Ausarbeitung ITSI - Pentesting

Latschbacher Lukas

April 28, 2024

Contents

1 Einleitung

In einer zunehmend digitalisierten Welt, in der Daten die Währung sind und Sicherheitsverletzungen täglich Schlagzeilen machen, ist der Schutz von Informationssystemen von entscheidender Bedeutung. Unternehmen, Regierungen und Organisationen sind sich der Notwendigkeit bewusst, ihre IT-Infrastruktur auf potenzielle Schwachstellen zu prüfen, um sich gegen Cyberangriffe zu verteidigen. In diesem Zusammenhang nimmt das Penetration Testing eine zentrale Rolle ein. Diese Ausarbeitung widmet sich daher der eingehenden Betrachtung des Penetration Testings im Kontext der IT-Sicherheit, insbesondere unter Berücksichtigung der Windows-Plattform.

Penetration Testing, auch bekannt als Ethical Hacking, ist eine proaktive Methode zur Identifizierung von Sicherheitslücken in einem Informationssystem. Dabei wird versucht, wie ein potenzieller Angreifer vorzugehen, um Schwachstellen aufzudecken, bevor sie von bösartigen Akteuren ausgenutzt werden können. Die Durchführung eines Penetration Tests erfordert ein tiefgreifendes Verständnis der zugrunde liegenden Technologien und Angriffstechniken sowie eine sorgfältige Planung und Durchführung, um die Integrität und Vertraulichkeit der getesteten Systeme zu wahren.

Insbesondere die Sicherheit von Windows-Systemen steht im Fokus vieler Organisationen, da Windows das am weitesten verbreitete Betriebssystem in Unternehmensumgebungen ist. Die Komplexität und Vielfalt von Windows-Systemen bieten sowohl Chancen als auch Herausforderungen für Sicherheitsfachleute. Daher ist es unerlässlich, ein fundiertes Verständnis der Windows-Sicherheitsmechanismen sowie der gängigen Angriffsmethoden zu entwickeln, um effektive Schutzmaßnahmen zu implementieren und Sicherheitsvorfälle zu verhindern.

Im Rahmen dieser Ausarbeitung werden wir zunächst die Grundlagen des Penetration Testings erläutern, einschließlich seiner Ziele, Methoden und Phasen. Anschließend werden wir uns eingehend mit der Sicherheit von Windows-Systemen befassen, indem wir potenzielle Angriffsvektoren identifizieren, Sicherheitsmechanismen analysieren und bewährte Praktiken zur Stärkung der Windows-Sicherheit diskutieren. Durch die Kombination von theoretischem Wissen und praktischen Einblicken wollen wir einen umfassenden Überblick über die Rolle des Penetration Testings im Kontext der Windows-Sicherheit bieten und damit einen wertvollen Beitrag zur IT-Sicherheit leisten.

2 Grundlagen von Pentesting

Penetrationtesting oder auch Pentesting ist dafür um Sicherheitslücken in IT-Systemen aufzufinden. Nicht nur Sicherheitslücken sondern auch die Schwierigkeit in ein System einzudringen wird durch einen Pentest bestimmt. Dadurch soll die Sicherheit erhöht werden und vor zukünftigen Angriffen geschützt werden. Sie werden von sogenannten "ethisch Hackern" durchgeführt, welche mit einer Genehmigung der Eigentümer Systeme angreifen um Securityissues aufzuspüren, damit diese danach behoben werden können. Die Angriffe finden mit den selben Methoden wie bei Angriffen von nicht ethischen Hackern statt. Weiters gibt es verschiedene Arten von Pentests, welche in einem der folgenden Kapitel erklärt werden.

2.1 Tools für Pentests

2.1.1 Vulnerability Scans

2.1.2 Port Scanning

2.2 Arten von Pentests

2.3 Phasen eines Pentests

2.3.1 Vorbereitung

2.3.2 Informationsbeschaffung

2.3.3 Bewertung der Ergebnisse

2.3.4 Angriffsversuch

2.3.5 Verfassung eines Berichts

3 Windows Sicherheit

4 Stichwörter

4.1 Cloud Computing und Internet of Things

4.2 Automatisierung, Regelung und Steuerung

4.3 Security, Safety, Availability

4.4 Authentication, Authorization, Accounting

4.5 Algorithmen und Protokolle

4.6 Konsistenz, Datenstruktur und Visualisierung