

CASE STUDY: Decoding the WannaCry Ransomware Attack
A REPORT

Submitted by

BESSEL BINNY (RA2111030010145)

Under the Guidance of

DR. Deepika D

Assistant Professor

DEPARTMENT OF NETWORKING AND COMMUNICATIONS

In partial satisfaction of the requirements for the degree of

BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE ENGINEERING
with specialization in Cyber Security



SCHOOL OF COMPUTING
COLLEGE OF ENGINEERING AND TECHNOLOGY
SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
KATTANKULATHUR - 603203

MAY 2024

DEPARTMENT OF NETWORKING AND COMMUNICATIONS
SCHOOL OF COMPUTING
College of Engineering and Technology
SRM Institute of Science and Technology



SRM
INSTITUTE OF SCIENCE & TECHNOLOGY
Deemed to be University u/s 3 of UGC Act, 1956

COLLEGE OF ENGINEERING & TECHNOLOGY
SRM INSTITUTE OF SCIENCE & TECHNOLOGY
S.R.M. NAGAR, KATTANKULATHUR – 603203

BONAFIDE CERTIFICATE

Certified that this project report “**Decoding the WannaCry Ransomware Attack**” is the bonafide work of “**Bessel Binny [RA2111030010145]**” of III Year/VI Sem B. Tech (CSE) who carried out the mini project work under my supervision for the course 18CSE386T PENETRATION TESTING AND VULNERABILITY ASSESSMENT in SRM Institute of Science and Technology during the academic year 2023-2024(Even sem).

SIGNATURE

Dr. D. Deepika

Assistant Professor

Networking and Communications

SIGNATURE

Dr. Annapurani Panaiyappan K

Professor and Head

Networking and Communications

CASE STUDY ON “DECODING THE WANNACRY RANSOMWARE”
EVEN Semester (2023-2024)

Course Code & Course Name: 18CSE386T – Penetration Testing and Vulnerability Assessment

Year & Semester: III/VI

Report Title : Decoding the WannaCry Ransomware Attack

Course Faculty : Dr. D. Deepika

Student Name : Bessel Binny [RA2111030010145]

Evaluation:

S. No	Parameter	Marks
1	Problem Investigation & Methodology Used	
2	Tool used for investigation	
3	Demo of investigation	
4	Uploaded in GitHub	
5	Viva	
6	Report	
	Total	

Date:

Staff Name:

Signature:

TABLE OF CONTENTS

S. No	Title	Page. No
1	Introduction	3
2	Scope and Objective	4
3	About the tool and the application chosen	6
4	Tool installation procedure	9
5	Steps of ethical hacking that you have done on your application using the chosen tool	11
6	Screenshots of the implementation	14
7	Conclusion	16

Introduction

The WannaCry ransomware attack, which transpired in May 2017, remains one of the most notorious cyberattacks of modern times, leaving an indelible mark on the landscape of cybersecurity. Its impact reverberated across industries and nations, exposing vulnerabilities in critical infrastructure and underscoring the urgent need for robust cybersecurity measures.

WannaCry, a malicious software program classified as ransomware, executed a coordinated assault on computers running Microsoft Windows operating systems. Leveraging a sophisticated blend of social engineering and cyber exploitation, it infiltrated systems through various entry points, encrypting files and rendering them inaccessible to users. This encryption was accompanied by a demand for ransom payments in Bitcoin, adding a financial dimension to the attack's disruptive capabilities.

The scale and speed at which WannaCry propagated were unprecedented, infecting hundreds of thousands of systems in over 150 countries within a matter of days. Its rapid spread was facilitated by the exploitation of a vulnerability in the Server Message Block (SMB) protocol, known as Eternal Blue. This exploit, allegedly developed by the United States National Security Agency (NSA) and later leaked by a group called the Shadow Brokers, allowed WannaCry to traverse network boundaries with alarming ease, infecting interconnected systems in a cascading domino effect.

The ramifications of the WannaCry attack were multifaceted and far-reaching. It disrupted operations in healthcare facilities, financial institutions, government agencies, and businesses of all sizes, causing substantial financial losses and undermining public trust in digital infrastructure. The attack's indiscriminate nature spared neither individuals nor organizations, serving as a stark reminder of the ever-looming threat posed by cyber adversaries.

