Team member B:

Ashik k

🔐 Exploitation Report – VSFTPD 2.3.4 Backdoor (Member B)

📌 Objective

To exploit a known backdoor vulnerability in **vsFTPd version 2.3.4** running on the Metasploitable2 target, using Metasploit Framework, and gain unauthorized **root shell access**.

🛠️ Tools Used

- **Kali Linux** (Attacker machine)

- **Metasploit Framework v6**

- **Metasploitable2** (Target IP: `192.168.56.102`)

🧪 Exploitation Process

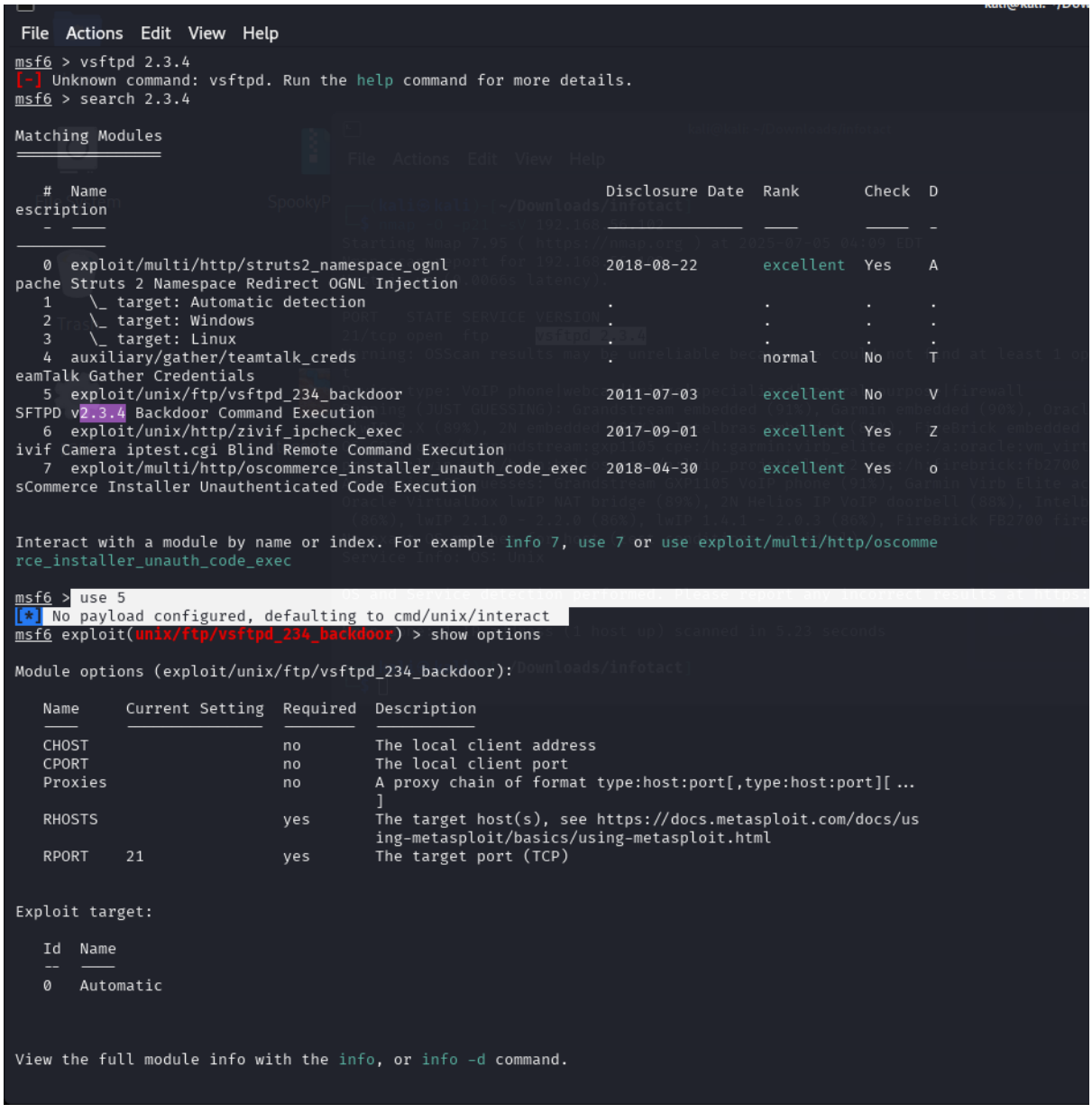
1️⃣ Launch Metasploit Console

Metasploit was launched using the `msfconsole` command on Kali.

