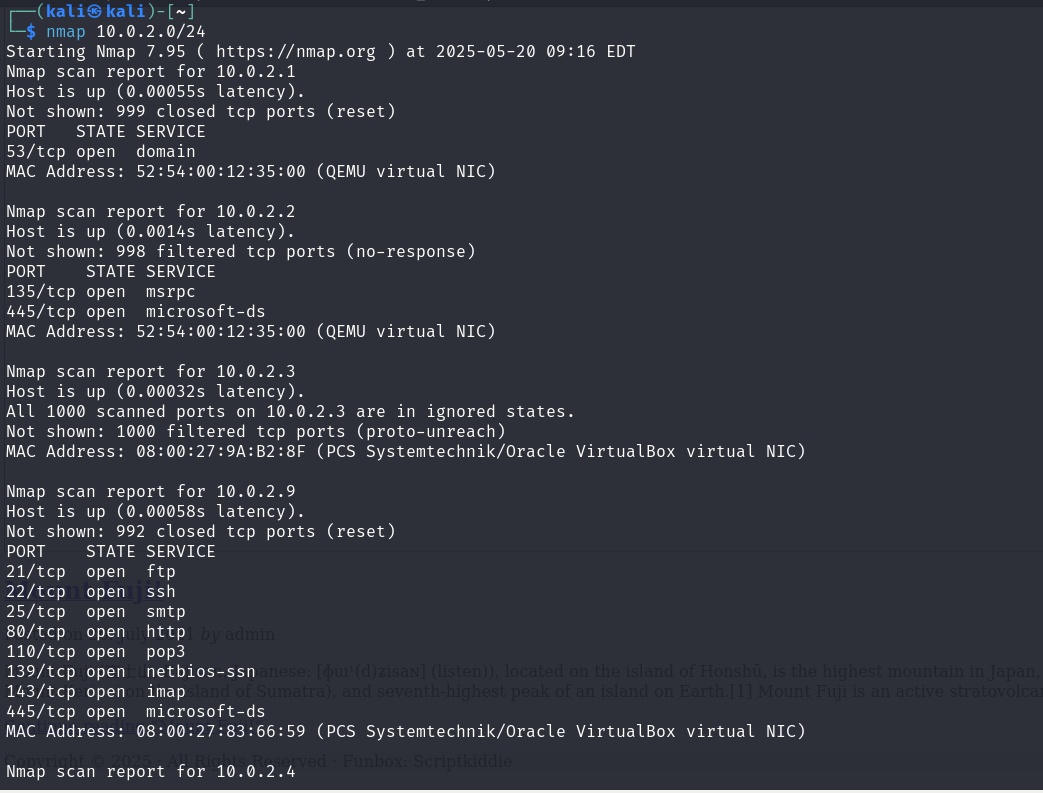
**VM Walkthrough: Funbox - Scriptkiddie**

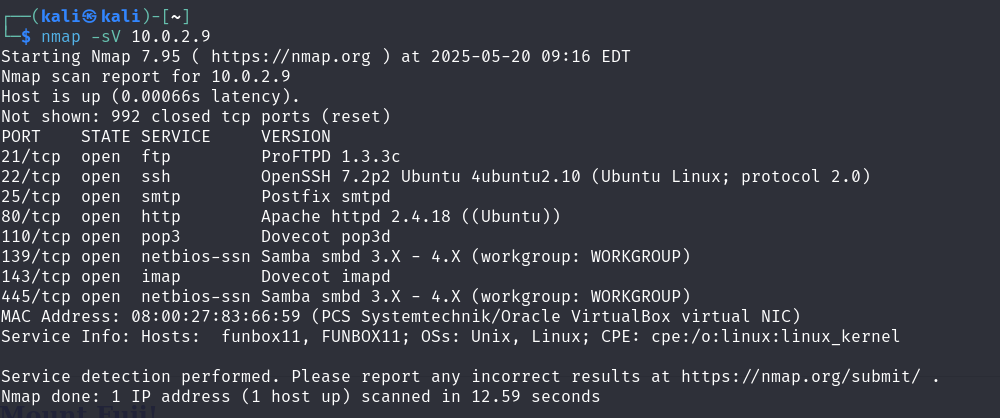


Found the IP address: 10.0.2.9  
My machine ip address: 10.0.2.4

**1. Initial Reconnaissance**

We begin by scanning the target system using Nmap to identify open ports and services.

