RED TEAM

EXERCISES

Performing simulated attacks on an organization's systems and networks to test their defensive capabilities and identify potent

TEAM:

P. Nithiyasri - 20BCE7035

Sarah Anne George – 20BCE7079

PROJECT REPORT

CONTENT

INTRODUCTION

In today's interconnected and digitized world, organizations face an ever-increasing number of cyber threats that can potentially disrupt operations, compromise sensitive data, and tarnish reputations. As a result, it has become imperative for organizations to continuously evaluate and improve their defensive capabilities to stay ahead of malicious actors. One approach that has gained significant prominence in recent years is the execution of red team exercises.

Red team exercises are simulated attacks conducted by a team of skilled cybersecurity professionals who adopt the mindset and tactics of real-world adversaries. These exercises aim to identify vulnerabilities in an organization's systems, networks, and personnel by subjecting them to realistic attack scenarios. By proactively assessing their security posture through red teaming, organizations can uncover weaknesses, validate existing security controls, and enhance their overall resilience against cyber threats.

The fundamental objective of red team exercises is not only to discover vulnerabilities but also to assess an organization's ability to detect, respond, and recover from sophisticated attacks. By adopting the mindset of an adversary, the red team attempts to exploit weaknesses in the organization's security controls, gaining insights into potential entry points and areas of improvement. This proactive approach allows organizations to remediate vulnerabilities before they can be exploited by actual threat actors.

AIM FOR OUR PROJECT

The aim of this topic is to explore the concept of red team exercises and their significance in enhancing an organization's security defenses. The objective is to provide a comprehensive understanding of red teaming as a proactive approach to identify vulnerabilities, assess defensive capabilities, and improve incident response procedures. This topic aims to highlight the benefits, challenges, and considerations associated with red team exercises, emphasizing their role in fortifying an organization's resilience against cyber threats. Ultimately, the aim is to emphasize the importance of red teaming as a critical component of a comprehensive cybersecurity strategy.

SOFTWARE REQUIREMENTS

- KALI LINUX
- CALDERA
- TARGET – METASPOITABLE

SETUP

This report aims to outline the process of connecting Kali Linux and Metasploitable within a virtual machine, along with the steps involved in conducting a comprehensive security assessment. By simulating real-world attack scenarios, security practitioners can gain insights into potential weak points in their systems, allowing for effective remediation and proactive defense strategies.

The initial phase involves setting up the Kali Linux distribution. Kali Linux, renowned for its rich array of pre-installed security tools, provides an extensive toolkit for penetration testing. We deployed Kali Linux on a virtual machine using virtualization software such as VMware or VirtualBox. This virtual environment ensures isolated and secure testing without affecting the underlying host system.

Metasploitable, a purposely vulnerable virtual machine, is an essential component for conducting penetration tests. It replicates various exploitable vulnerabilities to simulate real-world attack scenarios. We installed and configured Metasploitable alongside Kali Linux within the virtual machine environment to facilitate seamless communication between the two systems.

To enable communication between Kali Linux and Metasploitable, we established network connectivity within the virtual machine. This was achieved by configuring network settings, such as assigning IP addresses, subnet masks, and gateway addresses, ensuring that both systems were on the same network. This connectivity allows for efficient scanning, enumeration, and exploitation of vulnerabilities within the Metasploitable environment using Kali Linux tools.

INFORMATION GATHERING

Information gathering is a critical phase in various cybersecurity and intelligence-gathering activities. This summary covers several aspects of information gathering, including email footprinting, DNS information gathering, WHOIS information gathering, information gathering for social engineering attacks, information gathering for physical security assessments, and emerging trends and technologies in information gathering.

1. DNS Information Gathering: DNS information gathering involves querying DNS servers to obtain information about domain names, IP addresses, mail servers, and other related records. It helps in mapping network infrastructure, identifying potential vulnerabilities, and conducting reconnaissance for targeted attacks.

2. WHOIS Information Gathering: WHOIS information gathering involves querying WHOIS databases to retrieve registration and ownership details of domain names. It helps identify domain owners, contact information, registration dates, and other relevant data, aiding in investigations, cybersecurity research, and threat intelligence.

