

Abstract

1) Einleitung

2) Related Work

3) Analyse der Gefahren (jeweils unter Betrachtung der IT-Sec Grundsätze CIA)

3.1) Allgemeine Gefahren bei Netzwerkinfrastrukturen

#sehr kurz gehalten, Überblick

#soll die Verwendungsmöglichkeiten “gehackter” Infrastrukturen und somit auch die Motivation wiedergeben

3.2) Spezielle Gefahren für den physischen Host ausgehend von den virtuellen Maschinen

#welche “direkten” Angriffsmöglichkeiten existieren

#Netzwerk-Angriffe vernachlässigen da kein Unterschied zu allg. IT-Sec

3.3) Spezielle Gefahren für die virtuellen Maschinen ausgehend vom physischen Host

#wie bei vorherigem Punkt

3.4) [optional] evtl zusätzliche Risiken (SideChannelAttacks, VM2VM..)

4) Vermeidung der Gefahren

4.1) Allgemein

#wiederum nur kurz aber:

Security by Design (spielt bei VNE eine große Rolle)
ausführlicher

4.2) Angriff: Guest → Host

#Bspw.: Vermeidung von BufferOverflowAttacks via ASLR

#kein shared memory

...

4.3) Angriff: Host → Guest

#Zugriffsrechte für VM-spezifische Informationen limitieren

4.4) [optional]

5) Schlussfolgerung und Aussicht

Quellenangaben

Fragen:

Da der Titel sehr allgemein ist, stellt sich die Frage der Fokussierung.

Allgemein & breit → Abdeckung aller relevante Themen

Spezialisiert & tief → rein (S)VNE