Information gathering

Pentesting

Danae Townsend, Jordi Bru, Ignasi Juez, Mariona Jaramillo

Index

Penetration Testing

Reconnaissance

Scanning

Gaining access

Maintaining access

Analysis & Reporting

Information gathering and pentesting relationship

Information gathering and pentesting relationship

Information gathering and pentesting relationship

Information gathering and pentesting relationship

Information gathering and pentesting relationship

- It is used to perform security auditing on a system or network

Information gathering and pentesting relationship

- It is used to perform security auditing on a system or network

- Exploit known techniques to better understand a system

Information gathering and pentesting relationship

- It is used to perform security auditing on a system or network

- Exploit known techniques to better understand a system

- Obtain a perception on: how is this company regarded from the outside?

Information gathering and pentesting relationship

- It is used to perform security auditing on a system or network

- Exploit known techniques to better understand a system

- Obtain a perception on: how is this company regarded from the outside?

- Provide a report with potential vulnerabilities and attack vectors to a system

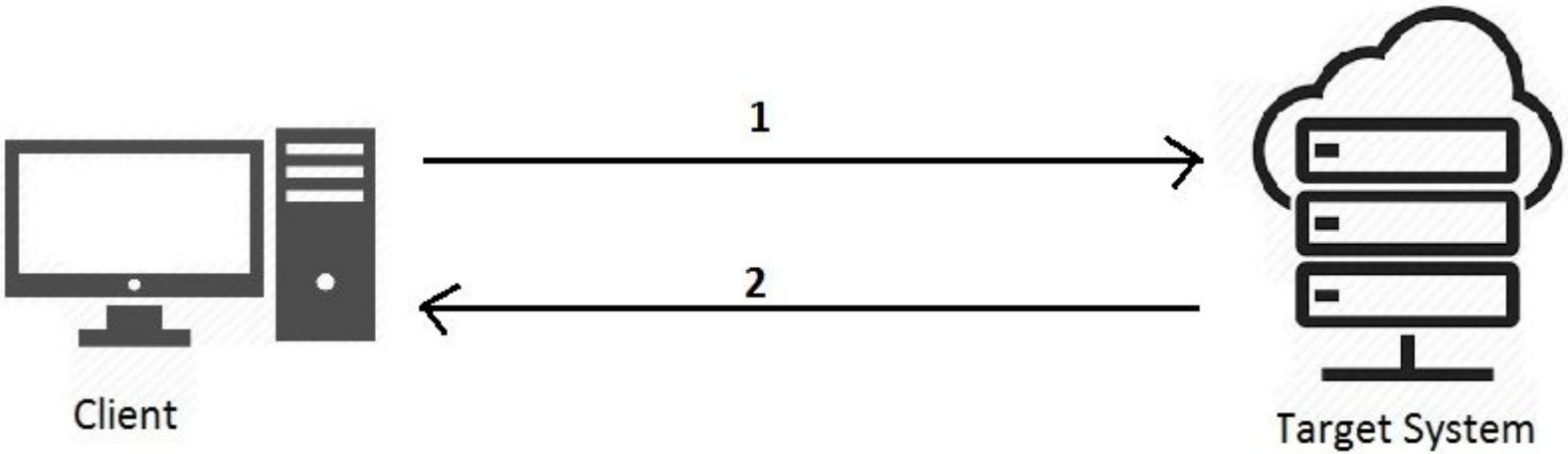
Information gathering techniques

a) Active information gathering

b) Passive information gathering

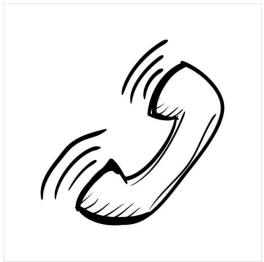
c) Social engineering

Active information gathering



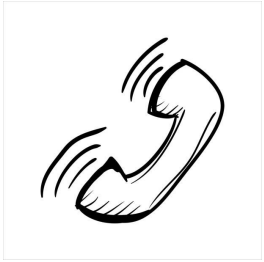
Active information gathering

Social

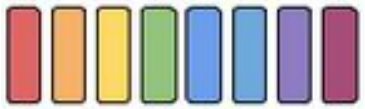


Active information gathering

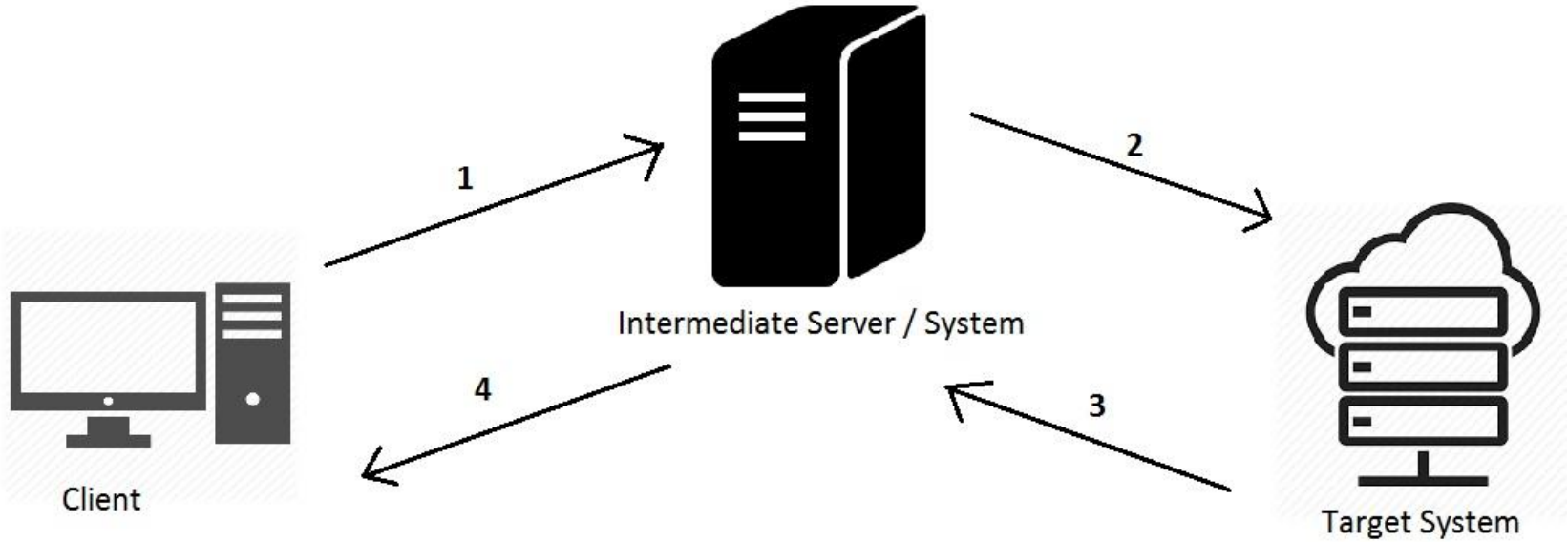
Social



Technical



Passive information gathering

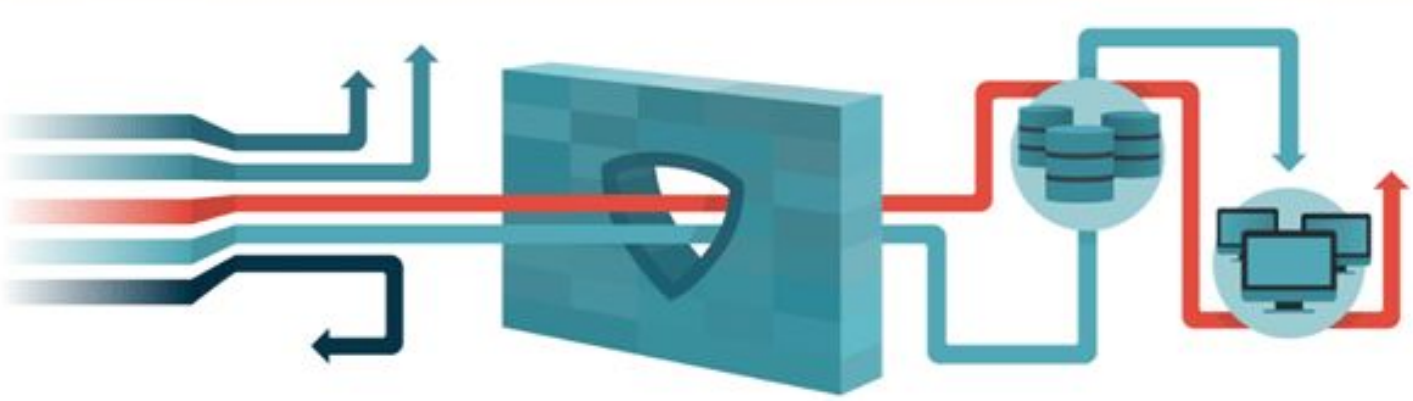


Passive information gathering

Targeted online resources and tools

- IP registrations
  - whois
- DNS
