Automated Malware Analysis - Setting up the Environment

Username : Pushkar

Password : KV Prashant

Who we are????

- Pushkar Pashupat(Push)
  - Security Researcher, working as independent consultant
  - CEH, Member of Matriux and null community
- K.V Prashant(kvbhai)
  - Security Consultant, working for IT services company
  - CISSP & CEH, member of null open security and hacking community

Agenda

- What is Malware analysis
- Automation
    - Virtualization
    - Sanboxing
- Tools of Trade
- Demo
- References

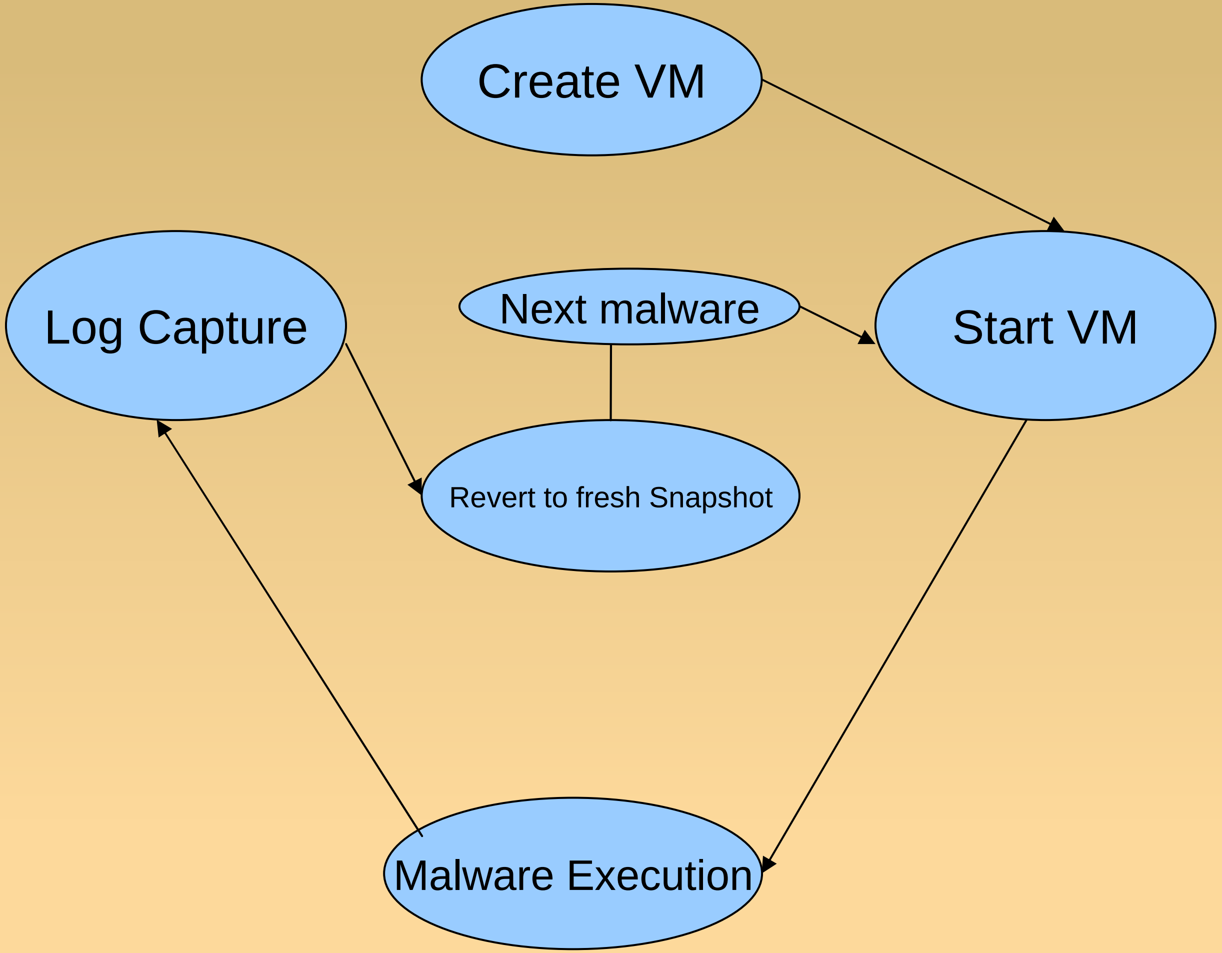
Malware Analysis

- What is Malware Analysis
  - Analysing executables for the purpose of determining its malacious behaviour
- Techniques of Malware Analysis
  - Static code analysis
    - Using debuggers and RE tools(w/o executing)
  - Dynamic analysis
    - Behavioural analysis(exectuing the malware)

