



International Journal on Recent Researches In Science, Engineering & Technology

A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy.

It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in DIIF and SJIF.

Research Paper

Available online at: www.ijrrset.com

Chief Editors 1 : Dr. M.Narayana Rao, Ph.D., Rtd. Professor, NIT, Trichy.

(Engg.&Technology division)

2 : Dr. N.Sandyarani, Ph.D., Professor,

Chennai based Engg.College, (Science division)

ISSN (Print) : 2347-6729

ISSN (Online) : 2348-3105

Volume 2, Issue 7,

July 2014

DIIF IF :1.46

SJIF IF: 1.329

System Level HoneyPot Detection and applications

Madhu Kumar and Dr. N. Shankarapani

Abstract - Literature review revealed, the effective techniques to detect the virtual machines . In our experiments we exploit the vulnerabilities of VMware , VBC and SEBEK, and detect them using the following techniques ; Magic number technique , virtual register sets technique and interrupt description table technique . In magic table technique our program takes the magic number , port number and command to execute as inputs and output whether it is VMware or VPC or is it a host machine. In IDT technique our program uses SIDT we trace the finger prints of virtual machine to determine its VMware or VPC . In detection of Sebek we look for the finger prints present in the memory and hijack the system call that is used by Sebek .