**Mr. Robot VM**

**Finding the IP Address of the Device on the same network**

Perform ifconfig command on Kali

inet: 10.0.2.15 netmask: 255.255.255.0

In netmask of Kali, you can see that it is divided in four segments. Three segments have 255 and one segment has 0. 255 digit is constant and 0 is a variable. Since segments with 255 are constant and are the first three blocks, this means that first three blocks of the IP address is same for all the devices in the NAT network.

Command: #nmap -sn 10.0.2.1/24

//The command displays(IP & MAC addresses) all the devices connected to the NAT network

//Here 8\*3=24 since each of the segment is an octet(8) and 3 constants

In networking, a subnet mask (or netmask) is a 32-bit binary number used to divide an IP address into network and host portions. The subnet mask is represented in decimal form for ease of use, and it is commonly expressed in what is called "dotted-decimal notation," where each octet (8 bits) of the 32-bit mask is represented as a decimal number separated by periods. For example, a subnet mask of 255.255.255.0 is a common subnet mask used in IPv4 networking.

In binary form, the subnet mask 255.255.255.0 is represented as:

11111111.11111111.11111111.00000000

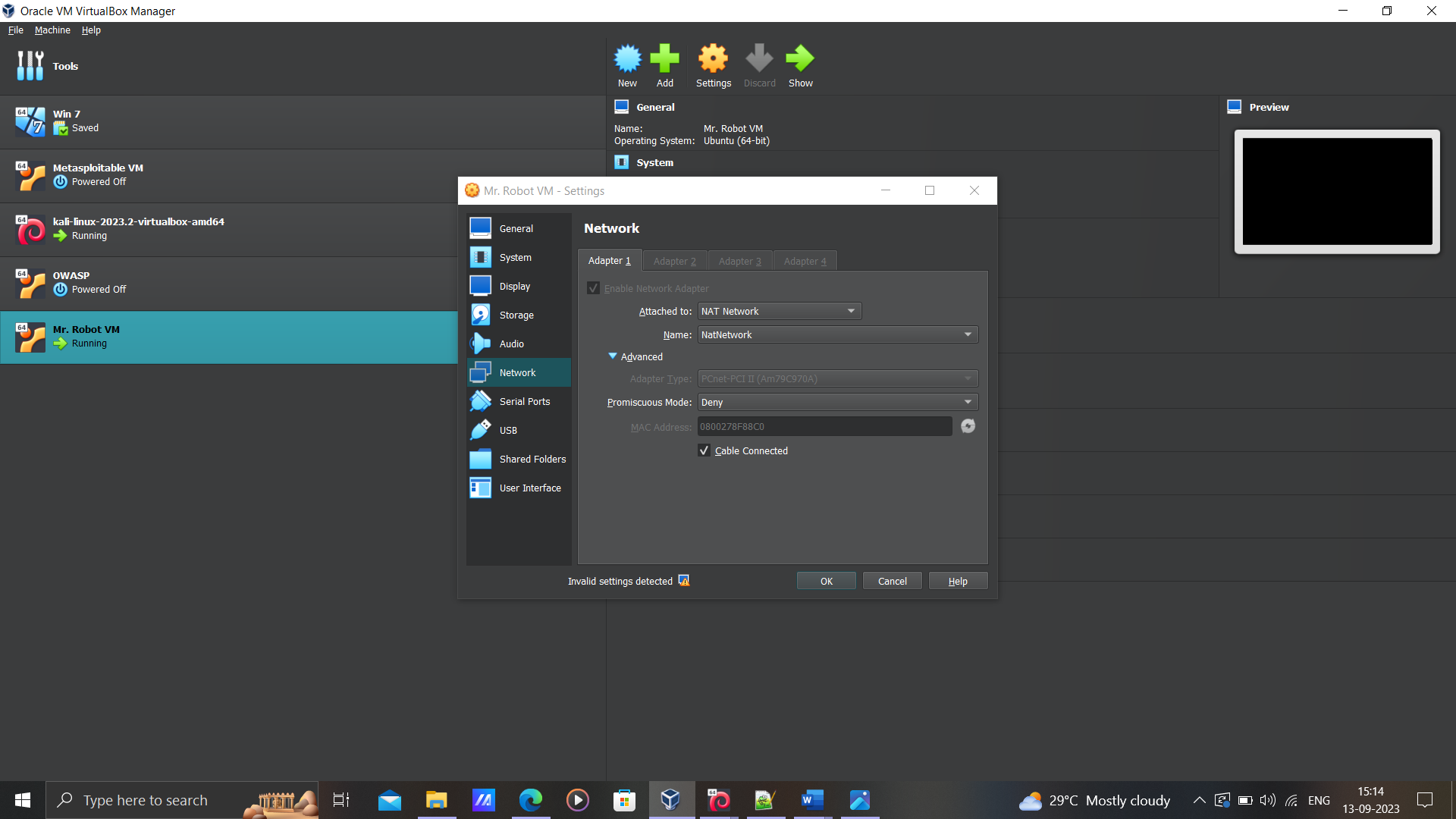
In this notation, the first 24 bits are set to '1' (representing the network portion), and the last 8 bits are set to '0' (representing the host portion). This means that the first 24 bits of the IP address determine the network to which the device belongs, and the remaining 8 bits can be used to address individual hosts within that network.