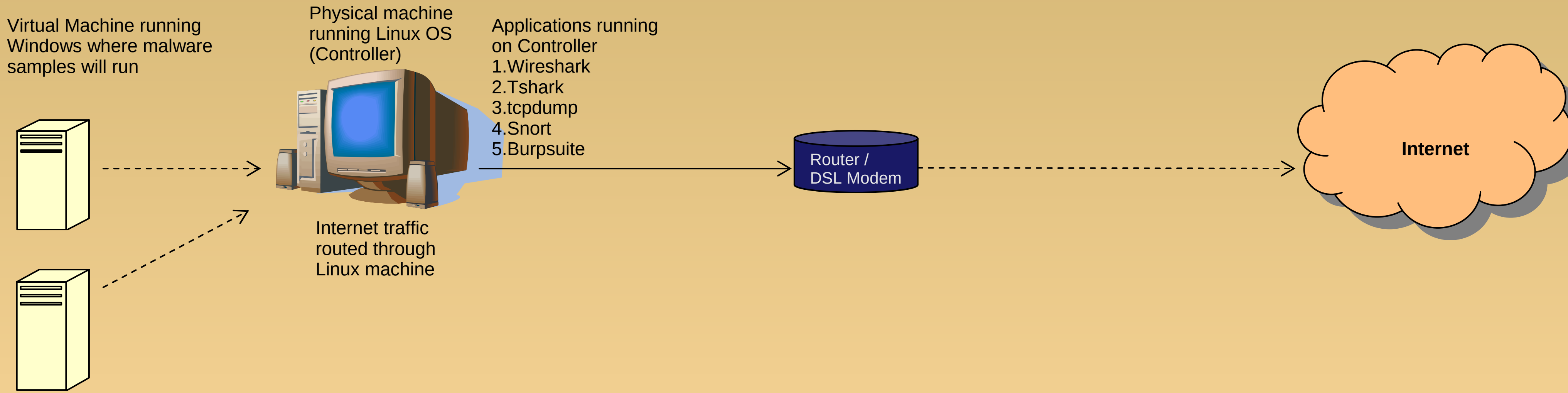
Automation

- Virtualization
  - Using virtual enviroment to execute the malwares and study the behaviour
- Sandboxing
  - Executing malwares in controled and monitored environment

Automation states



Network Level Analysis



Virtual Machine running Windows where malware samples will run

Physical machine running Linux OS (Controller)

Applications running on Controller
1.Wireshark
2.Tshark
3.tcpdump
4.Snort
5.Burpsuite

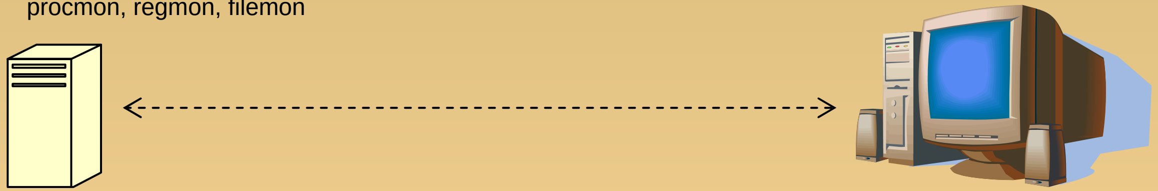
Internet traffic routed through Linux machine

Router / DSL Modem

Internet

Network Level analysis help in determining following:
1.Protocol used
2.Connections made to which IP
3.Post connection activities like if any further malwares are dropped

System Level Analysis



Windows Target machine,
running on target machine
1.Volatility
2.Sysinternal tools,
procmon, regmon, filemon

Controller machine running
1. Custom scripts to invoke
vm, start monitoring tools,
execute malware and revert
vm to clean snapshot

System Level analysis help in
determining following:
1.Registry edits
2.Process, Files created
3.Sockets created and ports used

Tools of Trade

- VirtualBox
- Sysinternal Suite
- Wireshark
- Volatility
- Inetsim
- Sandboxes like Sandboxie

Virtualbox commands

- Vboxmanage
  - startvm
  - guestcontrol -exec
  - snapshot
    - take
    - revert
  - controlvm
    - savestate
    - resume
    - poweroff

Pre-Execution Analysis

- PEScanner
- Strings
- VirusTotal
- Start procmon
- Start tshark

Post Execution

- Memory Dump Analysis
- Yara log analysis

Sandboxes

- Online Sandboxes
    - CWSandbox
    - ThreatExpert
    - Norman
- Offline Sandboxes
    - Sandboxie
    - cuckoo

Sandboxie

Executing programs without affecting actual system

Buster Sandboxie Analyser

- Wrapper around Sandboxie

Demo

Thanks For Tolerating us ☺

Thank You
Special Thanks to Matriux community and Manu Sir