

# PENTESTER ACADEMY

## Pentesting automation with **Reconmap**

Santiago Lizardo

September 4, 2021

## About the presenter



- ▶ Reconmap's founder
- ▶ +20 years doing software engineering
- ▶ Cyber security enthusiast
- ▶ <https://github.com/santiagolizardo>

# Reconmap's origin

## Pentesting pain points

- ▶ Repetition
- ▶ Ineffective collaboration
- ▶ Ineffective communication

# Reconmap's mission

Reconmap's mission is to accelerate the time it takes to do vulnerability assessment and pentesting, through the use of templating, automation and machine learning. From weeks to days, or days to hours.

# Reconmap's approach

- ▶ Templates to avoid repetition
- ▶ Automation and ML to speed up the process

## Result:

Pentesters spending more time doing research, and less time doing repetitive, boring, tedious work such as parsing files manually or creating handcrafted pentest reports for their clients.

# Reconmap's Today - September 2021

- ▶ 1 year old
- ▶ Open source and SaaS
- ▶ Small but growing community
- ▶ Used in production by people around the world

# Recomap's feature set













- ▶ Client, project, tasks management all in one.
- ▶ Reusable project and vulnerability templates
- ▶ Automatic pentest report generation (HTML, PDF, DOCX)
- ▶ Command line interface (CLI) and Rest API
- ▶ Integrated browser terminal
- ▶ Can scale to teams and projects of any size.
- ▶ Stats dashboard, user roles, documents, markdown, audit log, integrated search, tagging, data import/export, ...

# Pentesting step by step with Reconmap

1. Create client
2. Create project from scratch or template
3. Complete tasks in the project. Some might require running command automation.
4. Try exploit the vulnerabilities found
5. Generate report for client and share



# Step 1: Setup client

Clients					
Name	URL	Contact name	Contact email	Contact phone	
 Insecure Co.	<a href="http://in.se.cure">http://in.se.cure</a> 	John Doe	John.Doe@in.se.cure	+99 123 245 389	Edit 
 The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a> 	N/A	N/A	+1 951-692-7703	Edit 
 test	<a href="test">test</a> 	test	test@test.test	01	Edit 
 asdf	<a href="http://asdf.de">http://asdf.de</a> 	foo	foo@foo.de	1233245345	Edit 

# Step 1: Setup client

## Clients

Name	URL
Insecure Co.	<a href="http://in.se.cu">http://in.se.cu</a>
The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a>
test	<a href="#">test</a>
asdf	<a href="http://asdf.de">http://asdf.de</a>

Client

The OWASP Foundation

Details

Client's projects

Properties

Name

The OWASP Foundation

URL

<https://owasp.org>

Contact name

N/A

Contact email

N/A

Contact phone

+1 951-492-7703

Relations

Created by

Jane Doe

Timestamps

Created

3 weeks ago

Edit

Edit

Edit

Edit

# Step 1: Setup client

## Clients

Name	URL
Insecure Co.	<a href="http://in.se.cu">http://in.se.cu</a>
The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a>
test	<a href="#">test</a>
asdf	<a href="http://asdf.de">http://asdf.de</a>

### Client

#### The OWASP Foundation

Details Client's projects

#### Properties

Name The OWASP Foundation

URL <https://owasp.org>

Contact name

N/A

Contact email

N/A

Contact phone

+1 961-492-7703





#### Relations

Created by

## Users and Permissions

	Full name	Username	Role
<input type="checkbox"/>	Jane Doe	admin	administrator
<input type="checkbox"/>	Lead pentester	su	superuser
<input type="checkbox"/>	Infosec pro	user	user
<input type="checkbox"/>	Dear Customer	cust	client

