



MALWARE ANALYSIS

A Taste



DISCLAIMERS

- Content, views, anything expressed are strictly my own and not that of my employer.
 - Samples shared are malicious so exercise caution and only handle them in a safe environment.
-

CONTENTS

- Intro
 - Who does Malware Analysis?
 - Skill sets (in brief :p)
 - Malware Trends
- Lab Prep
- Exercise
- Exercise
- Exercise



WHO DOES MALWARE ANALYSIS?

- Incident Responders
 - Identifying malware used in Cyber Attacks
- Forensic Investigators
 - Identifying threat actors behind a Cyber crime
- Malware Researcher
 - Academic or Industrial purposes
- Or do a job search (:S) -

<https://www.google.com/search?q=malware+analysis+jobs&ibp=html;jobs>

SKILLZZZZZ

- Windows Malware
 - Windows Internals
 - Assembly, Windows file formats, etc
 - Dynamic/Static Analysis
- Staying on top of the Threat Landscape
 - Prevalent botnets
 - Prevalent malware campaigns
 - APT Groups
- Keeping in touch with Community <3
 - Nous Sommes Cyber / We Are Cyber
 - Others: NorthSec, MontreHack, MTLSec



<title>code ninja</title>

MALWARE TRENDS

Ransomware

Rootkits

Virus

EXPLOIT KITS

Bootkits

Stealers

BOTNETS

Fileless Attacks

RATS

Air Gap

WORMS

5 Stages

MALWARE LIFECYCLE

7 phases

Reconnaissance
Initial Compromise
Target

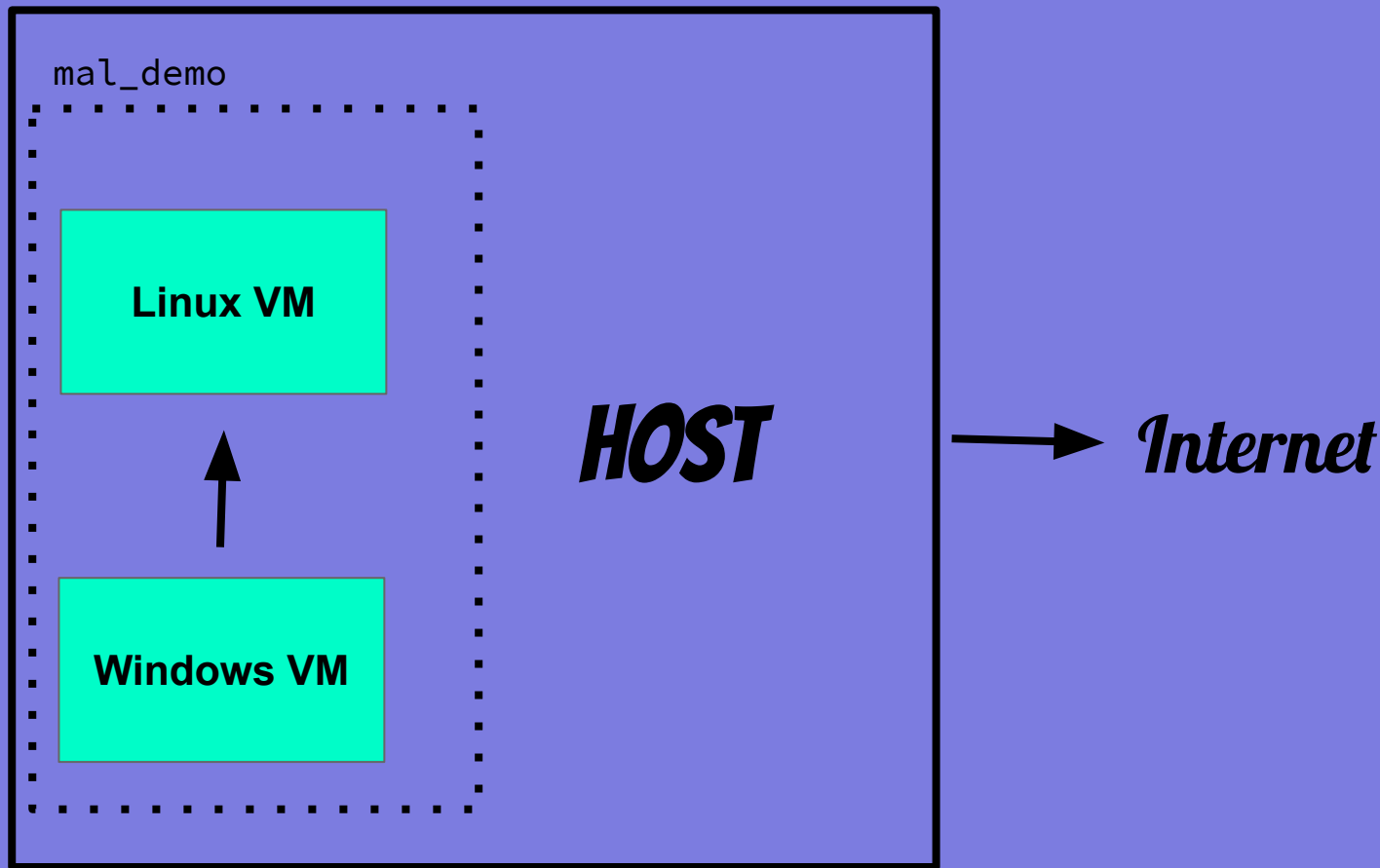
Infiltration
Exploitation
Privilege Escalation
Persistence
Lateral Movement