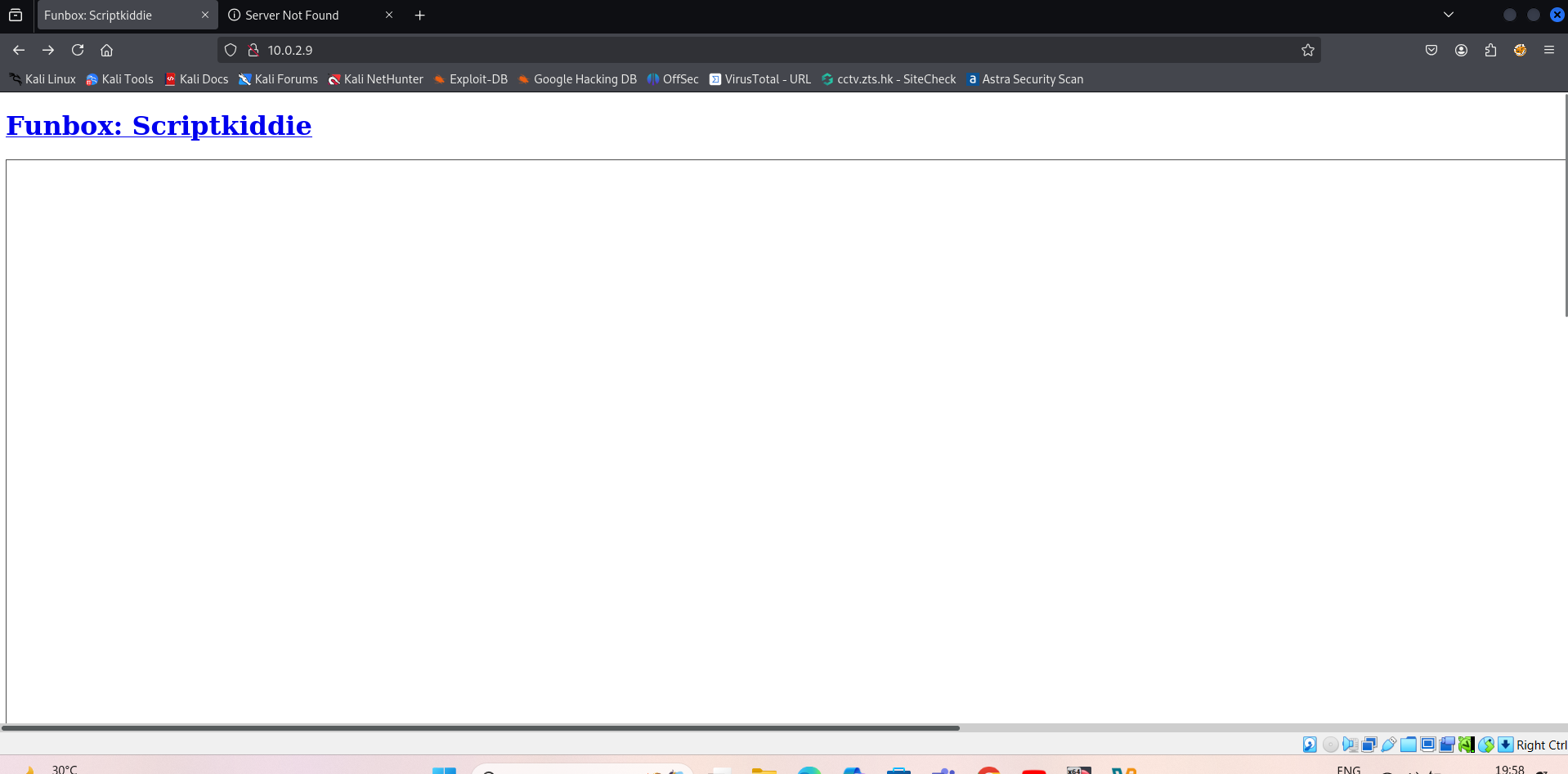
nmap -sV 10.0.2.9



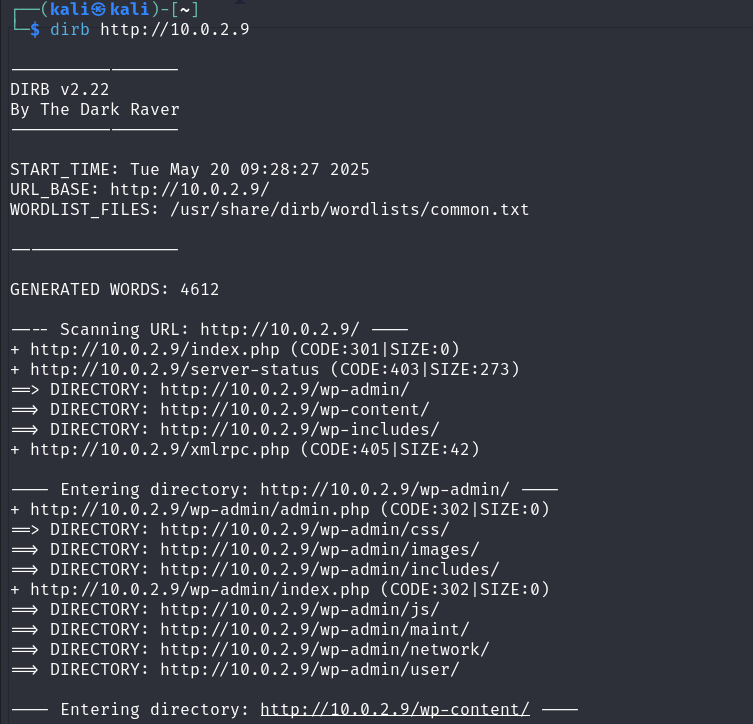
**Exploring HTTP (Port 80)**

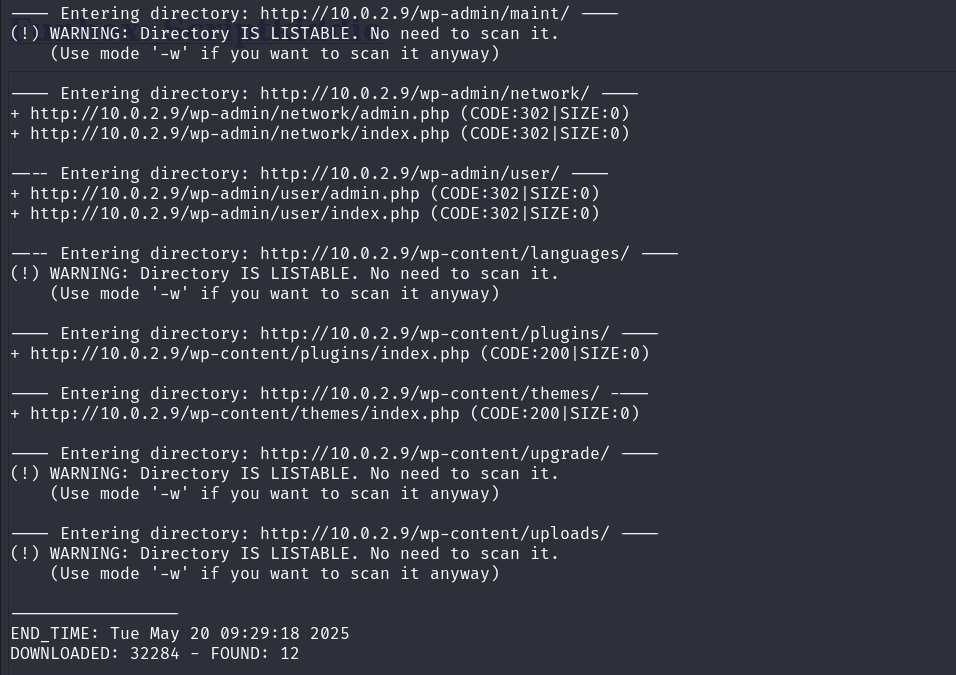
We visit the HTTP service via browser:

http://10.0.2.9

  
However, there is **no useful content** or application displayed on the main page.

