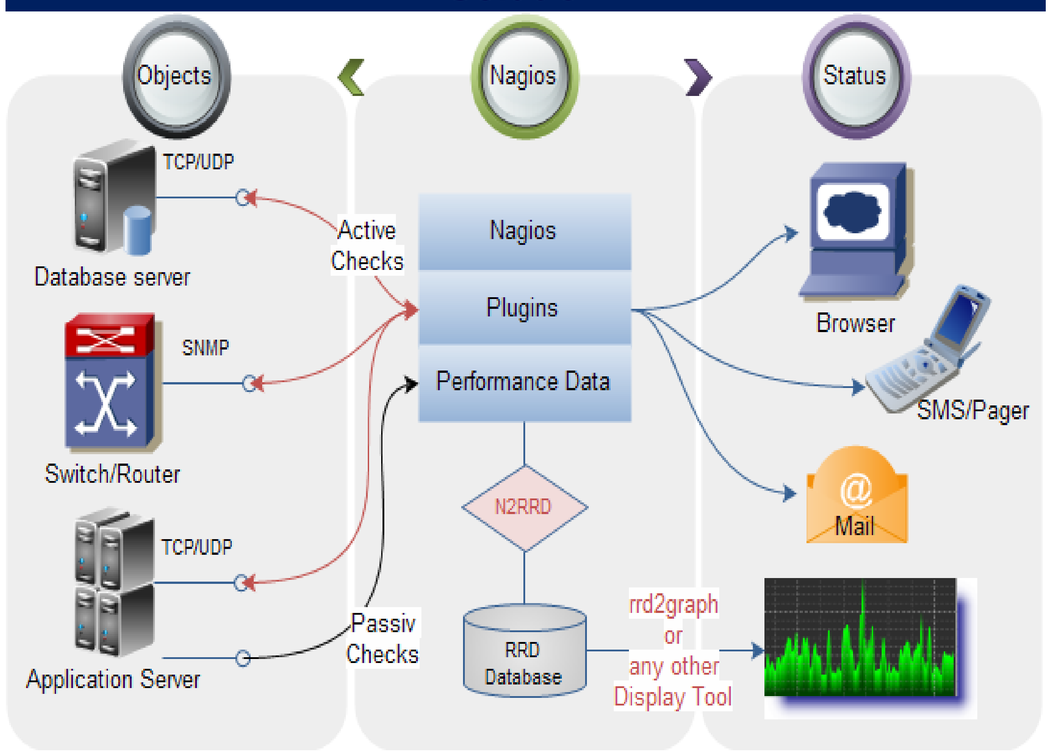
Insider Threat Detection And Protection (ITDP)

Nishanth Prakash, Salim Hariri, Youssif Al-Nashif

Problem

- An **Insider Threat** is a malicious threat to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
- The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

Solution

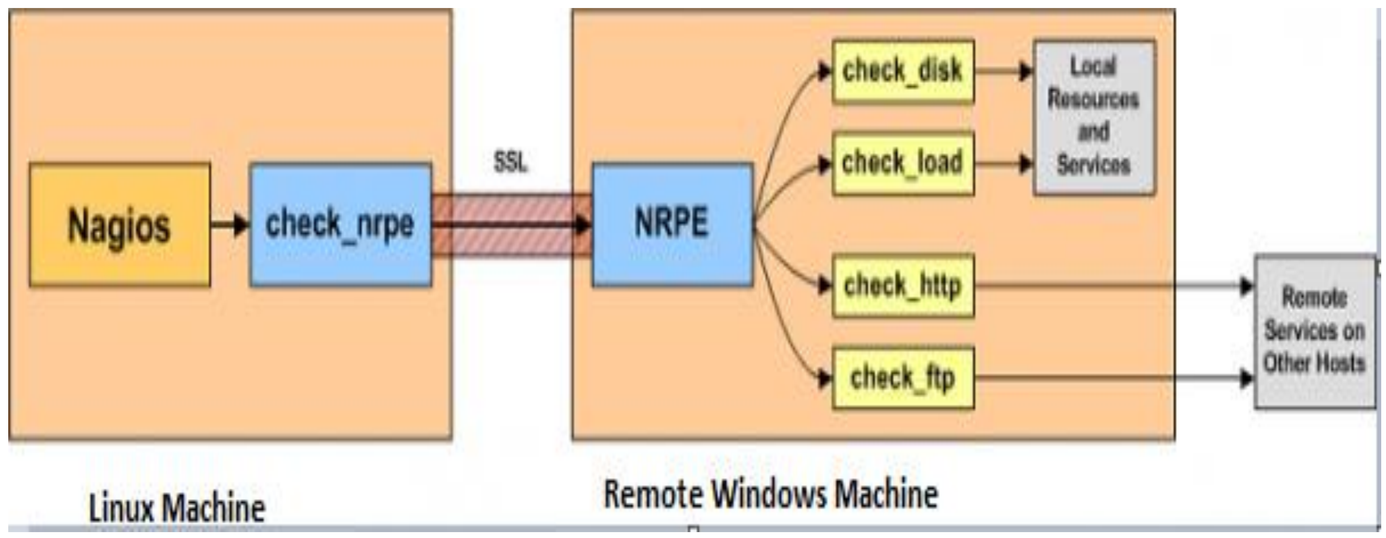


Nagios is a powerful monitoring system that enables organizations to identify and resolve IT infrastructure problems before they affect critical business processes**.**

By using Nagios, You Can,

1. Monitor Windows and Linux Systems
2. Respond to issues at the first sign of a problem
3. Automatically fix problems when they are detected
4. Coordinate technical team responses
5. Monitor your entire infrastructure and business processes

Present Work



- Monitoring the windows machine (host machine) from Linux system (installed on the Virtual Machine)
- The required Steps to be taken
- First a connection should be established between the Server and client. In our case Port Forwarding is done to establish a connection between the virtual machine (Server) and the Windows machine (Client)
- Second, some parameters of the NRPE configuration file must be changed. This configuration file resides on the widows machine.

Results

Showing 1-7 of 7 total records

Search... Go

Host	Service	Status	Duration	Attempt	Last Check	Status Information
192.168.5.11	Bugtest notifications enabled	Ok	19d 2h 11m 13s	1/5	2012-12-18 15:01:14	OK: Nothing to monitor
	CPU Usage	Ok	1d 5h 58m 14s	1/5	2012-12-18 15:02:33	CPU Load 2% (5 min average)
	Drive C: Disk Usage	Ok	1d 5h 59m 56s	1/5	2012-12-18 15:00:52	C:\ - total: 453.96 Gb - used: 182.54 Gb (40%) - free 271.41 Gb (60%)
	Drive D: Disk Usage	Ok	1d 5h 55m 36s	1/5	2012-12-18 15:05:12	D:\ - total: 232.88 Gb - used: 0.09 Gb (0%) - free 232.78 Gb (100%)
	Memory Usage	Ok	22h 3m 28s	1/5	2012-12-18 15:02:19	Memory usage: total:16296.13 Mb - used: 4268.26 Mb (26%) - free: 12027.86 Mb (74%)

- The GUI of the tool will give the status information about the parameters of the windows machine.
- The plugins such as **check_nrpe -H <host address> -c pdm_disk_c/d**, **check_nrpe -H <host address> -c pdm_cpuload** is used **to** check the System's Drive C and Drive D usage and CPU usage of the windows machine respectively.

This work is partially supported by AFOSR DDDAS award # FA9550-12-1-0241, and NSF awards IIP-0758579, DUE-1303362 and SES-1314631.

Cloud and Autonomic Computing Center

The University of Arizona