Introduction to Penetration Testing

Graham Weston

March 2014

Agenda

Introduction and background

Why do penetration testing?

- Aims and objectives
- Approaches

Types of penetration test

- What can be penetration tested?
- How to do a penetration test

Penetration test workflow

Tools, standards and techniques

What is a Penetration Test?

Wikipedia says:

*"A **Penetration Test**, or the short form pentest, is **an attack on a computer system with the intention of finding security weaknesses**, potentially gaining access to it, its functionality and data"*

What is a Hacker?

Wikipedia says:

*"A **hacker** is someone who **seeks and exploits weaknesses in a computer system or computer network**. Hackers may be motivated by a multitude of reasons, such as profit, protest, or challenge."*

So, what's the difference?

Their motives; both have overlapping skill sets.

The penetration tester (white hat)**:**

- Works with the knowledge and consent of the system owner
- Should not cause lasting damage to the target system
- Has constructive goals (to find security issues that can be fixed)
- Obliged to responsibly disclose their findings

The hacker (black hat)**:**

- Works to avoid detection by the system owner
- Actively works to conceal their capability (0-day exploits etc.)
- Has a range of nefarious motives:
  - Credibility in the underground community
  - Cause damage/disruption
  - Steal for material gain

ⓘ Health Warning

The tools and techniques discussed here are powerful:

- They should only be used under controlled conditions (and with the express consent of the owner of the system under test)
- Professional penetration testers are bound by strict codes of practise and ethics
- The distinction between penetration testing and hacking is entirely contextual

In short, don’t try this at home!

Why Do Penetration Testing?

Why do Penetration Testing?

To better understand and quantify the risks posed to a system by external attackers.

For example, what would happen if:

- A corporate web site was defaced or taken down?
- The passwords and customer details to your web-based banking service were published on the Internet?
- An attacker could gain access to the control systems of a major factory/power station/water plant?

A pentest gives a measure of confidence that the most significant risks to a system have been adequately mitigated.

Types of Penetration Test

Pentests can be categorised in to several main types:

- Physical (gaining physical access to facilities)
- Hardware (what can be done if an attacker has physical access to the system under test)
- Network (where an attacker has access to a network connected to the system under test)
- Web (focussing specifically on the web front-end to the system under test)

In practise, a pentest may span several of these areas.

What do I get from a Pen Test?

Ideally:

Independent verification that the system under test resists a range of common attacks and exploits.

Practically:

Information about the weaknesses identified in the system under test.

What *don't* I get from a Pen Test?

- Generally, a pentest focuses on finding a way to successfully attack and exploit the system under test at the time of testing.
- It's not an exhaustive audit of the system security.
- Pentests only identify vulnerabilities that are known about at the time of the test. Attack techniques are constantly evolving and improving.

A **vulnerability assessment** is a more detailed, extensive audit of the security of a system.

How to Do a Penetration Test

A practical approach:

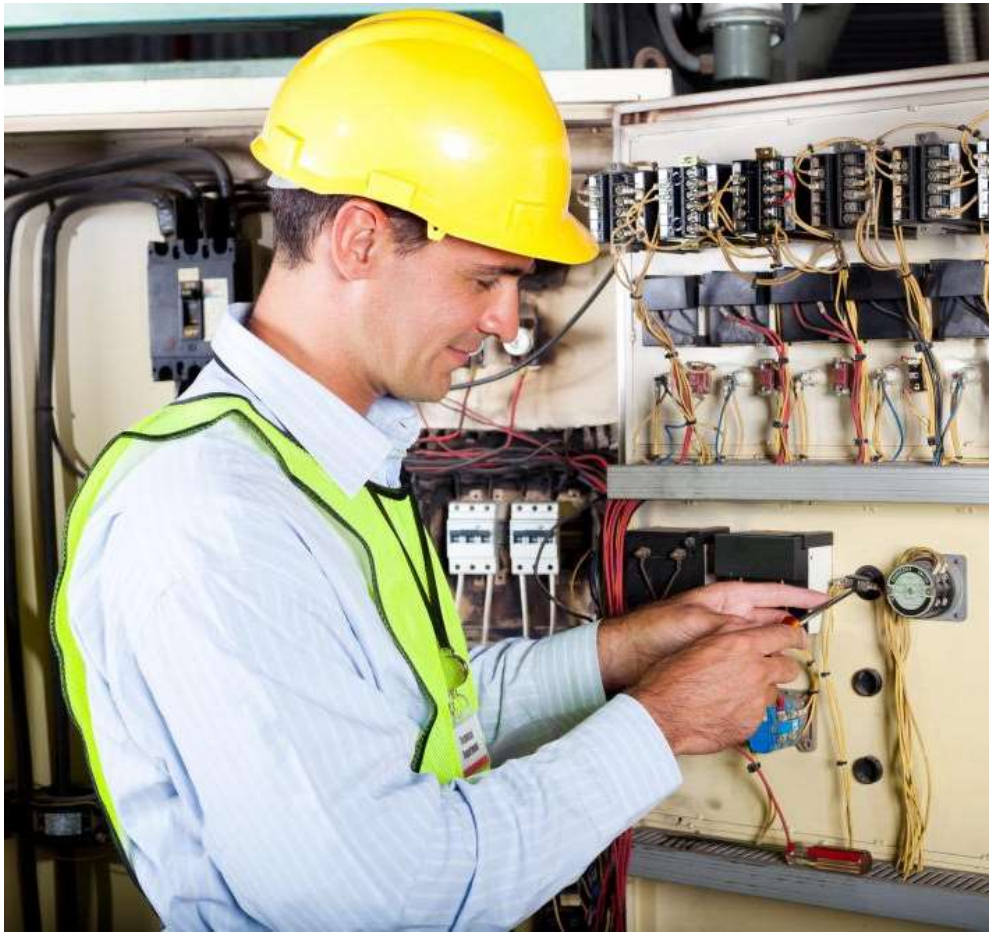
Scenario:

You are set a the challenge of carrying out a physical penetration test on an office building.

Your goal is to breach the security of the building and locate items of interest inside.

How would you do it?

A practical approach:

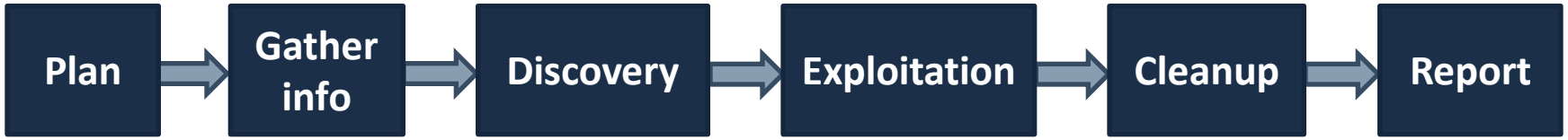


- Dress up as an aircon engineer?
- Carry a toolbag?
- Wear an ID badge?

A practical approach:

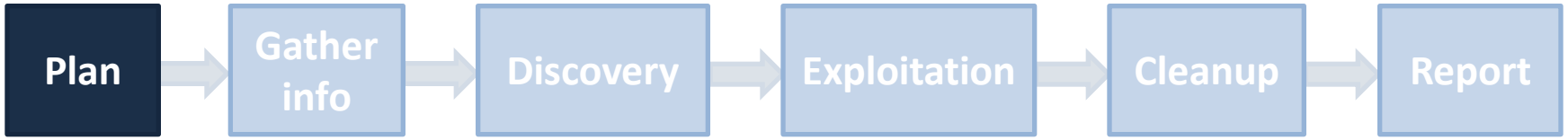
- Make a plan
- Gather information
  - How many doors are there? Where are they?
  - Are the doors locked? Can the locks be defeated?
  - Is it possible to get in any other way? A window, ventilation duct?
  - When is best to go in?
  - How best to avoid being noticed?
  - Once inside, how to identify what is of interest?
- Execute plan
- Report on weaknesses in physical security identified

Penetration Test Workflow



This practical, physical example maps on to a generic workflow that is widely applicable

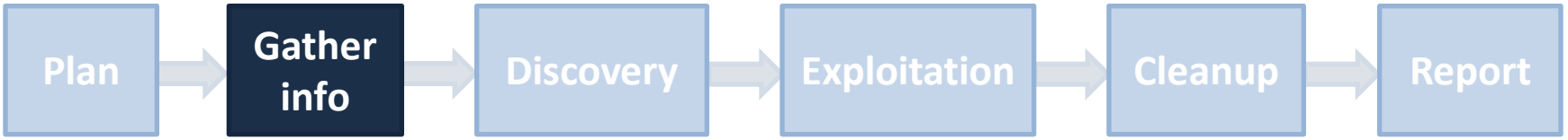
Pen Test Workflow - Plan



Planning:

- Define scope and requirements for test
- Plan test approach
  - White box
  - Black box
  - Hybrid (grey box)
- Identify suitable tools
  - COTS, open-source, bespoke

