Malware Analysis Fundamentals

INTRODUCTION AND SETTING UP YOUR MALWARE ANALYSIS LAB

Tyler Hudak
INCIDENT RESPONDER

@secshoggoth

Course Overview

Malware fundamentals

Setting up your lab

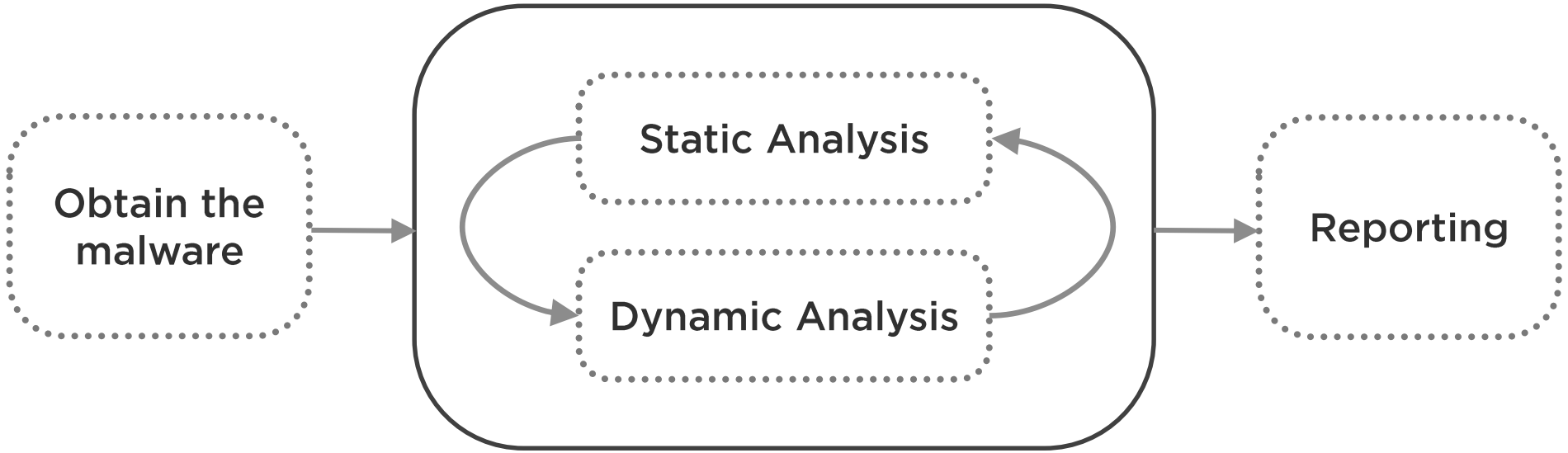
Examining malware characteristics

- Identifying malware
- Strings analysis
- PE header analysis

Monitoring malware behavior

Real malware demo and lab

Malware Analysis Process



Static Analysis – Analyzing malware without execution

Dynamic Analysis – Analyzing the behavior of malware through execution

Focus Your Analysis

Is the file malicious?

How does the malware modify the system?

Who does the malware contact and why?

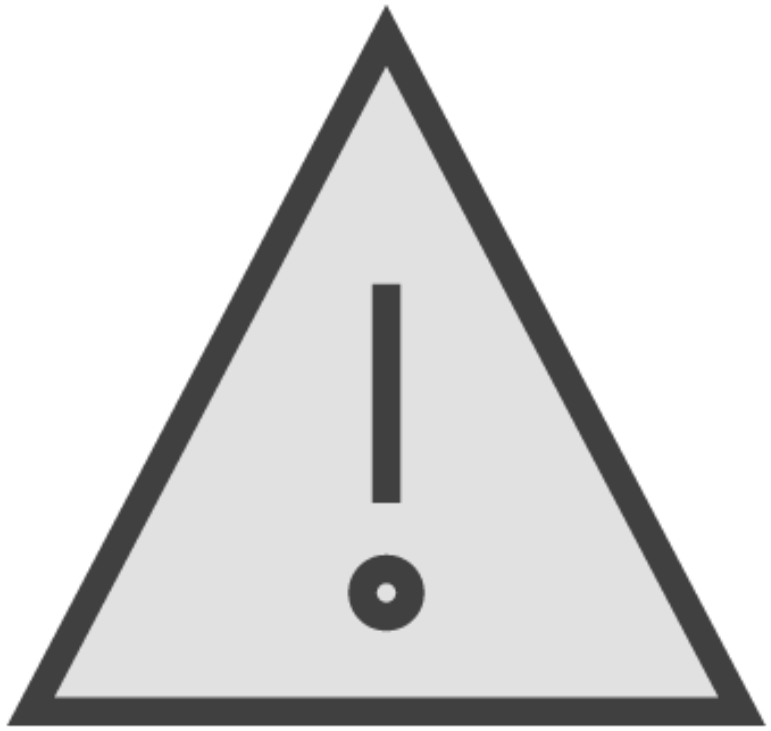
How can the malware be detected or removed?