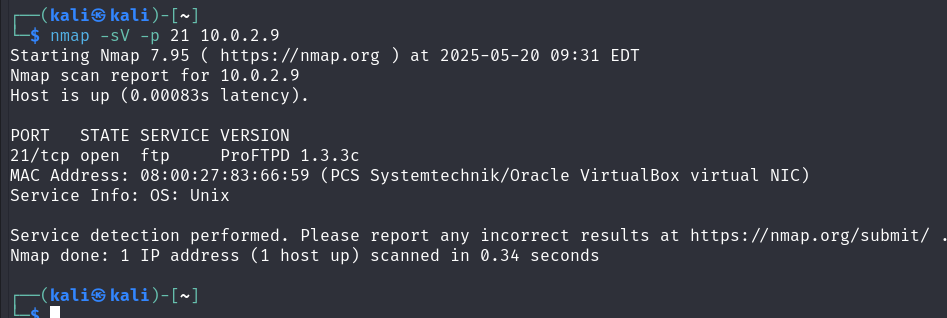
To dig deeper, we perform **directory brute-forcing** using dirb:  
Command Used: dirb http://10.0.2.9





This scan did not yield any significant results either, so we move on to explore the FTP service.

**3. FTP Enumeration (Port 21)**

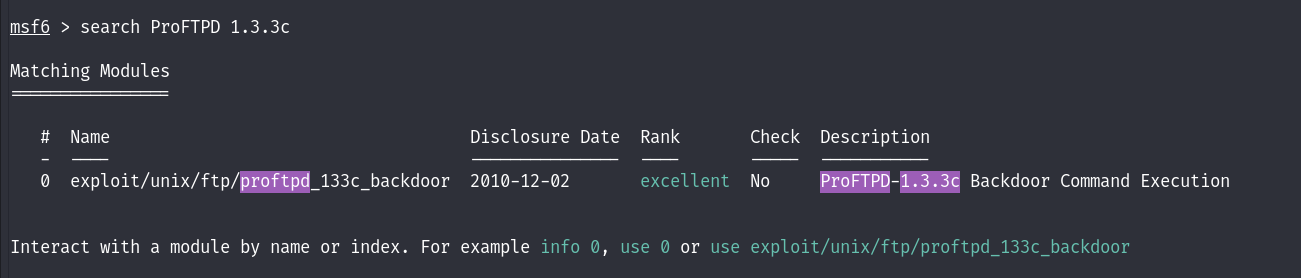


From the Nmap output, we see that the FTP service is running **ProFTPD 1.3.3c**, which is a known vulnerable version.