4. Information Gathering for Social Engineering Attacks: Social engineering attacks exploit human vulnerabilities. Information gathering for social engineering involves gathering personal information, social media profiles, organizational details, and other data to craft convincing and targeted attacks. It aids in building rapport, increasing success rates, and tailoring attacks to exploit specific individuals or organizations.

5. Information Gathering for Physical Security Assessments: Information gathering for physical security assessments involves collecting data about an organization's physical infrastructure, security measures, access points, and personnel. It aids in identifying potential weaknesses, assessing security controls, and planning effective physical security measures.

6. Emerging Trends and Technologies in Information Gathering: As technology advances, new trends and technologies in information gathering have emerged. These include leveraging open-source intelligence (OSINT), employing machine learning and artificial intelligence for automated data analysis, utilizing dark web monitoring tools, and exploring social media intelligence (SOCMINT) for gathering information.

VULNERABILITY IDENTIFICATION

In our project, we have conducted a comprehensive series of scans and meticulously analyzed the results to uncover potential vulnerabilities and entry points within our target organization. The objective was to identify any weaknesses that could potentially impact the security of our target organization, specifically focusing on the vulnerabilities present in the system known as "Metasploitable."

Identifying Each Vulnerability

We have performed a **Nmap scan** on the target machine, Metasploitable. The purpose of this scan was to gather information about open ports and services running on the target system. The Nmap scan revealed multiple open ports, including FTP, SSH, Telnet, SMTP, DNS, HTTP, RPC, SMB, MySQL, PostgreSQL, and VNC. These open ports could potentially indicate the presence of vulnerabilities or misconfigurations that could be exploited by malicious actors.

Assigning A Common Weakness Enumeration (CWE) Code To Each Vulnerability

To further classify and categorize the vulnerabilities, a Common Weakness Enumeration (CWE) code is assigned to each identified vulnerability. The CWE system provides a standardized framework for classifying and describing software weaknesses. Common CWE codes associated with vulnerabilities that could potentially be present based on the services running on the open ports mentioned include:

1) FTP (Port 21): CWE-284 (Improper Access Control)
2) SSH (Port 22): CWE-306 (Missing Authentication for Critical Function)
3) Telnet (Port 23): CWE-321 (Use of Hard-coded Cryptographic Key)
4) SMTP (Port 25): CWE-319 (Cleartext Transmission of Sensitive Information)

5) DNS (Port 53): CWE-284 (Improper Access Control)
6) HTTP (Port 80): CWE-311 (Missing Encryption of Sensitive Data)
7) SMB (Ports 139 and 445): CWE-200 (Information Exposure)
8) MySQL (Port 3306): CWE-89 (SQL Injection)
9) PostgreSQL (Port 5432): CWE-89 (SQL Injection)
10) VNC (Port 5900): CWE-321 (Use of Hard-coded Cryptographic Key)

Corresponding Open Web Application Security Project (OWASP) Category and Description for Each Vulnerability

- **FTP (Port 21):**

  OWASP Category: Insufficient Logging & Monitoring

  While not specifically tied to web applications, inadequate logging and monitoring practices in FTP servers can leave them susceptible to attacks and make it difficult to detect and respond to security incidents effectively.

- **SSH (Port 22):**

  OWASP Category: Broken Authentication

  Weak authentication mechanisms in SSH servers can allow unauthorized access to the system, compromising its security and potentially leading to unauthorized activities.

- **Telnet (Port 23):**

  OWASP Category: Broken Authentication

  Telnet's use of plain text transmission makes it vulnerable to interception and unauthorized access. It is recommended to use secure alternatives like SSH instead.

- **SMTP (Port 25):**

  OWASP Category: Sensitive Data Exposure

  Insecure configurations or outdated versions of SMTP servers can potentially expose sensitive information, such as email content or user credentials, to unauthorized parties.

- **DNS (Port 53):**

  OWASP Category: Insufficient Logging & Monitoring

  Inadequate logging and monitoring practices in DNS servers can leave them vulnerable to attacks like DNS cache poisoning or amplification, impacting the integrity and availability of DNS services.

- **HTTP (Port 80):**

  OWASP Category: Injection

  Vulnerabilities in web servers or web applications hosted on port 80 can allow attackers to inject malicious code or commands, leading to potential security breaches or data manipulation.