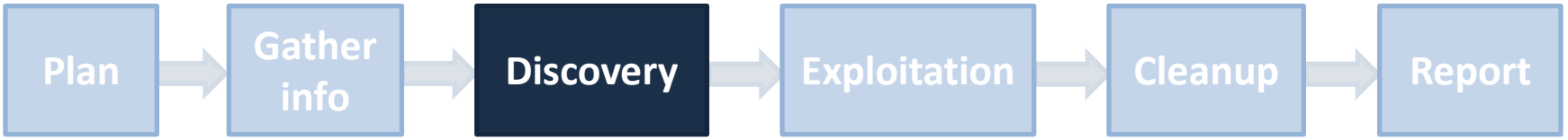
Pen Test Workflow – Gather Info



Information gathering:

- Identify components of target system
- COTS components
  - Identify versions
  - Look for publically disclosed vulnerabilities and exploits
- Bespoke components
- Inspection of source code and configuration information in white box scenario

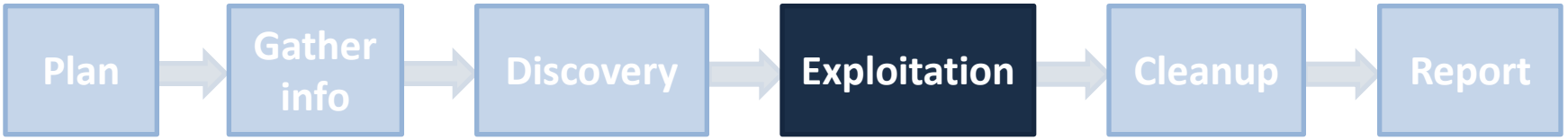
Pen Test Workflow – Discovery



Discovery:

- Practical investigation of target system
- Initial checks:
  - TCP ports open?
  - Services running?
  - Default/weak user credentials?
- Information leakage
- Automated tools/Industry standard checks (OWASP etc.)

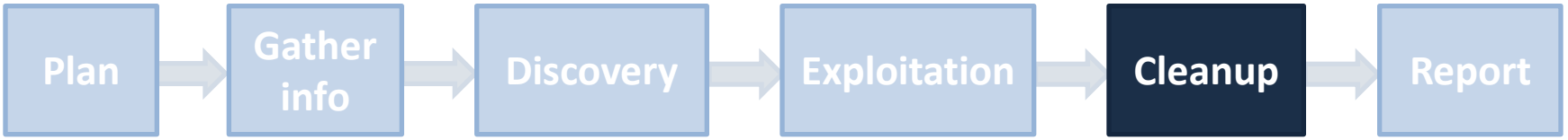
Pen Test Workflow – Exploitation



Exploitation:

- Using information gained in discovery phase, is it possible to exploit the system?
- Common attacks:
  - COTS tools (metaspolit, CANVAS and other frameworks)
  - Exploits in public domain (CVE database)
  - SQL injection, XSS, session hijacking etc.
- Identify areas for further investigation

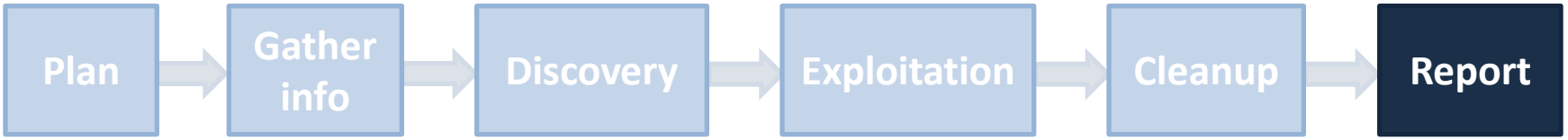
Pen Test Workflow – Cleanup



Cleanup:

- Document findings
- Make recommendations; identify risks not fully mitigated in scope of current task
- Reverse any changes made to target system

Pen Test Workflow – Cleanup



Report:

- Release formal documentation
- Identify next steps/way forward
- Closure with client

Tools, Standards and Techniques

Physical Engagements

Effectively implementing the building scenario discussed earlier.