**4. Exploiting ProFTPD 1.3.3c**

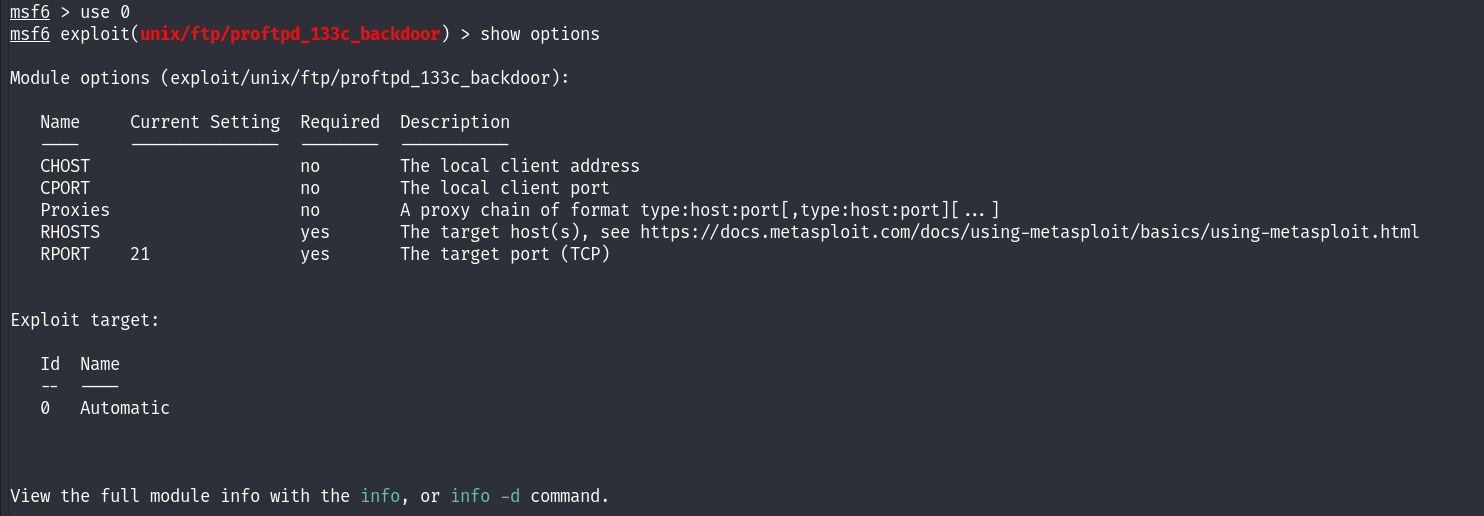
We search for exploits related to this version using **Metasploit**:

Command Used: search ProFTPD 1.3.3c

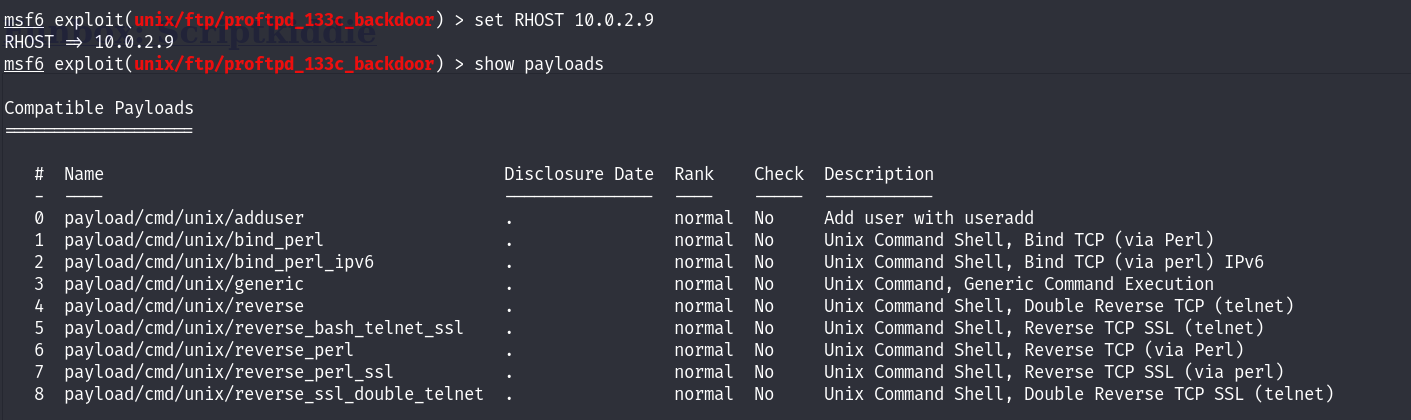


We identify a module that exploits the **mod\_copy** command injection vulnerability in ProFTPD 1.3.3c. We load the exploit module:

