**🧾Cybersecurity Portfolio**

**Establish a Reverse Shell on a Remote Server**

**🔍 Objective**

**Briefly explain what the lab was about and what skill or vulnerability it focused on**:

In this lab, I used Metasploit to exploit a vulnerability in UnrealIRCd, establish a reverse shell on a remote server, and retrieve a sensitive file.

**🛠️ Tools Used**

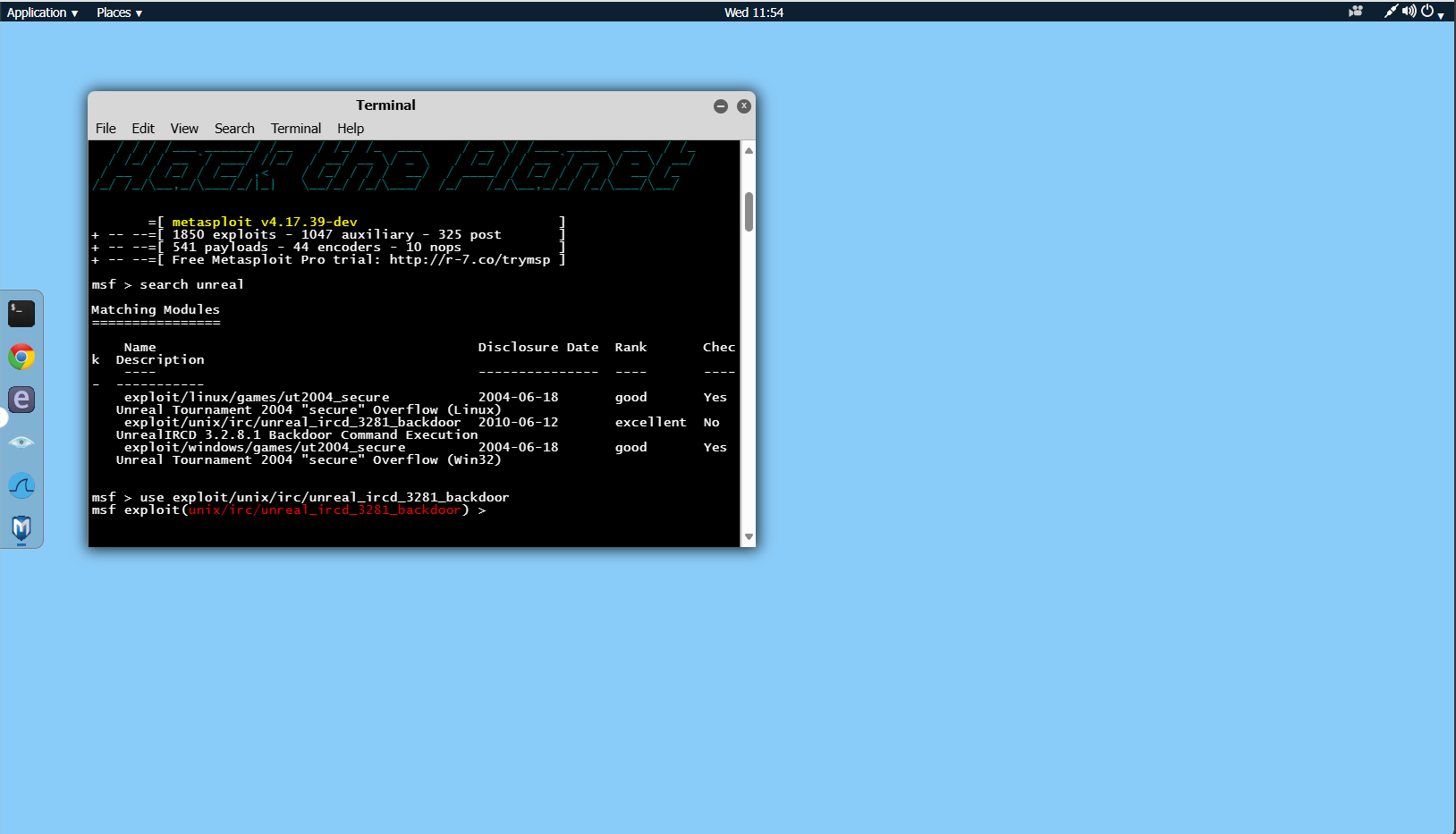
**List all tools, systems, and environments you used**:

