Projektarbeit im Studiengang CNB, 4. Semester

Thema:
„Angreifbare Systeme analysieren“

Betreuer:
Prof. Dr. Kaspar

Studierende:

- Deniz Gül
- Simon Janz
- Kai Rotter
- Max Wannenmacher
- Marcel Kienzle

Projektpartner: intern

Projektbeschreibung:

In regelmäßigen Abständen ereilen uns Meldungen über sogenannte Hackerangriffe. Ob erbeutete Nutzerdaten, Zugang zu E-Mail-Konten, oder die Beeinflussung von Wahlen – es vergeht kaum ein Tag ohne neue Warnungen vor Täuschungen und Angriffen in der heutigen digitalen Welt. Betroffen sind Privatpersonen, kleine und mittelständische Unternehmen sowie Großkonzerne, Regierungen und staatliche Institutionen.
Eine Vielzahl der Angriffe lässt sich laut Experten auf Sicherheitslücken zurückführen.

Innerhalb des Semesterprojektes *Angreifbare Systeme analysieren* konnten die Studierenden unter der Leitung von Herr Prof. Dr. Kaspar in eingerichteten Labor- bzw. Testumgebungen verschiedene Systeme auf Schwachstellen prüfen um dann im nächsten Schritt konkrete Angriffe durchzuführen. Durch das Erkennen von Schwachstellen in der eigenen Netzwerkumgebung kann man Angreifern zuvorkommen, Verwundbarkeiten schließen und die Netzwerkumgebung optimieren und absichern.

Die Projektteilnehmer konnten verschiedene Aufgaben in Form von virtuellen Maschinen mit vorgefertigten Schwachstellen auswählen und lernten dabei den Umgang mit Werkzeugen, die das Betriebssystem Kali Linux bietet. Dieses stellt eine Sammlung von Programmen bereit, mit denen die Sicherheit eines Computersystems getestet und Angriffsmöglichkeiten aufgedeckt werden können.

Die Aufgaben unterscheiden sich zum einen durch den Schwierigkeitsgrad, aber auch von der Vorgehensweise je nach Kenntnisstand. Dabei erstreckt sich das Spektrum von Passwörter knacken und Aushebeln von Sicherheitsvorkehrungen, über Angriffe auf Web-Anwendungen bis hin zu Aufgaben mit Rätselcharakter, sodass sich das Projekt als sehr abwechslungsreich gestaltete.

Ziel der Herausforderungen war es Schwachstellen zu identifizieren und geschickt auszunutzen, sodass Administratoren-Rechte (sog. Root-Rechte) im System erlangt werden. Als Angreifer hat man damit vollen Zugriff auf das Betriebssystem und dessen Ressourcen.

In wöchentlichen Treffen mit Herrn Prof. Dr. Kaspar und den Projektteilnehmern fand ein Austausch über den Fortschritt und die aufgetretenen Schwierigkeiten statt. Dabei wurde auch gemeinsam über Vorschläge nachgedacht, die neue Angriffswege eröffnen konnten.

Als Ergebnisse des Projekts wurden ausführliche Lösungen erarbeitet, die das Vorgehen schrittweise dokumentieren, speziell auch unter den Aspekten, welche Vorkenntnisse und welcher Zeitaufwand für eine Aufgabe benötigt werden. Abschließend soll aus den Ergebnissen eine Einschätzung möglich sein, für welche Lernzwecke eine Aufgabe geeignet ist.

Symbolfoto:

Link:
Die Webseite https://www.vulnhub.com stellt eine Vielzahl an Aufgaben zur Verfügung, welche die Möglichkeiten bieten praktische Erfahrung mit Sicherheitsüberprüfungen (sog. Penetrationstests) zu sammeln.