Cyber Scotland Week

Reconmap

Generating pentest reports with Reconmap

CyberScotland Week

Santiago Lizardo

Before the talk

- Time for Q&A
- Slides
- Survey

Agenda

1. Basic pentesting concepts
2. Reconmap's introduction
3. Reconmap's interactive demo
4. Q&A

About the presenter

- Software engineer and entrepreneur
- Based in Scotland
- Security advocate
- Reconmap's founder

Imposter syndrome

Figure: https://flic.kr/p/dQC9kt

Section outline

1. Basic pentesting concepts
   - Pentest definition
   - Objectives and benefits of pentesting
   - The pentesting methodology
   - The role of the pentester

Vulnerability assessment

- Assess security of network or apps
- Identifies vulnerabilities
- Involves scanning tools
- Produces a report

Vulnerability assessment

- Assess security of network or apps
- Identifies vulnerabilities
- Involves scanning tools
- Produces a report

False positives

Findings are not exploited, some of them could just be false positives.

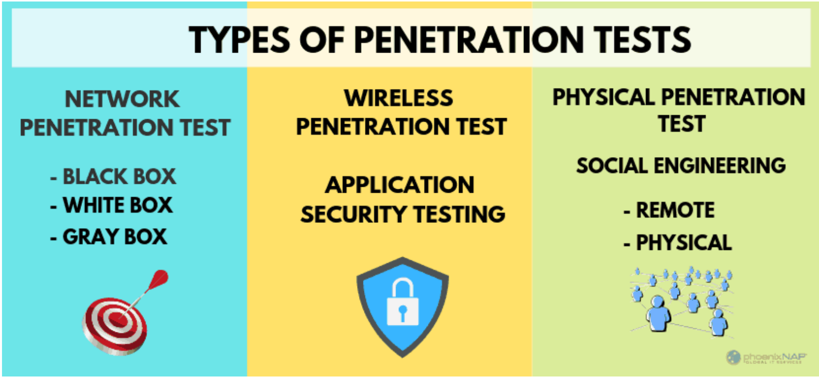
Pentest definition

- Assess security of network or apps
- Identifies vulnerabilities
- Use scanning tools
- **Vulnerabilities are carefully exploited**
- Produces a report

Pentest definition (continued)

- Systematic process
- Defined scope
- Legal
- Authorised

Types of pentesting



TYPES OF PENETRATION TESTS

NETWORK PENETRATION TEST

- BLACK BOX
- WHITE BOX
- GRAY BOX

WIRELESS PENETRATION TEST

APPLICATION SECURITY TESTING

PHYSICAL PENETRATION TEST

SOCIAL ENGINEERING

- REMOTE
- PHYSICAL

Figure: Source phoenixnap.com

Pentesting objectives

- Depict the current security level
- Identify gaps
- Quantify potential damage
- Validate/Invalidate security controls
- Decreases the possibility of real attacks

Business benefits

- Helps with compliance
  - ISO27001
  - PCI DSS
  - HIPPA
  - GLBA
  - FISMA/NIST
- Protects staff, customers and business partners
- Preserves company reputation
- Helps sustain business continuity

Cost of a pentest

Test size	Guide price[1]
Small	£1000-£3000
Medium	£3000-£5000
Large	£5000-£20000

[1] Source `bulletproof.co.uk`

Cost of a pentest

Test size	Guide price[1]
Small	£1000-£3000
Medium	£3000-£5000
Large	£5000-£20000

Cost

Data breaches costed £2.9M to orgs in 2020

[1] Source `bulletproof.co.uk`

Engagement length

- Typical engagements are 1 to 3 weeks*

[1] https://www.itgovernance.co.uk/blog/the-cost-of-a-data-breach-in-2020

Engagement length

- Typical engagements are 1 to 3 weeks*

Recovery time

Orgs take 280 days on average to detect and respond to an incident.[1]

[1] https://www.itgovernance.co.uk/blog/the-cost-of-a-data-breach-in-2020

When to perform a pentest

Reactively

- Prior to contracting a data breach insurance
- Before and after corporate milestones
- After noticing viruses, malware, spyware on the system
- After noticing unusual system patterns, traffic
- After system change & new system deployments
- After new system integrations
- After the release of new products/features

When to perform a pentest

Proactively

- Regularly as a preventive measure
- At least once a year

Penetration testing standards

- OSSTMM
- OWASP
- NIST
- PTES
- ISSAF

Pentesting workflow

- Pre-engagement, analysis and plan
- Information gathering and reconnaissance
- Discovering vulnerabilities
- Exploitation
    - Gaining access
    - Privilege escalation
    - Maintaining access
    - Covering tracks
- Analysis and reporting
- Re-test (aka post-fix verification)

Pre-engagement

- Paperwork
  - Rules of engagement
  - Contract
  - NDA
- Documentation sharing
- Setup
  - Sharing credentials
  - Lifting restrictions
  - ...