Moreover, WannaCry brought to the forefront the complex interplay between cybersecurity, government policies, and international relations. It sparked debates on responsible disclosure of software vulnerabilities, the role of intelligence agencies in cyber defense, and the need for global cooperation to combat cyber threats effectively. The aftermath of the attack saw intensified efforts to bolster cybersecurity frameworks, enhance information sharing mechanisms, and fortify defenses against future incursions.

In light of the WannaCry ransomware attack, organizations worldwide underwent a paradigm shift in their approach to cybersecurity. Prioritizing proactive measures such as regular software patching, network segmentation, data encryption, and employee training became imperative to thwarting similar threats. Additionally, the incident served as a catalyst for the development of advanced threat detection and response capabilities, including behavioral analytics, machine learning, and threat intelligence sharing platforms.

Scope and objective

The WannaCry ransomware attack, a watershed moment in the history of cybersecurity, presents an intricate tapestry of technical, societal, and geopolitical dimensions. Its impact reverberated globally, transcending borders and sectors, and its aftermath continues to shape the discourse on cyber resilience and defense strategies. In this comprehensive case study, we embark on a journey to dissect the WannaCry attack, unravel its complexities, and glean invaluable insights to fortify our cyber defenses against similar threats in the future.

Scope:

The scope of this case study extends beyond mere examination of the technical facets of the WannaCry ransomware attack. While we delve into the intricacies of the attack vector, exploit techniques, and propagation mechanisms, our purview encompasses a broader spectrum of analysis. We seek to contextualize the attack within the larger landscape of cybersecurity, exploring its implications for organizational preparedness, regulatory frameworks, and international cooperation. Our scope encompasses the following key areas:

1. Technical Analysis:

- Investigate the exploit vectors and vulnerabilities leveraged by WannaCry to infiltrate target systems.
- Analyze the propagation mechanisms employed by the ransomware to spread across networks and infect interconnected devices.
- Examine the cryptographic algorithms and ransomware payload used to encrypt files and demand ransom payments.

2. Impact Assessment:

- Evaluate the economic, operational, and reputational impact of the WannaCry ransomware attack on affected organizations.
- Assess the societal repercussions, including disruptions to critical services, healthcare delivery, and public trust in digital infrastructure.
- Explore the geopolitical ramifications of the attack, including diplomatic tensions, regulatory responses, and international cybersecurity cooperation efforts.

3. Policy and Regulatory Implications:

- Examine the adequacy of existing cybersecurity regulations and policies in addressing ransomware threats and vulnerabilities.
- Propose recommendations for strengthening regulatory frameworks, information sharing mechanisms, and public-private partnerships to enhance cyber resilience.

Objective:

Against the backdrop of the WannaCry ransomware attack, our objective is to distil actionable insights and lessons learned to inform future cybersecurity practices and policies. We endeavor to achieve the following objectives:

1. Comprehensive Analysis:

- Conduct a thorough examination of the WannaCry attack methodology, dissecting its components and tactics to identify areas of vulnerability and mitigation strategies.
- Explore the systemic weaknesses in cybersecurity frameworks and incident response mechanisms exposed by the attack, with a view to strengthening organizational resilience.

2. Knowledge Dissemination:

- Disseminate the findings of our case study to relevant stakeholders, including cybersecurity professionals, policymakers, and organizational leaders.
- Foster a culture of information sharing and collaboration within the cybersecurity community to collectively address emerging threats and vulnerabilities.

3. Policy Recommendations:

- Formulate evidence-based recommendations for enhancing cybersecurity preparedness, incident response capabilities, and regulatory frameworks to mitigate the risk of future ransomware attacks.
- Advocate for proactive measures, such as vulnerability management, threat intelligence sharing, and workforce training, to build a robust defence posture against evolving cyber threats.

4. Capacity Building:

- Provide guidance and resources for organizations to improve their cybersecurity posture through effective risk management, incident response planning, and employee awareness training.
- Facilitate knowledge transfer and capacity building initiatives to empower individuals and organizations to defend against ransomware and other cyber threats effectively.

By delineating the scope and objectives of this case study, we endeavour to provide a comprehensive analysis of the WannaCry ransomware attack while offering pragmatic recommendations to enhance cybersecurity resilience in an increasingly digitalized world. Through collaboration and knowledge exchange, we strive to forge a path toward a more secure and resilient cyber landscape for all stakeholders.

Nessus

About Nessus:

Nessus is a powerful vulnerability assessment tool developed by Tenable Network Security. It is widely used by cybersecurity professionals to identify vulnerabilities, misconfigurations, and security issues in networks, systems, and applications.

