INFOSECTRAIN

CompTIA

PenTest+

PT0-002

CERTIFICATION & TRAINING

CompTIA AUTHORIZED PARTNER

www.infosectrain.com | sales@infosectrain.com

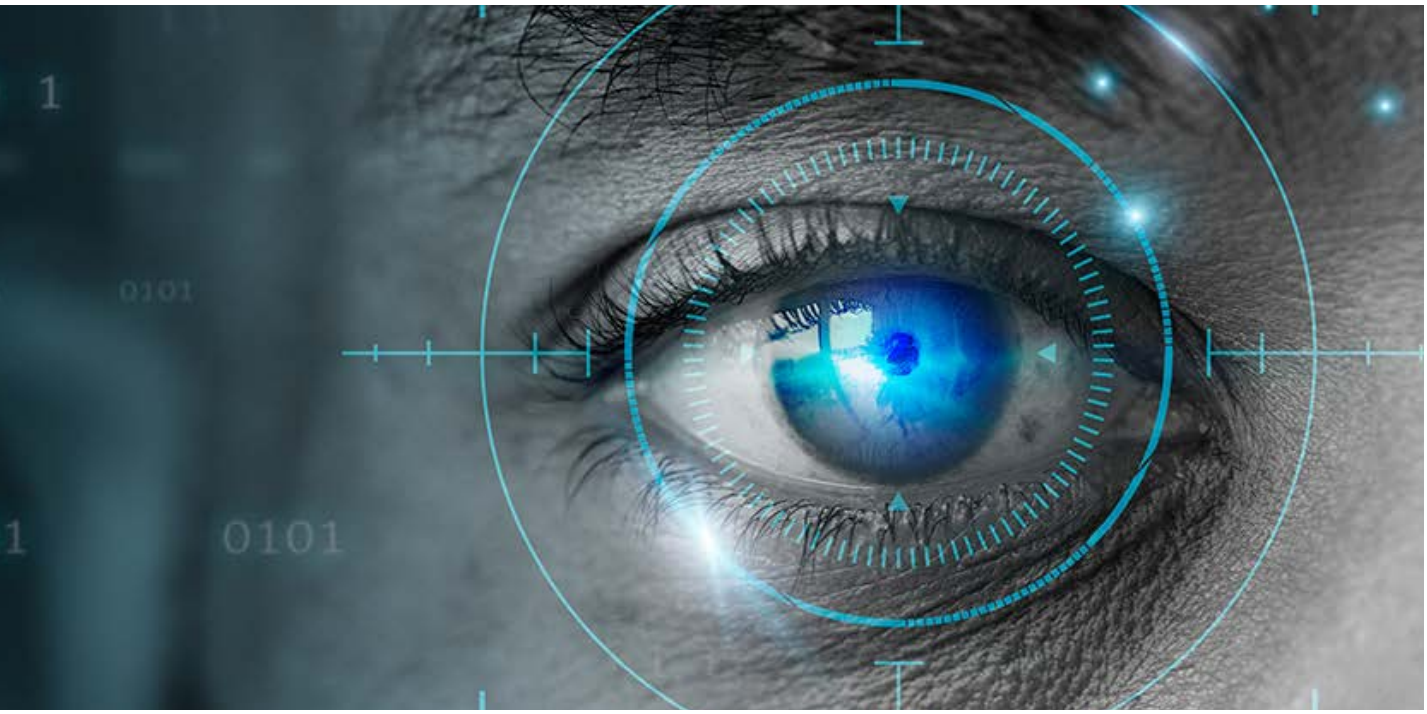
INFOSECTRAIN

Introduction

CompTIA PenTest+ is one of the most comprehensive courses that cover all the PenTesting stages. PenTest+ is the only exam that incorporates all aspects of vulnerability management. This course also includes all the latest techniques used against the expanded attack surfaces.

InfosecTrain has designed a CompTIA PenTest+ PT0-002 course where you will learn to plan and scope a penetration testing engagement, perform pen-testing using correct techniques, tools, and then analyze the outcomes, you will also learn how to understand the compliance and legal requirements, you will also be able to produce a written report containing proposed remediation techniques.

From the CompTIA PT0-002 course designed by InfosecTrain, you will also learn about Regulatory compliance considerations, location restrictions, rules of engagement, background checks of penetration testing teams, DNS lookups, open-source intelligence, enumeration, fingerprinting, scanning methods, attack methods, injection attacks, report audience, data structures and many more.



Target Audience

- Network and security professionals
- Cybersecurity engineers
- Network Architect
- Information Security Engineers

Prerequisites

- Network and security knowledge
- Minimum 3 to 4 years of experience in the field of information security or related area.