- **SMB (Ports 139 and 445):**

  OWASP Category: Sensitive Data Exposure

  Misconfigured or vulnerable SMB servers can expose sensitive information, such as file shares or user credentials, to unauthorized users, potentially leading to unauthorized access or data leakage.

- **MySQL (Port 3306):**

  OWASP Category: Injection

  SQL injection vulnerabilities in MySQL servers can allow attackers to manipulate database queries and potentially gain unauthorized access or perform unauthorized operations on the database.

- **PostgreSQL (Port 5432):**

  OWASP Category: Injection

  Similar to MySQL, SQL injection vulnerabilities in PostgreSQL servers can allow attackers to manipulate database queries and potentially gain unauthorized access or perform unauthorized operations on the database.

- **VNC (Port 5900):**

  OWASP Category: Insufficient Authentication

  Insecure authentication mechanisms in VNC servers can lead to unauthorized access to the remote desktop, compromising the confidentiality and integrity of the system.

Understanding and Defining Vulnerabilities

The Nmap scan of the target system, Metasploitable, revealed several potential vulnerabilities based on the open ports and services detected. These vulnerabilities include insecure configurations or weak credentials in the FTP (Port 21) service, weak SSH configurations or vulnerable server versions on Port 22, insecure transmission and weak authentication in the Telnet (Port 23) service, potential misconfigurations or vulnerabilities in the SMTP (Port 25) and DNS (Port 53) services, web server misconfigurations or vulnerabilities in the HTTP (Port 80) service, potential misconfigurations or vulnerabilities in the SMB (Ports 139 and 445) service, weak credentials or vulnerable versions in the MySQL (Port 3306) and PostgreSQL (Port 5432) services, and insecure VNC configurations or weak authentication on Port 5900. These vulnerabilities may pose risks such as unauthorized access, data manipulation, interception of sensitive information, or potential exploitation of known vulnerabilities.

BUSINESS IMPACT ASSESSMENT

Conduct a thorough Analysis of the Potential Business Impact and Potential Consequences of Each Vulnerability

Based on the output of the Nmap scan and the potential vulnerabilities identified, here is a thorough analysis of the potential business impact of each vulnerability:

- **FTP (Port 21):** Insecure FTP configurations or weak credentials could lead to unauthorized access to sensitive files. This may result in the exposure of confidential data, intellectual property theft, or compromise of customer information, potentially leading to reputational damage, legal liabilities, and financial losses.

- **SSH (Port 22):** Weak SSH configurations or vulnerable server versions can enable unauthorized individuals to gain remote access to critical systems. This could result in unauthorized data manipulation, system disruption, theft of sensitive information, or unauthorized privilege escalation. The potential business impact includes data breaches, service disruption, financial losses, and damage to the organization's reputation.

- **Telnet (Port 23):** Insecure transmission and weak authentication in Telnet can expose login credentials to eavesdropping or unauthorized interception. Attackers could exploit this vulnerability to gain unauthorized access to systems, manipulate data, or perform malicious activities, leading to data breaches, service disruptions, financial losses, and potential legal repercussions.

- **SMTP (Port 25):** Misconfigurations or vulnerabilities in the SMTP server can lead to unauthorized access, email abuse, or interception of sensitive information. This can result in compromised communication, loss of trust with customers or partners, reputational damage, legal issues, and financial losses associated with data breaches or regulatory penalties.

- **DNS (Port 53):** Misconfigured or vulnerable DNS servers can be exploited to redirect network traffic, manipulate DNS records, or launch DNS-based attacks. This can lead to service disruptions, website defacement, unauthorized access to sensitive information, or the diversion of legitimate traffic to malicious sites. The business impact includes reputational damage, loss of customer trust, financial losses, and potential legal implications.

- **HTTP (Port 80):** Web server misconfigurations or vulnerabilities in web applications hosted on Port 80 can lead to various attacks such as injection, cross-site scripting (XSS), or remote code execution. These vulnerabilities can result in data breaches, unauthorized access to sensitive information, defacement of websites, disruption of services, damage to brand reputation, financial losses, and legal consequences.

- **SMB (Ports 139 and 445):** Misconfigured or vulnerable SMB servers can allow unauthorized access to shared files or network resources. Attackers could exploit this vulnerability for unauthorized data access, lateral movement within the network, deployment of ransomware, or theft of sensitive information. The potential business impact includes data breaches, service disruptions, financial losses, reputational damage, and legal liabilities.

