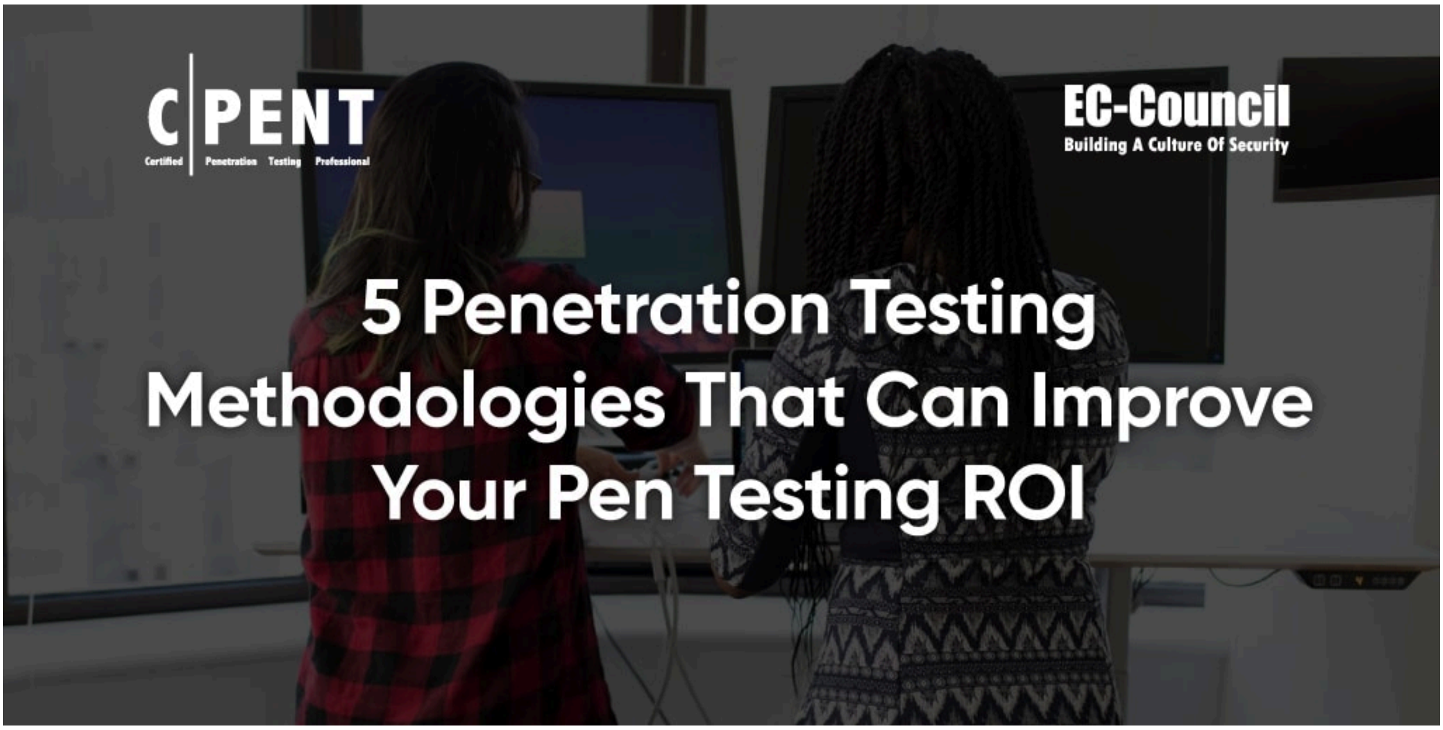
Five Methodologies That Can Improve Your Penetration Testing ROI

EC-Council ⋮ 7-9 minutes ⋮ 3/16/2022
DOI: 10.1016/b978-0-12-803843-7.00062-4, Show Details


C|PENT
Certified Penetration Testing Professional
EC-Council
Building A Culture Of Security
5 Penetration Testing Methodologies That Can Improve Your Pen Testing ROI

Penetration testing, also known as pen testing, is a valuable tool that your organization can use to find IT vulnerabilities and secure its network. However, it can be challenging to decide which pen testing techniques and standards to apply in your organization. Below, we lay out five of the top methodologies that you can apply to maximize your pen testing ROI.

