iGNITE Technologies

EASY WAY TO
GENERATE REVERSE SHELL

www.hackingarticles.in

Contents

Easy Way to Generate Reverse Shell

In this article, we will learn how to get a reverse in few easy steps. Usually, the problem when reverse shell commands is to remember its long and complicating syntax. But due to growing AI of our digital world, this problem tackled and dealt with. Let's see how it is done through this article.

What is Reverse Shell?

A reverse shell is a technique used in computer security and hacking that allows an attacker to gain control over a system through an established network connection. Reverse shells can be used for various purposes, including unauthorized access, data theft, and further exploitation of the compromised system.
A reverse shell, however, works in the opposite direction.

Here's a basic explanation of how a reverse shell typically works:

Listener/Server Side: The attacker sets up a listener (command and control/C2 server) on a machine they control. This listener waits for incoming connections.

Victim/Client Side: The attacker somehow tricks the target system into connecting back to their machine. This could be through techniques like exploiting vulnerabilities, social engineering, or other means.

Connection Establishment: Once the connection is established, the attacker gains a command shell on the target system. This shell allows them to execute commands on the target machine as if they were physically present.
Command Execution: The attacker can then issue commands on the target system, navigate the file system, run programs, and essentially control the system remotely.

Types of Reverse Shell

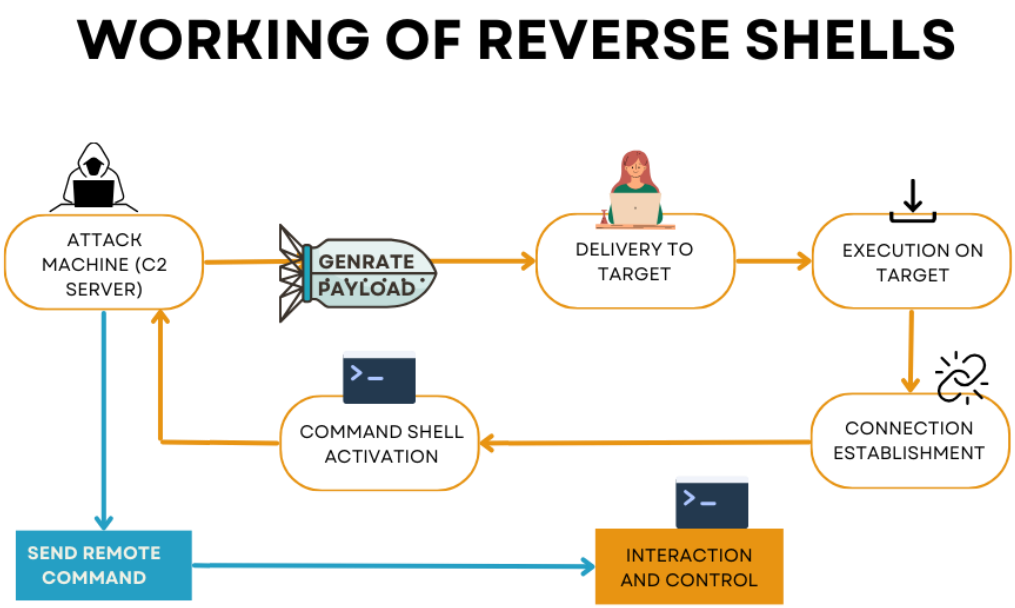
Reverse shell payloads are typically used by attackers to establish a connection back to their system. These payloads can be part of various hacking tools and frameworks. Here are some common types of reverse shell payloads:

Netcat (nc): Netcat is a versatile networking utility that can be used to create a basic reverse shell. The attacker sets up a listener using Netcat, and the victim connects back to it, establishing a shell.
Bash (Linux): A simple reverse shell can be achieved using Bash, the command shell for Unix-based operating systems. The attacker might use a one-liner command to create a reverse shell.

Python: Python is a powerful scripting language, and attackers often use it to create reverse shells. They can write a short script that opens a network connection and redirects input/output to that connection.
PowerShell (Windows): On Windows systems, PowerShell is a command-line shell that supports scripting. Attackers might use PowerShell to create reverse shells for Windows-based targets.
PHP: PHP is a server-side scripting language, and attackers can craft PHP scripts to establish reverse shell connections. These scripts are often injected into vulnerable web applications.
Ruby: Similar to Python, Ruby is a scripting language that can be used to create reverse shell payloads. Attackers might use Ruby scripts to exploit vulnerabilities and gain control over a system.
Metasploit Framework: Metasploit is a penetration testing framework that includes a variety of tools for exploiting vulnerabilities. It provides pre-built reverse shell payloads for different scenarios and platforms.
Java: Java-based reverse shells can be created to exploit systems where Java is installed. Attackers can use Java sockets to establish a connection back to their server.
C and C++: Attackers may also write custom reverse shell code in lower-level languages like C and C++ to avoid detection by antivirus software and intrusion detection systems.

Working of Reverse Shells

A reverse shell operates by initiating a connection between the target machine and the attacker's machine. Typically, the target machine sends a connection request to the attacker's machine. The attacker's machine functions as a listener, awaiting commands from the attacker.