So, when you see a subnet mask of 255.255.255.0, it means that the first three octets of the IP address are part of the network, and the last octet can be used to address individual devices within that network.



We can see the MAC Address in the Network Settings of the victim’s virtual machine. The MAC address matches the nmap scan made on the device with IP address 10.0.2.7.

Therefore the IP address of the black-box machine is 10.0.2.7.



**Mr. Robot Virtual Machine**

**Description:** Based on the show, Mr. Robot. This VM has three keys hidden in different locations. Your goal is to find all three. Each key is progressively difficult to find. The VM isn't too difficult. There isn't any advanced exploitation or reverse engineering. The level is considered beginner-intermediate.



Performing a Port Scan

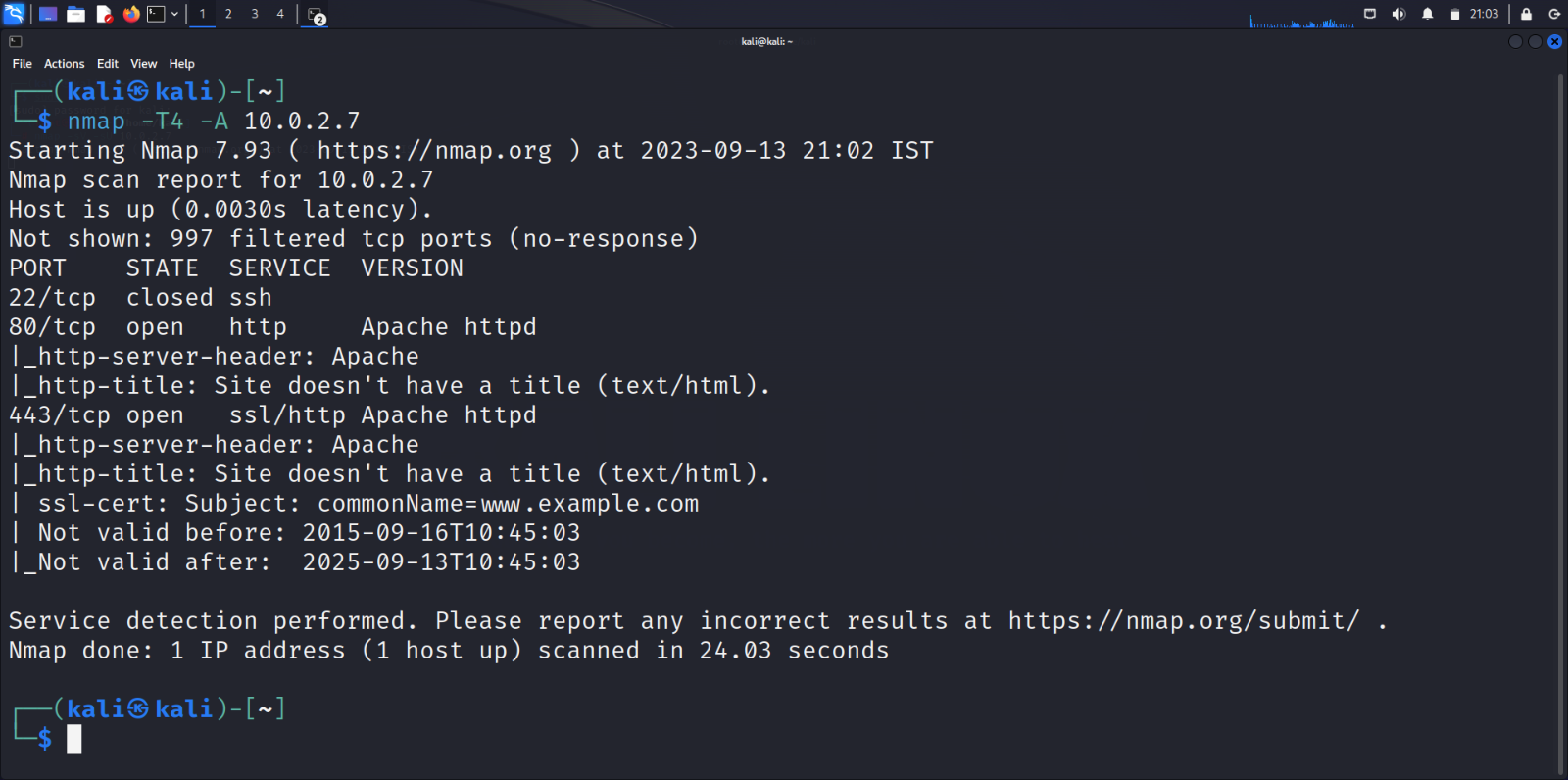
Command: #nmap -sV -sU 10.0.2.7

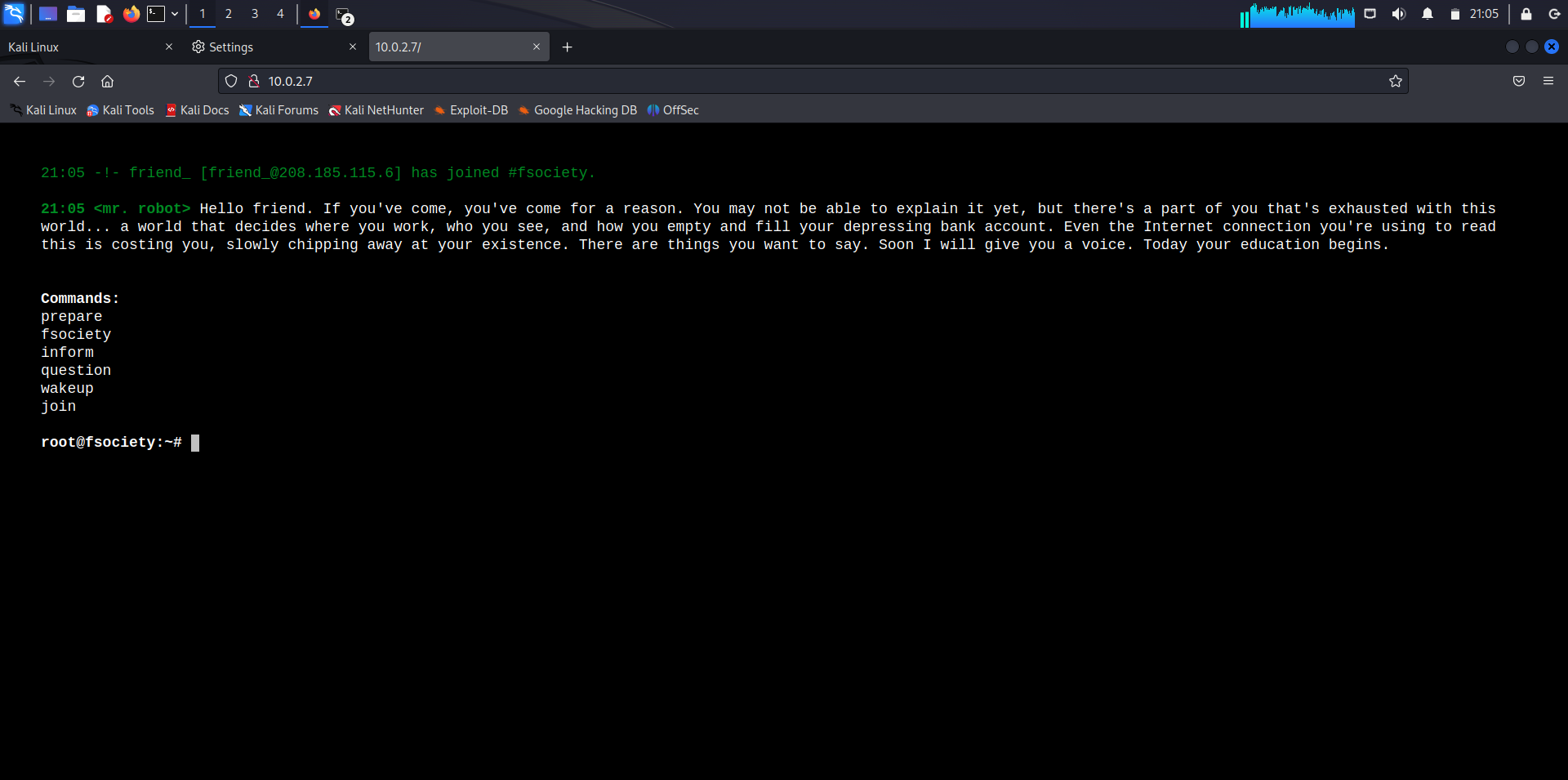
Command: #nmap -T4 -A 10.0.2.7

Open Ports

80 //http

443 //https



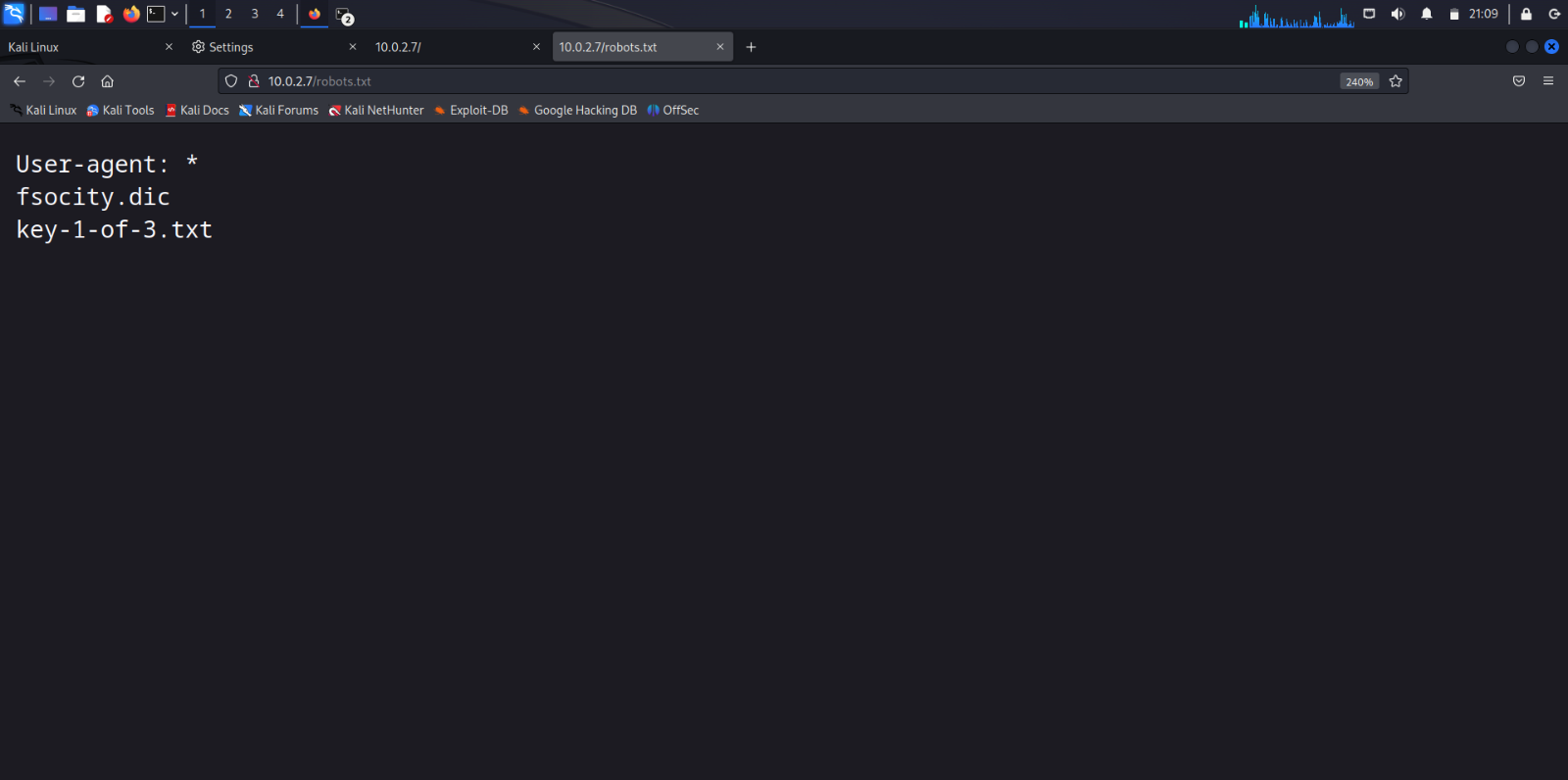


robots.txt

