scaling, serverless architectures, and container security ensures comprehensive protection.

Threat Intelligence Integration: Real-time threat intelligence feeds can improve vulnerability detection. Collaboration with threat intelligence platforms enhances proactive security.

Behavioral Analysis: Moving beyond static scanning, behavioral analysis can detect zero-day vulnerabilities and insider threats. Analyzing system behavior and network traffic provides valuable insights.

IoT and OT Security: Extending vulnerability scanners to cover IoT and OT devices is essential. Customized vulnerability checks for these areas can strengthen security.

User-Friendly Interfaces: Improving usability and accessibility encourages broader adoption. Intuitive dashboards and clear reports enhance the user experience.

Collaboration with DevOps: Integrating security seamlessly into the CI/CD process (DevSecOps) ensures robust protection without hindering development speed.

Quantitative Risk Assessment: Assessing risk quantitatively based on factors like exploitability and impact provides a more nuanced approach to vulnerability prioritization.

Community Contributions: Open-source vulnerability scanners benefit from community collaboration. Encouraging code reviews and feature enhancements fosters innovation