Packers

Compress or encrypt executables.

Obfuscates program internals.

May contain anti-analysis features.

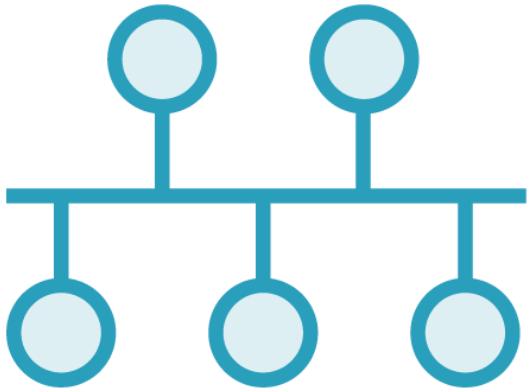


Live malware will be used!

Safety is extremely important!

Virtual Machine Precautions

Use a system you do not care about

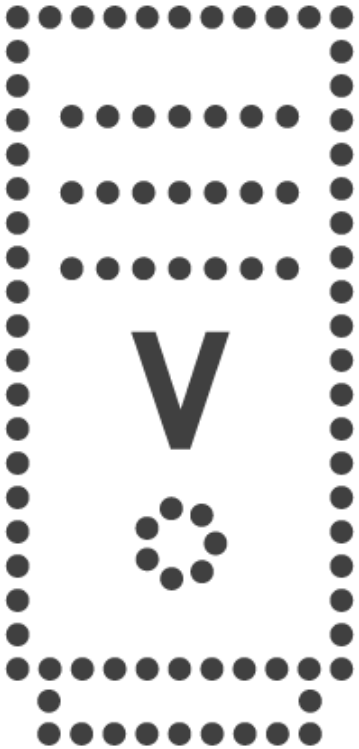


Segment the lab system from the rest of the network

Password protect your samples or defang your URLs

http:// → hxxp://

Virtual Machines

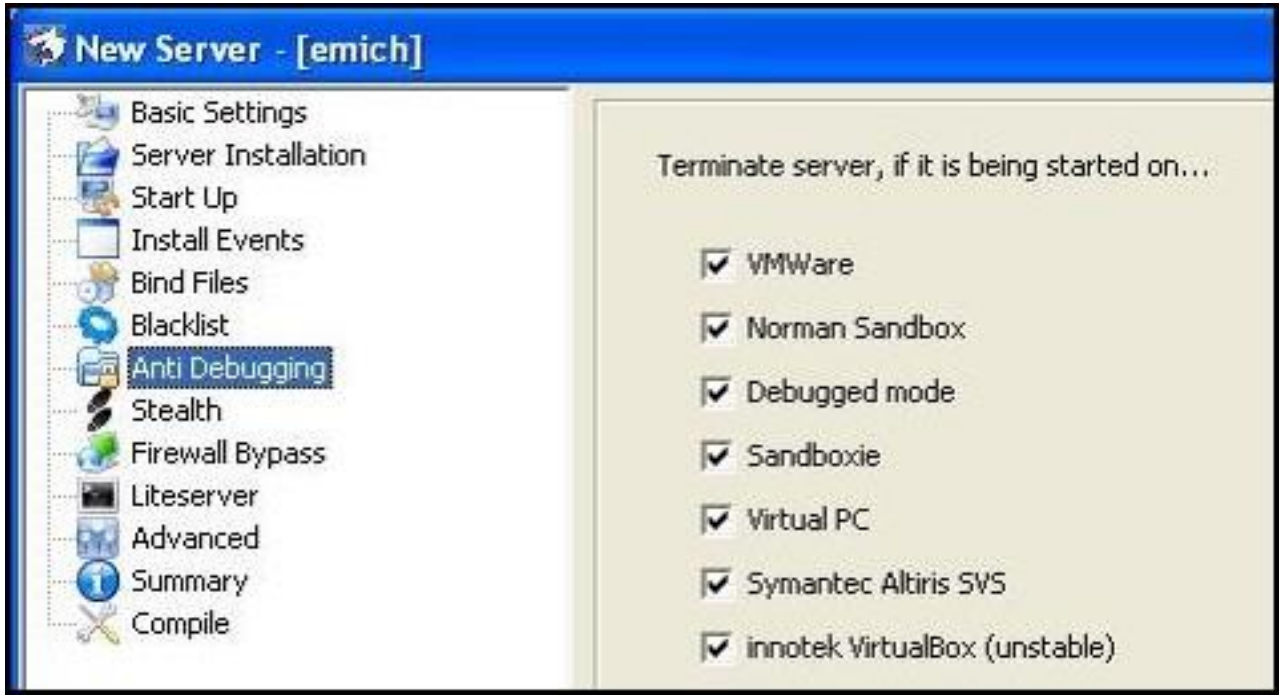


No additional systems required

Network segmentation built-in

Snapshot allows easy resetting

Malware Anti-analysis




```
0040120B push    ebx
0040120C push    ecx
0040120D push    edx
0040120E mov     eax, 'VMXh'
00401213 mov     ecx, 0Ah
00401218 mov     dx, 5658h
0040121C in      eax, dx
0040121D mov     [ebp+var_1C], ebx
```