This text files defines all the directories/webpages that is allowed or disallowed to be accessed by a spidering bot or other bots.

Ex: www.google.com/robots.txt

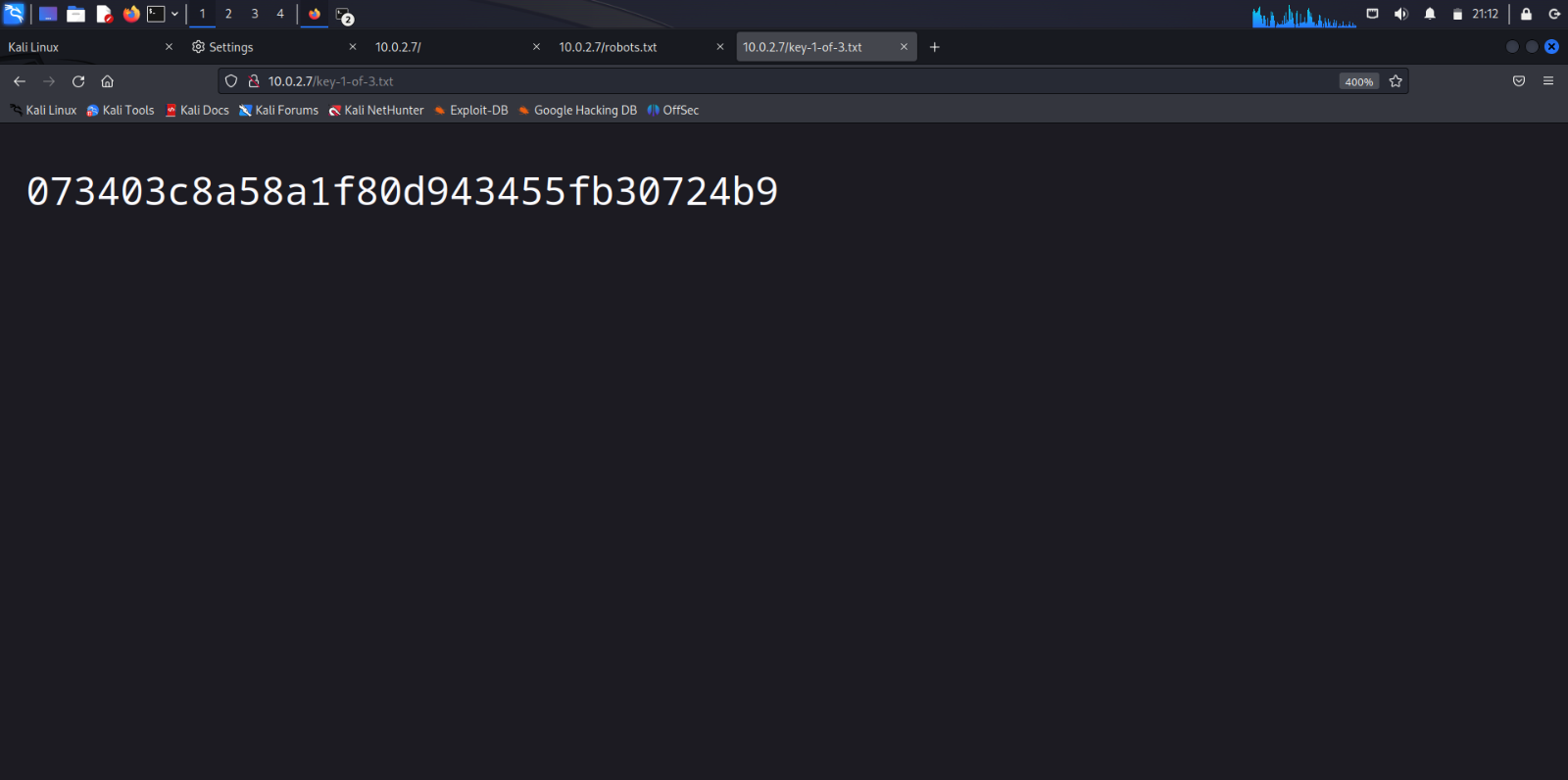
http://10.0.2.7/robots.txt



key-1-of-3.txt

The objective of the Mr. Robot Virtual Machine is to find 3 keys. The first of 3 keys is found.