## Step 2: Setup project

Project templates			
Name	Description	Number of tasks	
 Linux host template	Project template to show general linux host reconnaissance tasks	3	<a href="#">+ Clone and edit</a> <a href="#">Edit</a> <a href="#">Delete</a>
 Bounty Hunter Methodology	The Bug Bounty Hunter Methodology v3 by @jhaddix	11	<a href="#">+ Clone and edit</a> <a href="#">Edit</a> <a href="#">Delete</a>
 Sayaan Alam's bug hunting list	Bug hunting - List of tasks created by Sayaan Alam (@ehsayaan). A very systematic...	24	<a href="#">+ Clone and edit</a> <a href="#">Edit</a> <a href="#">Delete</a>
 Webapp pentesting project by <a href="https://hackercombat.com/">https://hackercombat.com/</a>		26	<a href="#">+ Clone and edit</a> <a href="#">Edit</a> <a href="#">Delete</a>

# Step 2: Setup project

The screenshot shows the 'WebGoat (test project)' configuration page in Burp Suite. The interface is dark-themed. At the top, there's a breadcrumb 'Projects' and a set of action buttons: 'Edit', 'Generate Report', 'Manage Members', 'Archive', and 'Delete'. Below this, the project name 'WebGoat (test project)' is displayed with a 'Project' tag. A sidebar on the left lists various project components: 'Name', 'Details', 'Targets', 'Tasks', 'Vulnerabilities', 'Notes', and 'Attachments'. The 'Details' tab is active, showing 'Project details' on the left and 'Relations' and 'Timestamps' on the right. The 'Project details' section includes fields for 'Visibility' (set to 'Private'), 'Status' (set to 'Active'), and 'Description' (a paragraph about WebGoat being an insecure application for testing vulnerabilities). The 'Relations' section shows the 'Client' as 'The OWASP Foundation' and 'Created by' as 'Jane Doe'. The 'Timestamps' section shows the project was 'Created' '3 weeks ago'. On the far right, there are three red trash icons for deleting the project, its client, and its creator.

Projects

Edit Generate Report Manage Members Archive Delete

Project

WebGoat (test project)

Name Details Targets Tasks Vulnerabilities Notes Attachments

Project details

Visibility Private

Status Active

Description

WebGoat is a deliberately insecure application that allows interested developers just like you to test vulnerabilities commonly found in Java-based applications that use common and popular open source components.

Relations

Client

The OWASP Foundation

Created by

Jane Doe

Timestamps

Created

3 weeks ago

## Step 2: Setup project

The screenshot displays a web application security tool interface. At the top, a navigation bar shows 'Projects' with a back arrow, and buttons for 'Edit', 'Generate Report', 'Manage Members', 'Archive', and 'Delete'. Below this, a project selection dropdown shows 'WebGoat (test project)'. The main content area is titled 'Web server pentest project' and has tabs for 'Details', 'Targets', 'Tasks', 'Vulnerabilities', 'Notes', and 'Attachments'. The 'Tasks' tab is active, showing a list of tasks with columns for Summary, Description, Assignee, Status, and Command. A '+ Add task' button is in the top right of the task list.

Summary	Description	Assignee	Status	Command	
Nessus		(nobody)	Done	nessus	Edit Delete
Run port scanner	Use nmap to detect all open ports	Lead pentester	Doing	nmap	Edit Delete
Run SQL injection scanner	Use sqlmap to test the application for SQL injecti...	(nobody)	Todo	sqlmap	Edit Delete
Check domain expiration date	Use whois or other tools to check when the doma...	(nobody)	Todo	whois	Edit Delete

# Step 3: Complete tasks and commands

Command

Nmap

network

DetailsRun instructionsTerminal

Instructions

1. Fill in the arguments

Host

scanme.nmap.org

2. Executermapon any terminal

Make sure you have a copy of **nmap** on a machine you trust. Download the CLI for MacOS/Linux and Windows from [Github](#).