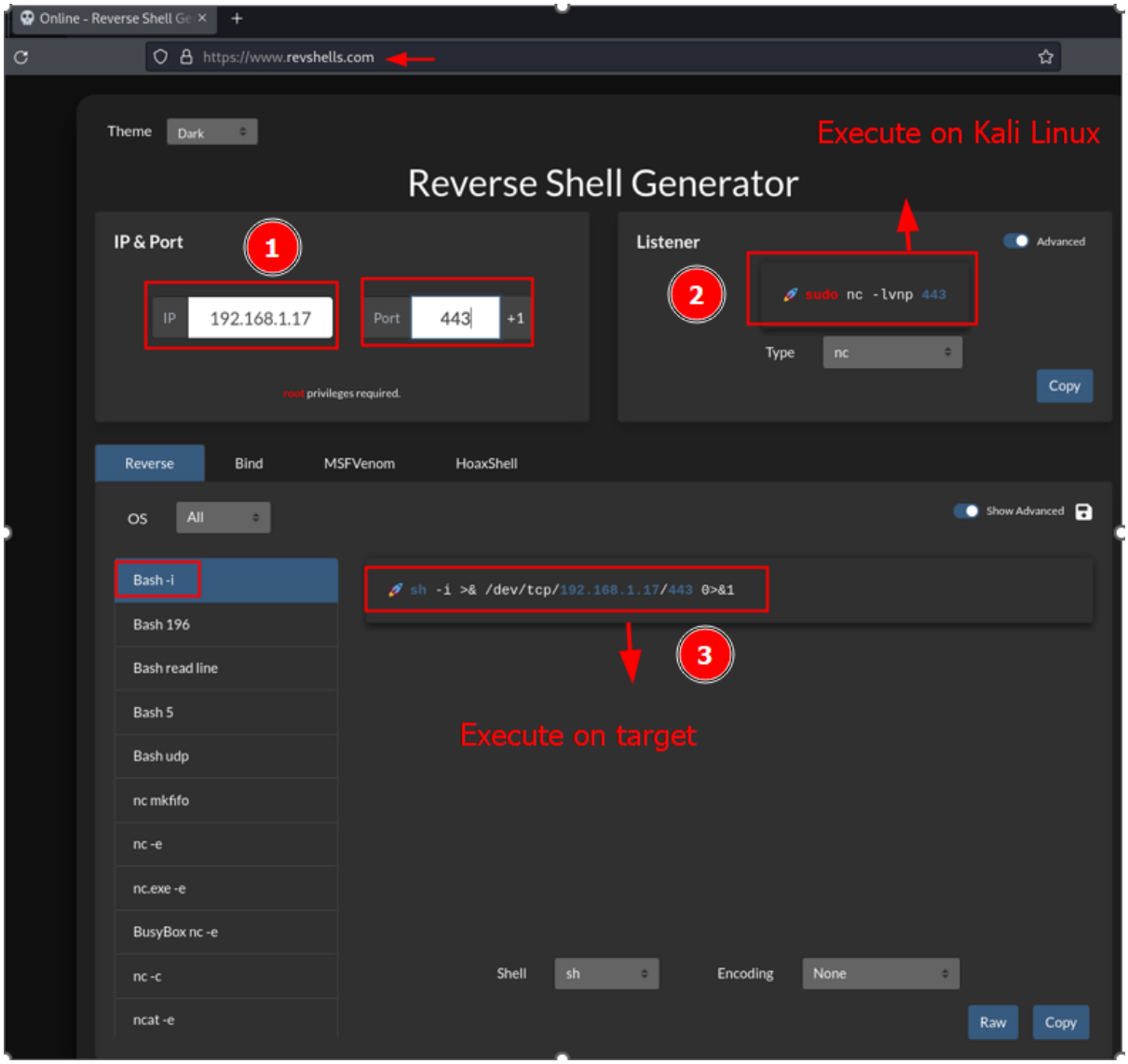


Various Type Reverse Shell Generator

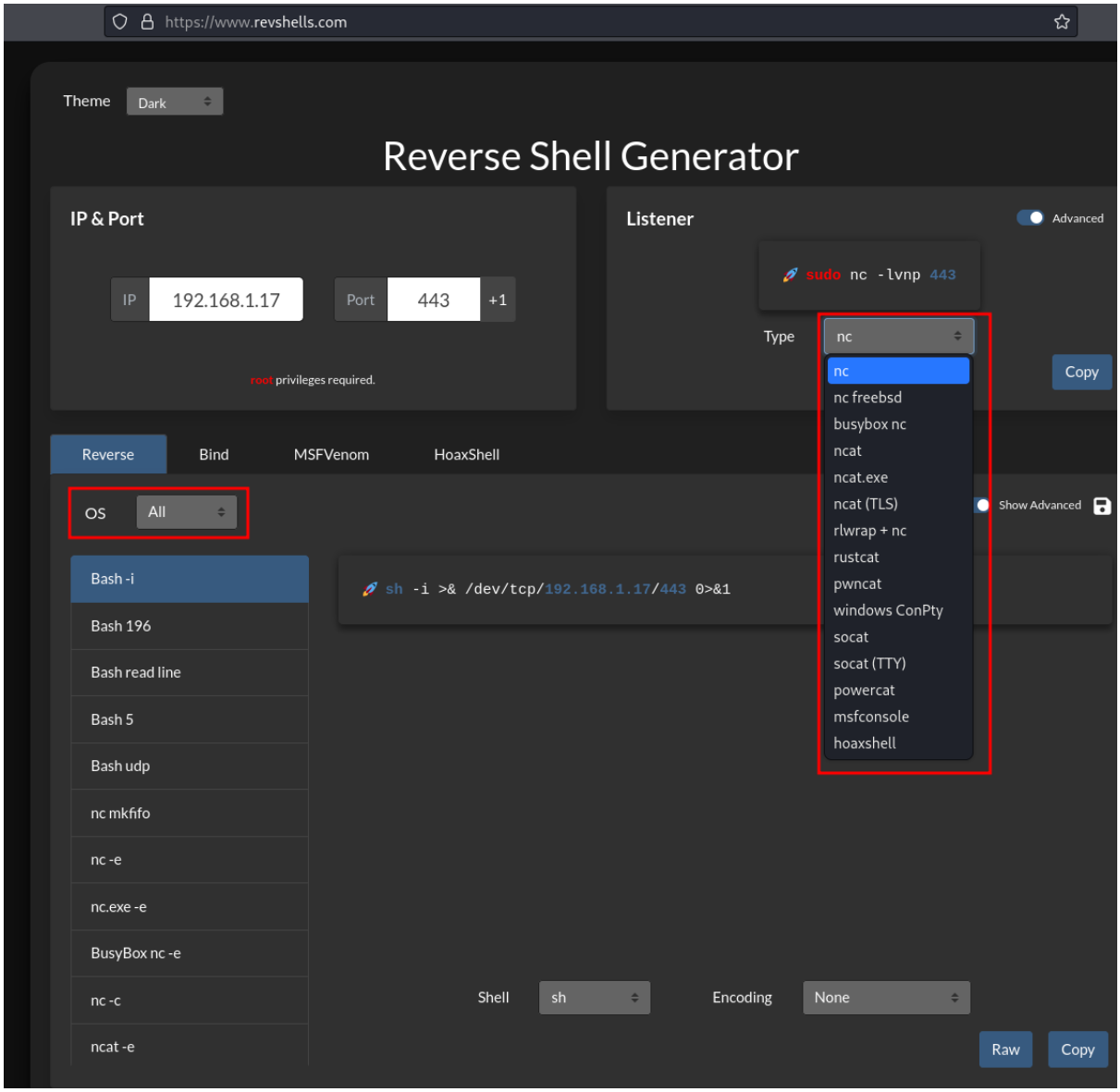
To Create a Reverse Shell, we need a reverse shell command and a listener command. And to generate that go to the following website:

Online Tool- Reverse Shell Generator -1

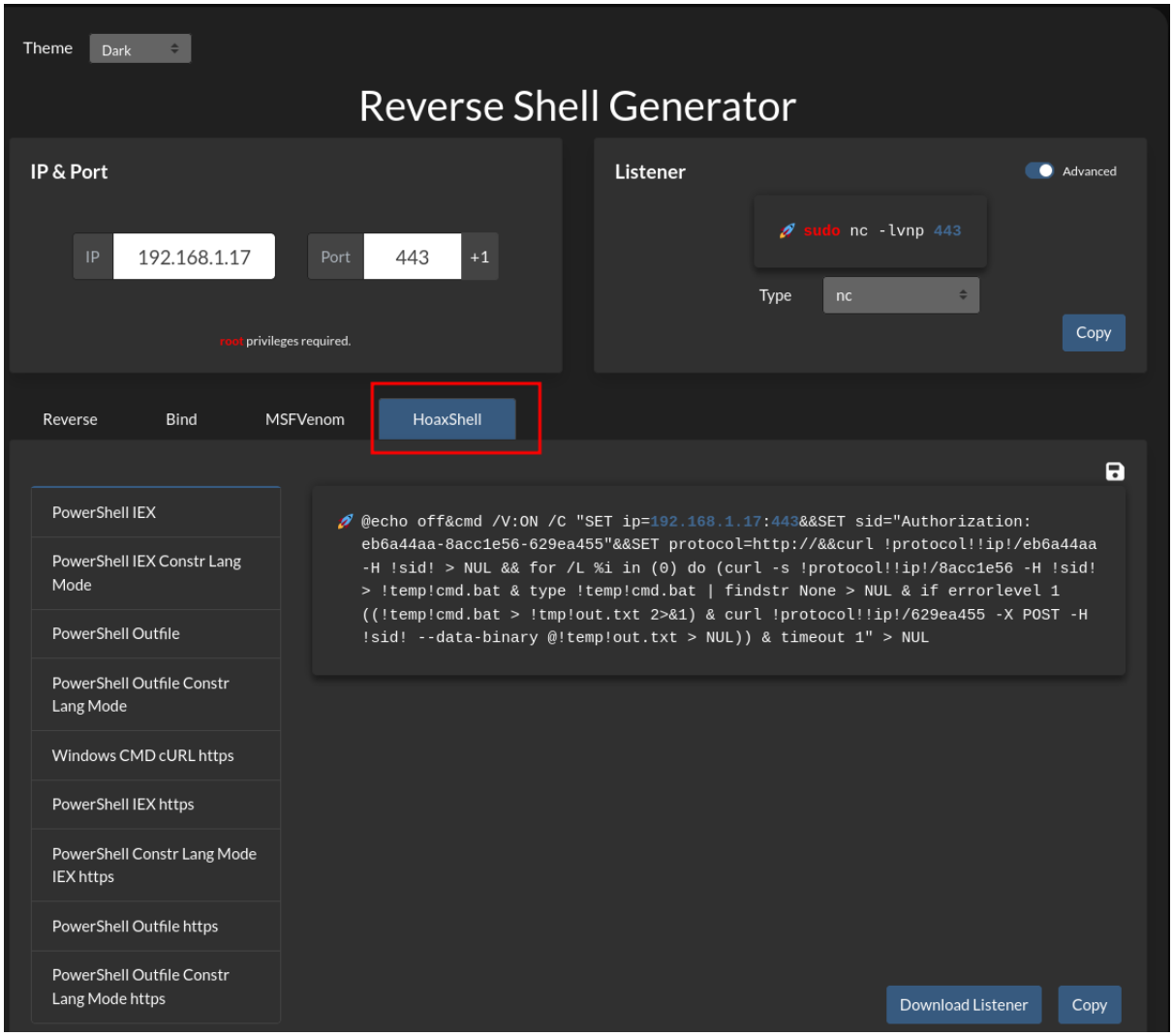
Once the www.revshells.com is loaded, give your Listerner IP <Attacker IP> address and Listener Port <Random Port>; as soon as you do this listener and reverse shell command will be generated as shown in the image below. Execute the reverse shell command on the victim's system and run the listener on your attacking machine. Once you do this, you will have your reverse shell.



As you can see in the image below, there are various options of the listener you can create such as powercat, busybox nc, socat, etc. Here we have created a netcat listenser. Even for the reverse shell we have options like bash, pearl, ruby, nc -c and many more.
From the image below you can also observe that you can create such reverse shell commands for all the operating systems such as Linux, Windows and Mac.



This Reverse Shell generator also provide us with the option to create Hoaxshell which is a powershell payload for windows. The same is shown in the image below:

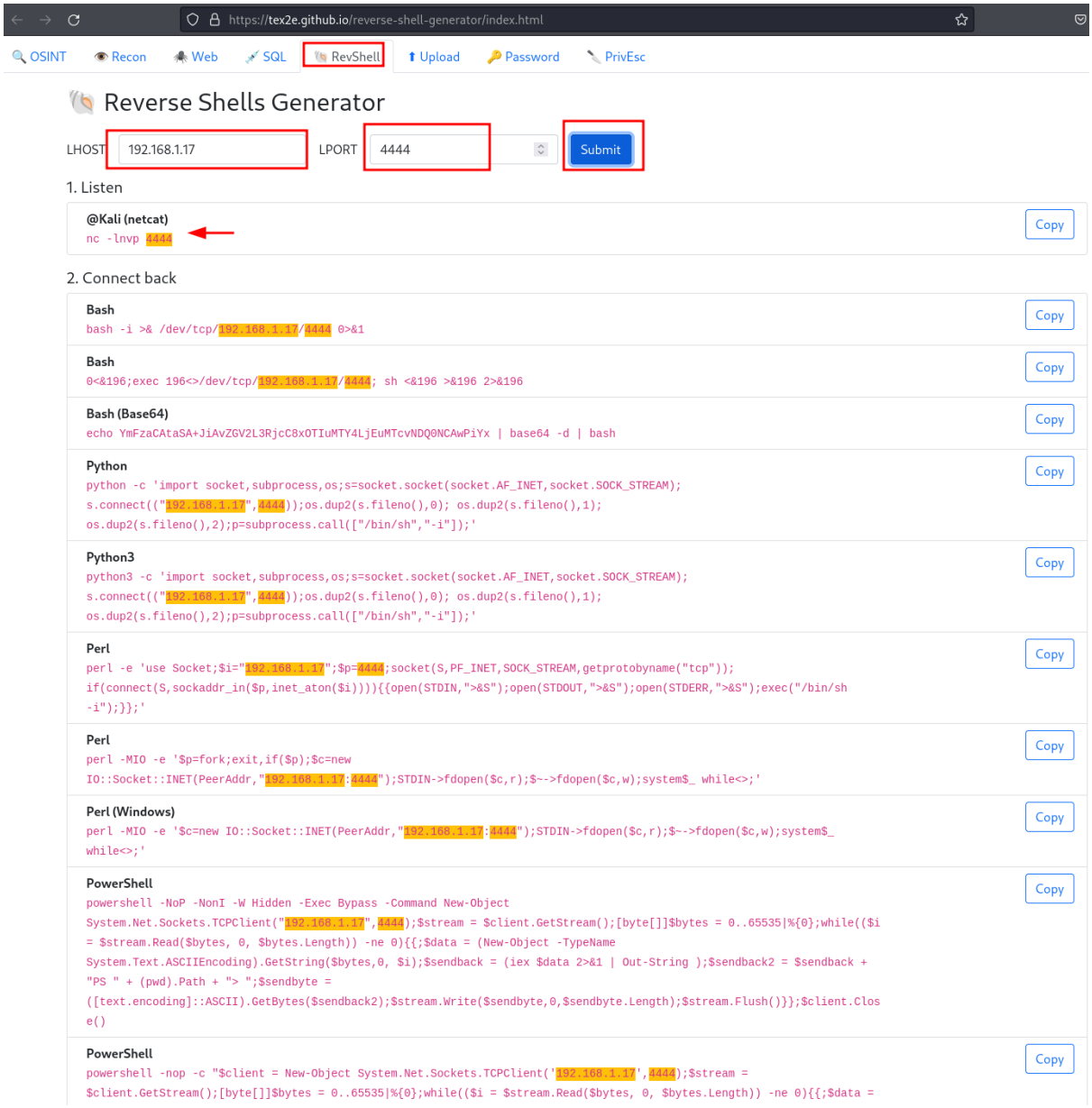


Reverse Shell Generator – 2

This is an amazing Online reverse shell generator. To use this generator, go to the following website:

https://tex2e.github.io/reverse-shell-generator/index.html

Once you are on the website, click on the '**RevShell'** from the menu bar. And then give your Local Host and Local Port as shown in the image below and then click on the 'Submit' button. After clicking on the submit button, you will have your listener. Simultaneously, it will also create multiple reverse shell commands for various Operating Systems as shown in the image below:

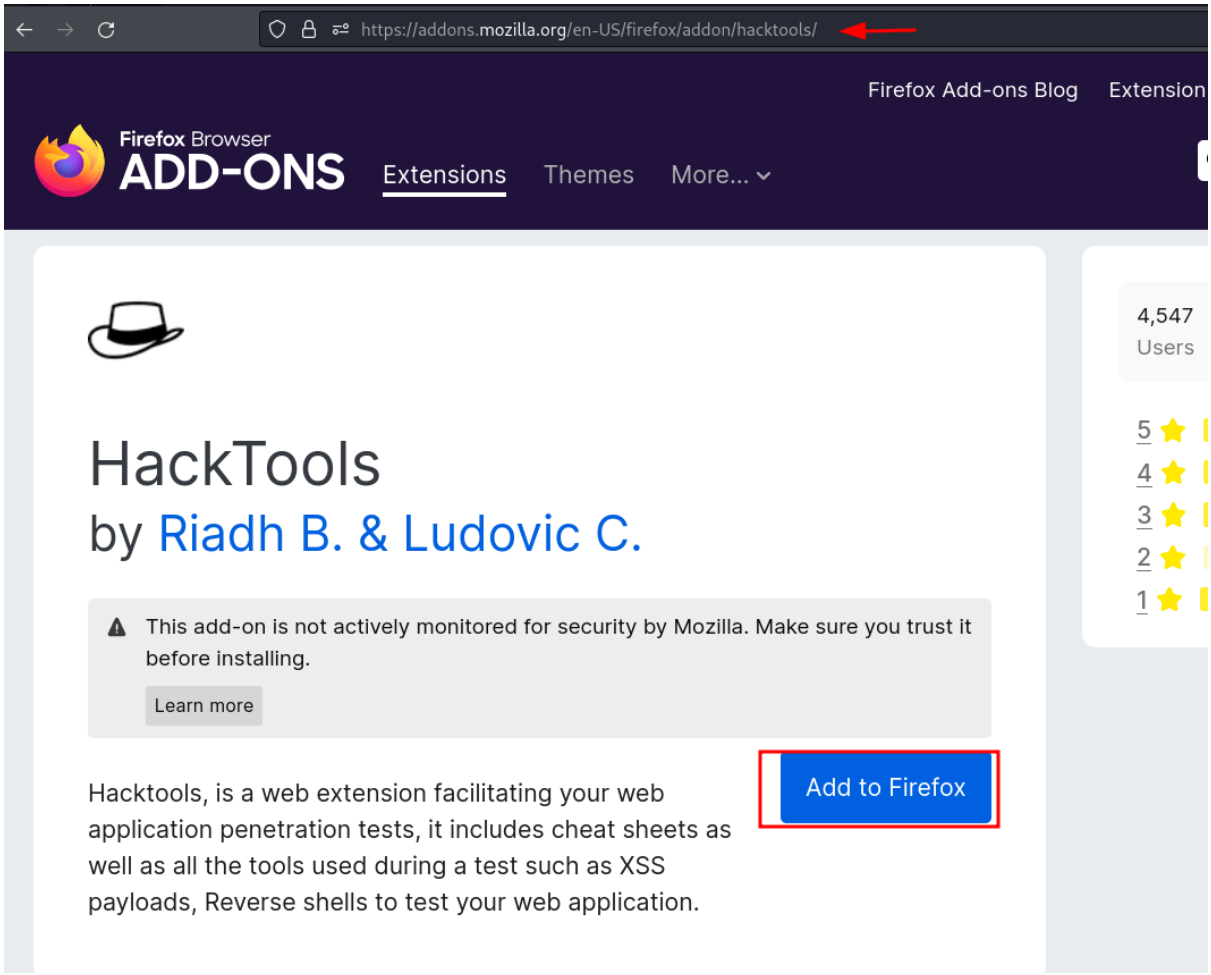


HackTool

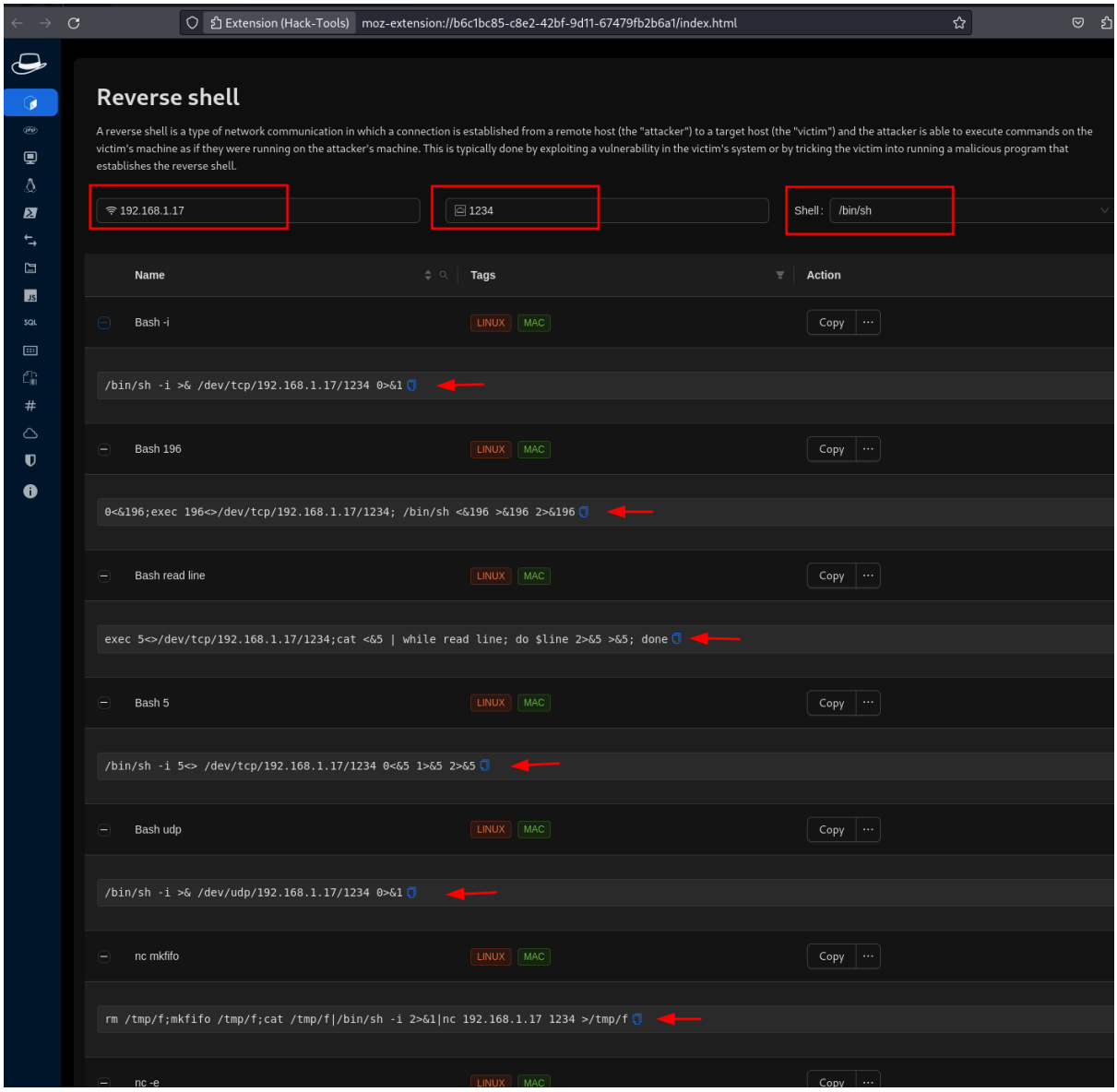
HackTools is an all-in-one browser extension designed for Red Team web pentesters. It streamlines web application penetration tests by providing cheat sheets and an array of