  - dig
  - fpdns
  - fierce
- Website Analysis
  - Wayback Machine
- Search Engines
  - Google
  - Duck Duck Go

Social Engineering



Types of social engineering

- Phishing
  - ❏ Deceptive Phishing
  - ❏ Spear Phishing
  - ❏ CEO Fraud
  - ❏ Vishing
  - ❏ Smishing

Types of social engineering

- Phishing
- Pretexting

Types of social engineering

- Phishing
- Pretexting
- Baiting

Types of social engineering

- Phishing
- Pretexting
- Baiting
- Quid Pro Quo

Pentesting in companies

Overview

Penetration testing can enhance a company's security in many ways:

1. Identify vulnerabilities via information gathering
2. Test the effectiveness of security measures
3. Test incident response plans

Top penetration testing companies

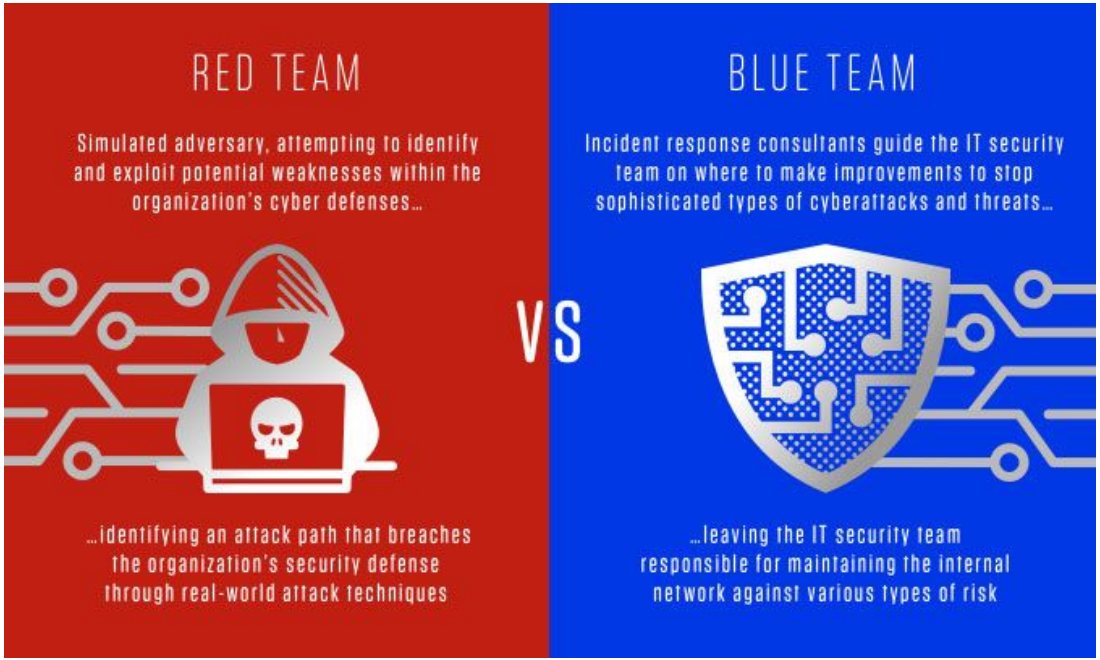
There are specialist organizations that carry out authorized pentesting against networks and applications from other organizations for many different types of sensitive data.

