



# Fishnet Framework

Ivan Nikolsky

Independent security researcher  
Founder and leader of the EntySec team



# Why Fishnet?

## Intuitive design

A simple and intuitive interface allows everybody to join the world of information security. The ability to launch scanners in few clicks, create a project or automatically and systematically solve a complex problem allows you to focus on more important tasks.

## Clear view

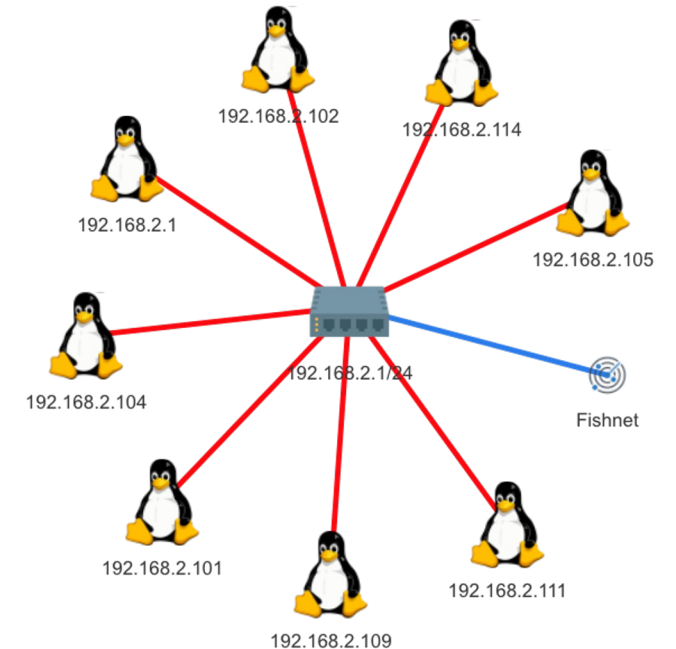
The complete absence of heaps, unnecessary pages and a bright and intrusive interface makes the tool easy to use. It does not distract your attention, and all the tools are sorted so that they are nearby if necessary. No reloads, all data is updated in real time without the need to reload the page.

## Multifunctional interface

There are lots of tools in a project that are aimed at completely different needs. You can scan networks and identify vulnerabilities, exploit them and observe external networks and resources.

## Isolated workspaces

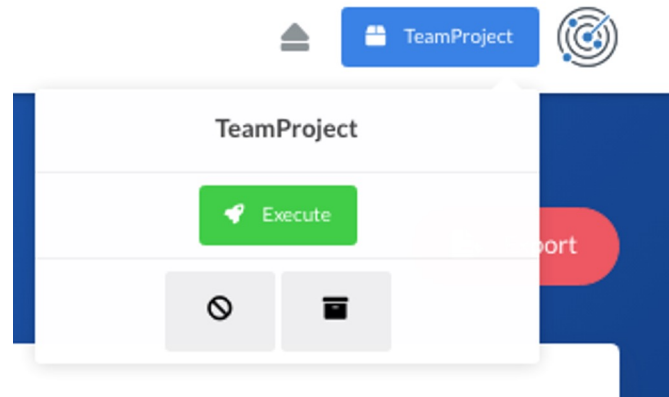
Observe network flaws in team or privately, isolated projects allow you to collaborate or work alone and won't let anybody else glance at your work.