- **MySQL (Port 3306):** Weak credentials or vulnerable versions of MySQL can result in unauthorized access, data manipulation, or injection attacks. Attackers could exploit this vulnerability to steal or modify critical data, disrupt database operations, or gain unauthorized privileges. The potential business impact includes data breaches, financial losses, operational disruptions, reputational damage, and regulatory non-compliance.

- **PostgreSQL (Port 5432):** Weak credentials or vulnerable versions of PostgreSQL can lead to unauthorized access, data manipulation, or injection attacks. Attackers could exploit this vulnerability to gain unauthorized control over the database, steal or modify sensitive data, disrupt services, or launch further attacks. The potential business impact includes data breaches, financial losses, operational disruptions, reputational damage, and potential legal and regulatory consequences.

- **VNC (Port 5900):** Insecure VNC configurations or weak authentication can allow unauthorized access to remote desktops. Attackers could exploit this vulnerability to view or manipulate sensitive information, install malware, or gain control over systems. The potential business impact includes unauthorized access to confidential data, loss of sensitive information, operational disruptions, reputational damage, financial losses, and potential legal implications.

Conducting A Business Impact Assessment

A comprehensive assessment of the potential business impacts on an organization that uses Metasploitable involves:

1. **Financial Impact:** Exploitation of vulnerabilities can lead to unauthorized access and data breaches, potentially resulting in financial losses due to legal fees, regulatory fines, customer compensation, and damage to the organization's reputation. Successful attacks can cause system downtime, service disruptions, or loss of critical data, leading to financial losses associated with recovery efforts, productivity loss, and missed business opportunities.

2. **Reputational Impact:** A security breach or unauthorized access to sensitive data can erode customer and stakeholder trust in the organization, potentially resulting in customer attrition, negative publicity, and damage to the brand reputation. Failure to address known vulnerabilities and secure the system can portray the organization as negligent in maintaining proper security measures, affecting its reputation and credibility in the market.

3. **Legal and Regulatory Impact:** Exploitable vulnerabilities may violate industry-specific regulations, data protection laws, or privacy standards, resulting in legal consequences, penalties, or sanctions. Breaches resulting from the exploitation of vulnerabilities can lead to legal actions, customer lawsuits, and potential liability for financial damages.

4. **Operational Impact:** Successful attacks can disrupt business operations, leading to downtime, loss of productivity, and potential financial implications. Unauthorized access to sensitive information or trade secrets can compromise the organization's competitive advantage, research and development efforts, and intellectual property.

5. **Customer Impact:** Unauthorized access to customer data can compromise their privacy and lead to identity theft, fraud, or other malicious activities, resulting in financial and reputational harm to the affected individuals. Customer trust can be significantly impacted if their data is compromised, potentially leading to customer churn, difficulty acquiring new customers, and decreased revenue.

6. **Regulatory Compliance Impact:** Failure to address vulnerabilities and secure the system can result in non-compliance with industry-specific regulations, data protection laws, or privacy standards, exposing the organization to legal and regulatory consequences.

Understanding Potential Consequences of Vulnerabilities

The potential consequences of the vulnerabilities identified in the Metasploitable system are significant and encompass financial losses, reputational damage, operational disruptions, compromised customer data, legal and regulatory consequences, and potential lawsuits. Unauthorized access can lead to data breaches and manipulation, while service disruptions can impact business operations and customer satisfaction. Data manipulation or destruction can compromise decision-making processes, while reputation damage can result in customer attrition and decreased market share. Legal and regulatory violations can lead to fines, penalties, and legal actions. It is crucial for the organization to prioritize the remediation of these vulnerabilities and implement robust security measures to mitigate these potential consequences effectively.

Assessing the Risk to the Business

The assessed risk to the business based on the identified vulnerabilities in the Metasploitable system is significant. With a combination of high likelihood of exploitation for some vulnerabilities, along with potential high-impact consequences such as data breaches, reputational damage, and legal liabilities, immediate attention and mitigation measures are necessary to protect the business from potential financial losses, operational disruptions, and damage to its reputation and customer trust.

