
- Bachelor- / Masterarbeit - Flow-basierte Scan-Erkennung

CASED	<p>Das neue Forschungs- und Entwicklungszentrum für IT-Sicherheit CASED (Center for Advanced Security Research Darmstadt) stellt sich mit seinen starken Partnern – der Technischen Universität Darmstadt, dem Fraunhofer Institut für Sichere Informationstechnologie und der Hochschule Darmstadt – einer immensen Herausforderung: In einer einzigartigen Kooperation von Informatikern, Ingenieuren, Physikern, Juristen und Betriebswirten, mit internationalen Forschungszentren und Industriepartnern, werden zukunftsweisende IT-Sicherheitslösungen erforscht, entwickelt und in die Anwendung und wirtschaftliche Verwertung gebracht.</p>		
Motivation	<p>Die Internet Underground Economy professionalisiert sich kontinuierlich. Wurden Internet-Angriffe in den Anfängen noch aus Spaß und Interesse an der Technik durchgeführt, so hat sich hieraus mit der stetigen Entwicklung des Internets ein Geschäftsmodell entwickelt. Basis dieser Angriffe stellt häufig das Kompromittieren an das Internet angeschlossener Endgeräte (PCs, Laptops, Server, etc.) dar. Zur Detektion interessanter Ziele bedienen sich Angreifer diverser Scanning-Mechanismen. Hierbei werden diverse IP-Adressbereiche nach bekannten und ausnutzbaren Schwachstellen durchsucht.</p>		
Aufgabenstellung	<p>Im Rahmen dieser Abschlussarbeit sollen Möglichkeiten der Verwendung von Netzwerk-Flowdaten – 5-Tupel bestehend aus Quell- und Ziel-IP Adressen, Quell- und Ziel Ports, Layer 4 Protokoll ID sowie Informationen über die Intensität des Datenverkehrs (Bit/s, Pakete/s) – zur Scan-Erkennung untersucht werden. Die Verwendung von Flowdaten führt unmittelbar zu einer Datenreduktion. Darüber hinaus enthalten Flowdaten keinerlei Nutzdaten des Internetverkehrs und sind somit datenschutzfreundlicher als auf Deep Packet Inspection basierende Ansätze. Die/der Studierende soll sich im Rahmen dieser Arbeit mit der Verarbeitung und Analyse von Flowdaten zur Detektion von Netzwerk-Scans beschäftigen.</p>		
Voraussetzungen	<ul style="list-style-type: none">• Kreatives, eigenständiges und engagiertes Arbeiten• Kommunikationsbereitschaft• Gute Programmierkenntnisse (z.B. C, Perl, Ruby)• Gute Kenntnisse gängiger Internetprotokolle IP• Kenntnisse im Bereich Modellbildung und Simulation sind vorteilhaft• Linux-Kenntnisse sind vorteilhaft• Sehr gute deutsche und/oder gute englische Sprachkenntnisse		
Starttermin	<p>Ab sofort</p>		
Kontakt	<table><tr><td>Sebastian Abt sebastian.abt@h-da.de 06151.16-8416</td><td>CASED Mornwegstraße 32 64293 Darmstadt</td></tr></table>	Sebastian Abt sebastian.abt@h-da.de 06151.16-8416	CASED Mornwegstraße 32 64293 Darmstadt
Sebastian Abt sebastian.abt@h-da.de 06151.16-8416	CASED Mornwegstraße 32 64293 Darmstadt		