# Is it flexible? Yes!

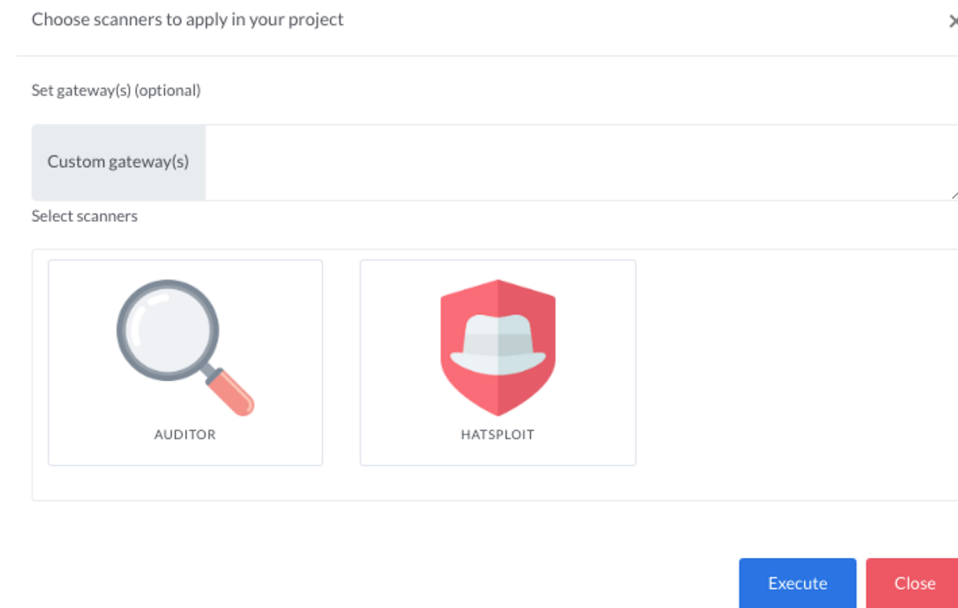
## Plugins

Expand Fishnet Framework functionality by adding custom scanners.



## Multiple checks at once

Execute multiple scanners at once on multiple targets, so less time will be spent. Just select scanners and click 'execute'.



# Where to use?

## Pentest / AD CTF

With Fishnet Framework it is much easier to explore the target network or system security flaws. Just set up Fishnet on your computer, create team and allow your mates to access the dashboard from their computers to begin the audit.

## Regular security audit

Fishnet is built not only for a professional pentester but for a regular user too, so anybody can find their network security flaws.

## RedTeam

The Fishnet Framework is easy to install and set up, and it automates all the critical checks that researchers need to perform, so less time is spent on tasks that could be done manually.



# Projects



Create a private project or team project

Fishnet projects

Active Archived

Active projects Create Project

Show  entries Search:

Name	Author	Team	Category	UUID	Action
Pentest1	admin		network	c57ffb49-751c-4572-acf0-2f4beeb06fd3	
TeamProject	admin	OffZone2022	network	19e2474e-4a6e-4f78-b2ac-b69e5737af36	

Showing 1 to 2 of 2 entries Previous 1 Next

# Collaboration



Create a team and do penetration testing with your mates

Create or manage your teams in pop-up menus

New team ×

Create a new Fishnet team

TEAM NAME  
OffZone2022

Team purpose

Users

Pentest

Mary Esina (Mariesowl)  
thecakeisfalse

Create Close

Fishnet teams ×

These are all teams created

Show  entries Search:

Name	Purpose	Leader	Participants	Action
OffZone2022	pentest	admin	2	

Showing 1 to 1 of 1 entries

Previous **1** Next

Close

# Collect statistics



**Fishnet** Dashboard Topology 9 Services Flaws 1 Attack Sessions Pentest1

### Dashboard

Pentest1 Dashboard Export

#### Audit statistics

1 Networks    9 Hosts    1 Flaws

#### Platforms

#### Flaws

#### Scan totals

SCANNED HOSTS: 9  
HOSTS LEFT: 0

Scanned    Not scanned

#### Recent vulnerabilities

Export

Name	Family	Host	Port	Rank	Action
Raspbian Default SSH Credentials	linux	192.168.2.115	22 ssh	Medium	

#### Active sessions

0

#### Hosts detected

Show  entries    Search:

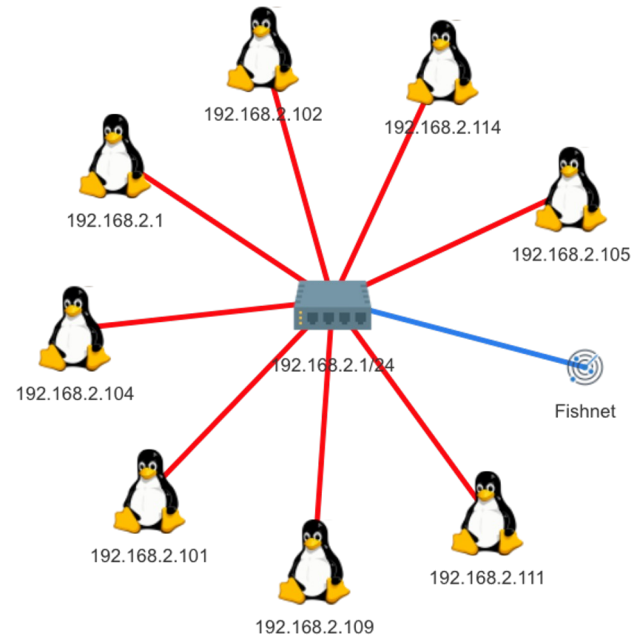
Host	Gateway	DNS	Platform	Vendor	Action
------	---------	-----	----------	--------	--------

# Clear diagrams

Pie charts



Network topology





Maps





# Managing vulnerabilities



Name	Family	Host	Port	Rank	Action
Raspbian Default SSH Credentials	linux	192.168.2.115	22 ssh	Medium	 



## Flaw details

### Flaw specification

Raspbian Default SSH Credentials **Medium**  
Bypass Raspberry PI SSH authorization using Raspbian default SSH password.

