

Metasploit: Getting Started

PENETRATION TESTING ETHICS AND PROCESSES



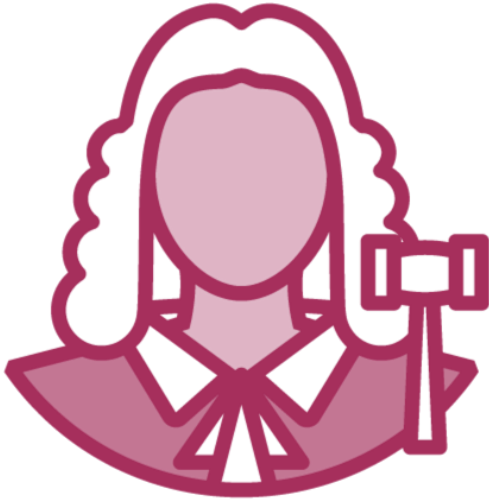
Keith Watson

INFORMATION SECURITY PROFESSIONAL

@ikawnoclast ikawnoclast.com



Penetration Testing and You



Combat crime



Validate security



Choose your path



Welcome to Globomantics



New Red Team member

- Assemble our toolkit
- Learn the tools

Focus on the Metasploit Framework



Course Overview



Penetration testing ethics and process

Metasploit Framework capabilities

Metasploit Framework architecture

Installing and configuring the Metasploit Framework

Preparing an attack

Launching an attack

Working with the Metasploit Framework



Module Overview



Ethics and Codes of Conduct

Testing Processes

Course Guidance



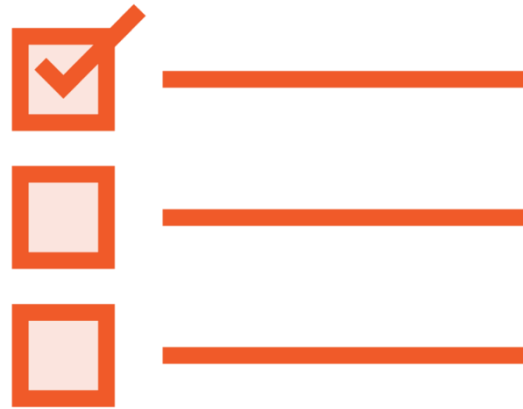
Ethics and Codes of Conduct



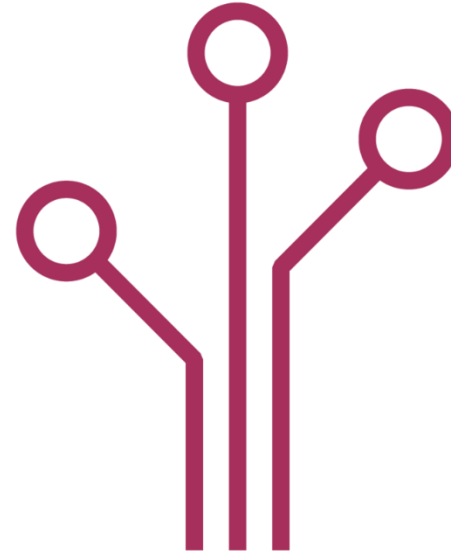
Ethics



Expectations



Codes of
conduct



Choices



Moral reasoning

The Power of Metasploit

Use for “Good”

- Identifies weaknesses
- Informs stakeholders
- Highlights needed changes
- Protects information
- Protects the organization
- Strengthens the profession

Use for “Evil”

- Identifies weaknesses
- Informs attackers
- Highlights targets to exploit
- Compromises information
- Compromises the organization
- Weakens the profession



Codes of Ethics



EC-Council Code of Ethics
(ISC)² Code of Ethics



EC-Council Code of Ethics

<https://www.eccouncil.org/code-of-ethics/>

1 Privacy

2 Intellectual property

3 Disclosure of dangers

4 Areas of competence

5 Software use

6 Deceptive financial practices

7 Property use

8 Disclosure to concerned parties

9 Good management

10 Knowledge sharing



EC-Council Code of Ethics

<https://www.eccouncil.org/code-of-ethics/>

11 Confidence

12 Ethical conduct

13 Association with malicious hackers

14 Purposefully compromise clients

15 Authorization

16 No Black Hat Activity

17 No underground hacking

18 No inappropriate references

19 No felony convictions



(ISC)² Code of Ethics

<https://www.isc2.org/ethics/>

Protect society, the common good, necessary public trust and confidence, and the infrastructure