Laws and regulations

The tester and the company define the limits of systems that can be subjected to penetration **beforehand** based on:

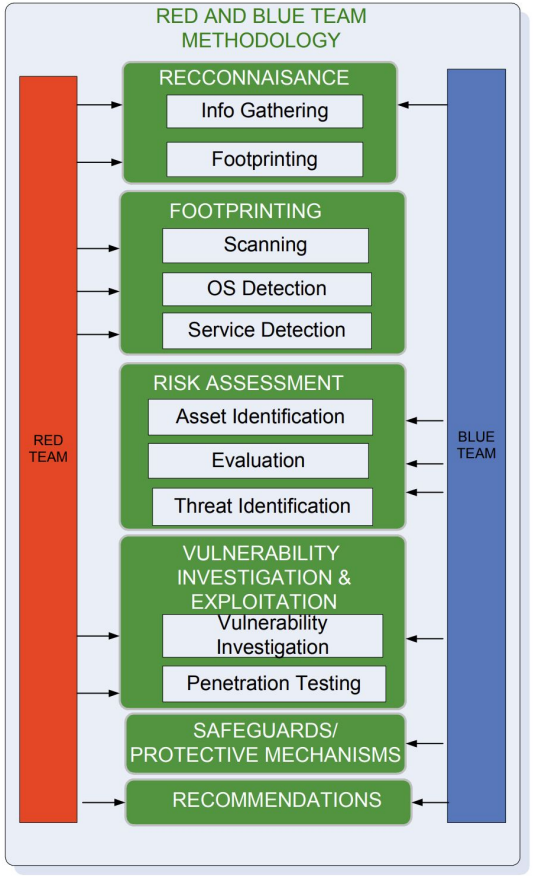
- Legal and ethical considerations
- Business - criticality

Teams


RED TEAM
Simulated adversary, attempting to identify and exploit potential weaknesses within the organization's cyber defenses...
...identifying an attack path that breaches the organization's security defense through real-world attack techniques
VS
BLUE TEAM
Incident response consultants guide the IT security team on where to make improvements to stop sophisticated types of cyberattacks and threats...
...leaving the IT security team responsible for maintaining the internal network against various types of risk

Methodology

A combined Red and Blue Team Methodology often concludes in better results because it aims to provide information on both exploitable means and defensive strategies.

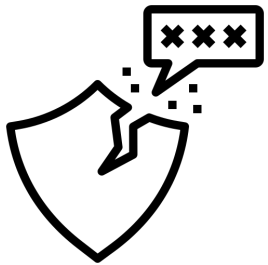


Information gathering in red and blue teams

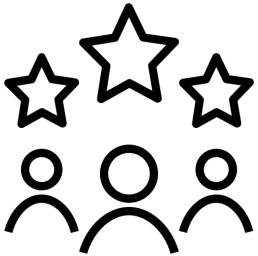
Divided into:

1. Briefings and meetings
2. Interviews
3. Document reviews
4. Internet and search engines
5. Network mapping
6. Port scans
7. Wireless scanning
8. Risk assessment