### Targets



Attack interface

Attack options

BLINDER no	PAYLOAD unix/generic/bash_reverse_tcp	LHOST 0.0.0.0
LPORT 8888	ENCODER ENCODER	RHOST 192.168.1.63
RPORT 8888		

Attack log Export

Execute

# Attack vulnerable devices



**Fishnet** Dashboard Topology 9 Services Flaws 1 Attack Sessions 1 Pentest1

Pentest1 Attack

Attack interface

Raspbian Default SSH Credentials Execute

Attack options

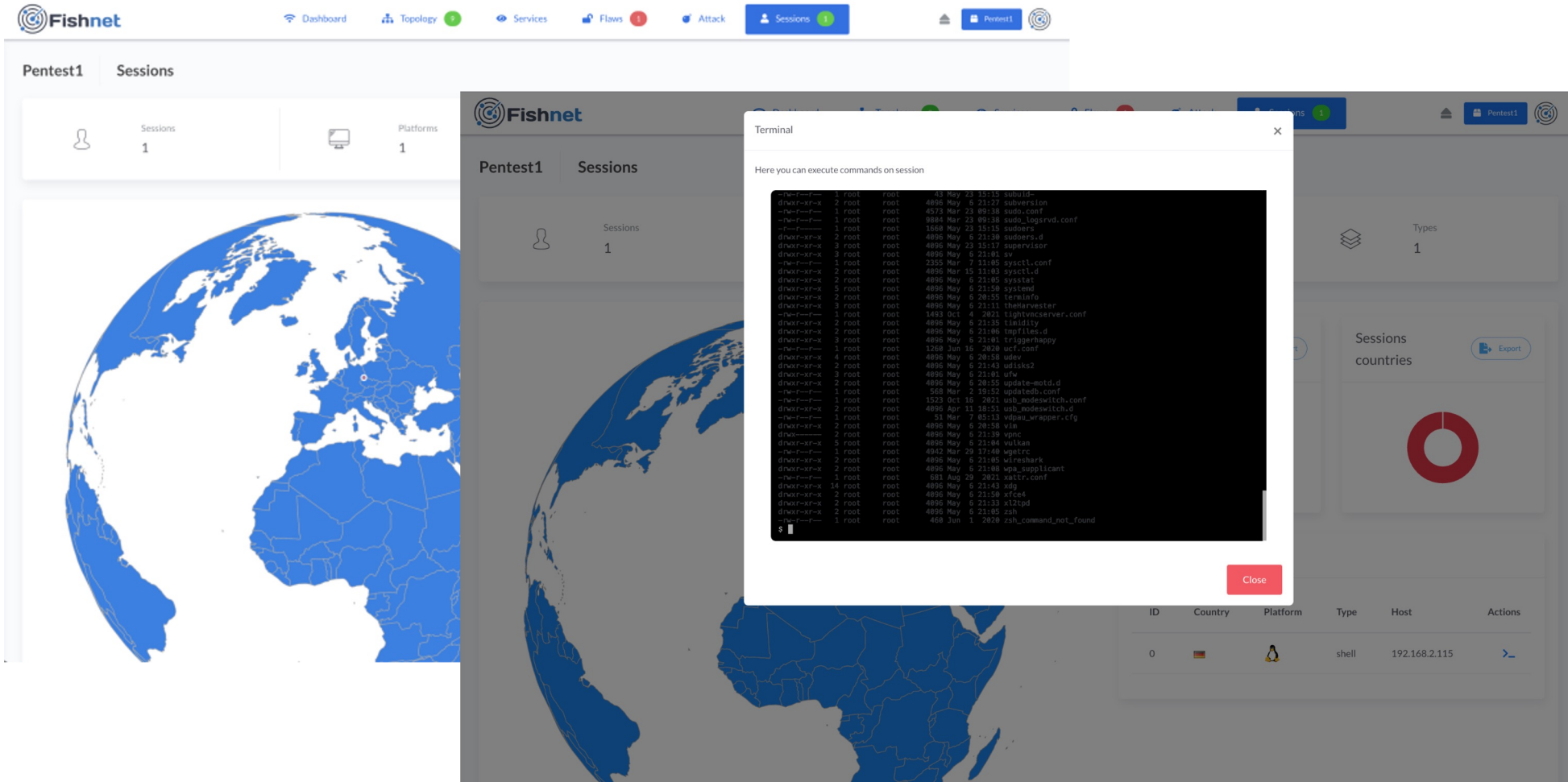
HOST 192.168.2.115	PORT 22	BLINDER no
PAYLOAD unix/generic/bash_reverse_tcp	LHOST 0.0.0.0	LPORT 8888

