Farah Alhamzawi

Independent Study and Mentorship

Mr.Green

26 September 2023

Research Assessment: Understanding Penetration Testing in Cybersecurity

Chickowski, Ericka. “Cybersecurity Penetration Testing Explained: What Is Pen Testing?” AT& T Cybersecurity, cybersecurity.att.com/blogs/security-essentials/cybersecurity-penetration-testing-explained. Accessed 26 Sept. 2023.

Penetration testing, often colloquially referred to as 'pen tests,' is a critical method in cybersecurity for evaluating and enhancing the security posture of software and systems. This research assessment explores the critical aspects of penetration testing, its types, phases, and benefits to businesses, as well as differentiating it from vulnerability scanning.

Penetration testing involves simulating real-world cyberattacks to identify security weaknesses in software and systems. Its primary purpose is to detect vulnerabilities before malicious hackers can exploit them proactively. Penetration tests go beyond automated vulnerability scans, focusing on uncovering gaps in protection that can result from the complex interplay of applications, systems, and security defenses in live environments.

Penetration tests are categorized into two main types: External Penetration Testing and internal penetration testing. External penetration testing tests simulate attacks outside an organization's network, targeting assets like web applications, website servers, open APIs, and DNS infrastructure. Internal penetration testing starts from within an organization's network, replicating attacks that malicious insiders or external attackers who have already infiltrated the network could be executed.

Types of Penetration Tests are white box testing, black box testing, grey box testing, social engineering attempts, and team engagements. The difference between the tests is that the white box provides detailed information about the target organization and systems, and black box testers receive partial information and may gain more as the testing progresses. While social engineering attempts are Pen testers use social engineering tactics to trick employees into providing access to systems, and ream engagements are structured scenarios involving red teams (pen testers) attacking blue teams' (defenders) assets.

There are five different Phases of Penetration Testing. The first phase is Scoping. This phase Defines test goals, rules of engagement, and target systems. The second phase is Recon and Scanning, which gathers intelligence on the network and systems, identifying vulnerabilities. Third is Gaining Access, which Exploits vulnerabilities to access systems, moving laterally and escalating privileges. Fourth is Maintaining Access and Evading Detection, in which Testers may seek persistence and assess the security team's detection capabilities. Finally, the last section is Reporting and Analysis, which is Detailed reporting on vulnerabilities exploited, sensitive data accessed, and recommendations for remediation.

Penetration testing offers several crucial advantages for organizations, it allows us to assess real-world cyber readiness, Uncover complex vulnerabilities, business logic flaws, and process weaknesses, Identify compliance violations and fulfill regulatory requirements, Document security gaps for auditing and executive review, and Prioritize remediation based on the exploitability of discovered issues.

Many organizations collaborate with Managed Security Service Providers (MSSPs) for penetration testing due to their specialized expertise. Ethical hackers within MSSPs possess deep knowledge and experience in mimicking attacks and providing valuable insights to organizations. This expertise is often challenging to replicate with in-house teams.

While vulnerability scanning tools are sometimes used within penetration testing, the two practices differ significantly. Vulnerability scanning primarily generates lists of known vulnerabilities and configuration flaws. In contrast, penetration testing identifies complex, emerging, or obscure vulnerabilities, including business logic flaws, ineffective network segmentation, etc.

In conclusion, penetration testing is a vital cybersecurity practice that helps organizations proactively identify and mitigate security vulnerabilities. Its multifaceted approach, encompassing various types, phases, and the involvement of specialized professionals, makes it an indispensable component of any comprehensive cybersecurity strategy.