essential tools, including XSS payloads, reverse shells, and more. This extension eliminates the need to search for payloads on different websites or in your local storage, offering one-click access to most tools.

Download the Hacktool extension from the following link :

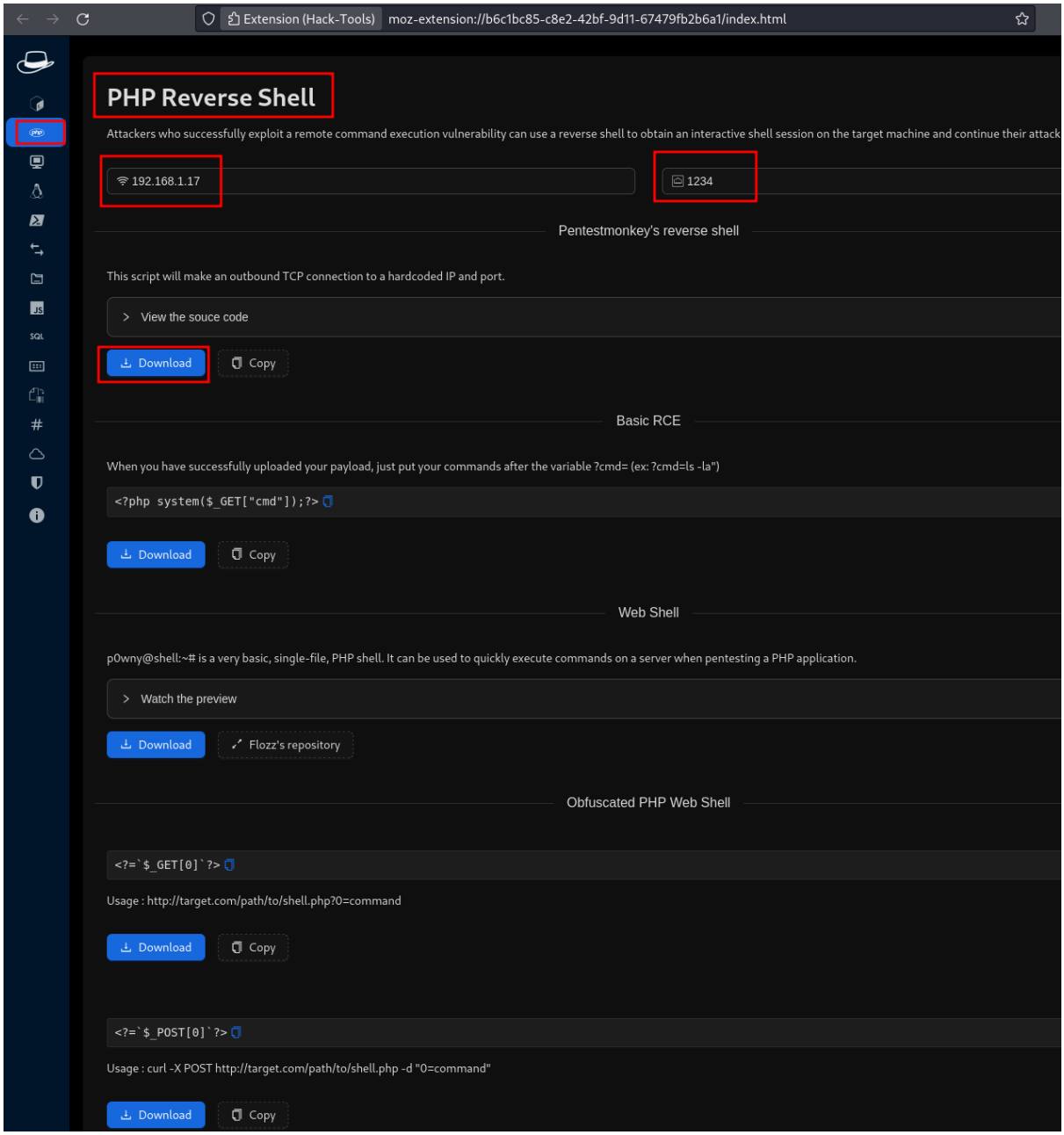
https://addons.mozilla.org/en-US/firefox/addon/hacktools/



Once the extension is downloaded, access it through the full screen option. From the side bar go to the Reverse Shell option and give you Local hot and Local Port along with the type of shell you want to create as shown in the image below. Once you do this, it will create various reverse shells for you to use as shown in the image below:



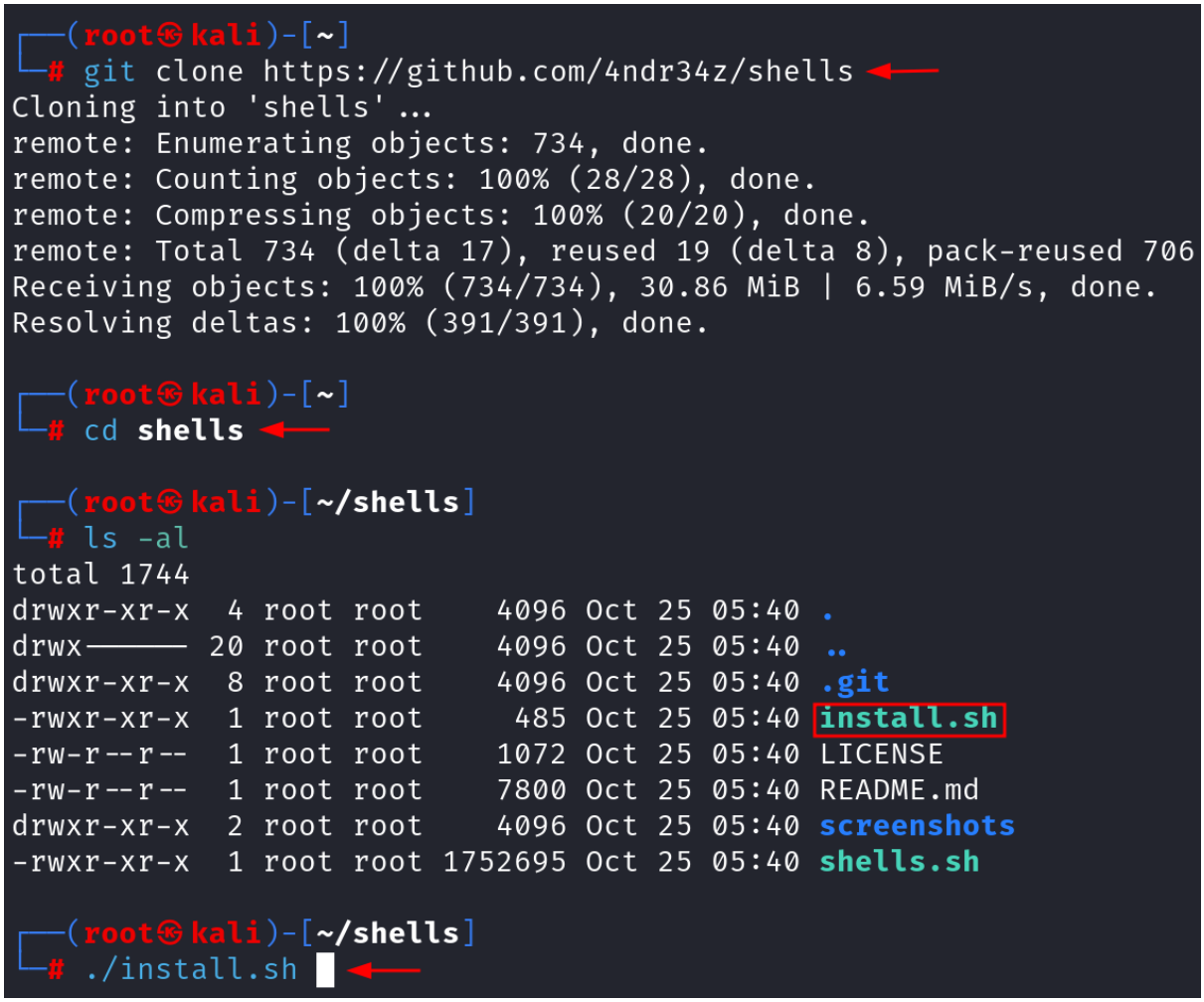
Through Hacktool, you can also create PHP Reverse shell by clicking on the second option on the side bar and give your Local host and Local Port. Now the extension will create various PHP reverse shell. You can simply download it and the run it on the victim's system and have a reverse shell.



Shellz

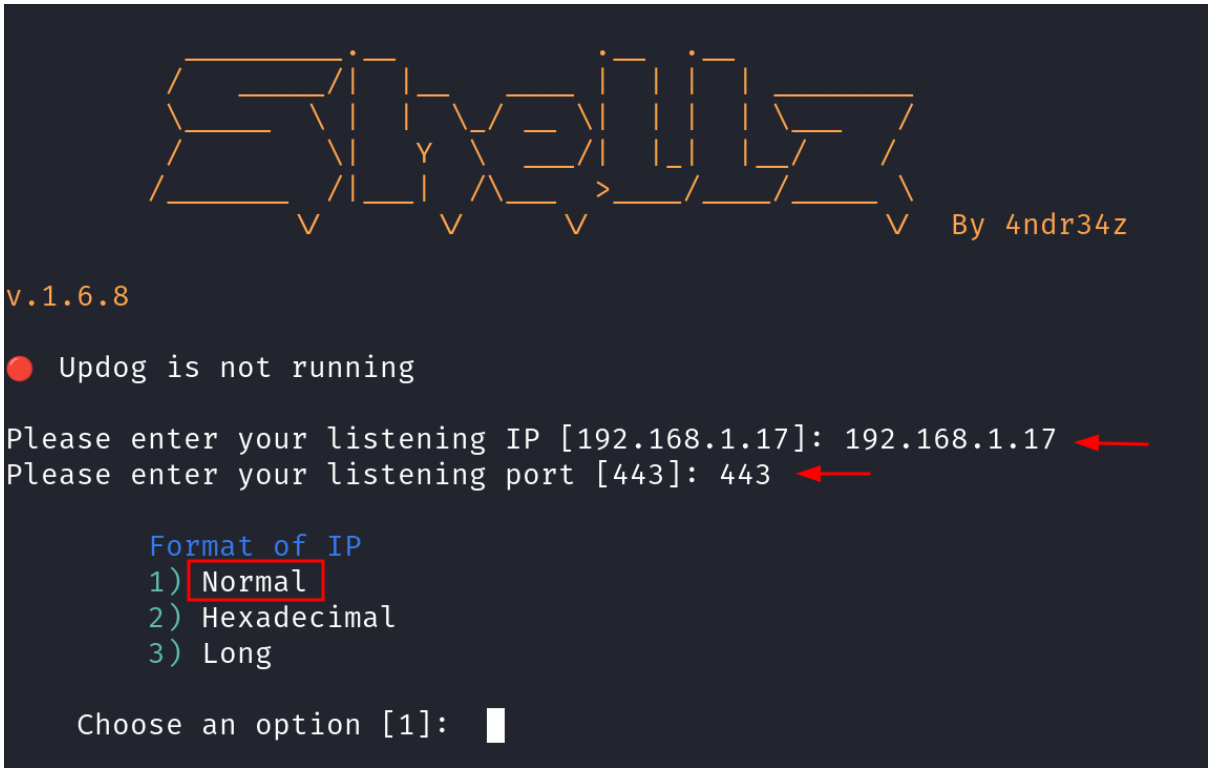
Shellz is a third-party tool which has made creating reverse shells a piece of cake. To download and install Shellz use the following set of commands as shown in the image below:

```
1. git clone https://github.com/4ndr34s/shells
2. cd shells
3. ./install.sh
```