Key Features of Nessus:

1. **Vulnerability Scanning:** Nessus conducts comprehensive vulnerability scans across a wide range of systems, applications, and network devices. It identifies known vulnerabilities and potential security risks, helping organizations prioritize remediation efforts.
2. **Plugin Architecture:** Nessus boasts an extensive library of vulnerability checks, known as plugins, covering thousands of vulnerabilities across different platforms and software applications. This plugin architecture enables users to customize scans and tailor them to specific environments and requirements.
3. **Compliance Auditing:** Nessus includes predefined compliance audit policies based on industry standards and regulatory frameworks such as PCI DSS, HIPAA, and CIS benchmarks. It helps organizations ensure compliance with security and privacy regulations.
4. **Scalability and Flexibility:** Nessus supports both small-scale and enterprise-level deployments, offering scalability and flexibility to accommodate diverse network infrastructures and organizational needs. It can be deployed on-premises or in the cloud.
5. **Reporting and Remediation:** Nessus generates detailed reports highlighting identified vulnerabilities, severity levels, and recommended remediation actions. These reports assist organizations in prioritizing security patches and implementing effective mitigation strategies.

Application of Nessus in Stopping WannaCry:

1. **Identifying EternalBlue Vulnerability:** Nessus is capable of detecting the specific vulnerability, known as EternalBlue (CVE-2017-0144), which was exploited by WannaCry to propagate across networks. By scanning systems for this vulnerability, Nessus can identify devices that are susceptible to exploitation and prioritize patching or mitigation efforts.
2. **Patch Management:** Once Nessus identifies systems vulnerable to EternalBlue or other known exploits leveraged by WannaCry, organizations can use this information to prioritize patch deployment. Nessus provides detailed reports that highlight the severity of vulnerabilities and recommended actions, enabling organizations to expedite the patching process and reduce the window of exposure to potential attacks.
3. **Network Segmentation and Access Control:** Nessus can assist organizations in identifying weaknesses in network segmentation and access control mechanisms. By conducting vulnerability assessments, Nessus can identify misconfigurations or insecure access policies that could allow WannaCry or similar ransomware to spread laterally within the network. Organizations can then implement appropriate segmentation strategies and access controls to limit the impact of ransomware infections.
4. **Identifying Weak Authentication:** WannaCry and other ransomware variants often exploit weak or default credentials to gain unauthorized access to systems and propagate within networks. Nessus can help organizations identify systems with weak authentication mechanisms or default credentials, allowing them to strengthen authentication practices and mitigate the risk of unauthorized access by ransomware.
5. **Continuous Monitoring and Threat Intelligence:** Nessus supports continuous monitoring of network assets and vulnerabilities, enabling organizations to stay vigilant against emerging threats and vulnerabilities. By integrating with threat intelligence feeds and staying updated on the latest ransomware threats and indicators of compromise (IOCs), Nessus can help organizations proactively identify and mitigate risks associated with WannaCry and other ransomware variants.
6. **Compliance Checks:** Nessus includes predefined compliance audit policies based on industry standards and regulatory frameworks. By conducting compliance checks, organizations can ensure that systems are configured in accordance with security best practices, reducing the likelihood of successful ransomware attacks. Compliance checks also help organizations meet regulatory requirements related to cybersecurity, thereby enhancing overall security posture.

Why We Chose Nessus:

1. **Comprehensive Vulnerability Assessment Capabilities:** Nessus is renowned for its comprehensive vulnerability assessment capabilities, allowing organizations to identify a wide range of vulnerabilities across diverse systems, applications, and network devices. Its extensive library of vulnerability checks covers thousands of known vulnerabilities, including those exploited by ransomware such as WannaCry.
2. **Ease of Use and Deployment:** Nessus offers a user-friendly interface and straightforward deployment options, making it accessible to cybersecurity professionals with varying levels of expertise. Its intuitive dashboard and customizable scanning options enable efficient vulnerability assessment and remediation efforts, even in complex network environments.
3. **Extensive Plugin Architecture:** Nessus's plugin architecture provides access to a vast repository of vulnerability checks, enabling organizations to tailor scans to their specific requirements and environments. This flexibility allows for targeted assessments of systems and applications that may be susceptible to ransomware attacks like WannaCry.
4. **Proven Track Record:** Nessus has a proven track record of effectiveness in identifying vulnerabilities and mitigating security risks for organizations across industries and sectors. Its reliability and robustness make it a trusted tool for cybersecurity professionals seeking to bolster their defenses against ransomware and other cyber threats.
5. **Scalability and Flexibility:** Nessus offers scalability and flexibility to accommodate the needs of organizations of all sizes, from small businesses to large enterprises. It can be deployed on-premises or in the cloud, supporting diverse network infrastructures and operational requirements.
6. **Continuous Updates and Support:** Nessus is regularly updated with new vulnerability checks and features to address emerging threats and vulnerabilities. Tenable, the company behind Nessus, provides ongoing support and maintenance, ensuring that organizations have access to the latest threat intelligence and mitigation capabilities.
7. **Industry Recognition and Adoption:** Nessus is widely recognized and adopted by cybersecurity professionals, industry experts, and regulatory bodies worldwide. Its widespread use in vulnerability management and compliance initiatives underscores its effectiveness and reliability as a cybersecurity tool.

