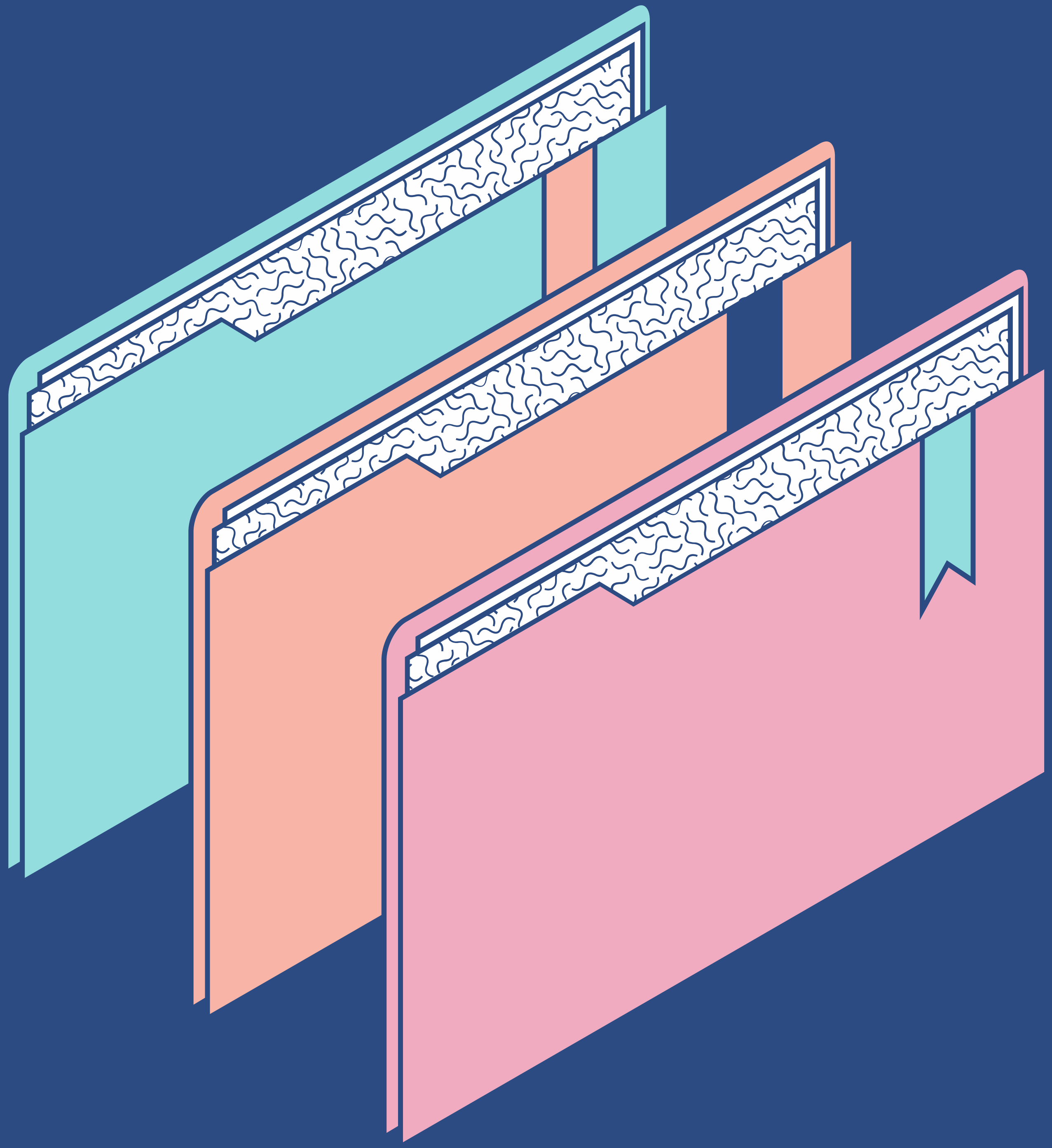
Introduction To Penetration Testing



What are Pentesters?

They are cybersecurity professionals who simulate cyberattacks on computer systems, networks, or applications to identify vulnerabilities. Their goal is to uncover weaknesses before malicious hackers can exploit them.