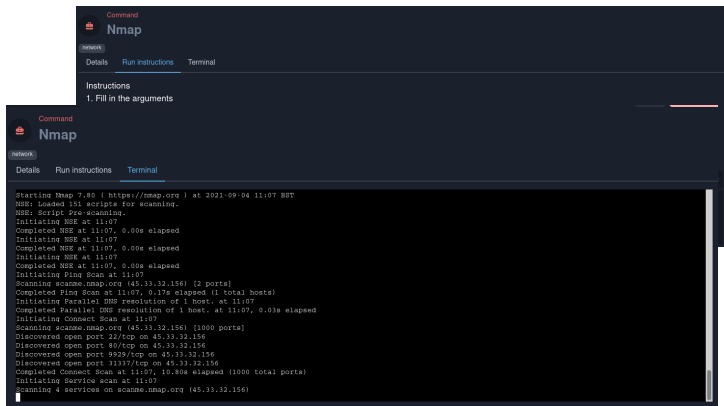
Once **nmap** is within reach execute the command shown below.

```
$ ./nmap command run -cld 2 -var Host=scanme.nmap.org
```

How does it work?

Reconmap will invoke the command **Nmap** from a **instrumentisto:nmap** container using the arguments `-v {{{Host|scanme.nmap.org}}}` `-oX nmap-output.xml` and upload the results to this server for analysis.

# Step 3: Complete tasks and commands















The image shows two overlapping windows from the Nmap application. The top window displays the 'Instructions' tab, which contains the text: '1. Fill in the arguments'. The bottom window displays the 'Terminal' tab, showing the output of an Nmap scan. The terminal text is as follows:


```
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-04 11:07 BST
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating NSE at 11:07
Completed NSE at 11:07, 0.00s elapsed
Initiating Ping Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [2 ports]
Completed Ping Scan at 11:07, 0.17s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:07
Completed Parallel DNS resolution of 1 host. at 11:07, 0.03s elapsed
Initiating Connect Scan at 11:07
Scanning scanme.nmap.org (45.33.32.156) [1000 ports]
Discovered open port 22/tcp on 45.33.32.156
Discovered open port 80/tcp on 45.33.32.156
Discovered open port 9929/tcp on 45.33.32.156
Discovered open port 31337/tcp on 45.33.32.156
Completed Connect Scan at 11:07, 10.80s elapsed (1000 total ports)
Initiating Service scan at 11:07
Scanning 4 services on scanme.nmap.org (45.33.32.156)
```







## Step 4: Verify exploitable vulnerabilities


Clients					
Name	URL	Contact name	Contact email	Contact phone	
 Insecure Co.	<a href="http://in.se.cure">http://in.se.cure</a> 	John Doe	John.Doe@in.se.cure	+99 123 245 389	Edit 
 The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a> 	N/A	N/A	+1 951-692-7703	Edit 
 test	<a href="test">test</a> 	test	test@test.test	01	Edit 
 asdf	<a href="http://asdf.de">http://asdf.de</a> 	foo	foo@foo.de	1233245345	Edit 

# Step 4: Verify exploitable vulnerabilities

 Clients

Name	URL
 Insecure Co.	<a href="http://in.se.cu">http://in.se.cu</a>
 The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a>
 test	<a href="#">test</a>
 asdf	<a href="http://asdf.de">http://asdf.de</a>

Client

 The OWASP Foundation

Details


Client's projects

Properties


Name	The OWASP Foundation
URL	<a href="https://owasp.org">https://owasp.org</a>
Contact name	N/A
Contact email	N/A
Contact phone	+1 951-492-7703

Relations

Created by

 Jane Doe

Edit




Timestamps

Created

3 weeks ago

Edit



# Step 4: Verify exploitable vulnerabilities

## Clients

Name	URL
Insecure Co.	<a href="http://in.se.cu">http://in.se.cu</a>
The OWASP Foundation	<a href="https://owasp.org">https://owasp.org</a>
test	<a href="#">test</a>
asdf	<a href="http://asdf.de">http://asdf.de</a>

Client

The OWASP Foundation

Details

Client's projects

Properties

Relations

Name

The OWASP Foundation

URL

<https://owasp.org>

Contact name

[https://owasp.org](#)

Contact email

N/A

Contact phone

+1 961-492-7703

## Users and Permissions

	Full name	Username	Role
	Jane Doe	admin	administrator
	Lead pentester	su	superuser
	Infosec pro	user	user
	Dear Customer	cust	client

# Step 5: Generate pentest report

Project reporting

Project report

PreviewRevisionsConfiguration

- The remote storage was not properly secured having the local, host and remote network cannot be reached anymore by the scanner.
- This scanner may have been blacklisted by the system administrator or by an automatic intrusion detection / prevention system that detected the scan.
- The remote host is now down, either because a user turned it off during the scan or because a select denial of service was effective.