Key\_1: 073403c8a58a1f80d943455fb30724b9



fsocity.dic

Opening the webpage automatically downloaded a file called fsocity.dic.



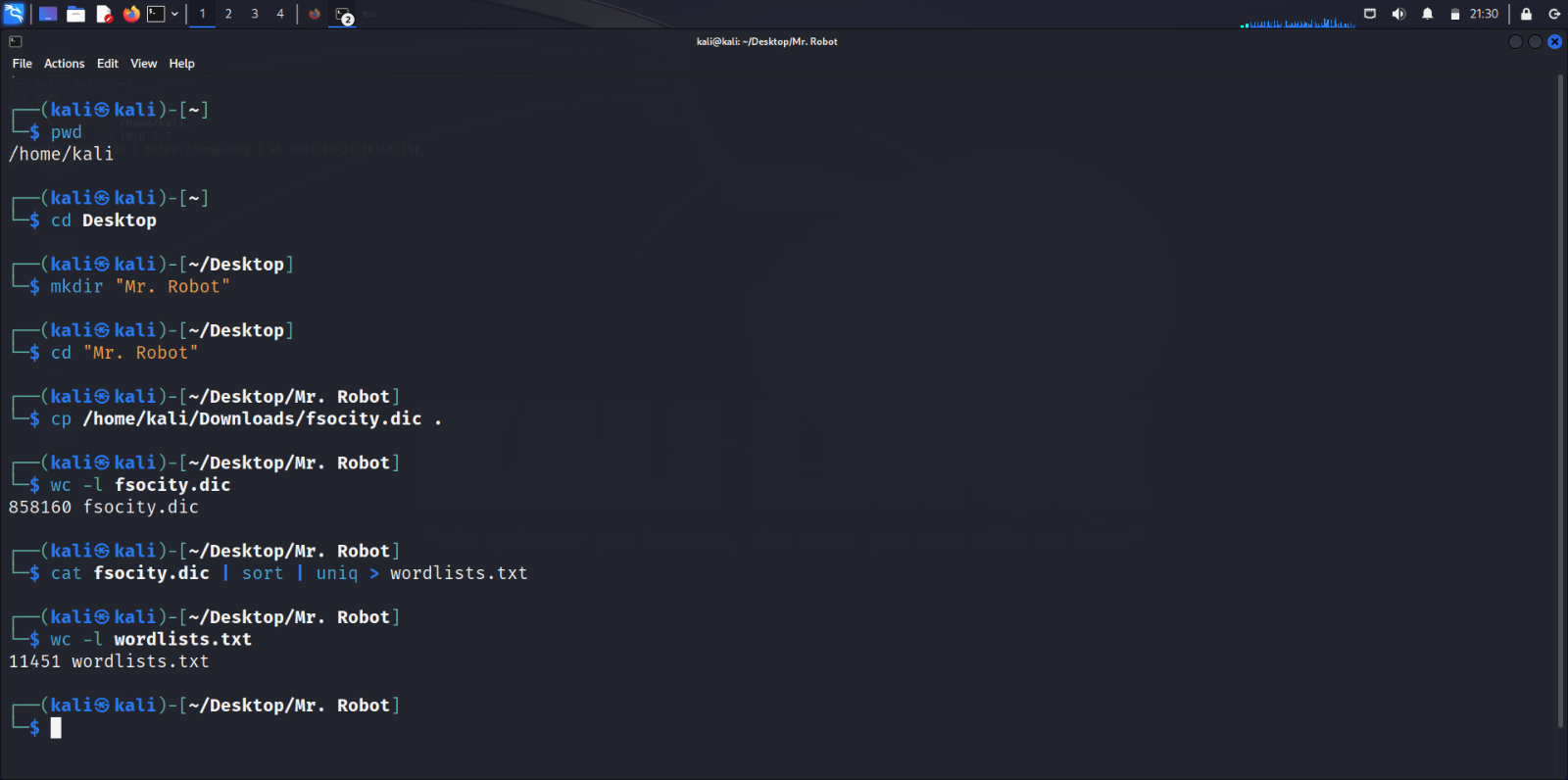
Command: wc -l fsocity.dic //Displays the number of words in the file

The file contains 858160 words.