Command & Control
Exfiltration

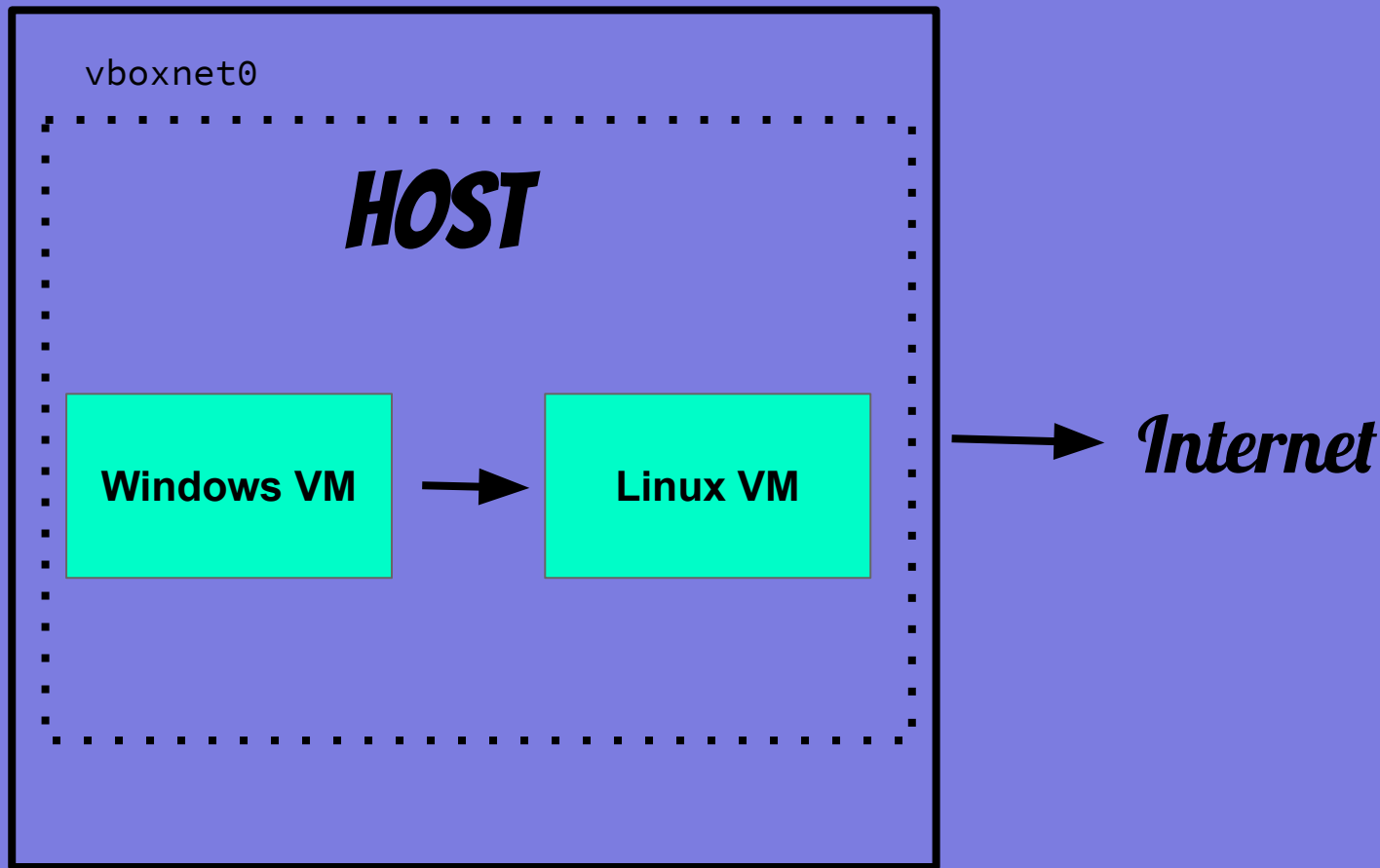
8 phases of the cyber kill chain

LAB SETUP

LAB SETUP
(INTERNAL
ADAPTER)



LAB SETUP
(HOST-ONLY
ADAPTER)



Other Lab Examples:

<https://blog.christophetd.fr/malware-analysis-lab-with-virtualbox-inetsim-and-burp/>


<https://executemalware.com/?p=175>

https://subscription.packtpub.com/book/networking_and_servers/9781788392501/1/ch01lvl1sec14/5-setting-up-the-lab-environment

Disable Windows Updates

STEP 1

Windows Update

 You're up to date
Last checked: 5/19/2020, 2:48 PM

Check for updates

[Change active hours](#)

[View update history](#)

[Advanced options](#)

STEP 2



Off

Automatically download updates, even over metered data connections (charges may apply)



Off

STEP 3

A feature update includes new capabilities and improvements. It can be deferred for this many days:

365 ▾

A quality update includes security improvements. It can be deferred for this many days:

30 ▾

STEP 4

Local Group Policy Editor

Computer Configuration ->
Administrative Templates ->
Windows Components ->
Windows Update

Windows Update			
Select an item to view its description.			
Setting	State	Comment	
Windows Update for Business			
Do not display 'Install Updates and Shut Down' option in Sh...	Not configured	No	
Do not adjust default option to 'Install Updates and Shut Do...	Not configured	No	
Enabling Windows Update Power Management to automati...	Not configured	No	
Turn off auto-restart for updates during active hours	Not configured	No	
Specify active hours range for auto-restarts	Not configured	No	
Allow updates to be downloaded automatically over metere...	Not configured	No	
Always automatically restart at the scheduled time	Not configured	No	
Specify deadline before auto-restart for update installation	Not configured	No	
Configure auto-restart reminder notifications for updates	Not configured	No	
Turn off auto-restart notifications for update installations	Not configured	No	
