UNIVERSITÄT SIEGEN

Lehstuhl IT-Sicherheitsmanagment
Prof. Dr. Kesdogan

Exercise 4: Smack Stasher

1 A revolution without dancing is a revolution not worth having!

Ein Server ohne Musik ist auch nicht tanzbar, deshalb ist `net.c` bei euch auf dem Server zu implementieren. Dummerweise fehlt da die Socket-Implementierung. Glücklicherweise braucht man nicht lange zu suchen um sprechende Beispiele zu finden, `portpingpong.c` ist ein passables Beispiel, mit dem man schnell einen Socket aufbauen kann[1].

2 There's no certainty — only opportunity.

In der Übung hattet ihr Gelegenheit die Erzeugung von Shellcode zu beobachten. Eure Aufgabe ist es jetzt einen Shellcode zu erzeugen, der euer Geburtsdatum in Sekunden seit Epoch möglichst genau zurückgibt. [2]

Der empfohlene Weg ist hierbei das Programm zunächst in C zu formulieren und lediglich den Binärstring des fertigen Kompilats zu verwenden. Es gibt aber auch hier Steigerungsmöglichkeiten, mit denen weitere Punkte zu verdienen sind: Shellcode, der eine Shell öffnet, Shellcode, der einen Port öffnet an der eine Shell auf Befehle lauscht. Punktabzug gibt es selbstedent für Shellcode, der aus den gängigen Shellcode-Datenbanken kopiert wurde.

3 Wait! Here comes the crescendo!

Wer Shellcode hat, will ihn ausführen. Diese Aufgabe erfolgt nun in mehreren Steigerungen bis zum Gipfelpunkt. Zunächst einmal soll es ausreichend sein, den Shellcode in einem eigenen Stack als Variable einzukompilieren und auszuführen. Aber natürlich ist dies nur die Aufwärmübung, der eigentliche Berg ist das Programm, dass eine unvorsichtige Seele auf seinem eigenen virtuellen Server installiert hat.

Führe eine Sicherheitsanalyse des Programmes aus Aufgabe 1 durch und zeige anhand eines Proof of Concept die gefundenen Fehler auf. Der Shellcode aus Aufgabe 2 darf dir dabei wertvolle Dienste leisten.

[1] wenn man sich ein wenig zurückhält und `exec` und `fork` ignoriert.
[2] Das Flag -fno-stack-protector kann helfen das Assemblat etwas lesbarer zu gestalten.

Kontakt: `fischer@wiwi.uni-siegen.de`