2 Load Exploit Module

The known exploit for `vsftpd 2.3.4` backdoor was loaded using:

“use exploit/unix/ftp/vsftpd_234_backdoor”



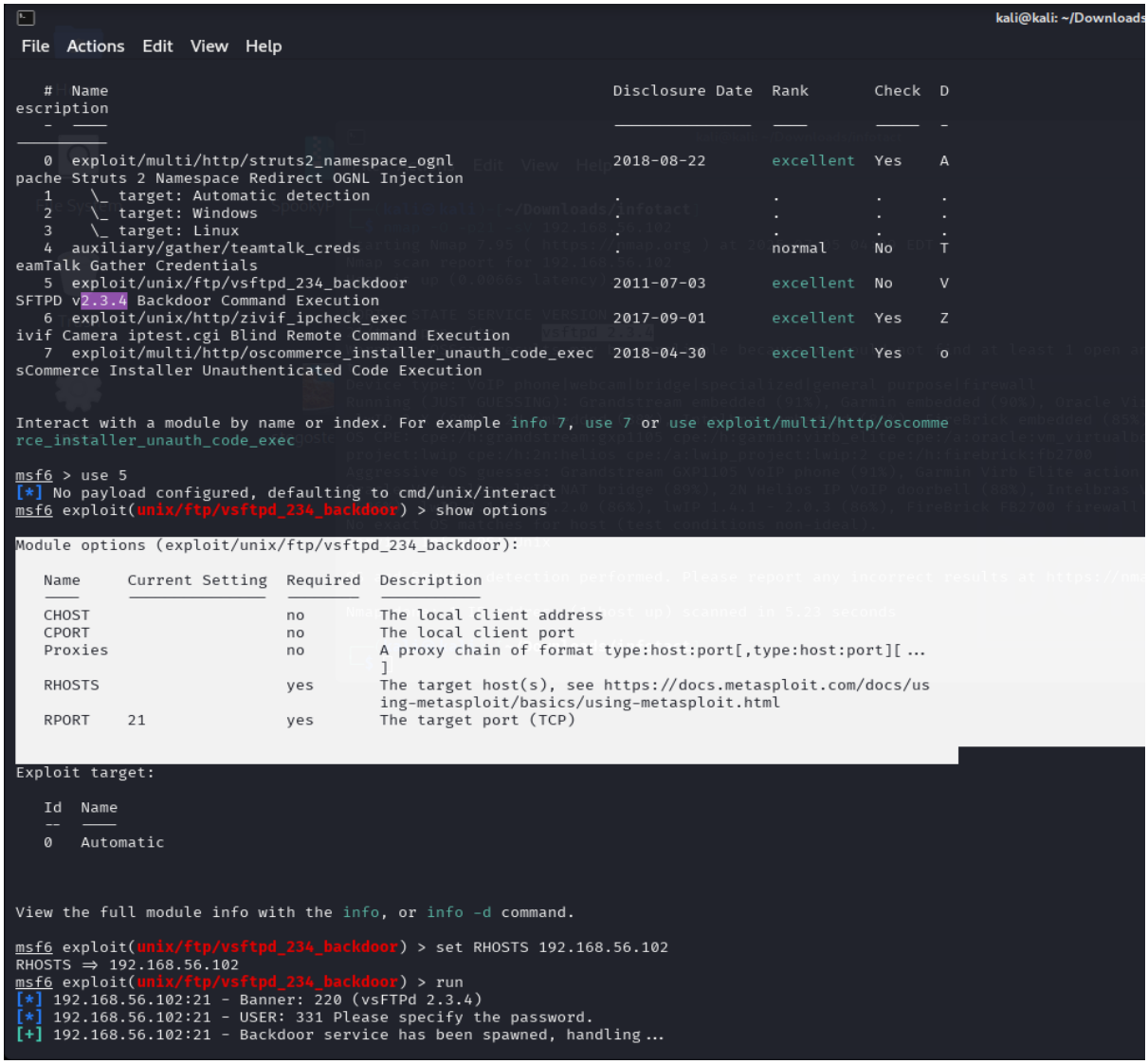
3 Configure Target IP

The target IP address was set using:

“set RHOSTS 192.168.56.102” (victim ip)

“show options”

This ensured the module had the correct target before execution.