Configure auto-restart required notification for updates	Not configured	No	
Configure Automatic Updates	Not configured	No	
Specify intranet Microsoft update service location	Not configured	No	
Automatic Updates detection frequency	Not configured	No	

Configure Automatic Updates

Configure Automatic Updates

☐ Not Configured Comment:

☐ Enabled

☒ Disabled

Supported on:

STEP 5

Create Shared Folders

WINDOWS VM

Create a shared folder via
VirtualBox

LINUX VM

Create a shared folder via
VirtualBox

1. `sudo adduser remnux vboxsf`
2. `sudo mount -t vboxsf
<host-share-folder> <vm-dir>`

DEMO

GROUND RULES

- To prevent running the sample accidentally; rename samples without an extension.
- If the sample is not being analyzed in a VM, analyze it on a platform you know it is unable to run on.
- If sharing malicious samples, pack them in a password protected archive.
- Always update analysis tools in events of malware leveraging a potentially new exploit :)
- Do not store important passwords or keyfiles in VMs.
- Isolate the network; use VPN

EXERCISE 1 (Downloader - downloads Coinminer)

MD5 - [c32df489536c50e2ae6f1f297b6211aa](#)

Malpedia [Lookup](#)

Dynamic Analysis Exercise

- Are any files created?
- Is there any network activity?
- Any other suspicious behavior?

EXERCISE 2 (Crimson RAT)

Report -

<https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf>

MD5 - [f078b5aeaf73831361ecd96a069c9f50](#)

Malpedia [Lookup](#)

Static Analysis Exercise

- Find the sample's Entry Point
- What part of the code demonstrates it is malicious?
- Is there any persistent techniques? (if so what are they)
- Is it exfiltrating data? (if so what are they)
- Can you find the command & control server info?

EXERCISE 3

Dropper - drops Silence banker / Truebot

MD5 - 404d69c8b74d375522b9afe90072a1f4

Malpedia Lookup

Mitre Att&ck Lookup

Report - <https://securelist.com/the-silence/83009/>