In any case, the audit of the remote host might be incomplete and may need to be done again.

**Signing is disabled on the remote SMB server.**

**Solution**

Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'Server signing'. See the [see also](#) links for further details.

Severity	Medium
Category	Undefined
CVSS score	5.0

Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.

# Step 5: Generate pentest report

The screenshot displays the 'Project reporting' interface, specifically the 'Project report' page. The page has a dark theme with a sidebar on the left containing 'Preview', 'Revisions', and 'Configuration' tabs. The main content area shows a 'New report version' form with fields for 'Name' (containing 'log 1.0 - 202103') and 'Description' (containing 'log initial version, Draft'). Below the form is a 'Save version' button. A table lists the 'Report versions' with columns for 'Name (Description)', 'Datetime', and 'Downloads'. The table contains three entries: '1.2 reviewed | Report reviewed and sent to the client' (1 week ago), '1.1 ( Initial version after corrections )' (2 weeks ago), and '1.0 ( Initial version )' (3 weeks ago). Each entry has 'HTML' and 'PDF' download links, a 'Send by email' button, and a 'Delete' button.

**Project reporting**  
**Project report**

Preview Revisions Configuration

**New report version**

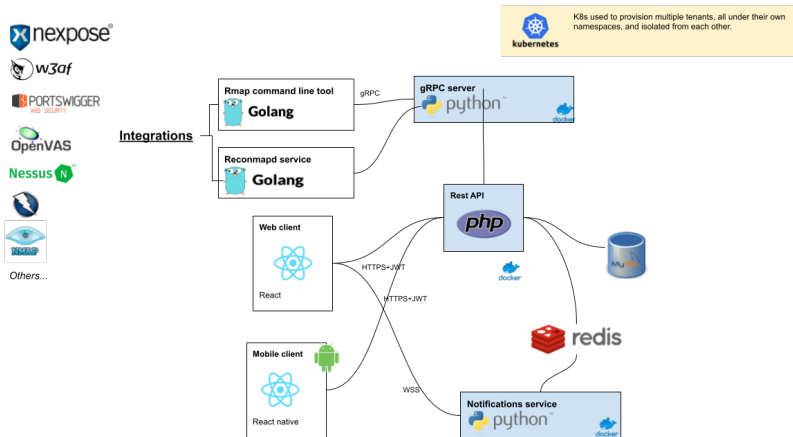
Name  
log 1.0 - 202103

Description  
log initial version, Draft

Save version

Name (Description)	Datetime	Downloads
1.2 reviewed   Report reviewed and sent to the client	1 week ago	<a href="#">HTML</a> <a href="#">PDF</a> <a href="#">Send by email</a> <a href="#">Delete</a>
1.1 ( Initial version after corrections )	2 weeks ago	<a href="#">HTML</a> <a href="#">PDF</a> <a href="#">Send by email</a> <a href="#">Delete</a>
1.0 ( Initial version )	3 weeks ago	<a href="#">HTML</a> <a href="#">PDF</a> <a href="#">Send by email</a> <a href="#">Delete</a>

# Architecture



# Coming features

- ▶ Complex workflows (reviewers)
- ▶ Independent customer's portal
- ▶ Secret management
- ▶ More integrations

# How to get started?

## Manual setup

Follow [setup instructions](#)

Requires significant time to  
install and maintain  
Community support (chat)

## SaaS

[Affordable hosting](#)

Ready in minutes  
Technical support (phone,  
email, chat)  
Always latest version



# Staying in touch



- ▶ [Github](#) community
- ▶ [Twitter](#) updates
- ▶ [Facebook](#)
- ▶ [Gitter](#) chat

## Pentester academy

- ▶ [DamianGoh13](#)
- ▶ [Pentesteracademy.com](#)