Softwareprojekt
Domain Hunter

Dozenten	Prof. Dr. Christian Dietrich, Nurullah Demir, Tobias Urban
Titel des Projekts	Entwicklung eines Systems zum Aufspüren von Domain-Hijackings
Zuordnung zu Studienrichtungen	PI, (TI, MI, WI)
Liste der Module, die inhaltlich vorausgesetzt werden	EPR, OPR, ADS Grundlagen-Datenbanken und Rechnernetze (REN) sind von Vorteil
Implementierungssprache bzw. eingesetzte Technologien	Python, PostgreSQL. Nach Absprache können weitere Technologien bei Bedarf genutzt werden
Gewünschte Gruppengröße	4-5

Motivation

Domains spielen eine wichtige Rolle im Internet, egal ob für das Web oder den Email-Verkehr. Angreifer haben in den letzten Jahren vermehrt die Zugangsdaten von Domains abgegriffen und die Domains so umkonfiguriert, dass sie beispielsweise den Email- oder Web-Verkehr abfangen können. Man spricht dann auch von Domain Hijacking. In diesem Softwareprojekt soll ein System konzipiert und implementiert werden, dass “umkonfigurierte” Domains versucht zu identifizieren und Metadaten zu den Domains ermittelt.

Aufgabenstellung

Konkret soll eine Menge an wichtigen Domains zusammengestellt werden, wie etwa von internationalen Organisationen wie der UN oder Non-Profit-Organisationen und ähnlichen. Diese werden dann regelmäßig über das Domain Name System aufgelöst und Abweichungen können Indikatoren für sog. Domain Hijacking sein. Über weitere Metadaten (DNS-Zoneninformationen, Whois, gehostete Inhalte) kann die Erkennung verbessert werden. Die Implementierung kann beispielsweise mit der Programmiersprache Python und der objektrelationalen Datenbank PostgreSQL erfolgen.

Ziel soll sein, interessante Fälle von Domain Hijacking zu identifizieren und ggf. genauer zu untersuchen.