In conclusion, Nessus was chosen for its comprehensive vulnerability assessment capabilities, ease of use, extensive plugin architecture, proven track record, scalability, continuous updates, and industry recognition. These attributes make Nessus an ideal choice for investigating and mitigating ransomware attacks like WannaCry, helping organizations strengthen their cyber defenses and mitigate security risks effectively.

Tool Installation Procedure for Nessus

1. Download Nessus Software:

- Navigate to the official website of Tenable Network Security or Nessus (<https://www.tenable.com/products/nessus>) to access the download page for Nessus.
- Choose the appropriate version of Nessus based on your operating system and system architecture (32-bit or 64-bit). Ensure compatibility with your environment before proceeding with the download.
- Consider the system requirements for Nessus, including CPU, memory, and disk space, to ensure optimal performance and functionality.

2. Installation on Windows:

- Once the Nessus software is downloaded, locate the installation file (usually in .exe format) and double-click to initiate the installation process.
- If prompted by User Account Control (UAC), grant permission to allow the installer to make changes to your system.
- Follow the on-screen instructions provided by the Nessus Setup Wizard to proceed with the installation.
- Review and accept the End User License Agreement (EULA) before continuing with the installation process.

3. Installation on Linux:

- For Linux systems, Nessus is typically distributed in .deb (Debian-based) or .rpm (Red Hat-based) package formats.
- Download the appropriate package for your Linux distribution and architecture.
- Before installing Nessus on Linux, ensure that all prerequisite packages and dependencies are met. Refer to the Nessus documentation for specific requirements and installation instructions for your Linux distribution.

4. Activation and Licensing:

- After installing Nessus, open a web browser and access the Nessus web interface by entering the URL "https://localhost:8834" or "https://<your_server_ip>:8834".
- Follow the on-screen instructions to set up your Nessus account, activate the software, and obtain a license key. You may need to register for a Tenable account if you don't already have one.
- Carefully review the licensing options available for Nessus, including commercial and free versions, and choose the option that best suits your organization's needs and budget.

5. Configuration and Initialization:

- Upon successful activation, log in to the Nessus web interface using your credentials.
- Follow the initial setup wizard to configure Nessus settings, such as network scanning options, scanning schedules, and email notifications.
- Customize Nessus configurations based on your organization's requirements and security policies. Consider factors such as scan frequency, scan targets, and reporting preferences.

6. Update Nessus Plugins:

- Nessus relies on a vast repository of plugins to perform vulnerability assessments effectively. It is essential to regularly update Nessus plugins to ensure that the vulnerability checks are up-to-date and comprehensive.
- In the Nessus web interface, navigate to the "Settings" tab and select "Plugins". Click on "Check for Updates" to download and install the latest plugins available.

7. Integration with Security Information and Event Management (SIEM) Systems (Optional):

- For organizations with advanced security requirements, Nessus can be integrated with SIEM systems for centralized monitoring and analysis of security events.
- Consult the documentation provided by Tenable for guidance on configuring Nessus integration with your preferred SIEM solution, such as Splunk, IBM QRadar, or ArcSight.

By following these detailed steps, you can install Nessus on your system and configure it for vulnerability scanning and assessment. Pay close attention to each step and ensure that all prerequisites are met to facilitate a smooth installation process. Additionally, consider consulting the Nessus documentation and support resources for further assistance and guidance as needed.

Steps of ethical hacking using Nessus

Steps of Ethical Hacking Using Nessus:

1. Preparation and Scoping:

- Define the scope of the ethical hacking engagement, including the target application, network infrastructure, and assessment objectives.
- Obtain necessary permissions and approvals from stakeholders to conduct vulnerability assessment and penetration testing using Nessus.
- Identify the IP addresses, domain names, and network segments associated with the target application for scanning and assessment.