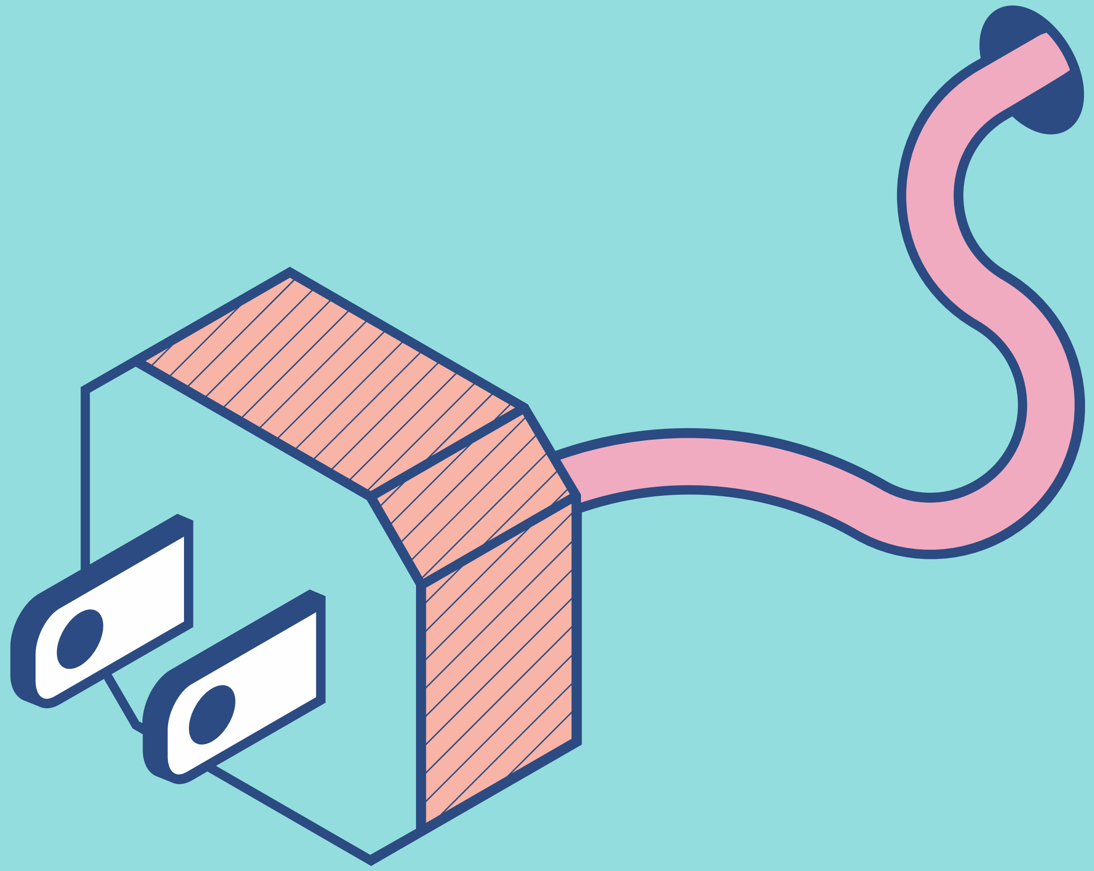
Penetration Tests Terms

- **vulnerability**: A weakness or flaw in a system's design, implementation, or configuration that could be exploited to compromise its security.

