Ausarbeitung ITSI - Pentesting

Latschbacher Lukas

April 29, 2024

Contents

1 Einleitung

Die folgende Ausarbeitung handelt von Penetration Testing und ist für das Fach IT-Security geschrieben. Diese dient als Grundlage für die mündliche Reife- und Diplomprüfung und ist dafür ausgearbeitet. Die folgenden Kapitel handeln von den Grundlagen von Pentesting und von der Sicherheit von Windows.

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