Command: cat fsocity.dic | sort | uniq > wordlist.txt

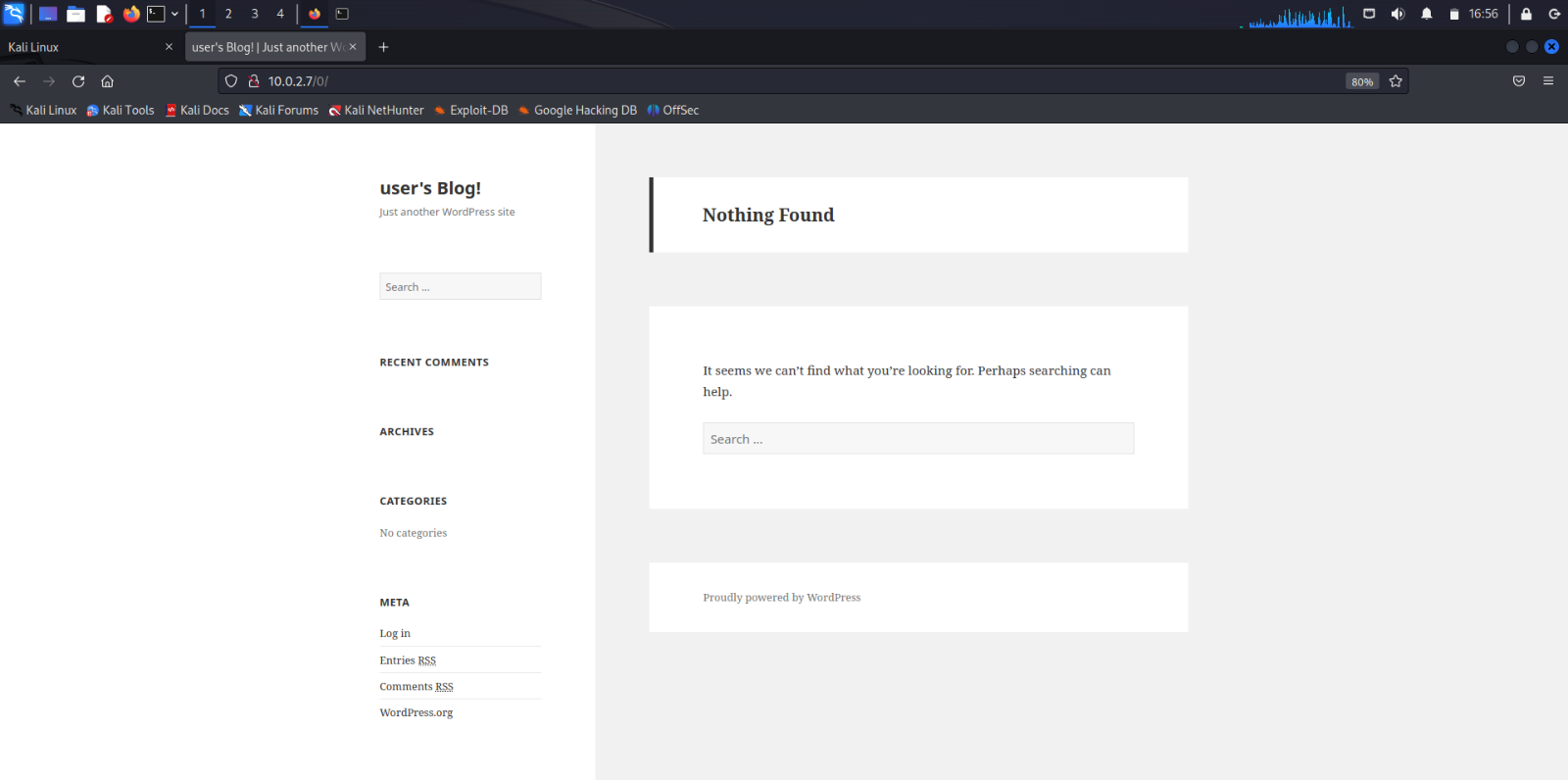
//Sorts the fsocity.dic file and writes the unique words onto another file.