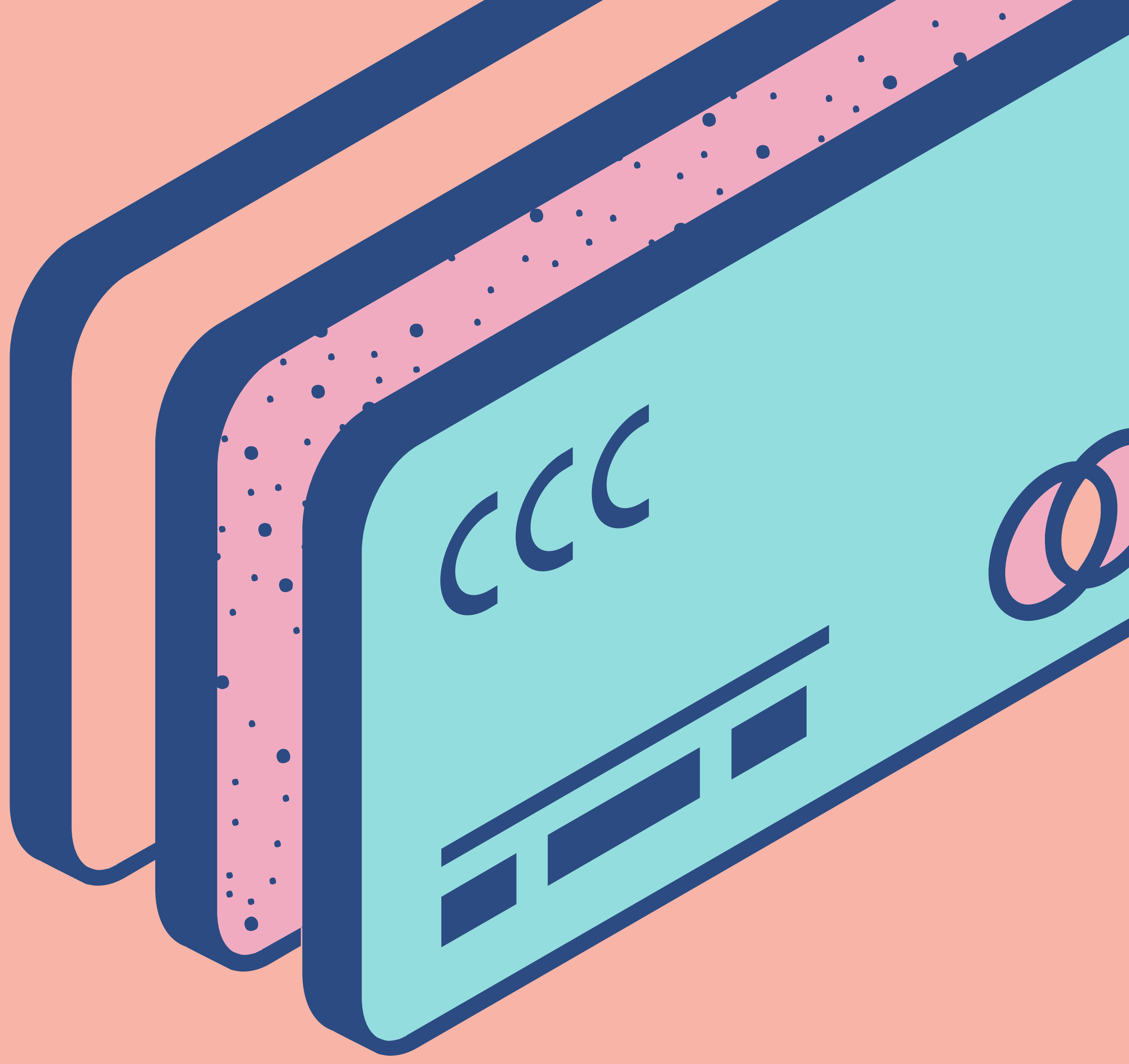
- **Exploit**: A piece of software, code, or technique that takes advantage of a specific vulnerability to compromise a system.

- **Payload**: Malicious code or software delivered and executed on a target system after a successful exploit

- **CVE:** is a dictionary of publicly known information security vulnerabilities and exposures.



Responsibilities of Penetration Testers



Identifying Vulnerabilities

- Use automated tools and manual techniques to identify vulnerabilities.
- Analyze the results of vulnerability scans and assessments.

