**Walkthrough: Devel HTB Machine**

This report outlines the penetration testing process for "Devel," a beginner-level Windows machine. The goal was to gain administrative access and retrieve the root flag. The machine's relative simplicity highlights the security risks associated with default program configurations.

**1. Initial Reconnaissance and Service Enumeration**

An Nmap scan on the target IP address, 10.10.10.5, revealed two open ports:

* **Port 21/tcp:** Running Microsoft FTPd, allowing anonymous login.
* **Port 80/tcp:** Hosting a Microsoft IIS httpd 7.5 web server.
* A screenshot of a computer

  AI-generated content may be incorrect.

**2. Gaining a Foothold - Anonymous FTP and Web Shell Upload**

Anonymous FTP login was permitted, allowing access to the web server's directories. This presented an opportunity to upload a malicious file. An aspx format reverse TCP handler was created using msfvenom. This shell.aspx file was then uploaded to the FTP server using the put shell.aspx command

A computer screen shot of a black screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.



A screen shot of a computer

AI-generated content may be incorrect.

**3. Establishing a Session - Metasploit Multi/Handler**

After uploading the web shell, a multi/handler was set up in msfconsole with the payload windows/meterpreter/reverse\_tcp. The local host and port were configured, and the handler was initiated. By navigating to http://10.10.10.5/shell.aspx in a web browser, a Meterpreter session was successfully established on the target machine

**4. Privilege Escalation - Local Exploit Suggester and kitrap0d**

To achieve root access and retrieve the root flag, it was necessary to upgrade the Meterpreter shell. The local\_exploit\_suggester module within Metasploit was used to identify potential privilege escalation vulnerabilities.

Based on the suggestions and prior experience, the kitrap0d exploit (exploit/windows/local/ms10\_015\_kitrap0d) was chosen for its effectiveness on IIS environments. The Meterpreter session was set, and the exploit was executed, leading to a successful privilege escalation.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer program

AI-generated content may be incorrect.

**5. Flag Retrieval**

With elevated privileges, the user and root flags were located at the following paths:

* User flag: C:\Users\babis\Desktop\user.txt
* Root flag: C:\Users\Administrator\Desktop\root.txt

A screenshot of a computer

AI-generated content may be incorrect.