**Phase 3: Defense Implementation Against FTP Exploit**

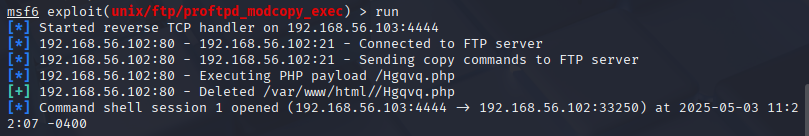
**Overview**

In this phase, we simulated an FTP attack on a vulnerable ProFTPD service using Metasploit. The goal was to exploit the mod\_copy module to gain remote access, then implement a defense to block the attack. We applied a configuration-based fix, retested the exploit, and confirmed the defense was successful.

**1. Vulnerability and Exploit Overview**

The target machine was initially vulnerable to an FTP-based attack leveraging the mod\_copy module in the ProFTPD service. The attacker exploited this vulnerability using the Metasploit module unix/ftp/proftpd\_modcopy\_exec to upload a malicious PHP payload into the web root directory (/var/www/html) and execute it via HTTP, resulting in a successful reverse shell.

**Successful shell from original attack**



A computer screen shot of a computer

AI-generated content may be incorrect.

**2. Defensive Strategy**

To mitigate the vulnerability without disabling FTP entirely, we applied a configuration-based defense by modifying file permissions on the web directory used in the exploit.

A screenshot of a computer

AI-generated content may be incorrect.

This secured the directory by revoking write access from all non-root users, thereby blocking the attacker's ability to upload executable payloads.

**Modified permission output**

**3. Post-Defense Exploit Attempt**

After applying the defense, the same Metasploit attack was launched again from the attacker machine. This time, the payload delivery failed with an error indicating that the web directory was no longer writable, and no reverse shell was established.

**Failed exploit output after defense**

A screen shot of a computer

AI-generated content may be incorrect.