Exploitation

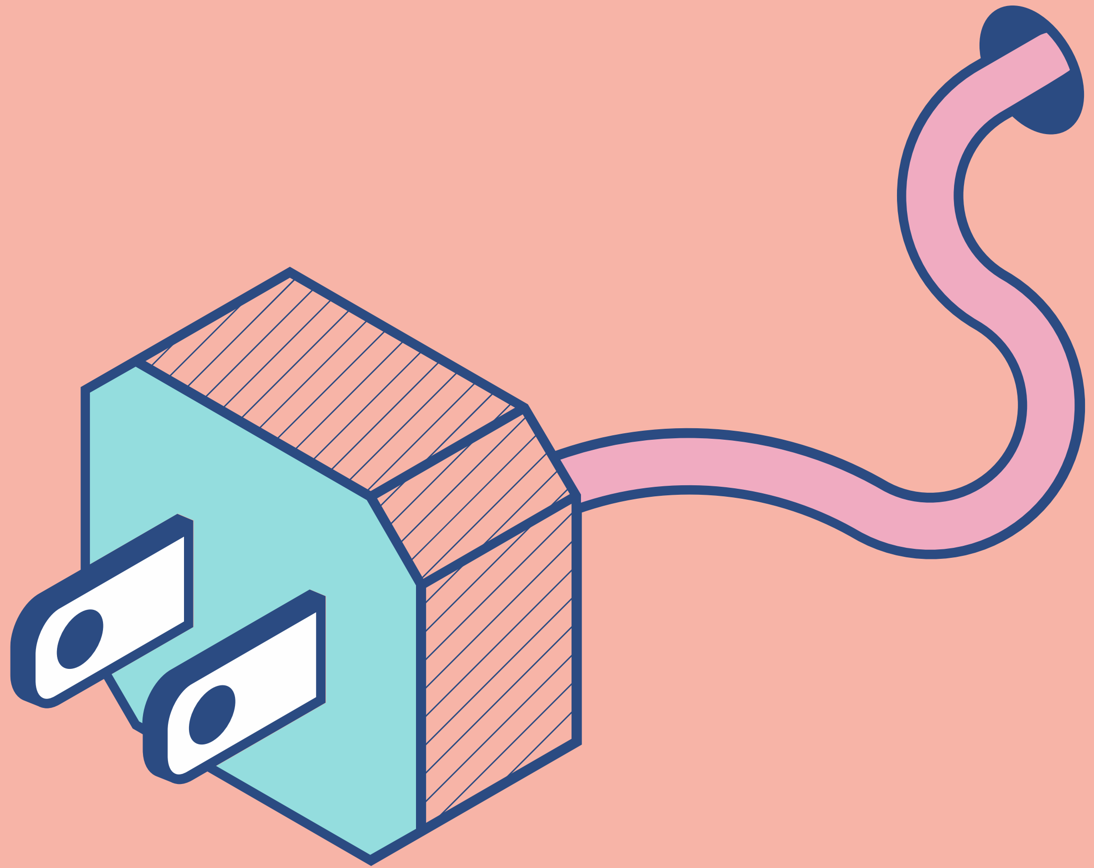
- Attempt to exploit identified vulnerabilities to determine their impact.
- Follow ethical guidelines to avoid causing damage to systems.

Documentation

- Maintain detailed records of the testing process, methodologies, and results.

Types of Pentesters ?

- **White Box Testers**: Have complete knowledge of the system being tested.
- **Black Box Testers**: Simulate an external hacker with no prior knowledge of the system.
- **Gray Box Testers**: Have partial knowledge, of simulating an insider threat.



Phases of Penetration Testing

1

RECONNAISSANCE

- Gather information about the target.
- Use passive methods like public information and social engineering.