4 Run Exploit

The exploit was executed using:

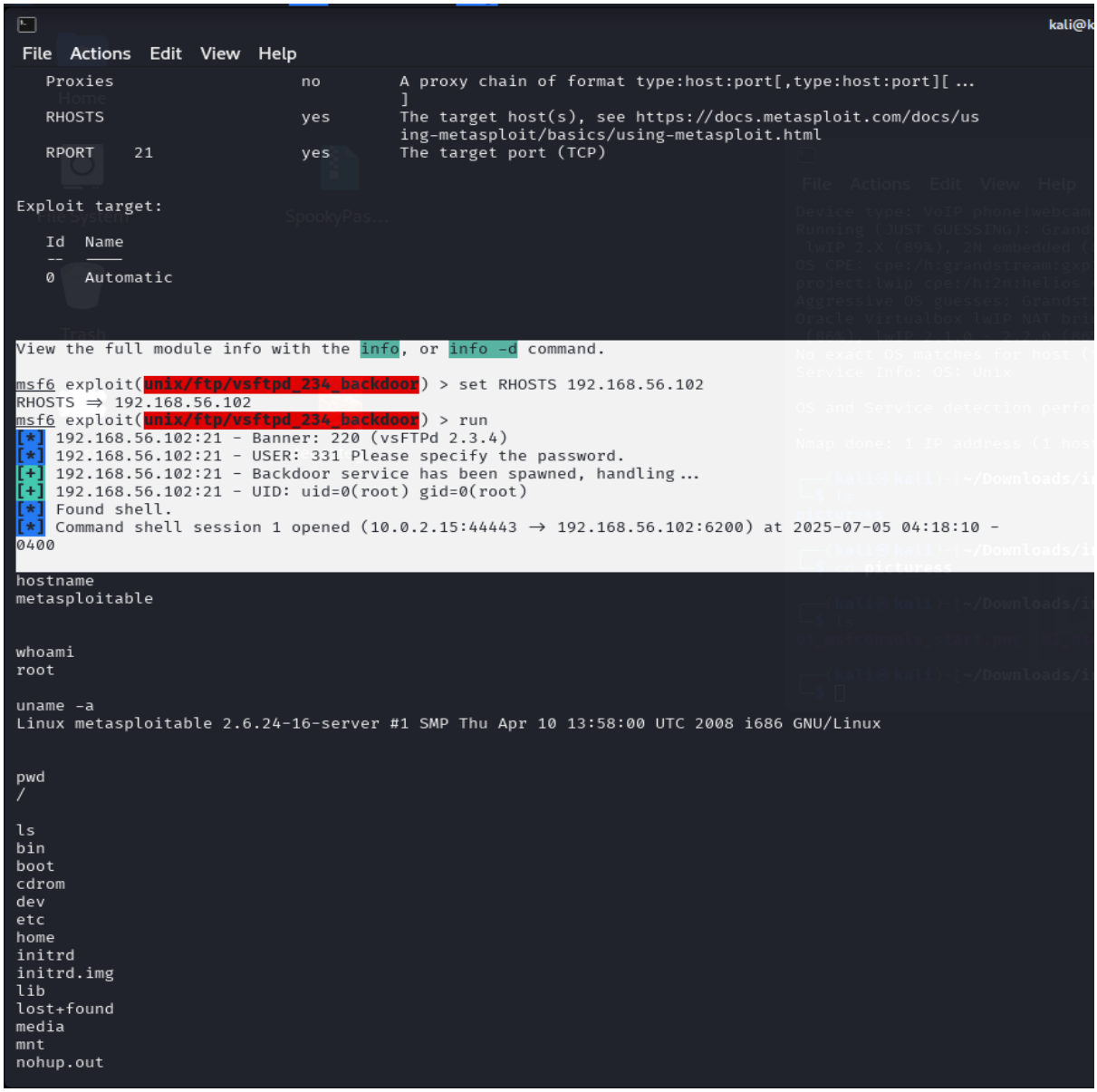
“run”

The exploit connected successfully to the FTP service, triggered the backdoor, and opened a shell as **root**:

- Backdoor service spawned

- UID confirmed as `0 (root)`

- Command shell session opened



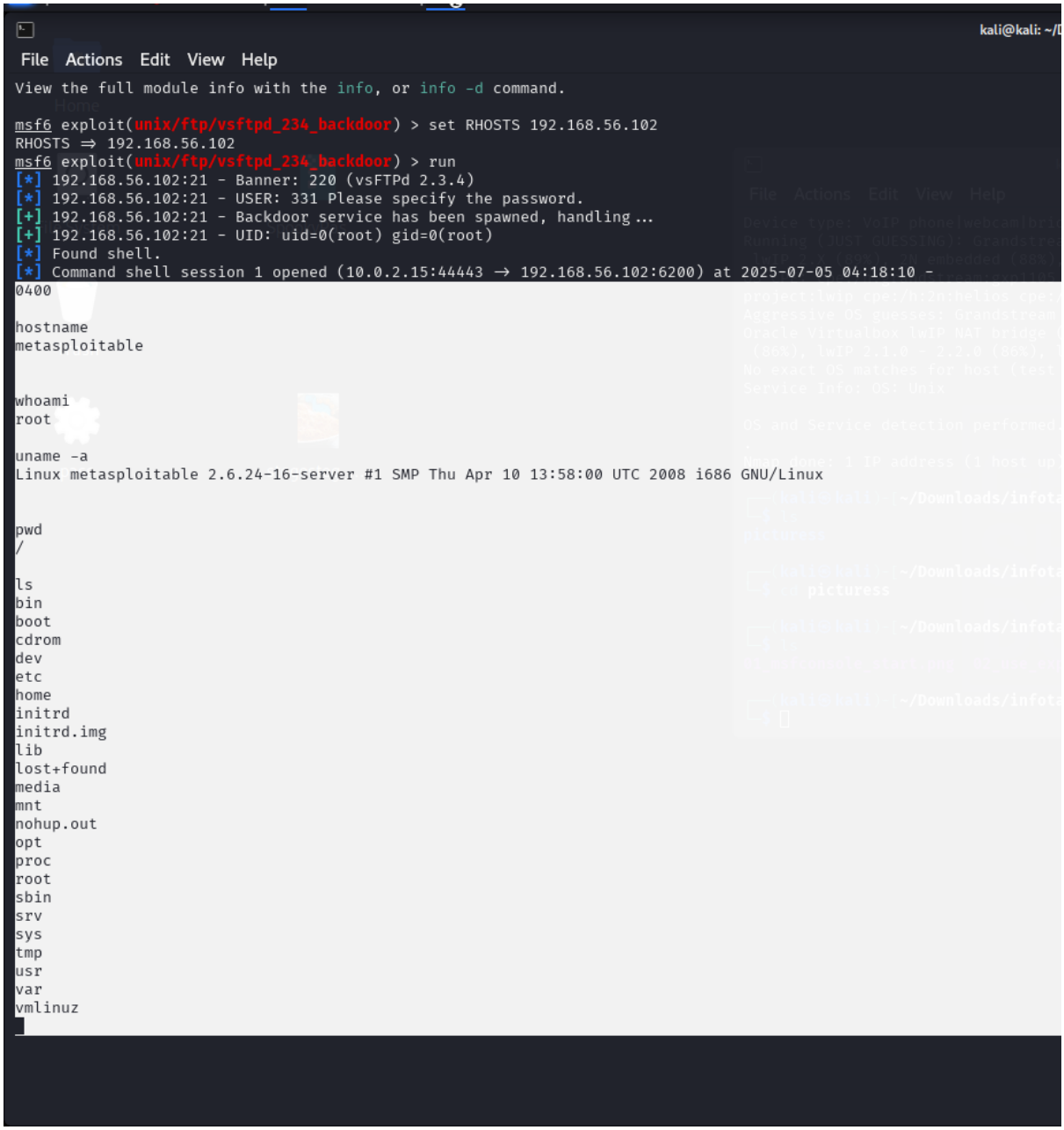
5 Verify Shell Access

Inside the shell, the following commands were executed to confirm successful root access and gather system info:

“hostname”

“whoami”

“id”



