01

Penetration Testing

What is Pen-Testing?

Penetration testing is:

- Designed to assess and investigate one’s security before an attacker does
- A simulated event or test to discover and exploit vulnerabilities or weaknesses in a system with a goal of strengthening overall security posture

Why should you Pen-Test?

$4,350,000

The average cost of a data breach is 4.35 million and according to Acronis' annual end-of-year Cyberthreats Report, the average cost of a data breach is expected to exceed a cost of $5,000,000 per incident this year. Keeping a consistent security testing program reduces the overall chances of a breach and empowers users with a better understanding of their where they can improve their security operations.

Penetration Testing Methodology

A penetration testing methodology is a comprehensive methodological approach that is used in pen-testing to identify vulnerabilities and weaknesses in the overall security posture of an organization

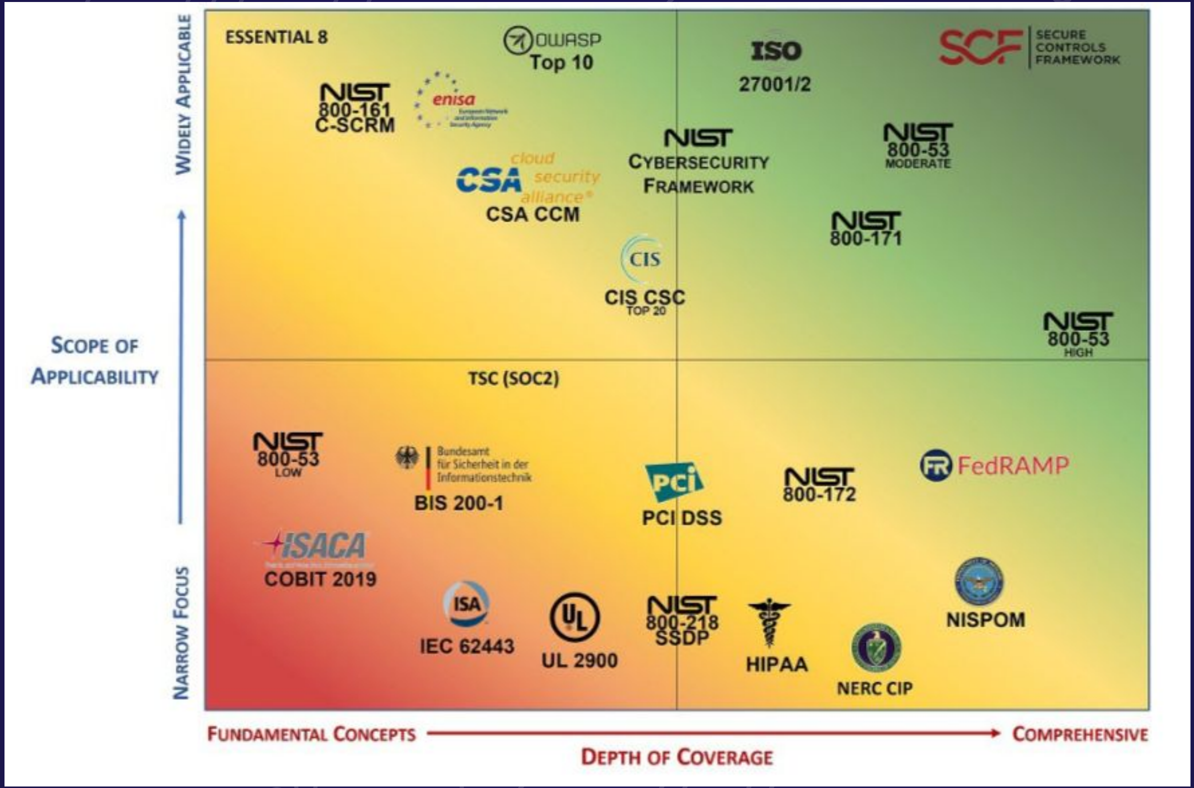
Advantages

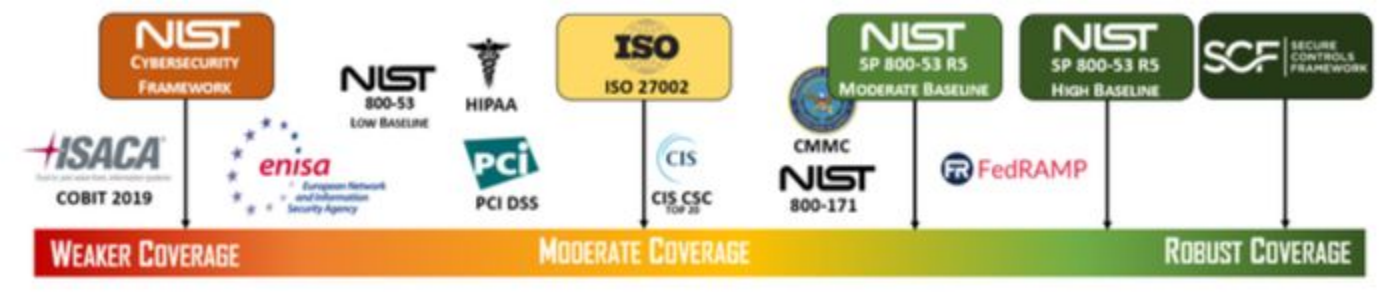
1. Clear Methodical and systematic approach to testing

2. Ensures that tests are reliable, accurate and consistent across the board

Pen-testing methodologies need to be extremely comprehensive and accurate to ensure that the penetration test is performed successfully

Cybersecurity Frameworks




NIST Cybersecurity Framework
ISACA
COBIT 2019
enisa
European Network and Information Security Agency
NIST 800-53 Low Baseline
HIPAA
PCI DSS
ISO
ISO 27002
CIS
CIS CSC Top 20
CMMC
NIST 800-171
NIST SP 800-53 R5 Moderate Baseline
FedRAMP
NIST SP 800-53 R5 High Baseline
SCF Secure Controls Framework
Weaker Coverage
Moderate Coverage
Robust Coverage

Cybersecurity frameworks are sets of documents describing guidelines, standards, and best practices designed for risk management. The frameworks exist to reduce an organization's exposure to weaknesses and vulnerabilities that hackers and other cyber criminals may exploit. These frameworks can serve as a starting point for organizations to choose which security controls work best and remove some of the guesswork in securing digital assets. Frameworks provide a reliable, standardized, systematic way to mitigate cyber risk regardless of the environment's complexity.