2

ENUMERATION

- Extract additional information about the target

3

VULNERABILITY ANALYSIS

- Identify and assess potential vulnerabilities

4

EXPLOITATION

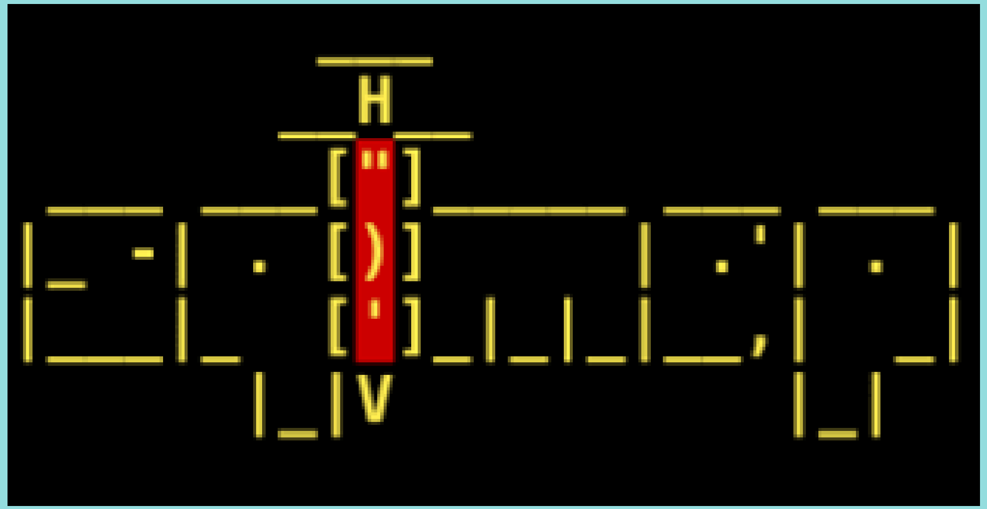
- Attempt to exploit identified vulnerabilities.