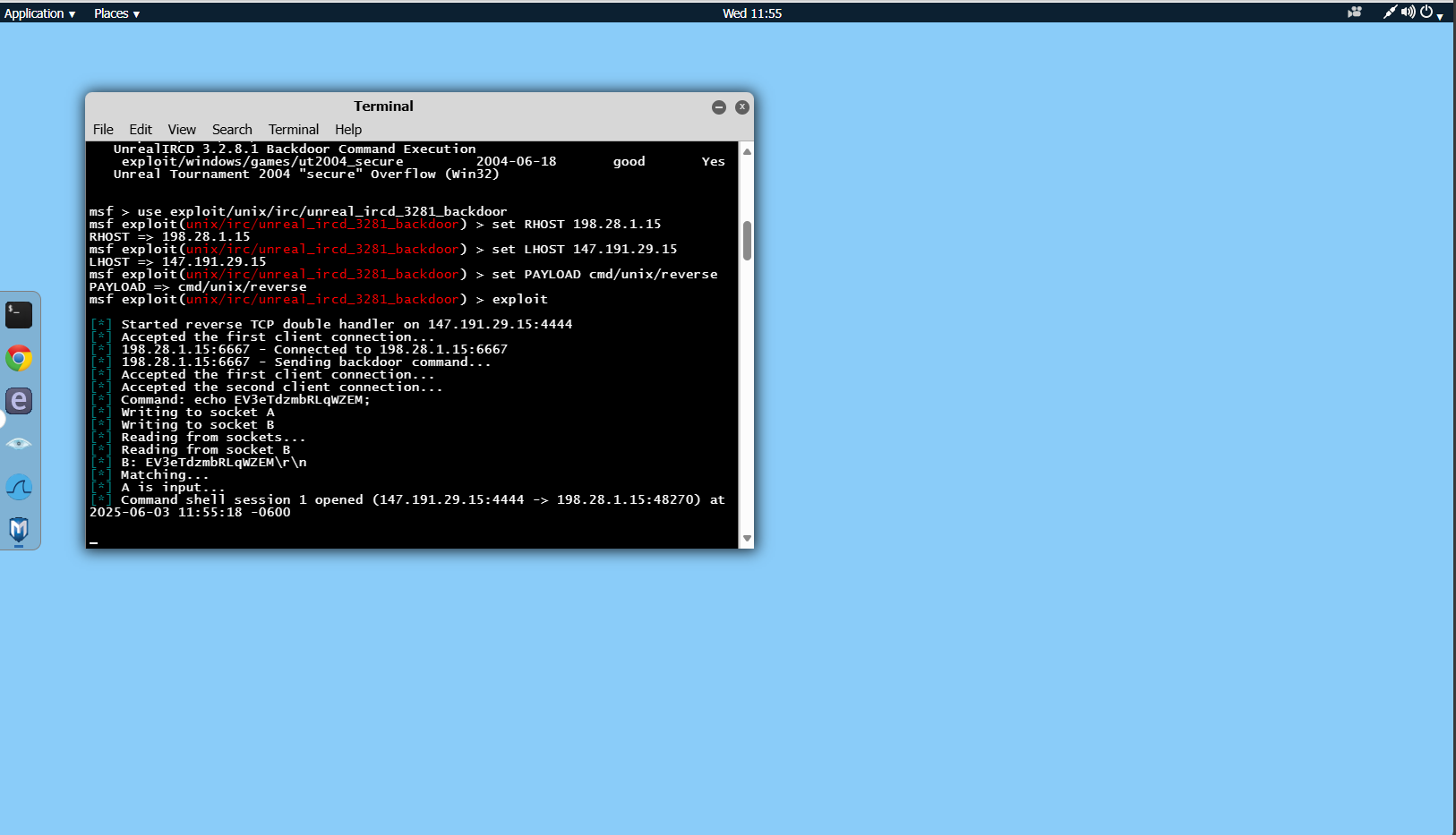
* Kali Linux
* Metasploit Framework
* Zenmap
* Target IP: 198.28.1.15
* Attacker IP: 147.191.29.15

