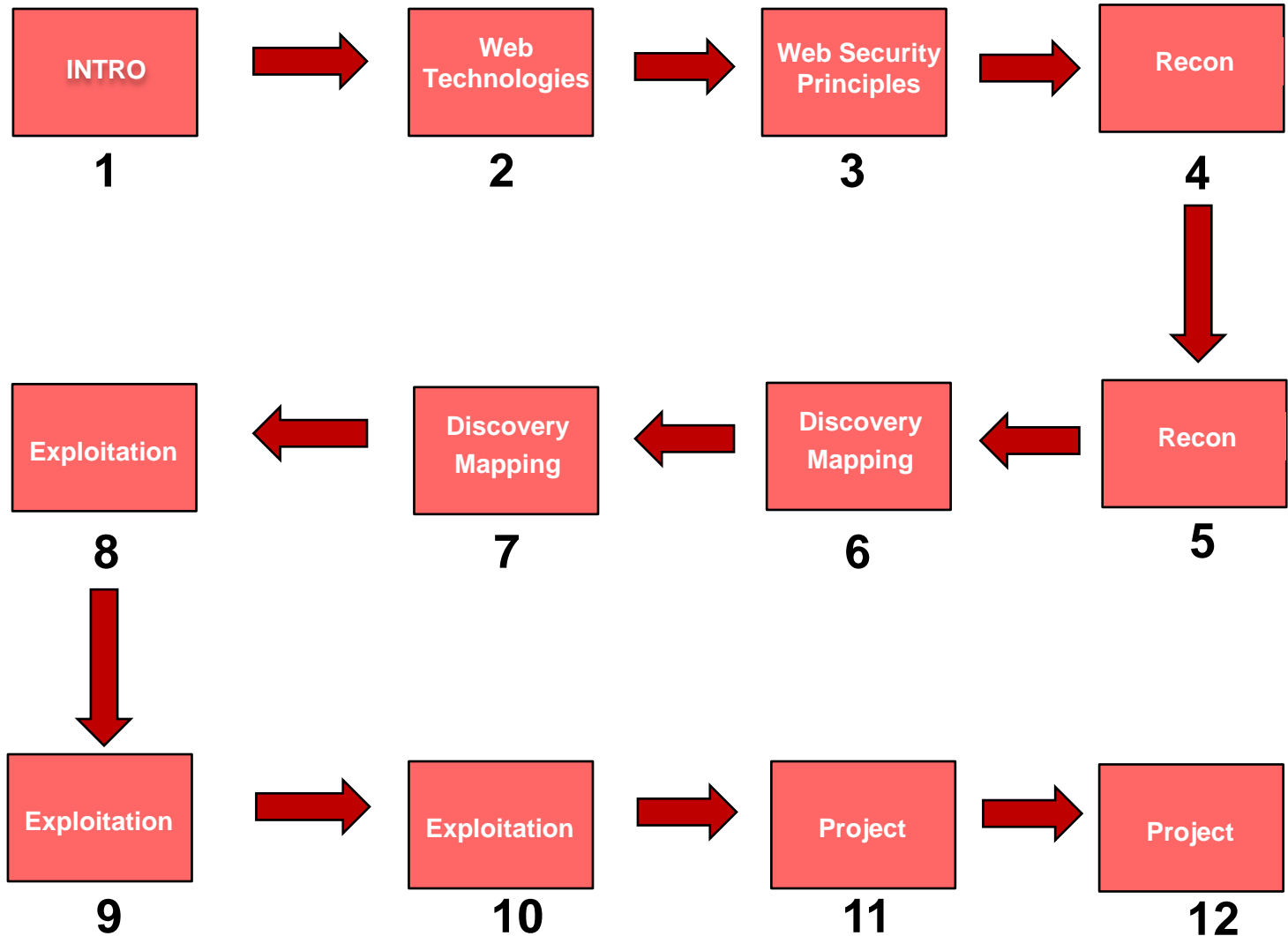


Web App & Data Base Security

Project

Web App & Data Base Security



Executive Summary

Provide, in a nutshell, what has been found from the tests about the company's system.

- Methodology used;
- How many domains, Ips, devices found and assessed;
- Be straightforward about what you found and what could be caused if any of the findings have been compromised.

Recon

- Information about:
 - DNS;
 - IP ranges;
 - Domain names;
- Diagrams and spreadsheets;
- List of tools used with a brief description for each one.

Mapping

- List of open ports;
- Service version;
- Information about the service latest version and security advisory or exploits available;
- List of tools used with a brief description for each one.

Discovery

- List of vulnerabilities by each host found on the internet;
- Focus on Critical and Highs;
- Highlight the ones that have exploits available on the Internet;
- Check the CVEs and provide description for each vulnerability;
- List of tools used with a brief description for each one.

Exploitation

- List of hosts that have been exploited;
- Screenshots or logs have to be provided to prove that they were exploited;
- Step by step on how to do it has to be provided too;
- Recommendation on how to fix the issue;
- List of tools used with a brief description for each one.

Requirements

- Deadline: one week after the course completion;
- 20 pages long in PDF sent to rcunha23@gmail.com

Questions