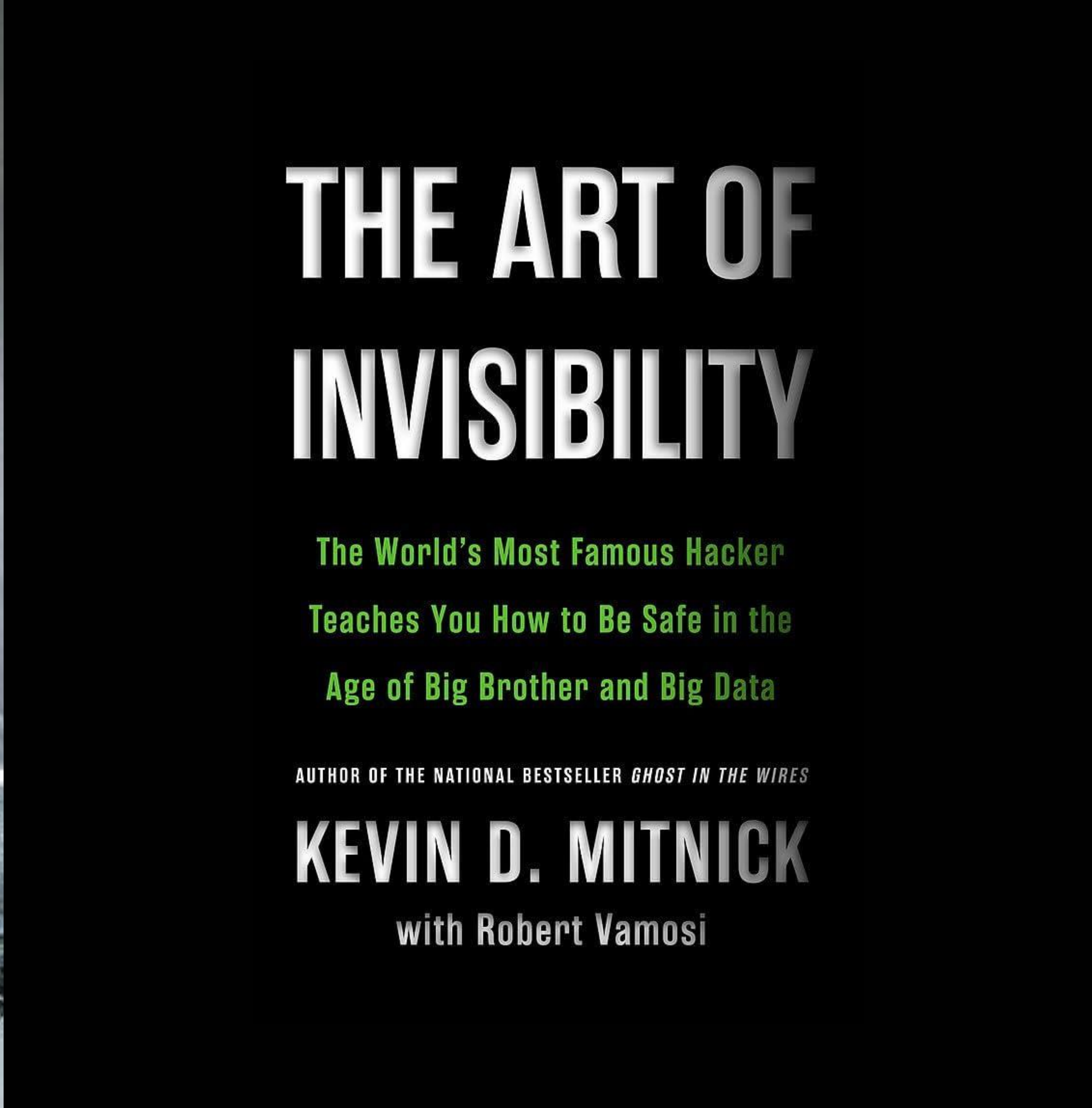
5

REPORTING

- Create a detailed report of findings.
- Include an executive summary, technical details, and recommended mitigations.

Tools Used For Penetration testing





THE ART OF INVISIBILITY

The World's Most Famous Hacker Teaches You How to Be Safe in the Age of Big Brother and Big Data

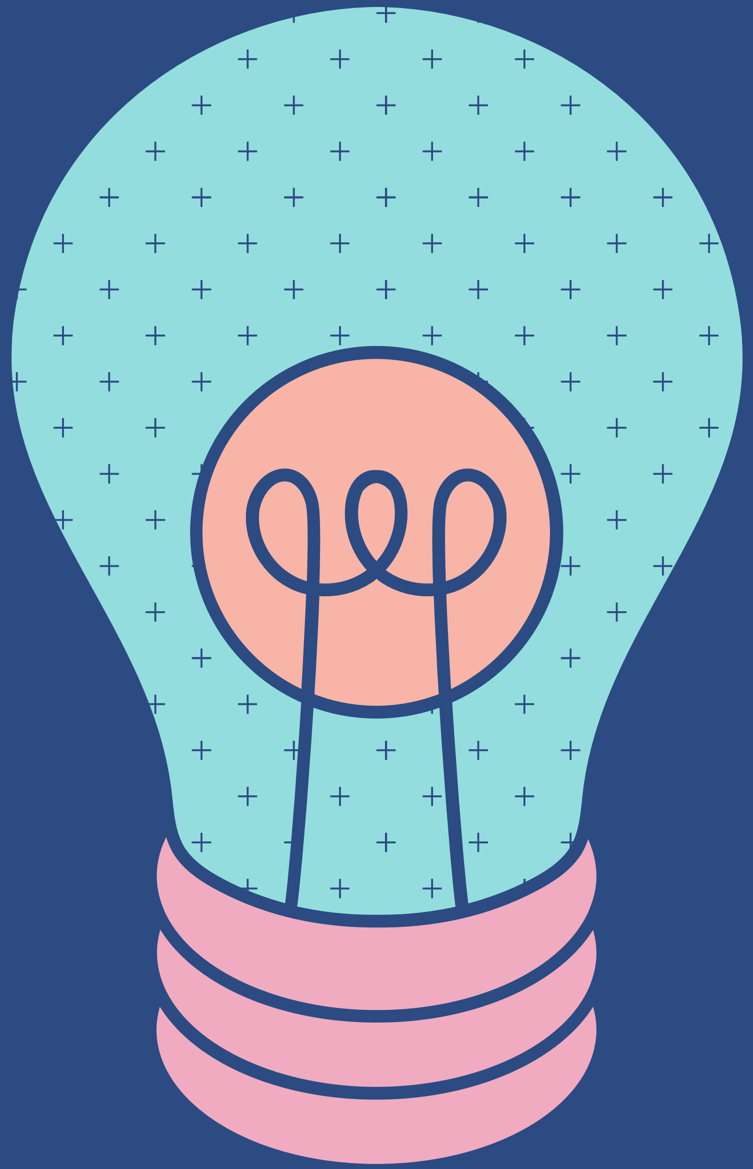
AUTHOR OF THE NATIONAL BESTSELLER *GHOST IN THE WIRES*

KEVIN D. MITNICK

with Robert Vamosi

“In the world of cybersecurity, hackers are the artists, and penetration testers are the critics, working together to create a masterpiece of resilience and security."

UNKNOWN



Do you have any questions?

We hope you learned something new.