
- Bachelor/Master Thesis -

Flow-based Network Scan Detection

CASED	<p>In CASED (Center for Advanced Security Research Darmstadt) collaborate the Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology and the University of Applied Sciences Darmstadt in the fast developing field of IT Security. In a unique cooperation, which combines different areas of expertise from these renowned institutions, progressive IT security solutions are researched, developed and implemented into industrial economy: CASED brings together computer scientists, engineers, physicists, legal experts and business economists. Read more on www.cased.de.</p>		
Motivation	<p>The internet underground economy is becoming continuously more professional. While in the early days internet attacks were performed for fun and because of interest, with the evolution of the internet a business model driven by the underground economy has emerged. To be able to anonymously and effectively perform internet attacks, devices connected to the net (e.g. PCs, mobile devices, servers) have to be compromised. In order to detect devices that can be compromised, IP address ranges are scanned for specific known vulnerabilities.</p>		
Task	<p>In this thesis, the possibility of using network flow data – i.e. 5-tuples consisting of source and destination IP addresses, source and destination TCP/UDP port numbers, the layer 4 protocol number as well as timing and intensity information – for network scan detection shall be investigated. Using network flow data for this task leads to highly reduced data sets and, due to fact that network flow data do not contain any payload information, better preserves the end user's privacy in contrast to deep packet inspection based approaches. During this thesis, the student shall work on the whole chain of flow data processing and analysis. For scan detection, appropriate pattern recognition techniques shall be applied.</p>		
Requirements	<ul style="list-style-type: none">• High motivation, creativity and ability to work independently• Good communication skills• Good programming skills (e.g. C, Perl, Ruby)• Good knowledge of common internet protocols• Good knowledge of pattern recognition and ML techniques• Knowledge of Linux operating system is a plus• Very good knowledge of the German or English language		
Start date	Immediately		
Contact	<table><tr><td>Sebastian Abt sebastian.abt@h-da.de 06151.16-8416</td><td>CASED Mornewegstraße 32 64293 Darmstadt</td></tr></table>	Sebastian Abt sebastian.abt@h-da.de 06151.16-8416	CASED Mornewegstraße 32 64293 Darmstadt
Sebastian Abt sebastian.abt@h-da.de 06151.16-8416	CASED Mornewegstraße 32 64293 Darmstadt		