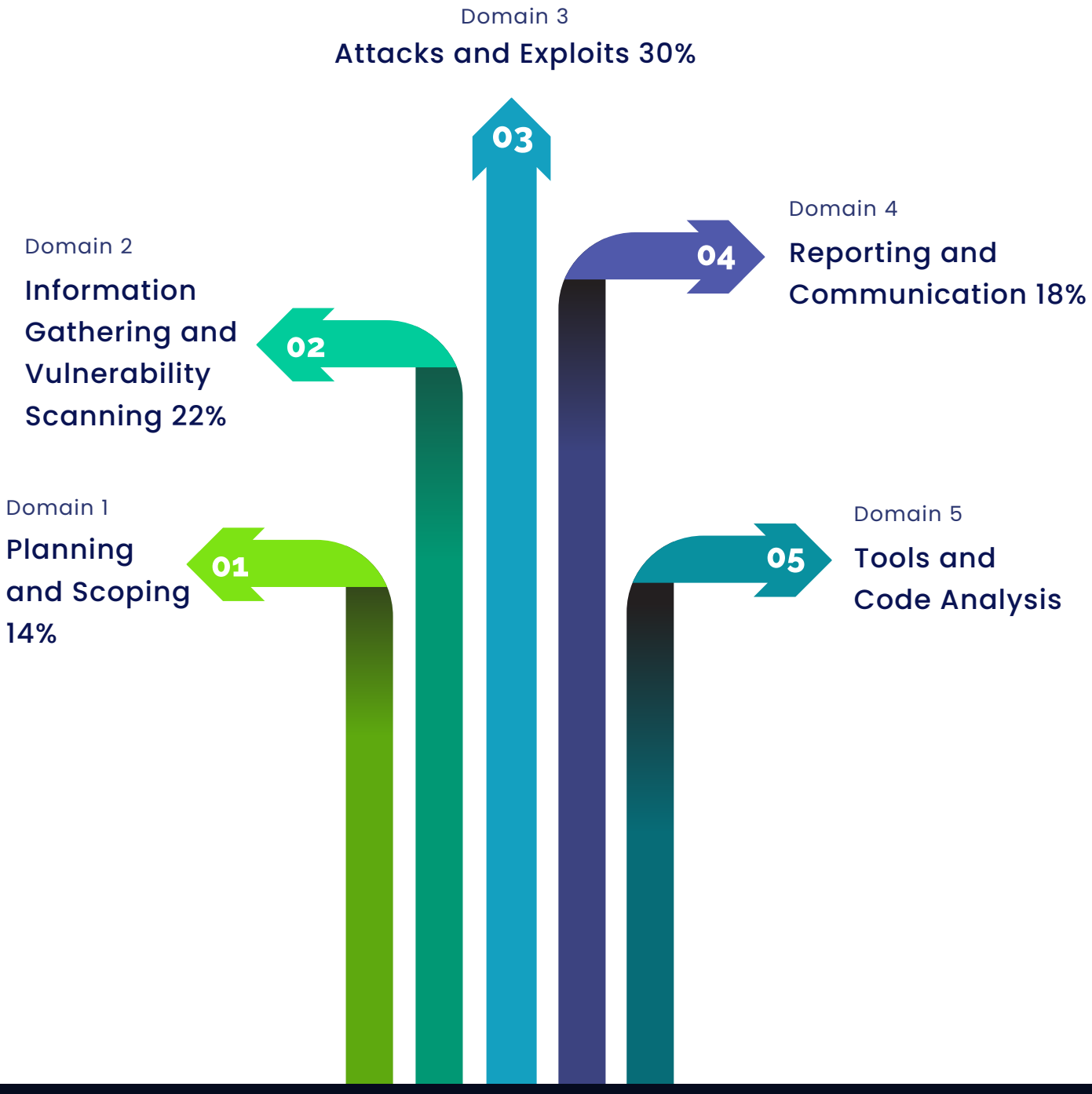
INFOSECTRAIN

Why Infosec Train?

Certified & Experienced Instructor	Flexible Schedule	Access to the recorded sessions
Post Training Support	Tailor Made Training	4 hrs/day in Weekend/ Weekday

INFOSECTRAIN

CompTIA PT0-002 domains



Course Content

1.0 planning and scoping

1.1 Compare and contrast governance, risk, ad compliance concepts

1.2 Explain the importance of scoping organizations/customer requirements

1.3 Given a scenario, demonstrate an ethical hacking mindset by maintaining professionalism and integrity.

2.0 Information gathering and vulnerability scanning

2.1 Given a scenario, perform passive reconnaissance

2.2 Given a scenario, perform active reconnaissance

2.3 Given a scenario, analyze the results of a reconnaissance exercise

2.4 Given a scenario, perform vulnerability scanning

3.0 Attacks and Exploits

3.1 Given a scenario, research attack vectors and perform network attacks

3.2 Given a scenario, research attack vectors and perform wireless attacks

3.3 Given a scenario, research attack vectors and perform application-based attacks

3.4 Given a scenario, research attack vectors and perform attacks on cloud technologies

3.5 Explain common attacks and vulnerabilities against specialized systems

3.6 Given a scenario, perform a social engineering or physical attack

3.7 Given a scenario, perform post-exploitation techniques

4.0 Reporting and Communication

4.1 Compare and contrast important components of written reports

4.2 Given a scenario, analyze the findings and recommend the appropriate remediation within a report

4.3 Explain the importance of communication during the penetration testing process

4.4 Explain post-report delivery activities

5.0 Tools and Code Analysis

5.1 Explain the basic concepts of scripting and software development

5.2 Given a scenario, analyze a script or code sample for use in a penetration test

5.3 Explain use cases of the following tools during the phases of a penetration test

www.infosectrain.com | sales@infosectrain.com