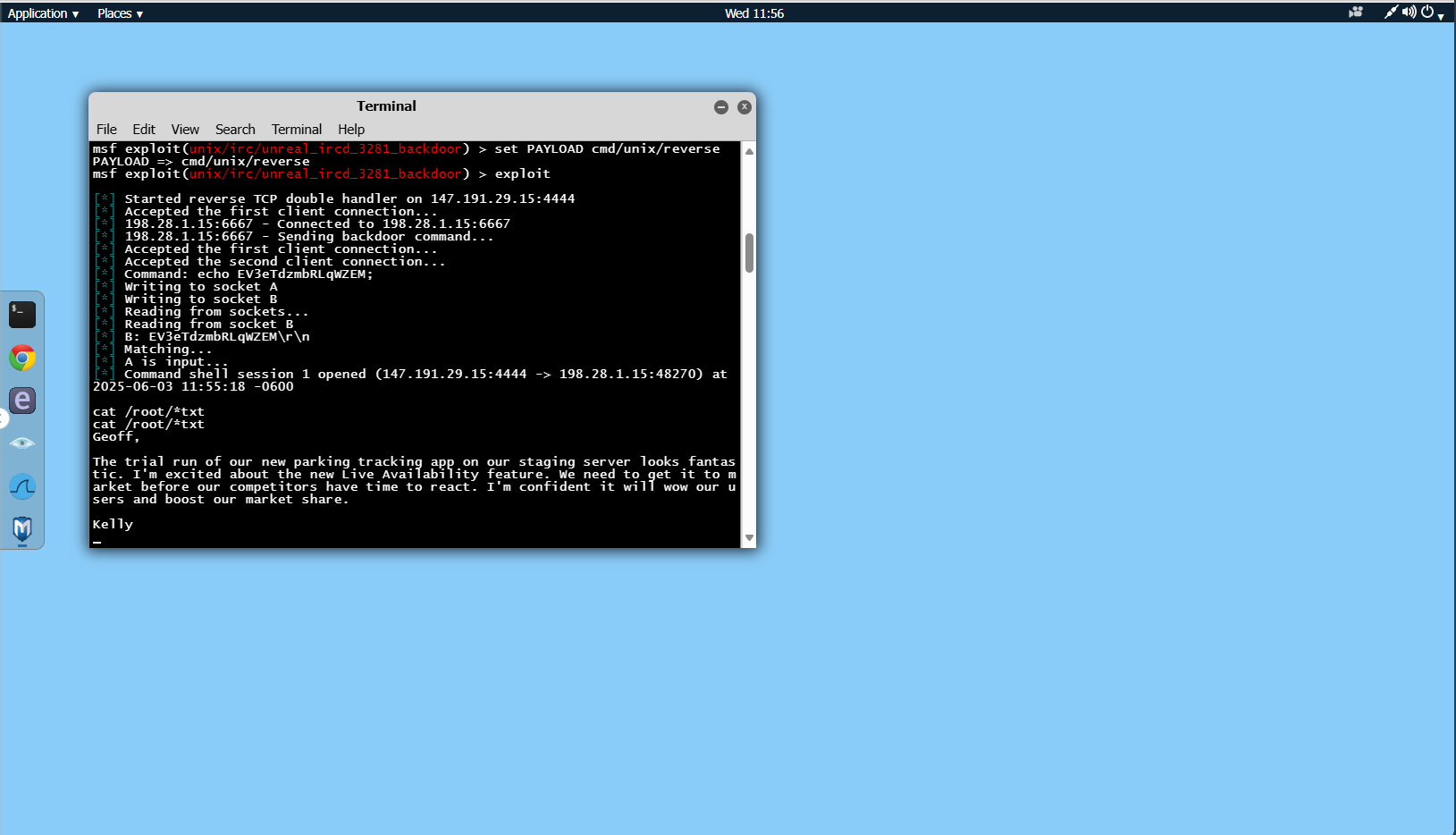
**📜 Lab Steps Taken**

**Write a step-by-step list of what you did. Include commands if applicable:**

1. Launched Metasploit using msfconsole.
2. Searched for UnrealIRCd exploits: search unreal.
3. Used exploit: exploit/unix/irc/unreal\_ircd\_3281\_backdoor.
4. Set RHOST, LHOST, and PAYLOAD.
5. Executed the exploit with exploit.
6. Gained a reverse shell and read the target file using cat /root/\*.txt.







**✅ Result**

**Explain what happened — was it successful? What did you learn?**

Successfully established a reverse shell and retrieved the target .txt file, demonstrating the risk of backdoored software and improper network segmentation.

**💡 Reflections / Lessons Learned**

This lab helped me understand how attackers can exploit known vulnerabilities in outdated services and gain unauthorized access to critical systems.