Raffael Fischer

Josip Valencic

Diplomanden	Raffael Fischer, Josip Valencic
Examinator	Ivan Bütler
Experte	Philipp Sieber
Themengebiet	Sicherheit

Backdoor Research

Security Training

Ausgangslage: Die European Cyber Security Challenge ist ein CTF (Capture-the-Flag) Hacking Wettbewerb, bei welchem neun Europäische Nationen mit 10er Teams gegeneinander antreten um dabei ihre Fähigkeiten im Bereich Cyber Angriff und Verteidigung zu überprüfen. Wie seit Snowden bekannt ist, basiert die NSA und andere Geheimdienste auf der Platzierung von Backdoors. Entsprechend müssen zukünftige Security Spezialisten in der Lage sein, solche Backdoors zu erkennen und entfernen. Zu diesem Zweck werden im Rahmen dieser Studienarbeit drei Anwendungen mit Backdoors erstellt, welche am CTF 2016 eingesetzt werden.

Vorgehen/Technologien: In der Analysephase wurden existierende Backdoors gesucht und analysiert. Mit diesem Wissen konnten bereits erste Rückschlüsse für die Umsetzung der eigenen Anwendungen gewonnen werden. Anschliessend wurden aus früheren HSR Projekten der Studenten geeignete Applikationen evaluiert, in welche sich für die Backdoor Arbeit eignen. Anschliessend sind für drei dieser eigenen Applikationen entsprechende Backdoors implementiert worden. Die Applikationen sind auf das CTF System des Hacking-Lab abgestimmt.

Ergebnis: Als Ergebnis der Analysephase steht eine Übersicht von Backdoors bereit. Im Rahmen der Umsetzung sind zwei der drei geplanten Backdoor-Applikationen verfügbar. Bei der dritten C++ basierten Applikation kam es zu unerwarteten Multi-Threading Problemen und Segmentation Faults. Die Backdoors aller Anwendungen haben unterschiedliche Charakteristiken und erfordern auch ein entsprechend anderes Vorgehen für die Aktivierung. Sie eignen sich für die Nutzung im CTF Wettbewerb. Die Backdoors lassen sich durch Security Spezialisten finden und entfernen, so wie es im CTF vorgesehen ist.