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, ...

Who is it for?

Any InfoSec professional:

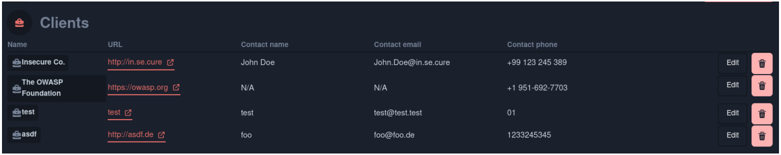
- Blue, Purple and Red teams
- Pentesters
- Bug bounty hunters
- Ethical hackers
- Security researchers

Individual or teams

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

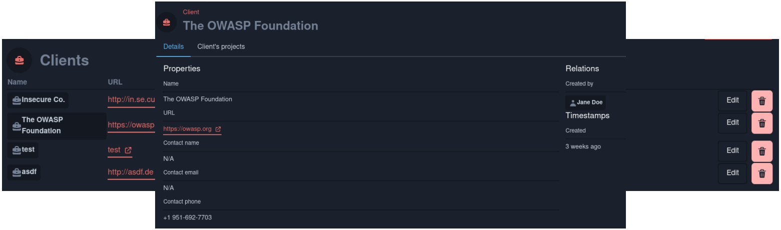
Step 1: Setup client



Clients

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

Step 1: Setup client



Clients

Name	URL
Insecure Co.	http://in.se.cu
The OWASP Foundation	https://owasp
test	test
asdf	http://asdf.de

Client

The OWASP Foundation

Properties

Name: The OWASP Foundation

URL: https://owasp.org

Contact name: N/A

Contact email: N/A

Contact phone: +1 951-692-7703

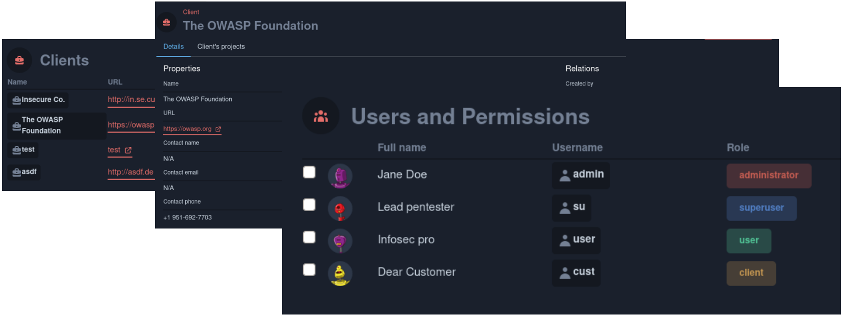
Relations

Created by: Jane Doe

Timestamps

Created: 3 weeks ago

Step 1: Setup client



Clients

Name	URL
Insecure Co.	http://in.se.cu
The OWASP Foundation	https://owasp
test	test
asdf	http://asdf.de

Client

The OWASP Foundation

Properties

Name

The OWASP Foundation

URL

https://owasp.org

Contact name

N/A

Contact email

N/A

Contact phone

+1 951-692-7703

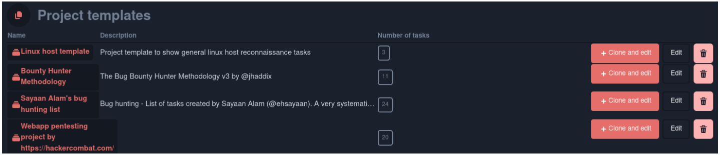
Relations

Created by

Users and Permissions

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

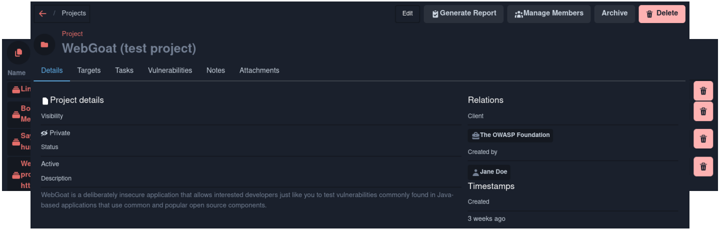
Step 2: Setup project



Project templates

Name	Description	Number of tasks			
Linux host template	Project template to show general linux host reconnaissance tasks	3	+ Clone and edit	Edit	🗑
Bounty Hunter Methodology	The Bug Bounty Hunter Methodology v3 by @jhaddix	11	+ Clone and edit	Edit	🗑
Sayaan Alam's bug hunting list	Bug hunting - List of tasks created by Sayaan Alam (@ehsayaan). A very systemati…	24	+ Clone and edit	Edit	🗑
Webapp pentesting project by https://hackercombat.com/		20	+ Clone and edit	Edit	🗑