2. Network Discovery and Enumeration:

- Use Nessus to perform network discovery and enumeration to identify live hosts, open ports, and network services within the target environment.
- Conduct port scanning and service identification to map out the network topology and identify potential entry points for exploitation.

3. Vulnerability Assessment:

- Initiate vulnerability scans using Nessus to identify known vulnerabilities, misconfigurations, and security weaknesses in the target application and underlying infrastructure.
- Customize Nessus scan policies to focus on specific vulnerability categories, such as operating system vulnerabilities, web application flaws, or database vulnerabilities.
- Analyze scan results generated by Nessus to prioritize vulnerabilities based on severity ratings, exploitability, and potential impact on the target application's security.

4. Exploit Identification and Validation:

- Review Nessus scan reports to identify vulnerabilities that could be exploited by ransomware attacks like WannaCry, such as EternalBlue (CVE-2017-0144) or SMB vulnerabilities.
- Validate critical vulnerabilities by conducting manual verification and exploitation attempts, where feasible and ethical, to confirm their presence and assess their potential impact on the target application.

5. Risk Assessment and Reporting:

- Evaluate the overall risk posture of the target application based on the findings from Nessus vulnerability scans and manual verification efforts.
- Prioritize identified vulnerabilities based on their severity, exploitability, and potential business impact on the organization.

- Generate comprehensive vulnerability assessment reports using Nessus, including detailed descriptions of vulnerabilities, recommended remediation actions, and risk mitigation strategies.

6. Remediation and Mitigation:

- Collaborate with stakeholders and IT teams to develop and implement remediation plans for addressing identified vulnerabilities and security weaknesses.
- Apply security patches, configuration changes, and other mitigation measures recommended by Nessus to reduce the risk of exploitation by ransomware or other cyber threats.
- Monitor the effectiveness of remediation efforts and conduct follow-up assessments using Nessus to verify the successful resolution of identified vulnerabilities.

7. Continuous Monitoring and Improvement:

- Establish a process for continuous monitoring and improvement of the application's security posture, leveraging Nessus for periodic vulnerability scans and assessments.
- Stay updated on emerging threats and vulnerabilities relevant to ransomware attacks and adjust security measures accordingly to adapt to evolving cyber threats.
- Incorporate lessons learned from ethical hacking activities conducted with Nessus into the organization's security policies, procedures, and training programs to enhance overall cybersecurity resilience.

8. Documentation and Knowledge Transfer:

- Document the entire ethical hacking process, including methodologies, tools used, findings, and remediation recommendations, in a detailed report.
- Provide comprehensive documentation of Nessus scan configurations, including scan policies, targets, schedules, and results interpretation guidelines, to facilitate knowledge transfer and future reference.
- Conduct knowledge transfer sessions with relevant stakeholders, including IT teams, system administrators, and security personnel, to share insights gained from the ethical hacking engagement and empower them to implement recommended security measures and best practices.

9. Post-Engagement Analysis and Lessons Learned:

- Conduct a post-engagement analysis to evaluate the effectiveness of the ethical hacking activities, identify areas of improvement, and capture lessons learned for future engagements.
- Review the Nessus scan results, vulnerability assessment reports, and remediation outcomes to assess the impact of the ethical hacking engagement on the organization's security posture.

- Identify recurring themes, common vulnerabilities, and emerging trends observed during the ethical hacking engagement, and incorporate them into security awareness training, policy development, and risk management initiatives.