Popular Pentest Methodology and Standards

1. OSSTMM

The Open Source Security Testing Methodology Manual (OSSTMM) is a peer-reviewed pen testing methodology (Institute for Security and Open Methodologies, 2010). It provides a scientific framework for network pentesting and vulnerability assessment and offers a comprehensive guide that can be properly utilized by a certified pen tester. The OSSTMM covers five categories (Rounsavall, 2017):

- Data and information controls
- Cyber Security awareness among personnel
- Fraud and social engineering controls
- Controls for networked devices, including computers and wireless devices
- Physical security controls

One of the main benefits of the OSSTMM is its high level of flexibility. If pen testers apply the OSSTMM properly, they can use it to resolve vulnerabilities found on multiple devices, including computers, servers, wireless devices, and more.

2. OWASP

The Open Web Application Security Project (OWASP) Foundation (2020, 2021, 2022) maintains pen testing methodologies and comprehensive guides for testing web, mobile, and firmware devices. When executed properly, the OWASP methodologies can help pen testers identify a series of vulnerabilities in a network's firmware and mobile or web applications.

3. NIST

The National Institute of Standards and Technology (NIST; 2022) is an agency within the U.S. Department of Commerce. NIST's goal regarding information security standards is not to establish one specific methodology but rather to create a series of pen testing standards (Scarfone et al., 2008). While the federal government is required to meet the NIST standards, other networks often also adhere to them.

The NIST standards should be considered the absolute minimum, not the only standards that a business or other organization should meet. Any certified pen tester must be familiar with the network and application pen testing methodologies created by NIST.

4. PTES

The Penetration Testing Execution Standard (PTES; 2014) framework is a pen testing methodology that encompasses seven sections:

- Pre-engagement interactions
- Intelligence gathering
- Threat modeling
- Vulnerability analysis
- Exploitation
- Post-exploitation
- Reporting

PTES (2012) also provides an extensive technical guide that enables pen testers to execute the methodology.

5. ISSAF

The Information System Security Assessment Framework (ISSAF) is a specialized approach to pen testing (Open Information Systems Security Group, 2006). Its extensive guidebook—which clocks in at over 1,200 pages—lays out the framework behind this testing methodology. The ISSAF's comprehensible approach is easy for individual organizations and pen testers to customize, allowing for the creation of personalized testing plans. Any penetration tester using multiple tools should adhere to the ISSAF methodology.

It is important to note that the ISSAF goes well beyond simple pen testing: It also encompasses the creation of tools that can be used to educate other individuals who have access to a network. It also ensures that individuals who use a given network adhere to appropriate legal standards.

Want to Learn More?

Cyberthreats to your organization will continue to evolve and accelerate, but robust pen testing can support your network's security. Applying a tried-and-true pen testing methodology ensures that you're getting the best possible ROI from your network pen testing.

Hiring a certified pen tester can yield significant benefits for your organization. Certified pen testing professionals understand the latest network threats and know how to conduct pen testing using various methodologies. The EC-Council Certified Security Analyst (E|CSA) certification program teaches invaluable information about pen testing. It is one of a series of penetration testing certifications offered by EC-Council. Other options include our Certified Penetration Testing Professional (C|PENT) and our Licensed Penetration Tester Master (L|PT) courses.

Enroll in the E|CSA course today to ensure that you can manage and mitigate any threats to your network.

References

Institute for Security and Open Methodologies. (2010). OSSTMM 3: The Open Source Security Testing Methodology Manual. *https://www.isecom.org/OSSTMM.3.pdf*

National Institute of Standards and Technology. (2022, January 11). About NIST. *https://www.nist.gov/about-nist*

Open Information Systems Security Group. (2006). Information System Security Assessment Framework (ISSAF). *https://untrustednetwork.net/files/issaf0.2.1.pdf*

OWASP Foundation. (2020). OWASP web security testing guide. *https://owasp.org/www-project-web-security-testing-guide/*

OWASP Foundation. (2021). OWASP firmware security testing methodology *https://scriptingxss.gitbook.io/firmware-security-testing-methodology*

OWASP Foundation. (2022). OWASP mobile security testing guide. *https://owasp.org/www-project-mobile-security-testing-guide/*

Penetration Testing Execution Standard. (2012). PTES technical guidelines. *http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines*

Penetration Testing Execution Standard. (2014). High level organization of the standard. *http://www.pentest-standard.org/index.php/Main_Page*

Rounsavall, R. (2017). Storage area networking security devices. In J. R. Vacca (Ed.), Computer and information security handbook (3rd ed.), pp. 879–894. Elsevier. *https://doi.org/10.1016/B978-0-12-803843-7.00062-4*

Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115). National Institute of Standards and Technology, U.S. Department of Commerce. *https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf*

Share this Article