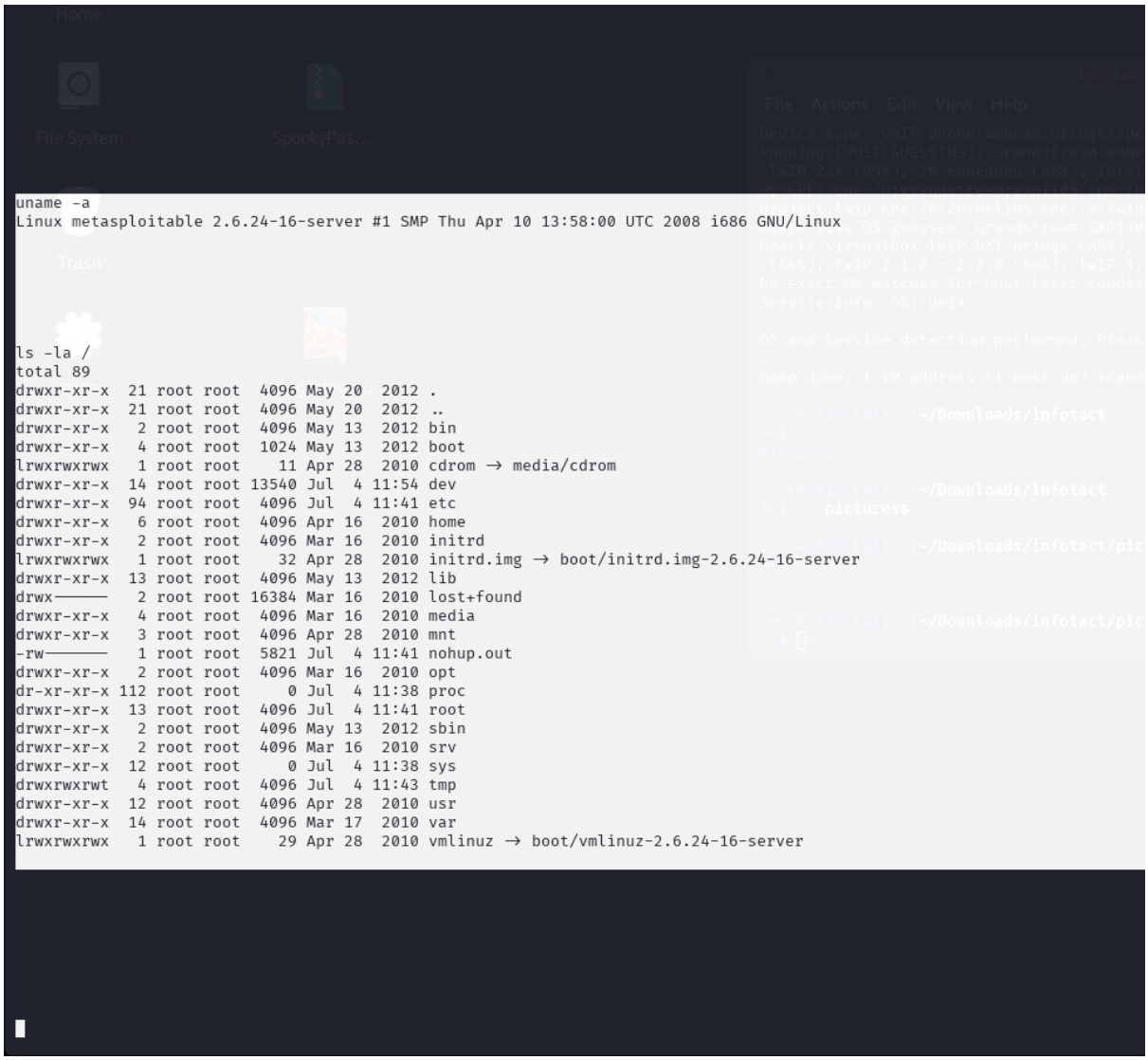
6 System Information & File Access

Further enumeration was done using:

“uname -a”

“ls -la /”

This helped validate the target OS and access level.



✅ Outcome

Root access was successfully gained on the target system using the VSFTPD backdoor. This highlights the critical risk of running outdated software with known exploits.

🔒 CVE Reference

- **CVE-2011-2523** – vsftpd 2.3.4 Backdoor Command Execution

Screenshots:

01_msfconsole_start

02_use_exploit_command

03_show_options_output

04_exploit_run_success

05_shell_root_proof

06_shell_system_info