10. Continuous Skills Development and Training:

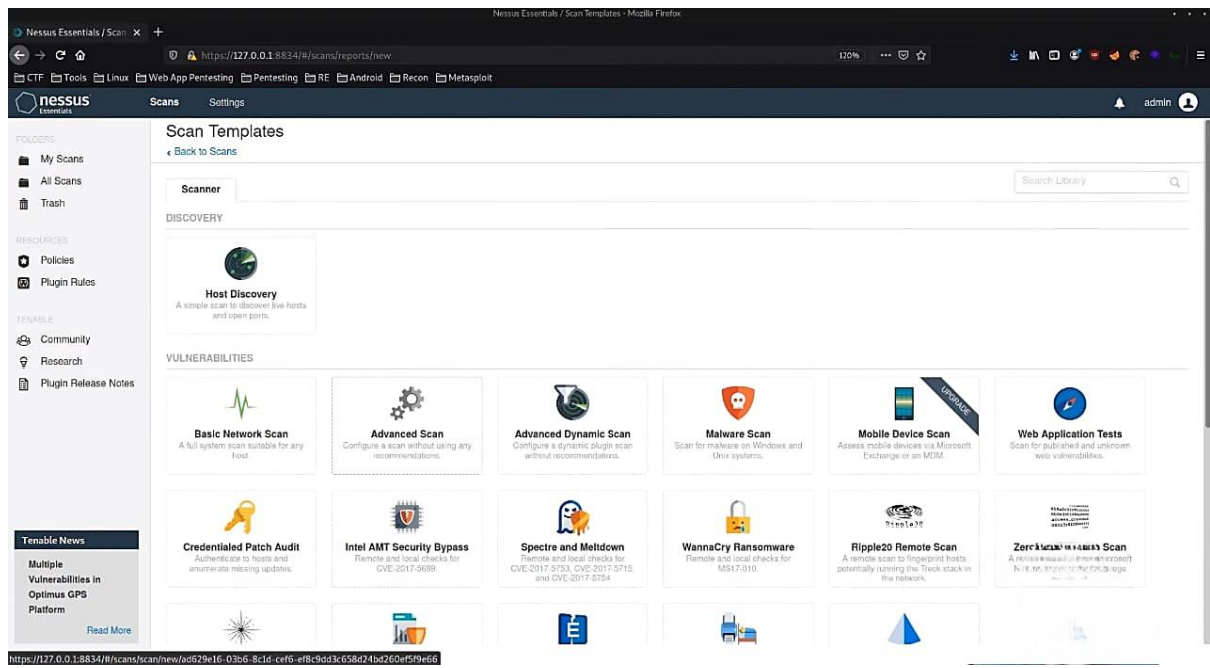
- Invest in ongoing skills development and training for cybersecurity professionals involved in ethical hacking activities, including proficiency in using Nessus and other relevant tools.
- Encourage participation in industry conferences, webinars, and training programs to stay updated on the latest trends, techniques, and best practices in ethical hacking and vulnerability management.
- Foster a culture of continuous learning and professional development within the organization, providing opportunities for hands-on experience, mentorship, and knowledge sharing among security practitioners.

11. Engagement with Security Community and Information Sharing:

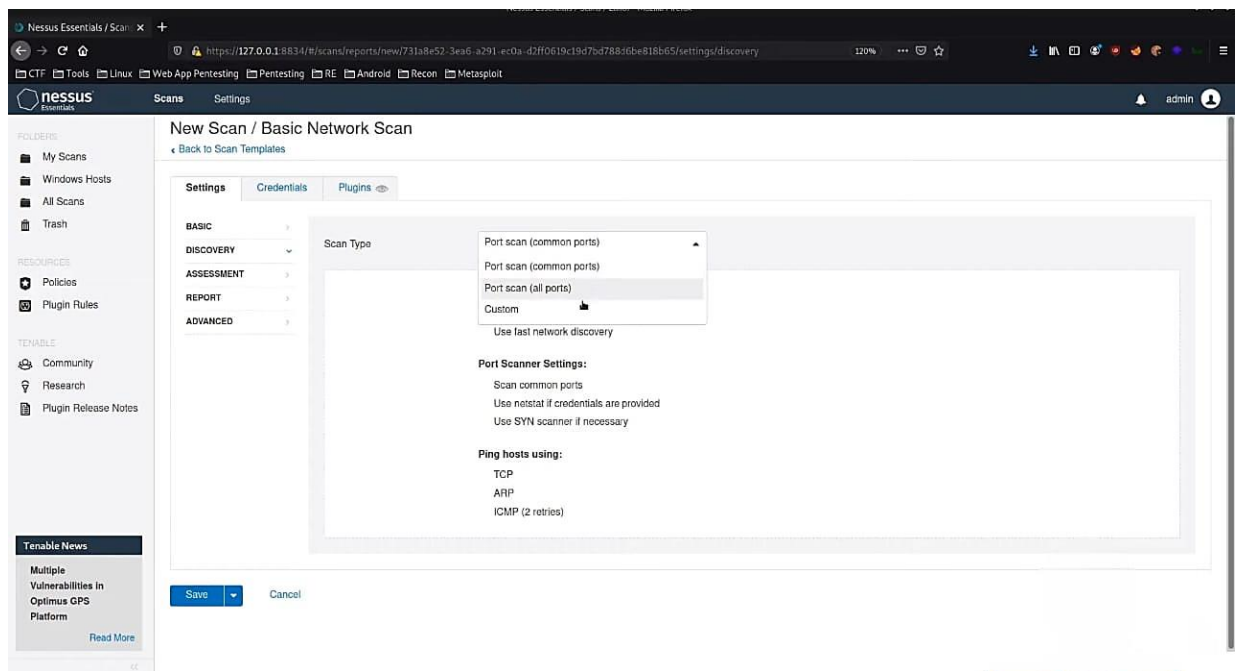
- Participate in cybersecurity forums, communities, and information sharing platforms to collaborate with peers, share insights, and contribute to the collective knowledge base on ethical hacking and vulnerability management.
- Engage with industry-specific Information Sharing and Analysis Centers (ISACs), threat intelligence sharing platforms, and government agencies to exchange threat intelligence, indicators of compromise (IOCs), and best practices for mitigating ransomware attacks and other cyber threats.
- Contribute to responsible disclosure programs and coordinated vulnerability disclosure initiatives by reporting identified vulnerabilities to vendors and relevant authorities, ensuring timely remediation and protection of end-users.