Determine scope

- Targets
  - Web app
  - Mobile apps
  - Database
  - Network
  - Wireless
- End user and social engineering attacks
- DDos and performance tests
- Internal/External
- Physical/Remote

Determine scope (continued)

- Testing hours/days (eg workdays vs weekends)
- Locations
- Network range
- Teams

Analysis and reporting

Typical report

- Summary
- Findings
- Recommendations
- Methodology

Communication

- Executive summary delivered to leadership
- Project closure meeting organised to discuss

Analysis and reporting (examples)

Pentest report examples → `https://pentestreports.com`

- Over 150 example reports
- Stored on Github
- Source of learning and inspiration

Re-test

- The company is expected to close the gaps
- After the gap-closure, a time frame is determined by both parties for verification tests
- Findings in the report are reevaluated in the verification tests

Pentester

- Plans and designs penetration tests
- Carry out tests and other simulations
- Creates reports and offer recommendations
- Advises management on security improvements
- Work with other employees to improve organizational cybersecurity

Pentester tools

- From notebooks and post its to text files and wikis
- (Power)Shell scripts
- Security tools (Zap, Burp, nmap, ...)
- Jira/Trello/Gitlab, ...
- Word/Libreoffice
- Email/Chat

Becoming a pentester

- Courses
- University degrees
    - Computer science
    - Ethical hacking/Cybersecurity
        - Abertay University
- Practice, practice practice

Becoming a pentester (continued)

- Capture the flag/Interactive
  - Hackthebox.eu
  - PentesterLab.com
  - VirtualHackingLabs.com
- Cybrary
- PentesterAcademy

Bug bounty programs

To receive recognition and compensation for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

Becoming a pentester (continued)

Certifications

- EC-Council CEH and LPT
- IACRB CPT and CEPT
- OSCP, OSCE
- CREST Practitioner, Registered, Certified Tester
- CompTIA PenTest+

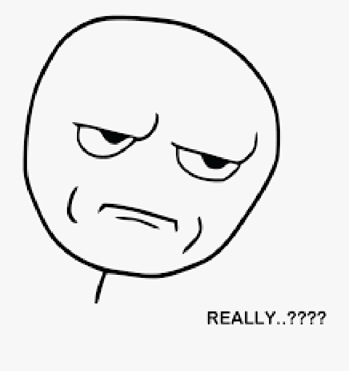
Section outline

2 Reconmap's introduction
- Reconmap's mission
- Features
- Technical overview
- Typical workflow

Reconmap mission

Reconmap is making of every software engineer a penetration tester

Reconmap mission



Reconmap mission (continued)

- Make security testing more accessible
- Help (infosec)engineers collaborate better
- Accelerate project delivery
- Maximise returns

What is Reconmap?

- Collaboration platform for InfoSec projects
- Automation and reporting tool for pentesters
- Also...
  - Early-stage project
  - Open-source and SaaS
  - Developed in Dundee[1]

[1] with contributions from Argentina and the world

Who is it for?

- InfoSec pros and teams looking to become more efficient
- Other technical minded people[1] wanting to
  - Learn about security
  - Perform basic security on their projects

[1] devs, devops, it admins, sys admins, qa, etc...

Reconmap's functionality

- Project/Methodology templating
- Task management
- Shared space for
  - Files (docs, results, screenshots, etc)
  - Notes
- Automation tool

Features

- Database
  - Commands
  - Vulnerabilities
  - Notes
- Command automation
- Report generator

Commands

Custom commands

- Any arbitrary command
- Exec and dependencies installed by the user
- No upload integration

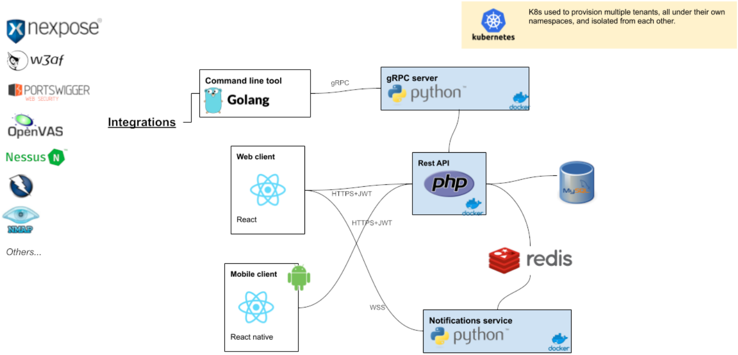
Rmap commands

- Container based
- Dependencies included
- Portable to Windows/Macos/Linux
- Tighter integration with dashboard

Reconmap's code

- Open-source
- On Github → `https://github.com/reconmap`
- Easy to setup local environments
- Open for contributors

Reconmap's architecture



Others...

Integrations

Command line tool

Golang

gRPC

gRPC server

python

docker

K8s used to provision multiple tenants, all under their own namespaces, and isolated from each other.

kubernetes

Web client

React

HTTPS+JWT

Rest API

php

docker

MySQL

HTTPS+JWT

redis

Mobile client

React native

WSS

Notifications service

python

docker

API

- RESTful API
- OpenAPI specs
- Fully featured
- Used by CLI, Web and mobile clients
- `https://api.reconmap.org/docs/`

Typical workflow

1. Create client
2. Create project from template
3. Complete tasks
4. Some tasks require running commands
5. Reconmap (*rmap*) runs the command, upload results, and analyses them
6. User annotates and triage vulnerabilities
7. Generate and share the report

Reconmap's demonstration

- General tour
- Pentest generation walk-through

Reconmap's present

- Young project ($\sim$ 7 months, part-time)
- Usable, but not complete
- Evolving fast (releases every 2 weeks)

Reconmap's future

- Immediate term
  - Polish up
  - Expand docs
  - Expand test coverage

- Short term
  - Add more integrations
  - 2FA
  - Item triage
  - Better analytics

Reconmap's future

Medium term

- Machine learning for classification
- Non-interactive agents
- Many other things!

Recap

1. Basic pentesting concepts
    - Pentest definition
    - Objectives and benefits of pentesting
    - The pentesting methodology
    - The role of the pentester
2. Reconmap's introduction
    - Reconmap's mission
    - Features
    - Technical overview
    - Typical workflow
3. Reconmap's interactive demo
    - Present and future
4. Q&A

More information

Documentation

`https://reconmap.org`

SaaS

`https://reconmap.com`

Code

`https://github.com/reconmap`

Twitter

`https://twitter.com/reconmap`

Questions?