Aula 04

Engenharia Reversa e Análise de Malware

Ronaldo Pinheiro de Lima
crimescibernéticos.com@gmail.com

Aula 04

3. Laboratório para Análise de Malwares

3.1. Máquina virtual

3.2. Preparação do ambiente

3.3. Lab-03-01
Uso de máquina virtual e simulação de rede com FakeNet

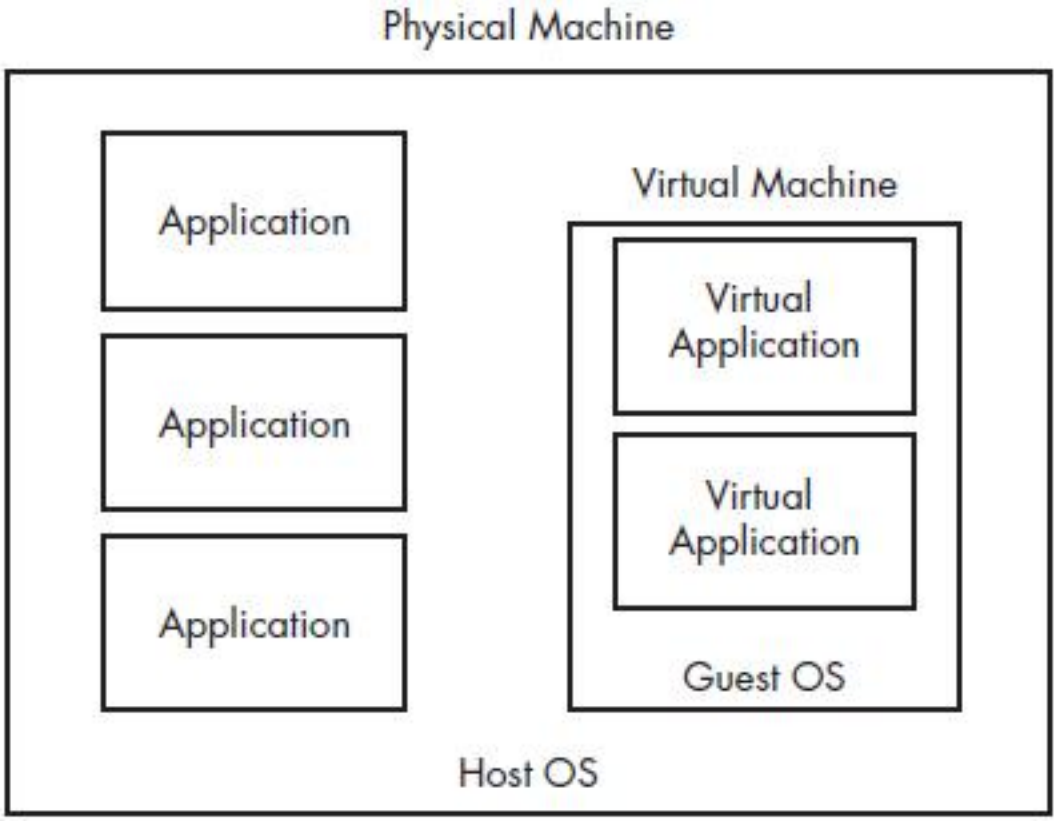
Laboratório para análise de malwares

- ambiente seguro
- não utilizar computador de produção

Máquina virtual

- “computador dentro de outro computador”
- SOs convidados em SO hospedeiro (host)
- isolamento do malware * (0-day)
- restauração e backup simples
- menos recursos computacionais
- VMWare e VirtualBox

Máquina virtual



Preparação do ambiente

- sempre manter software virtualização atualizado
- cuidados com conexões de rede

Configurações de rede

- Host-only
- NAT/Shared
- Bridged
- Cabo de rede conectado/desconectado

Configurações de rede

Acesso	Host-only	NAT/Shared	Bridged
VMs podem acessar outras VMs	Sim	Sim	Sim
VMs podem acessar o hospedeiro	Sim	Sim	Sim
VMs podem acessar outros computadores	Não	Sim	Sim
O hospedeiro pode acessar VMs	Sim	Sim	Sim
Outros computadores podem acessar VMs	Não	Não	Sim

Recomendações:

- inicialmente não execute o malware com Internet
- análise inicial e **host-only** com rede simulada
- quando necessário Internet: NAT (fácil) ou bridged

Informações pessoais

- retire todas as informações pessoais da máquina

Recursos adicionais da VM

- VMware Tools e Adicionais para convidado
- facilita compartilhamento de arquivos

Pastas compartilhadas

- mapear como somente-leitura

Ferramentas

- instalar todas previamente (Aula 01)

Snapshots

- após instalar ferramentas tirar snapshot limpo

Passo a Passo – uso de VM para análise de malwares

1. criar VM com SO limpo (WinXP 32-bit SP3)
2. configurações e instalação de ferramentas
3. tire um snapshot
4. transfira o malware para a VM
5. faça a análise do malware
6. toma nota dos resultados, transfira para a máquina host dados obtidos, tire screenshots de telas
7. reverta a VM para o snapshot inicial

Lab 03-01

Uso de VM e simulação de rede com FakeNet

Material necessário:

- VM
- FakeNet (http://practicalmalwareanalysis.com/fakenet/)
- Wireshark
- Arquivo: Lab-03-01.exe

Obrigado!

A explicação detalhada de todos os tópicos está na apostila.

Ronaldo Pinheiro de Lima
crimescibernetico.com@gmail.com
http://www.crimescibernetico.com
@crimescibernet