Hackerworkshop der Universität Bonn im Rahmen der Vertiefungsphase 2022

Der zweiwöchige Hackerworkshop der Universität Bonn vom 13.06.22 bis zum 23.06.22 zielte darauf ab, uns einen Einblick in das Thema Cybersecurity zu geben, indem uns verschiedene Angriffsmethoden auf vulnerable Computersysteme aufgezeigt und erklärt wurden. In verschiedenen Aufgaben und Übungen konnten wir diese Methoden dann anwenden und uns vorgegebene Programme „hacken“, d. h. mit diversen Methoden das Verhalten des Programms so beeinflussen, dass bspw. eine Passwortabfrage umgangen wurde oder sensible Daten ausgelesen werden konnten.

 [1]

Die erlernten Methoden lassen sich zeitlich und inhaltlich grob in drei Themenblöcke unterteilen: Am ersten Tag haben wir uns serverseitige Cybersecurity angeschaut, d.h. Angriffe, die darauf abzielen, den Server zu – aus Entwicklersicht ungewolltem – Verhalten zu bewegen, sodass dieser Daten aus der zu Grunde liegenden Datenbank ausgibt, löscht oder manipuliert. Bei einer echten Webseite könnten dies im Zweifel datenschutzrechtlich schützenswerte Daten wie Kreditkartendaten oder Telefonnummern und E-Mail-Adressen sein. Solche SQL-Injections funktionieren, indem man in einer Suchmaske der Webseite o. ä. gezielt Daten eingibt, die der Server als Programmcode statt als Text interpretiert. Dadurch hat man die Möglichkeit, mit der Datenbank zu arbeiten, als hätte man direkten Zugriff darauf. Zur Übung wurde uns eine durch die Universität gehostete Beispielwebseite „Zwitscher“ zur Verfügung gestellt, auf der Nutzer Beiträge posten konnten. Durch SQL-Injections konnten wir die persönlichen Daten der Nutzer auslesen.

An einen weiteren Tag beschäftigten wir uns mit Wifi-Security. Dazu schauten wir uns zunächst die Grundlagen der Netzwerkkommunikation (Netzwerkprotokolle, Aufbau Datenpakete, etc.) an. In Bezug auf drahtlose Kommunikation (WLAN), stand vor allem die Frage, wie eine abhörsichere Kommunikation zwischen Router und mobilen Endgerät möglich ist, wenn alle Geräte mitlesen können und das Gerät keine Möglichkeit hat, zu prüfen, ob es überhaupt mit dem Router kommuniziert (Stichwort: Man-in-the-midde-attack) im Vordergrund. Über einen kleinen Exkurs zu einfachen Verschlüsselungsmethoden (z. B. Caeser- oder Xor-Verschlüssselung) haben wir uns der Funktionsweise der komplizierten Verschlüsselung RC4 des WPA-Standards, die den drahtlosen Netzwerkverkehr sicher macht, und des FMS-Angriffs angenähert.

Der Fokus der Vertiefung lag jedoch im Wesentlichen eher auf dem Hacken von auf dem Computer installierten Programmen. Dafür schauten wir uns zunächst die genaue Funktionsweise eines Computers und die Programmiersprache C an, in welcher die von uns zu hackenden Programme geschrieben wurden. Beim Einstieg ins Hacken bietet sich besonders diese Programmiersprache an, da C sehr hardware-nah ist. Der Programmierer muss zwar kleinschrittiger programmieren, da es kaum vorgefertigte Funktionen gibt. Dafür ist der Compiler jedoch wesentlich einfacher und infolgedessen vorhersehbarer gestaltet. Als Hacker weiß man so genau, wie die Daten im Arbeitsspeicher liegen. Dies ermöglichte es uns, über einen Bufferowerflowangriff Programmvariablen zu beeinflussen, indem wir in ein Eingabefeld längere Daten eingaben, als das Programm erwartete. Durch die Funktionsweise von C, wurden diese Daten dann in den Speicherplatz der nächsten Variablen geschrieben. Aufgrund unserer Kenntnis zum Aufbau des Stacks, d. h. der Ablage der temporären Daten wie Variablen, konnten wir gezielt bestimmte Variablen beeinflussen. In den zwei Wochen Vertiefung steigerte sich die Schwierigkeit immer weiter, indem Sicherheitsmaßnahmen zur Verhinderung des durch uns getätigten Angriffs hinzugefügt wurden. Anhand der Aufgaben wurde uns dann weiteres theoretisches Wissen zum Aufbau des Stacks und zur Funktionsweise von Pointern vermittelt, sodass wir die immer anspruchsvoller werdenden Aufgaben lösen konnten.

[1] Par Ecole polytechnique - Innovation & Research Symposium Cisco and Ecole Polytechnique 9-10 April 2018 Artificial Intelligence & Cybersecurity, CC BY-SA 2.0, https://commons.wikimedia.org/w/index.php?curid=74844244

Neben Bufferoverflowangriffen beschäftigten wir uns auch noch mit Binary Patching. Beim Binary Patching verändert man gezielt die Binarydatei des Programms. Vereinfacht gesprochen stehen Blöcke von Bytes in der Binarydatei immer für bestimmte Assembler-Befehle. Assembler ist eine sehr einfach strukturierte Programmiersprache, die jeden einzelnen Schritt für den Prozessor darstellt. Mit Hilfe eines Tools zum Dekompilieren (Umwandeln des Programms in halbwegs lesbaren Code, in unserem Fall in die Programmiersprache C) des Programms, Ghidra, und eines Debuggers, konnten wir die Assemblerbefehle dem Programmcode zuordnen. Wir konnten dann einzelne Assemblerbefehle abändern. Bspw. konnten wir an der Stelle des Passwortabgleichs aus dem Ist-gleich-Zeichen ein Ungleich-Zeichen machen. So wurden durch das Programm alle Passwörter akzeptiert, die dem gewünschten Passwort nicht entsprachen und das Programm war “gehackt”.

Zum Abschluss der zweiwöchigen Vertiefung gab es am letzten Tag ein Capture-the-flag, bei dem wir unsere erlernten Fähigkeiten als Gruppe erneut unter Beweis stellen konnten. Bei capture-the-flag gibt es viele verschiedene Aufgaben, die man lösen muss, um an die “flag” zu kommen. In unserem Fall handelte es sich größtenteils um Programme, welche gehackt werden mussten, um eine Passwortabfrage zu umgehen. Die “flag” wurde uns dann anschließend im passwortgeschützten Bereich angezeigt.

Auch wenn die von uns gehackten Programme eigens für diesen Zweck geschrieben wurden, lassen sich die Grundprinzipien der Angriffsmethoden auch auf moderne Programme übertragen bzw. bilden die Grundlage für andere Angriffsmethoden. Dieser Workshop hat es insofern geschafft, uns die Idee und den Ansatz des Hackens zu vermitteln und entsprechende Möglichkeiten aufgezeigt, Programme gegen einfache Cyberangriffe zu schützen.

Neben den Inhalten der Vertiefung wurden wir auch über das Unigelände geführt und haben uns mit Studenten, die auch in der Fachschaft Physik engagiert sind, und den Dozenten über das Unileben unterhalten. So konnten wir neben dem Inhalt auch noch viel zu Lerninhalten, der Arbeitsatmosphäre und den Abläufen an der Uni mitnehmen.

Caspar Thielmann