VULNERABILITY PATH AND PARAMETER IDENTIFICATION

Vulnerability path and parameter identification is a crucial aspect of vulnerability assessment and management. It involves identifying the specific paths and parameters within an application or system that may be vulnerable to exploitation. This process helps security professionals understand the attack surface and prioritize remediation efforts. This section will cover the methods to identify vulnerability paths and parameters, the types of vulnerabilities involved, common tools and techniques used, best practices, and challenges and limitations associated with this process.

Based on the Nmap scan output, the following vulnerability path and parameter identifications can be made:

FTP (Port 21): The FTP service is open, indicating that it may be susceptible to known FTP vulnerabilities such as weak authentication, improper configuration, or outdated software versions.

SSH (Port 22): The SSH service is open, suggesting that there could be vulnerabilities related to SSH authentication, encryption, or configuration weaknesses.

Telnet (Port 23): The Telnet service is open, which raises concerns about potential vulnerabilities associated with plaintext communication, weak authentication, or remote code execution.

SMTP (Port 25): The SMTP service is open, indicating potential vulnerabilities related to email server configuration, relay abuse, or email spoofing.

HTTP (Port 80): The HTTP service is open, suggesting the possibility of web application vulnerabilities, such as SQL injection, cross-site scripting (XSS), or insecure server configurations.

MySQL (Port 3306): The MySQL service is open, which could imply vulnerabilities related to weak database authentication, SQL injection, or outdated MySQL versions.

PostgreSQL (Port 5432): The PostgreSQL service is open, indicating the potential for vulnerabilities associated with database security, query injection, or misconfigurations.

VNC (Port 5900): The VNC service is open, suggesting vulnerabilities related to weak authentication, lack of encryption, or potential remote desktop protocol vulnerabilities.

Unknown Services (Ports 8180, 8787, 44200, 44259, 49558, 50219): The open ports with unknown services indicate the need for further investigation to identify the associated services and assess potential vulnerabilities.

DETAILED INSTRUCTION FOR VULNERABILITY REPRODUCTION

Reproducing vulnerabilities is a crucial step in the vulnerability management process as it helps validate the existence and impact of a vulnerability, understand its root cause, and verify the effectiveness of proposed fixes. Here is a detailed instruction for vulnerability reproduction, including methods to find the importance of it, components of a well-written vulnerability reproduction instruction, steps for reproducing vulnerabilities, best practices for writing effective vulnerability reproduction instructions, tools and techniques for verifying vulnerability fixes, and challenges and limitations of vulnerability reproduction instructions.

To reproduce the vulnerabilities identified in the output of the Nmap scan, follow these instructions:

1. FTP (Port 21): Attempt to connect to the FTP service using common FTP clients or command-line tools to check for any misconfigurations or weak credentials that may allow unauthorized access.

2. SSH (Port 22): Use an SSH client to connect to the SSH service and check if weak or default credentials are in use. Additionally, verify if the SSH server version is outdated, as this could potentially be exploited.

3. Telnet (Port 23): Connect to the Telnet service using a Telnet client and check for weak or default credentials. Telnet is an insecure protocol, so consider disabling or switching to a more secure alternative.

4. SMTP (Port 25): Interact with the SMTP service using an email client or Telnet to check for any misconfigurations or vulnerabilities that could potentially allow unauthorized access or email relay.

5. DNS (Port 53): Use DNS tools or utilities to perform DNS queries and check for any vulnerabilities like DNS zone transfers, DNS cache poisoning, or misconfigured DNS settings.

6. HTTP (Port 80): Access the web application hosted on port 80 using a web browser and conduct a thorough security assessment. Look for common web vulnerabilities like injection flaws, cross-site scripting (XSS), cross-site request forgery (CSRF), or misconfigurations that could lead to unauthorized access or data exposure.

7. RPC (Port 111): Research and test for known vulnerabilities related to RPC services, such as remote code execution or unauthorized access. Check for proper access controls and ensure that only necessary RPC services are exposed.

8. NetBIOS-SSN (Port 139) and Microsoft-DS (Port 445): Research and test for vulnerabilities associated with these services, such as SMB vulnerabilities or weaknesses that could potentially lead to unauthorized access or information disclosure.

9. Other Services: For the remaining open ports, research and identify potential vulnerabilities associated with each specific service (e.g., MySQL, PostgreSQL, VNC, IRC) and perform relevant testing and analysis based on their respective protocols and functionalities.