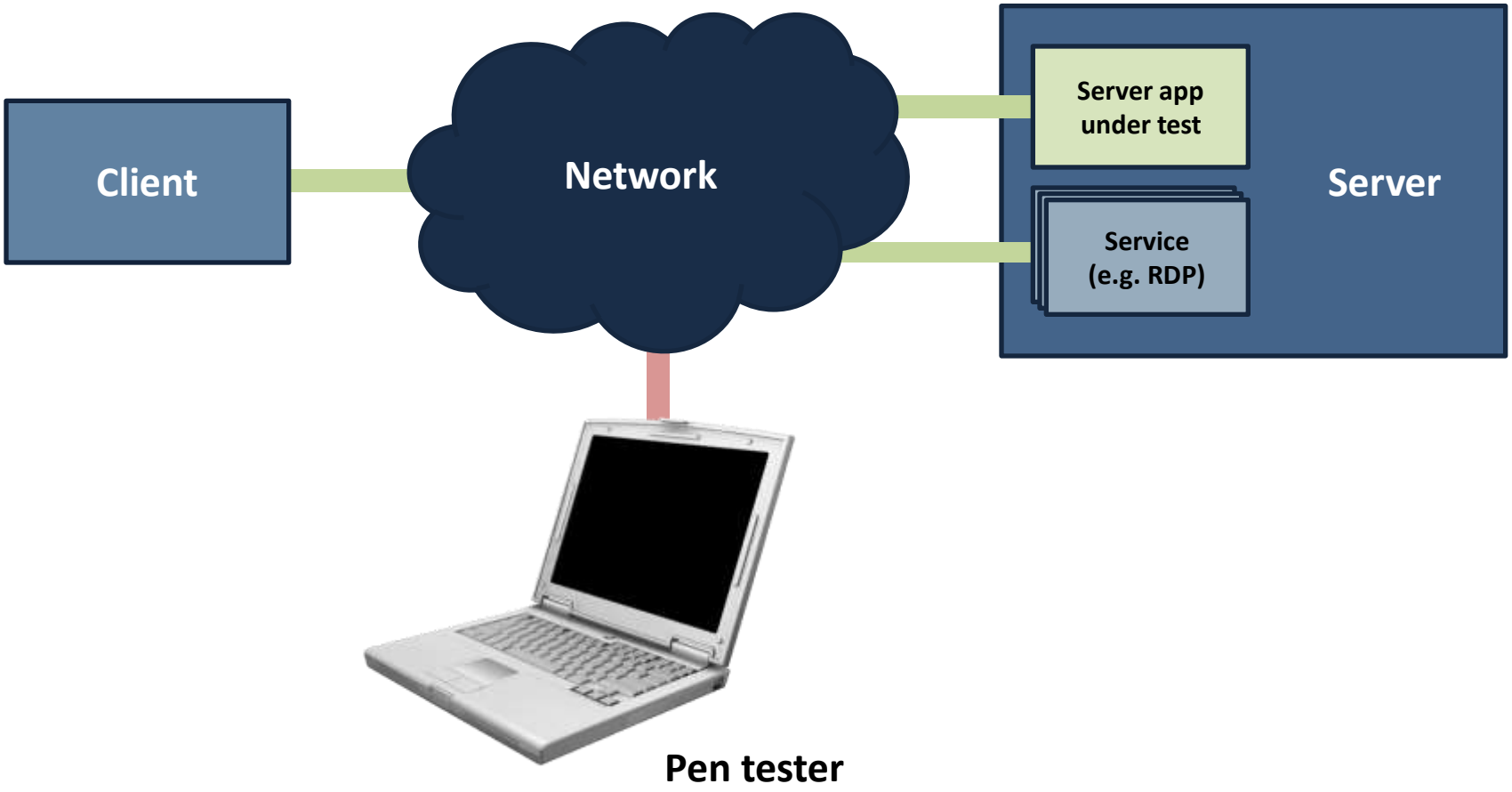
Techniques:

- Social engineering
- Identifying and defeating access controls
- Remote attacks

Tools:

- Specialised hardware
- Uniform and ID badges

Network Engagements



Automated Tools

The good news:

- Commercial and open-source tools take away much of the hands-on complexity, using GUIs to drive the process
- In many cases, it is possible to deliver quick wins without coding, scripting, or having a detailed understanding of the underlying technologies
- High-level tools produce a visualisation of the target network allowing you to deploy exploits and navigate it graphically

The bad news:

- They are not a panacea; automated tools will only find well-known, existing vulnerabilities
- Finding really valuable vulnerabilities is a more labour-intensive process, dependent on a skilled pen-tester

Popular Standards

OWASP (Open Web Application Security Project)

www.owasp.org

OSSTMM (Open Source Security Testing Methodology Manual)

www.osstmm.org

NIST (National Institute of Standards and Technology)

csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

PTES (Penetration Testing Execution Standard)

www.pentest-standard.org

Conclusions

Conclusions

- The fundamental concepts for a pentest are common across a range of activities, ranging from a building to a web-app
- The best approach for each engagement should be tailored using a combination of external standards, knowledge of the target system and tester experience.
- There are standards, such as OWASP, which provide a good (but not exhaustive) approach.
- Commercial and open-source tools offer a range of useful functionality:
  - Automating common and labour intensive tasks
  - Managing the workflow
  - Visualising the target network
  - Deploying exploits in a point-and-click paradigm

Questions?