Framework	Description
NIST 800-53	A comprehensive info security management guide that includes specific controls and requirements. By following this framework, orgs can ensure that their pen-testing efforts are aligned with industry best practices Commonly used by medium-large businesses such as: Defense Contractors, Government Contractors, Technology Businesses, General Business, Retail, Healthcare, Insurance
ISO 27001/2	An international standard that provides guidelines for info security management, including a set of controls and requirements as part of an org's risk management strategy ISO 27001 lays out the framework to create an Information Security Management System . ISO 27002 contains the best practices of what goes into building a security program. Commonly used by medium to large businesses such as: Retail, Healthcare, Insurance

Framework	Description
NIST SP 800-171	A set of security requirements for protecting Controlled Unclassified Information in nonfeder systems and orgs, which includes requirements for performing pen testing as a part of security assessment and authorization process Can be used by any size org. Commonly used for: Defense Contractors. Government Contractors. Technology Businesses
OWASP	A comprehensive guide that provides testers with a framework for testing web applications for security vulnerabilities
NIST CSF	Comprises of risk-based guidelines that can help organizations identify and improve cybersecurity practices . Works great for smaller and unregulated businesses

The phases of penetration testing are a specific course taken by a pen-test provider to conduct the pentest of a target website or network. Each phase depends on the goal and range or “scope” of the penetration test.