COMPREHENSIVE AND DETAILED REPORTING

Comprehensive and detailed reporting plays a critical role in cybersecurity and risk management by providing organizations with valuable insights, actionable information, and a clear understanding of their security posture. This section covers the importance of comprehensive and detailed reporting, key components of such reports, strategies for effective reporting, challenges in implementing comprehensive and detailed reporting, the impact of reporting on decision-making, and best practices for creating comprehensive and detailed reports.

Red team exercises are a crucial component of a comprehensive cybersecurity strategy. By simulating real-world attacks, organizations can proactively identify vulnerabilities, assess defensive capabilities, and improve incident response procedures. In this report, we outlined the process of connecting Kali Linux and Metasploitable within a virtual machine, conducted information gathering, identified vulnerabilities, and assessed their potential business impact.

The setup phase involved deploying Kali Linux and Metasploitable within a virtual machine environment to facilitate secure testing. Network connectivity was established between the two systems, enabling efficient scanning and exploitation of vulnerabilities. Information gathering techniques such as DNS and WHOIS information gathering, social engineering attack reconnaissance, and physical security assessment were discussed, emphasizing the importance of collecting relevant data to understand potential attack vectors.

Vulnerability identification involved conducting a Nmap scan on the target system, Metasploitable, and assigning Common Weakness Enumeration (CWE) codes to each identified vulnerability. The corresponding Open Web Application Security Project (OWASP) category and description were provided for each vulnerability, allowing for a deeper understanding of the potential risks associated with each vulnerability.

A business impact assessment was conducted to evaluate the potential consequences of each vulnerability. This assessment considered financial, reputational, legal and regulatory, operational, and customer impacts. By understanding the potential business impacts, organizations can prioritize vulnerability remediation efforts, allocate resources effectively, and mitigate risks that could lead to financial losses, reputational damage, legal consequences, or operational disruptions.

In conclusion, red team exercises and vulnerability assessments are critical for organizations to enhance their security defenses and stay ahead of cyber threats. By identifying vulnerabilities, assessing their potential impact, and implementing necessary security measures, organizations can improve their overall resilience and protect their sensitive data, operations, and reputation from malicious actors. Red teaming should be considered an essential practice in any organization's cybersecurity strategy to ensure continuous improvement and readiness against evolving threats.

CONCLUSION

Red team exercises are a crucial component of a comprehensive cybersecurity strategy. By simulating real-world attacks, organizations can proactively identify vulnerabilities, assess defensive capabilities, and improve incident response procedures. In this report, we outlined the process of connecting Kali Linux and Metasploitable within a virtual machine, conducted information gathering, identified vulnerabilities, and assessed their potential business impact.

The setup phase involved deploying Kali Linux and Metasploitable within a virtual machine environment to facilitate secure testing. Network connectivity was established between the two systems, enabling efficient scanning and exploitation of vulnerabilities. Information gathering techniques such as DNS and WHOIS information gathering, social engineering attack reconnaissance, and physical security assessment were discussed, emphasizing the importance of collecting relevant data to understand potential attack vectors.

Vulnerability identification involved conducting a Nmap scan on the target system, Metasploitable, and assigning Common Weakness Enumeration (CWE) codes to each identified vulnerability. The corresponding Open Web Application Security Project (OWASP) category and description were provided for each vulnerability, allowing for a deeper understanding of the potential risks associated with each vulnerability.

A business impact assessment was conducted to evaluate the potential consequences of each vulnerability. This assessment considered financial, reputational, legal and regulatory, operational, and customer impacts. By understanding the potential business impacts, organizations can prioritize vulnerability remediation efforts, allocate resources effectively, and mitigate risks that could lead to financial losses, reputational damage, legal consequences, or operational disruptions.

In conclusion, red team exercises and vulnerability assessments are critical for organizations to enhance their security defenses and stay ahead of cyber threats. By identifying vulnerabilities, assessing their potential impact, and implementing necessary security measures, organizations can improve their overall resilience and protect their sensitive data, operations, and reputation from malicious actors. Red teaming should be considered an essential practice in any organization's cybersecurity strategy to ensure continuous improvement and readiness against evolving threats.