Step 2: Setup project



Project

WebGoat (test project)

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

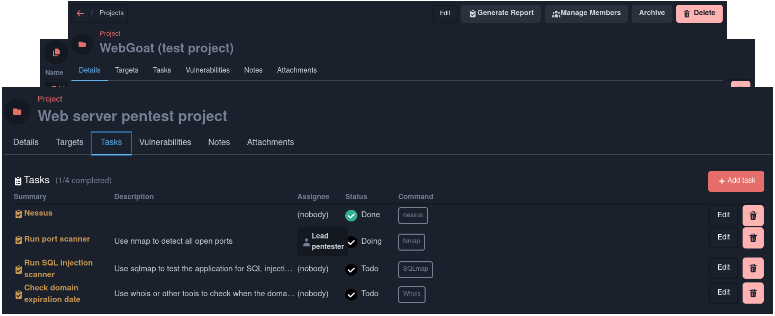
Jane Doe

Timestamps

Created

3 weeks ago

Step 2: Setup project



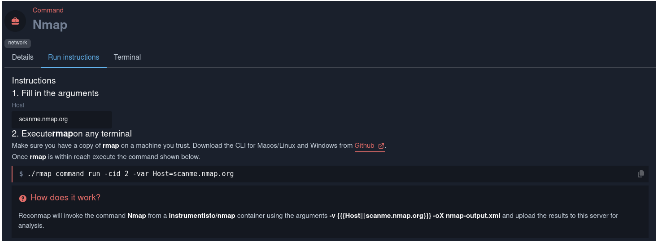
Project

Web server pentest project

Tasks (1/4 completed)

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

Step 3: Complete tasks and commands



Instructions

1. Fill in the arguments

Host

scanme.nmap.org

2. Execute**rmap**on any terminal

Make sure you have a copy of **rmap** on a machine you trust. Download the CLI for Macos/Linux and Windows from Github.

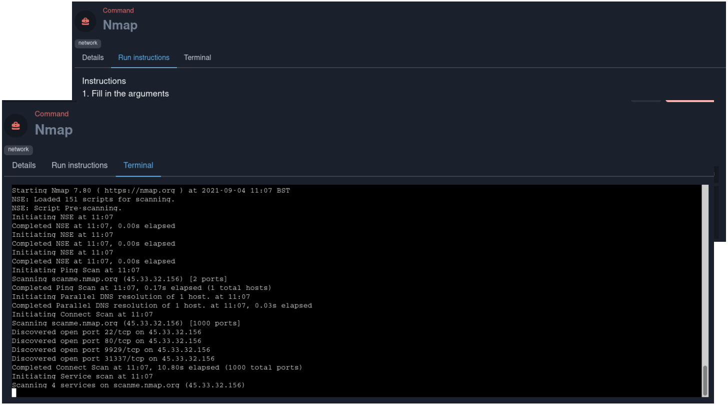
Once **rmap** is within reach execute the command shown below.

```
$ ./rmap command run -cid 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

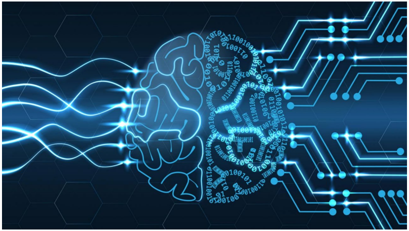


Instructions

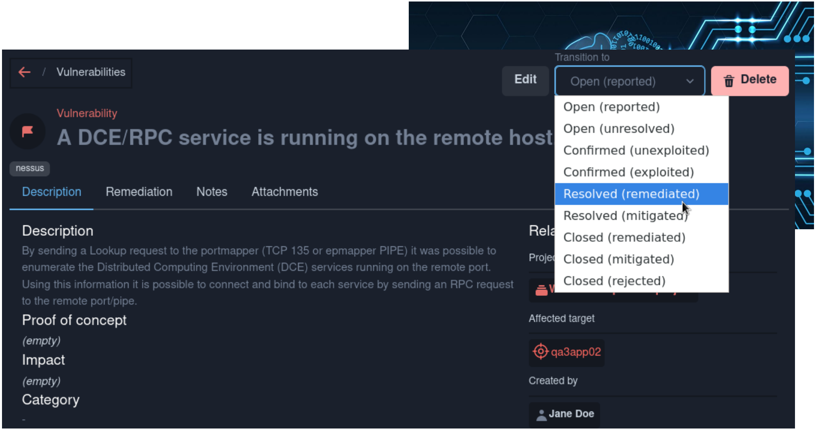
1. Fill in the arguments

