Aufgabenstellung

Modul:	Dept I WIPRO HS24

Titel:	Metasploit shellcode encoder Module for arm shellcodes
Ausgangslage und Problemstellung:	Shellcode encoders are useful to adapt existing shellcode to certain restrictions. Usually to avoid so-called bad characters (e.g. NULL bytes), i.e. certain byte values that lead to undesirable side effects. The metasploitframework includes several shellcode encoders for various cpu architectures. For arm (armle, armbe, aarch64), one of the most common cpu architectures for embedded and iot devices, such an encoder is missing.
Ziel der Arbeit und erwartete Resultate:	The aim of the work is to create an arm shellcode encoder module for the metasploit framework. The encoder should be as generic as possible and be able to avoid a configurable number of bad characters.
Gewünschte Methoden, Vorgehen:	Software development and evaluation methodology suitable for the task. No specific requirements regarding the methodology.
Kreativität, Methoden, Innovation:	Depending on the thesis (Wirtschaftsprojekt or Bachelor thesis) the scope can be adapted. Topics such as polimorphic shellcode encoders and integration of target-specific encryption offer the opportunity to expand the topic.
Sonstige Bemerkungen:	Requirements: - Good understanding of assembly [ideally, arm assembly]. - Knowledge of binary exploitation - Mindset to learn the additional skills (e.g., how to write a metasploit encoder module). A plus is: - Experience in reverse engineering. - Knowledge of the Ruby scripting language .

Projektteam

Student:in 1:	David Jäggli
Betreuer:in:	Gilbert Oliver

Auftraggeber

Firma:	armasuisse W+T
Ansprechperson:	Daniel Hulliger
Funktion:	TBD
Strasse:	Feuerwerkerstrasse 39
PLZ/Ort:	3603 Thun
Telefon:	+41798241461
E-Mail:	bernhard.tellenbach@ar.admin.ch
Website:	https://www.cydcampus.admin.ch/

Version 13.06.2023 / bcl