Technische Universität München
Lehrstuhl für Netzarchitekturen und Netzdienste
Prof. Dr. Georg Carle

Thesis
(B.Sc. or M.Sc., IDP)

A Pen-Testing Framework for the Munich Research Network

Motivation

The LRZ is responsible for the Munich Research Network (MWN) and first contact in case of abuse complaints. However, administration within the MWN is decentralised, with each institutional sub-network administrated by local personnel. This leads to a certain overhead when complaints from external networks have to be forwarded to local administrators. It is thus very desirable that this overhead be minimised. The key to this is preemptive detection of possible vulnerabilities. This can be done with network scans inside the MWN. These scans can also be carried out over a certain time span, which allows to detect activity patterns of remote hosts.

The goal of this student thesis is thus to design and implement a scanning framework for use within the MWN. The framework shall be able to carry out scans, store results to a database and analyse them semi-autonomically. Local MWN administrators must be able to learn of ongoing scanning efforts and also request LRZ scans of their systems.

This thesis is jointly supervised by LRZ and our Chair.

Your Task

First, you will analyse which information can be collected about remote systems, using a set of tools.

Then, you will design the new framework. Where applicable, you may use integrate existing tools (nmap, metasploit). You will need to consider scans from both within the LRZ and from rented remote hosts. The system must also accept scanning requests from other administrators.

The next step is to implement a prototype and carry out first experiments. Much attention will be have to paid to reproducibility of results and automatisation of scans and analysis. This includes automatic notification of responsible administrators if vulnerabilities are found, and checking after a certain time if these have been fixed.

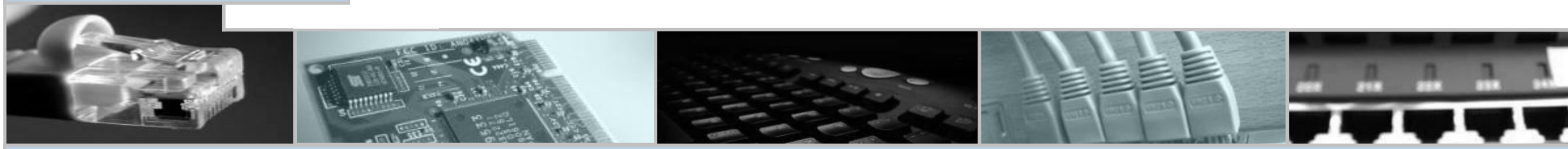
It is also expected that you write a good documentation.

Requirements

A solid knowledge of networking technologies is expected. You will need to use a variety of tools and program in at least one scripting language. You should not be afraid of the odd handling of C code.

Keywords

Network scans, network security



Felix v. Eye, PD Dr. Hommel, Ralph Holz
holz@net.in.tum.de