```
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: Exploit vulnerabilities



Step 4: Exploit vulnerabilities



Transition to: Open (reported)

Vulnerability

A DCE/RPC service is running on the remote host

Description

By sending a Lookup request to the portmapper (TCP 135 or epmapper PIPE) it was possible to enumerate the Distributed Computing Environment (DCE) services running on the remote port. Using this information it is possible to connect and bind to each service by sending an RPC request to the remote port/pipe.

Proof of concept

(empty)

Impact

(empty)

Category

-

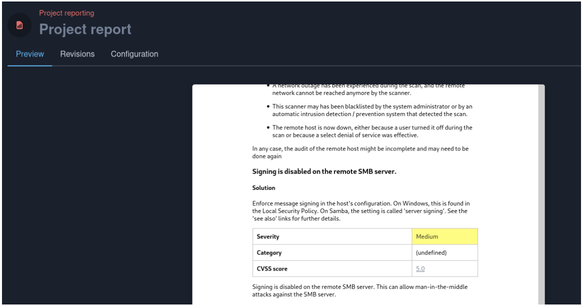
Affected target

qa3app02

Created by

Jane Doe

Step 5: Generate pentest report



- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may has 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.

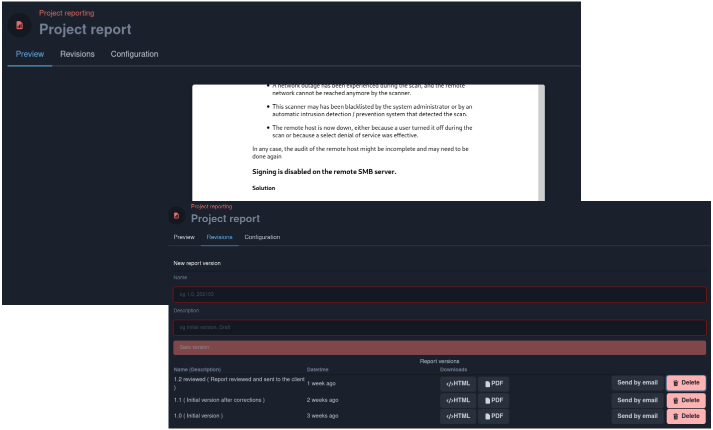
Solution

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



- A network outage has been experienced during the scan, and the remote network cannot be reached anymore by the scanner.
- This scanner may has 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

New report version

Name

eg 1.0, 202103

Description

eg Initial version, Draft

Save version

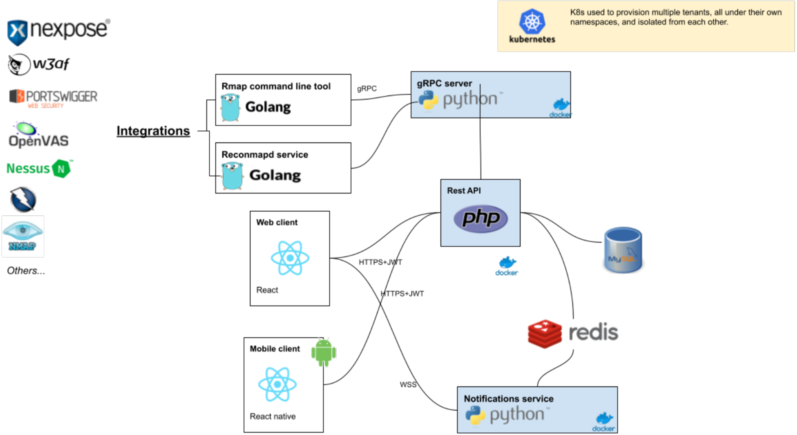
Report versions

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

Demo

Live demo

Architecture



Coming features

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

How to get started?

Manual setup

Follow setup instructions

Easy to install, more difficult to maintain
Community support (chat)

SaaS

Affordable hosting

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

Staying in touch

Reconmap

- https://github.com/reconmap
- https://twitter.com/reconmap
- https://facebook.com/reconmap
- Gitter chat

PENTESTER ACADEMY

- https://www.pentesteracademy.com
- https://twitter.com/DamianGoh13