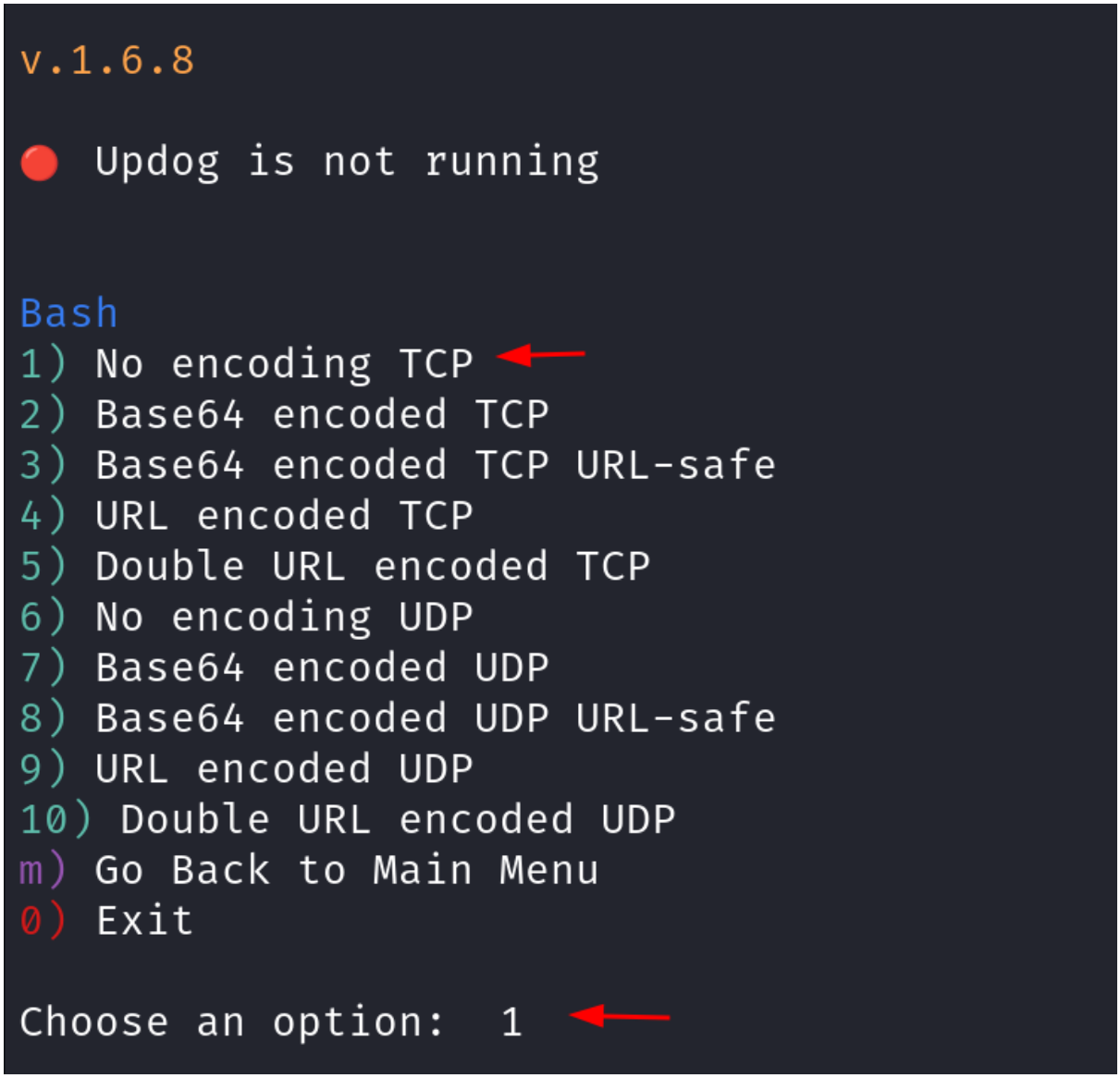


Once the tool is up and running, it will ask you about the type of reverse shell you want to create. As we wanted to create a bash shell, we chose the option 3 as shown in the image below:

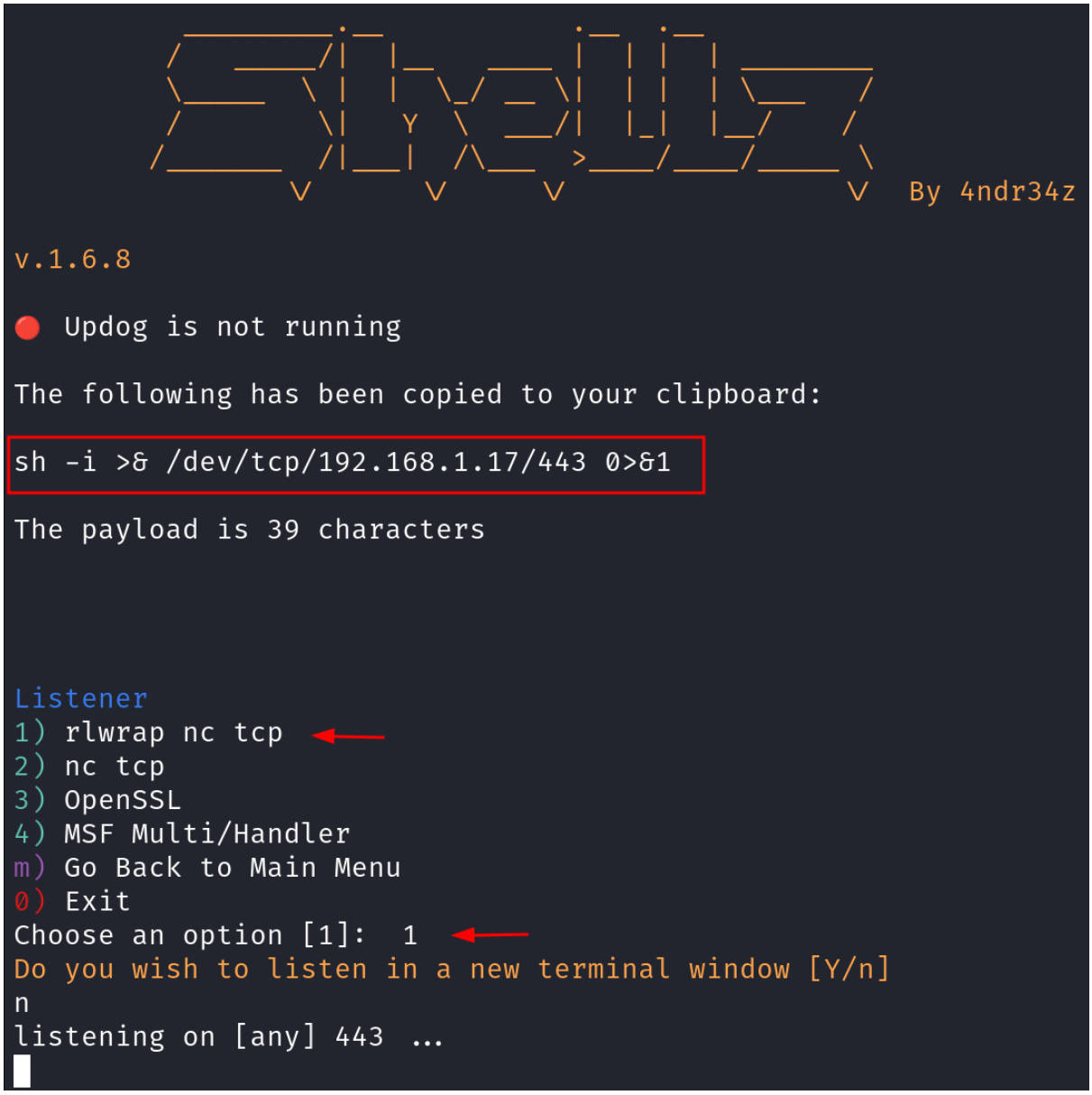
After choosing the type of shell you want to create, it will ask you for Local IP and Local Port. Now choose the type of your IP as shown in the image below:



After this, it will ask you to if you want to encode your shell. Choose whatever option you like as we did not want to encode our shell, we chose then **option 1** just like it shown in the image below:

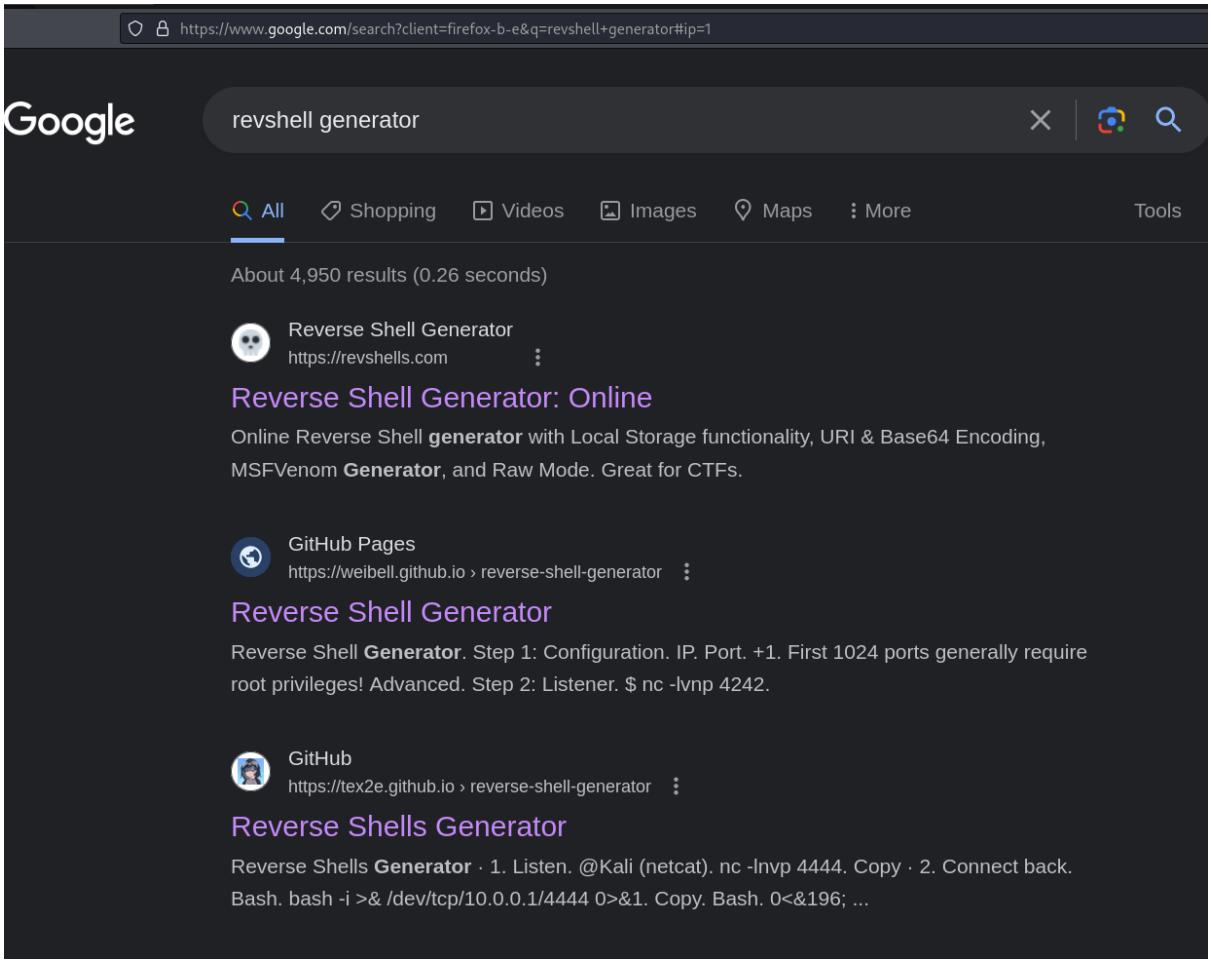


And finally, it will give you the reverse shell command that you can execute on you r victim's system. Then it will ask you the type of listener you want to create. Here, we chose netcat listener by typing in **number 1** as shown in the image below:



After this, you can tell the tool where you want your session which can be either same window or a new terminal window just like we have done it. Voila! You will have your session as shown in the image below:

To our knowledge, these were the best four easiest methods to create reverse shells. If you try and google reverse shell generator, it spat out multiple results which you can use too.



Just like shown in the image above, you can choose and try any method or website you like.

Mitigation

To defend against reverse shells, it's essential to implement strong security measures, including firewalls, intrusion detection systems, and regular software updates. Security professionals should monitor network traffic for suspicious activity and follow best practices for secure system administration.

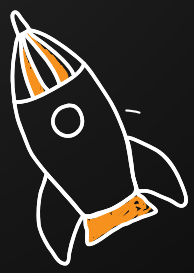
iGNITE Technologies

JOIN OUR TRAINING PROGRAMS

CLICK HERE

BEGINNER

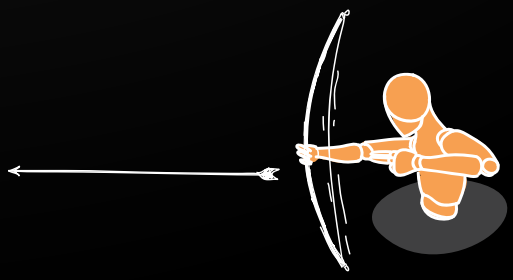
- Ethical Hacking
- Network Pentest
- Bug Bounty
- Wireless Pentest
- Network Security Essentials



ADVANCED

- Burp Suite Pro
- Android Pentest
- Web Services-API
- Advanced Metasploit
- Pro Infrastructure VAPT
- CTF
- Computer Forensics

EXPERT



- Red Team Operation
  - APT's - MITRE Attack Tactics
  - Active Directory Attack
  - MSSQL Security Assessment
- Privilege Escalation
  - Windows
  - Linux