Act honorably, honestly, justly, responsibly, and legally

Provide diligent and competent service to principals

Advance and protect the profession



Testing Processes



Without a Standard



Sloppy and incorrect results

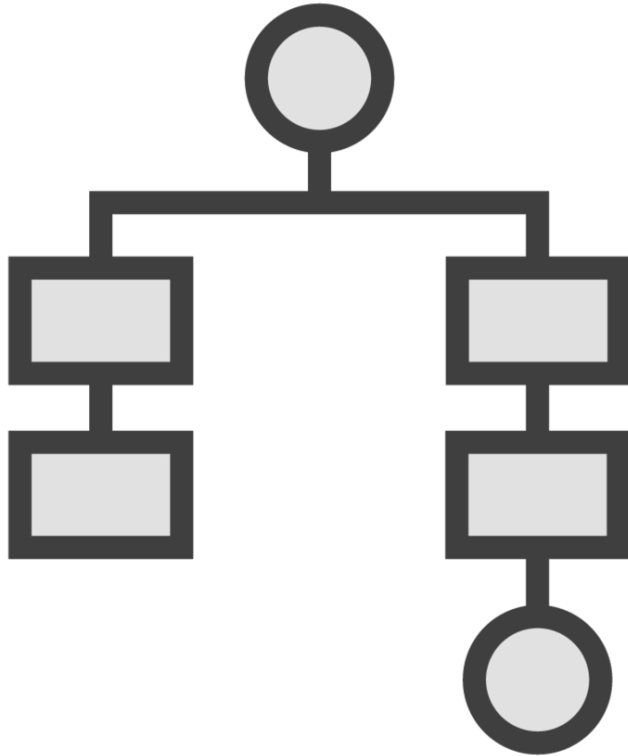
Inaccurate and invalid reports

Inconsistent delivery of testing

Poor customer value

The Penetration Testing Execution Standard

<https://www.pentest-standard.org/>



Created by experienced pen testers

Not a formal standard

Valuable to clients and pen testers

Show expectations of skills for professional penetration tester

Seven sections organized into an engagement timeline



Pre-engagement interactions

Intelligence gathering

Threat modeling

Vulnerability analysis

Exploitation

Post-exploitation

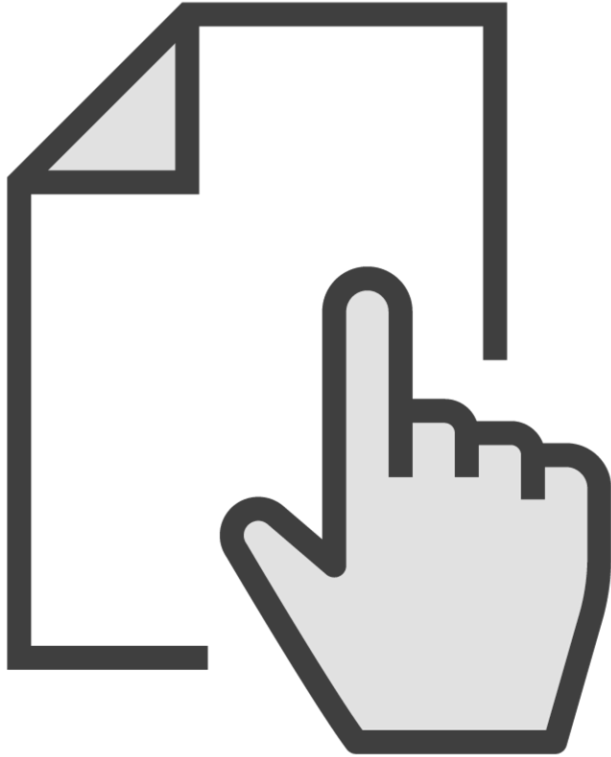
Reporting



Course Guidance and Summary



Course Guidance



The Metasploit Framework is big

Some technical experience is needed

Follow the module order

Install Kali Linux and experiment

Have fun!



Module Summary



Ethics

Codes of Ethics

Processes in Penetration Testing



Up Next:

Metasploit Framework Capabilities