Command Used: use exploit/unix/ftp/proftpd\_modcopy\_exec

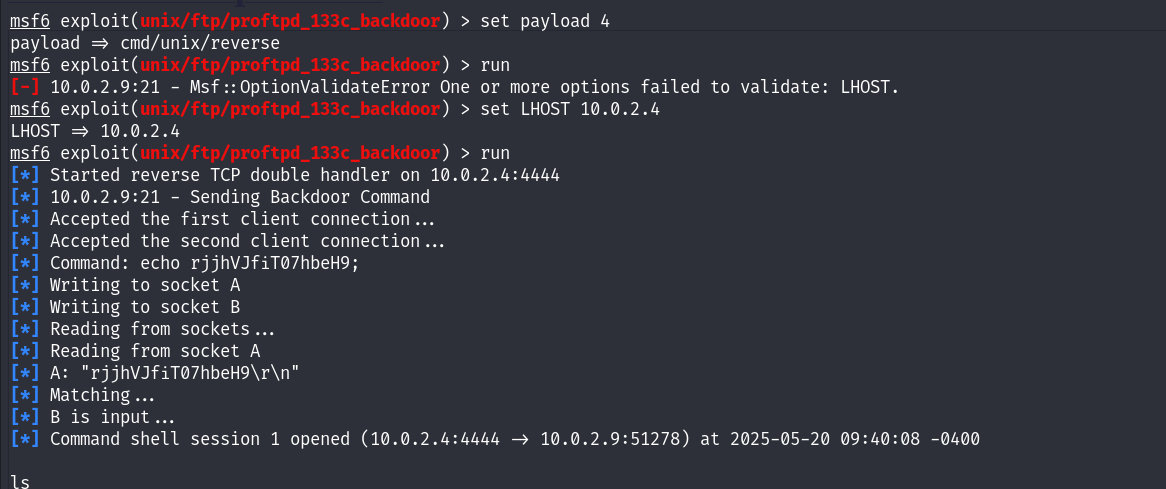


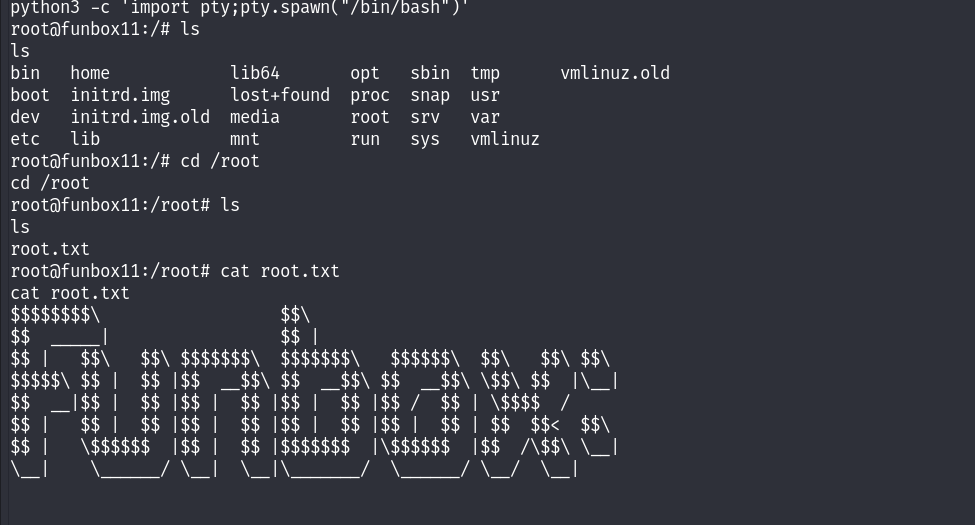
Set RHOST 10.0.2.9 – Vulnhub machine



**5. Shell Access**

Upon successful exploitation, we receive a **shell session** on the target machine. Further exploration and privilege escalation techniques grant us **root access**.





**6. Summary**

* **Vulnerability:** ProFTPD 1.3.3c mod\_copy command injection
* **Exploit Tool:** Metasploit
* **Result:** Gained root shell on target machine