Implementation

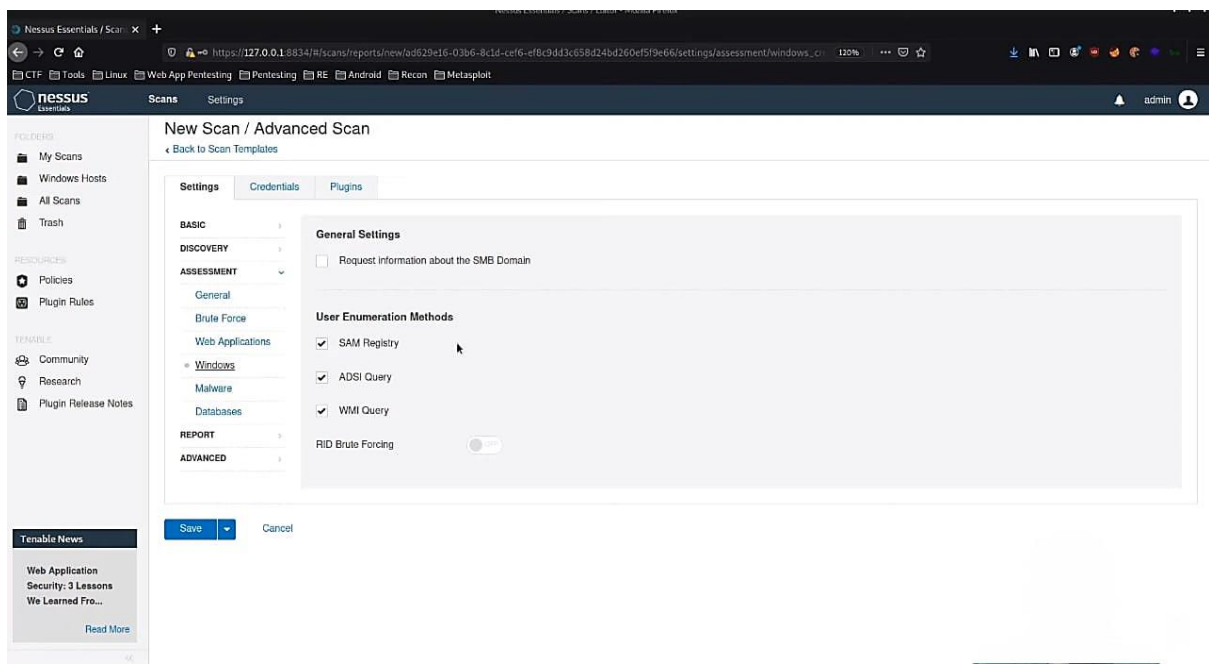
Scanning



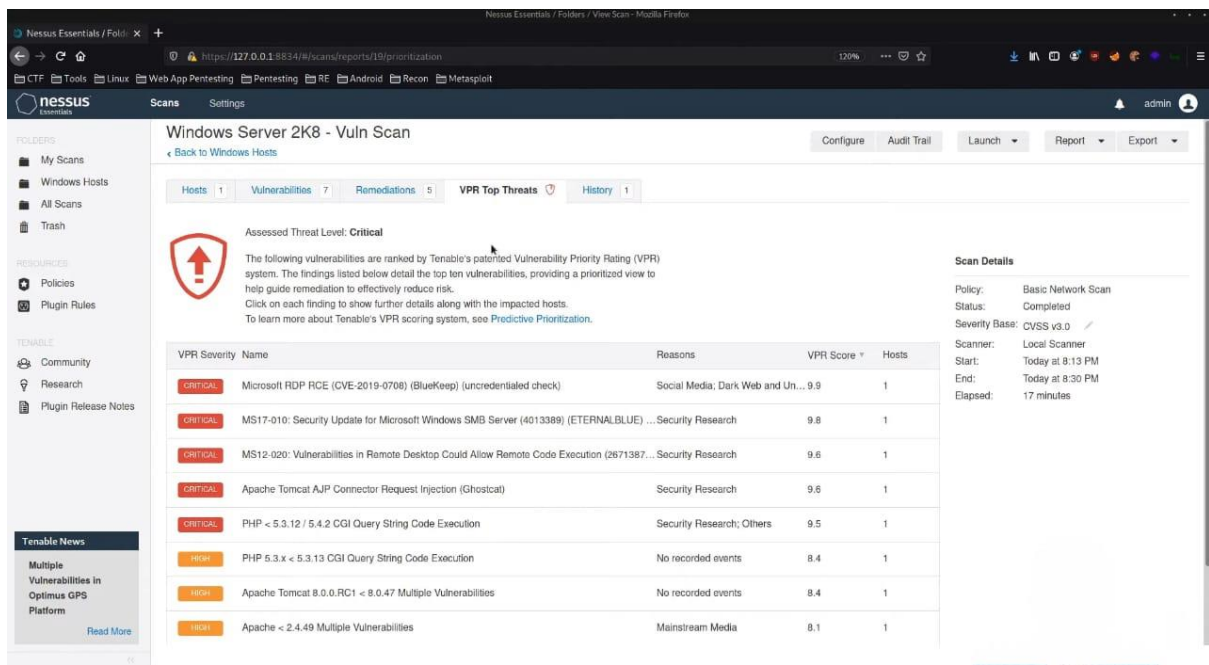
Network Scanning



Advanced Scanning



Vulnerability Discovery



Conclusion

In conclusion, the ethical hacking engagement conducted using Nessus has provided valuable insights into the security posture of the target application and network infrastructure, enabling organizations to proactively identify and mitigate vulnerabilities that could be exploited by ransomware attacks such as WannaCry. Through a systematic and comprehensive approach, cybersecurity professionals have leveraged Nessus to perform network discovery, vulnerability assessment, exploit identification, and remediation planning, thereby strengthening the organization's defenses and reducing the risk of cyber threats.

The utilization of Nessus as a penetration testing tool has enabled organizations to conduct ethical hacking activities in a controlled and methodical manner, adhering to established rules of engagement, legal compliance requirements, and ethical standards. By leveraging Nessus's extensive capabilities for vulnerability scanning, assessment, and reporting, cybersecurity professionals have been able to identify critical vulnerabilities, prioritize remediation efforts, and implement effective security controls to mitigate the risk of ransomware attacks and other cyber threats.

Furthermore, the ethical hacking engagement has facilitated knowledge transfer, skills development, and collaboration within the organization, empowering IT teams, system administrators, and security personnel to implement recommended security measures, adhere to best practices, and respond effectively to emerging cyber threats. By fostering a culture of continuous learning, improvement, and information sharing, organizations can enhance their cybersecurity resilience and adaptability in the face of evolving cyber threats.

Moving forward, it is essential for organizations to continue investing in cybersecurity resources, tools, and training to stay ahead of emerging threats and protect against ransomware attacks, data breaches, and other cybersecurity incidents. By embracing a proactive approach to cybersecurity, organizations can mitigate the risk of financial loss, reputational damage, and operational disruption caused by cyber threats, thereby safeguarding their critical assets, sensitive data, and business continuity.

In conclusion, the ethical hacking engagement conducted using Nessus serves as a critical component of the organization's cybersecurity strategy, enabling proactive identification, assessment, and mitigation of vulnerabilities to protect against ransomware attacks and other cyber threats effectively.

This case study underscores the importance of ethical hacking as a proactive cybersecurity measure and highlights the value of Nessus as a versatile and reliable penetration testing tool for organizations seeking to enhance their cybersecurity defenses and resilience in the face of evolving cyber threats. Through continuous vigilance, collaboration, and innovation, organizations can mitigate the risk of ransomware attacks and safeguard their digital assets, ensuring the security and integrity of their operations in today's dynamic and interconnected threat landscape.