Stages	Description
Reconnaissance	The initial phase - gathers info about the target system/network
Scanning & Enumeration	Uses tools to scan the target network for vulnerabilities
Vulnerability Analysis	Attempts to exploit any identified vulnerabilities to gain unauthorized access to the target system/network
Exploitation	Uses attack methods such as password cracking or social engineering to gain access to sensitive info or systems
Post-Exploitation	Attempts to maintain access to the target system/network, escalate privileges, & gather info about the target environment
Reporting	The final stage - documents the findings of the test and recommends necessary remediation
Retesting	Retests parts that needed to be fixed

Penetration Testing Approaches

Black Box

External “No Knowledge” Penetration Test

- Simulates a real world attack with uniformed attacker
- Made easier by deploying a series of exploits known as the “Trial and error approach”
- Can take 6 weeks depending on scope of project
- Companies can pay anywhere between $10k-25k

Gray Box

“Partial knowledge” or access to internal network or web application

- Reporting provides a more focused and efficient assessment of your networks security
- May begin with user privileges and be told to escalate privileges to domain admin or asked to gain access to source code and system architecture diagrams

White Box

Internal “Full Knowledge” Penetration Testing

- Access to source code and environment
- In depth security audit of business security system
- Tends to be a more thorough pen-test but may require use of code analyzers and debuggers
- Can take 2-3 weeks to complete and costs between $4k-20k

Types of Penetration Testing

Network Services (Infrastructure pen-testing)

Identifies vulnerabilities in network infrastructure (servers, firewalls, routers, switches, printers etc)

Client Side

Identifies vulnerabilities and security weaknesses in client-side software or application (Putty, email clients, internet browser, Adobe Suite, Microsoft office)

Social Engineering

Malicious actors try to persuade or trick users into giving them sensitive information (Phishing Attacks, Vishing, Smishing, Tailgating, etc.)

Web Application

Identifies vulnerabilities in web applications. Targets web-based apps, browsers, and their components

Wireless

Involves identifying and examining the connection of every device to the organization's WiFi (IoT devices, tablets, laptops, smartphones, etc.)

Physical

Pen-tester attempts to compromise physical barriers to access a business infrastructure, building, systems, or employees the primary benefit is to expose weaknesses and vulnerabilities in the physical controls of an organization such as locks, barriers, cameras, sensors, etc.

Penetration Testing Tools & Applications

Kali Linux *(formerly known as BackTrack Linux)* is an open-source, Debian-based Linux distribution aimed at advanced Penetration Testing and Security Auditing. It does this by providing common tools, configurations, and automations which allows the user to focus on the task that needs to be completed, not the surrounding activity.

Kali Linux contains industry specific modifications as well as several hundred tools targeted towards various Information Security tasks, such as Penetration Testing, Security Research, Computer Forensics, Reverse Engineering, Vulnerability Management and Red Team Testing.

Kali Linux is a multi-platform solution, accessible and freely available to information security professionals and hobbyists.

Metasploit

Metasploit is the world's leading open-source penetrating framework used by security engineers as a penetration testing system and a development platform that allows to create security tools and exploits. The framework makes hacking simple for both attackers and defenders.

The various tools, libraries, user interfaces, and modules of Metasploit allow a user to configure an exploit module, pair with a payload, point at a target, and launch at the target system. Metasploit's large and extensive database houses hundreds of exploits and several payload options

nessus® Professional

Nessus is an open source remote security scanning tool, which scans a computer and raises an alert if it discovers any vulnerabilities that malicious hackers could use to gain access to any computer you have connected to a network. It does this by running over 1200 checks on a given computer, testing to see if any of these attacks could be used to break into the computer or otherwise harm it.

Unlike other scanners, Nessus does not make assumptions about your server configuration that can cause other scanners to miss real vulnerabilities. Nessus is very extensible, providing a scripting language for you to write tests specific to your system once you become more familiar with the tool. Its also provides a plug-in interface, and many free plugins are available from the Nessus plugin site.   These plugins are often specific to detecting a common virus or vulnerability.

intruder

The Intruder vulnerability scanner is a cloud-based software tool that finds and prioritizes cybersecurity weaknesses, helping organizations avoid the most serious security risks.

Intruder is rich with basic functionality. It enables you to scan all of your servers, clouds, website, and industry devices to find, identify, and prioritize missing updates and missing patches, misconfiguration (a common source of breaches especially in the cloud today), encryption issues, and much more.

Intruder’s continuous vulnerability monitoring system ensures that you are secured against even the very latest threats and have time to act before it’s too late. Cyber attackers typically move quickly to adopt exploits to leverage the latest vulnerabilities. Continuous vulnerability scanning helps enterprises that may not have a full threat research program.