Decision maker



Vulnerabilities and risks

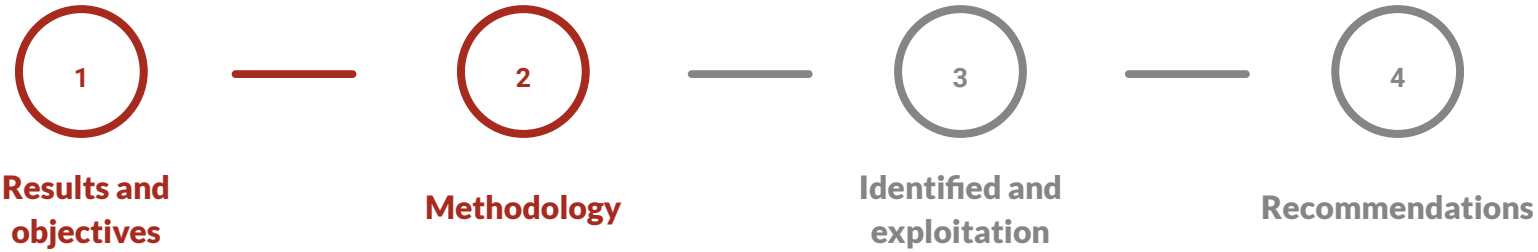


Technical and professional team

Clear and detailed

Reports and security audits

Essentials



Results and objectives

Executive summary.

- Purpose of the test.
- Key findings focused on a commercial level.
- Strategic recommendations

Positive, significant, constructive. Avoid technical terms.

Methodology

- Resources and work done.
- Pentest’s plan
- Explain the method used

Phases: preparation, information gathering, vulnerability detection, exploitation, post-exploitation, results analysis and reporting. (PTES)

Tools

Related to the purpose of information gathering.

- Scanning for vulnerabilities. **Acunetix**
- Data base pentetration testing. **SQL Map**
- Packet capture. **Burp suite**

Rank	Detection Accuracy	Vulnerability Scanner
1	94%	Acunetix
2	91%	Netsparker
3	44%	Wapiti
4	19%	Arachni
5	16%	Burp Suite Professional

Identified and exploitation

- Description of the root of origin
- Impact
- Probability of occurrence

References

G. Ollmann, "Passive Information Gathering Part 1: Introduction to Passive Information Gathering," Technical Information [Online]. Available: http://www.technicalinfo.net/papers/PassiveInfoPart1.html

A. S. Laxmi Kowta, K. Bhowmick, J. R. Kaur and N. Jeyanthi, "Analysis and Overview of Information Gathering & Tools for Pentesting," 2021 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, 2021, pp. 1-13, doi: 10.1109/ICCCI50826.2021.9457015.

S. Gupta, A. Singhal and A. Kapoor, "A literature survey on social engineering attacks: Phishing attack," 2016 International Conference on Computing, Communication and Automation (ICCCA), Greater Noida, India, 2016, pp. 537-540, doi: 10.1109/CCAA.2016.7813778.

"6 Common Phishing Attacks and How to Protect Against Them", Tripwire, 01-Jul-2019. [Online]. Available: https://www.tripwire.com/state-of-security/6-common-phishing-attacks-and-how-to-protect-against-them.

Yeo, John. (2013). Using penetration testing to enhance your company's security. Computer Fraud & Security. 2013. 17–20. 10.1016/S1361-3723(13)70039-3.

N. Veerasamy, "High-Level Methodology for Carrying out Combined Red and Blue Teams," 2009 Second International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 416-420, doi: 10.1109/ICCEE.2009.177.

M. Alharbi, "Writing a Penetration testing report", SANS Inst., vol. 1, pp. 8–13.

Thanks for your attention

Jordi Bru

jordi.bru@estudiantat.upc.edu

Danae Townsend

danae.townsend@estudiantat.upc.edu

Mariona Jaramillo

mariona.jaramillo@estudiantat.upc.edu

Ignasi Juez

ignasi.juez@estudiantat.upc.edu