Sorted and unique wordlist contains 11451 words.



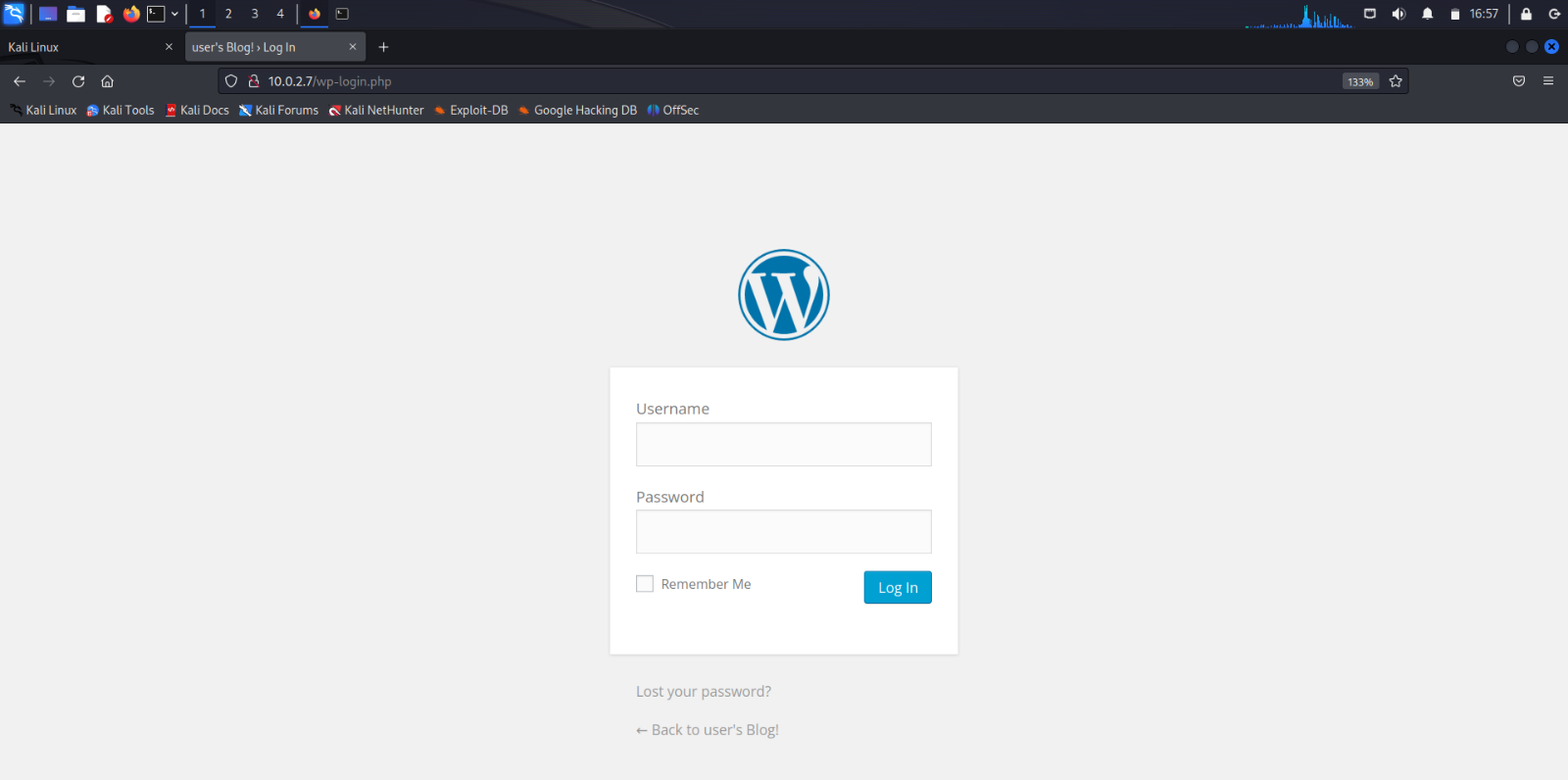
Wordpress page

URL: http://10.0.2.7/0/



Wordpress Login page

URL: http://10.0.2.7/wp-login.php



Logging in with wrong credentials