Attack log Export

```
[*] Exploiting 192.168.2.115...
[*] Sending payload stage (74 bytes)...
[*] Starting TCP listener on port 8888...
[*] Establishing connection (192.168.2.115:35474 -> 0.0.0.0:8888)...
[+] Shell session 0 opened at 2022-08-11 14:12:51 UTC!
[+] Exploit module completed!
```

Fishnet © Fishnet - developed by EntySec

# Manage sessions



**Fishnet** Dashboard | Topology | Services | Flaws | Attack | Sessions | Pentest1




**Pentest1 Sessions**

Sessions: 1 | Platforms: 1

Types: 1

Sessions countries

Export

ID	Country	Platform	Type	Host	Actions
0			shell	192.168.2.115	

```
Terminal
Here you can execute commands on session

dhn0r-xvnx 1 root root 4899 May 23 21:15 subd0l
dhn0r-xvnx 2 root root 4899 May 6 21:27 subv3r510n
dhn0r-xvnx 1 root root 4572 Mar 23 49:38 sudo.conf
dhn0r-xvnx 1 root root 9884 Mar 23 49:38 sudo_logrwd.conf
dhn0r-xvnx 1 root root 1688 May 23 15:15 sud0rs
dhn0r-xvnx 2 root root 4899 May 6 21:28 sud0rs.d
dhn0r-xvnx 3 root root 4899 May 23 15:17 supervisor
dhn0r-xvnx 3 root root 4899 May 6 21:01 sv
dhn0r-xvnx 1 root root 2355 Mar 7 11:05 systcl.conf
dhn0r-xvnx 2 root root 4899 Mar 15 11:03 systcl.d
dhn0r-xvnx 2 root root 4899 May 6 21:05 systcl1
dhn0r-xvnx 3 root root 4899 May 6 21:28 systclm
dhn0r-xvnx 2 root root 4899 May 6 20:53 t3rnslf3
dhn0r-xvnx 3 root root 4899 May 6 21:11 th3Harv3st3r
dhn0r-xvnx 1 root root 1493 Oct 4 2021 t1gtr0v3r53rv3r.conf
dhn0r-xvnx 2 root root 4899 May 6 21:35 t1d1ly
dhn0r-xvnx 2 root root 4899 May 6 21:06 t3pfil3s.d
dhn0r-xvnx 1 root root 4899 May 6 21:06 t1g3rph3pp3
dhn0r-xvnx 1 root root 1258 Jun 16 20:58 t3cf.conf
dhn0r-xvnx 4 root root 4899 May 6 20:58 t3d3v
dhn0r-xvnx 2 root root 4899 May 6 21:03 t3d1s32
dhn0r-xvnx 2 root root 4899 May 6 21:01 t1w
dhn0r-xvnx 2 root root 4899 May 6 20:55 updat3-mtd.d
dhn0r-xvnx 1 root root 1508 Mar 2 19:52 updat3nb.conf
dhn0r-xvnx 1 root root 1523 Oct 16 2021 usb_n0d3switch.conf
dhn0r-xvnx 1 root root 4899 Apr 11 18:51 usb_n0d3switch.d
dhn0r-xvnx 1 root root 53 Mar 7 05:13 w0p0n_wrapp3r.cfg
dhn0r-xvnx 2 root root 4899 May 6 20:58 v1w
dhn0r-xvnx 2 root root 4899 May 6 21:39 vpmc
dhn0r-xvnx 5 root root 4899 May 6 21:04 w0ll3m
dhn0r-xvnx 1 root root 4942 Mar 29 17:46 w0p0strc
dhn0r-xvnx 2 root root 4899 May 6 21:05 w1reshark
dhn0r-xvnx 1 root root 4899 May 6 21:06 w0p0_applic3nt
dhn0r-xvnx 1 root root 681 Aug 9 2021 x1t1r.conf
dhn0r-xvnx 14 root root 4899 May 6 21:43 x3g
dhn0r-xvnx 2 root root 4899 May 6 21:29 x1c04
dhn0r-xvnx 2 root root 4899 May 6 21:11 x1t1p.d
dhn0r-xvnx 2 root root 4899 May 6 21:05 x3h
dhn0r-xvnx 1 root root 488 Jun 1 2020 x3h_c0mm3nt_n0t_f0und
$
```



# Questions?

- Ivan Nikolsky  
<https://github.com/enty8080>
- EntySec  
<https://github.com/EntySec>
- Fishnet Framework  
<https://github.com/Fishnet>





**NO  
OFF  
ONE  
2022**