Hiding Your Virtual Machine

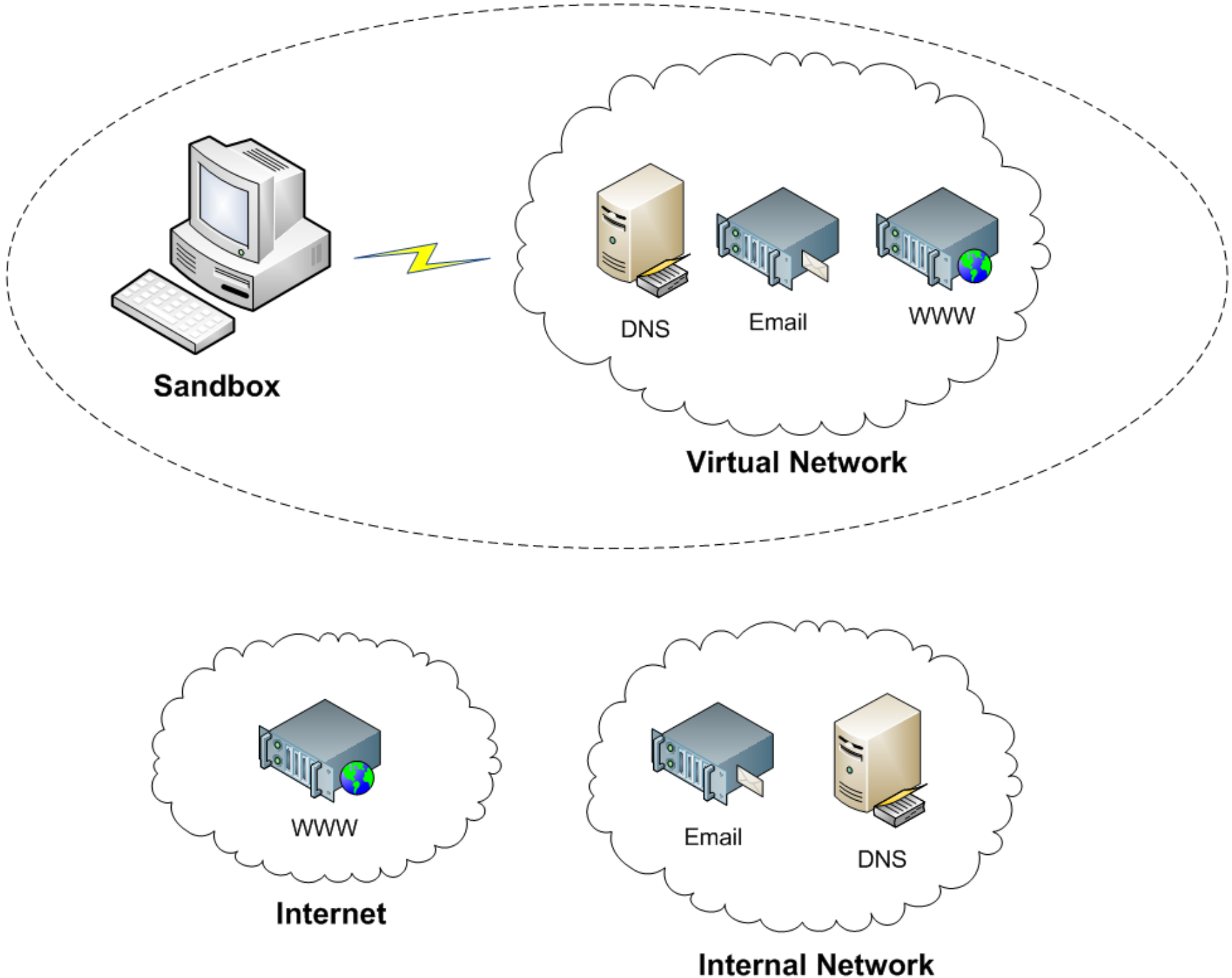
Make the VM look as real as possible

Install common end-user software

Open multiple files and documents

Don’t install VM guest tools

Trick the malware into thinking it is online


Sandbox
DNS
Email
WWW
Virtual Network
WWW
Internet
Email
DNS
Internal Network

FakeNet

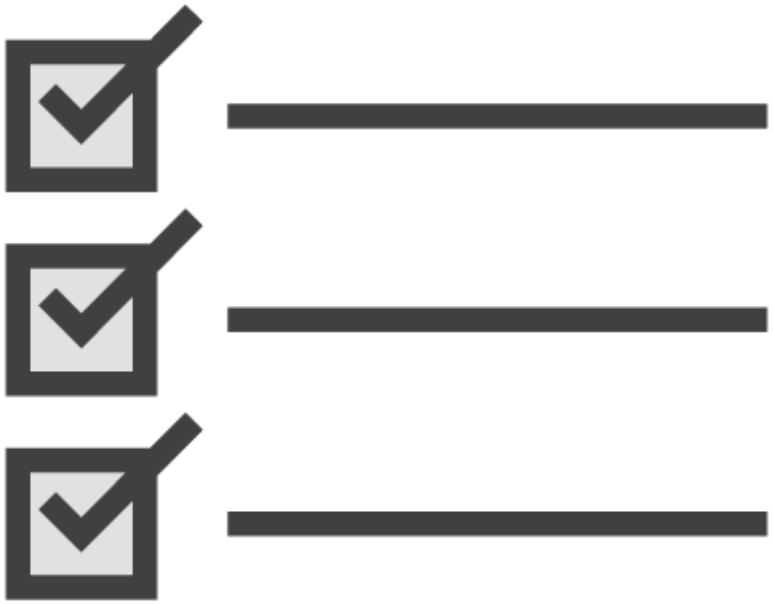
Tricks malware into thinking it's online

Intercepts on HTTP, SMTP, and more

Logs connections and PCAP

https://practicalmalwareanalysis.com/fakenet/

VM Installation Checklist



- Install the OS and patches
- Install and run your analysis tools
- Set up host-only networking
- Additional maintenance tasks
- Snapshot!

Demo

Configure a virtual machine for analysis

Summary

- Roadmap
- Malware analysis process
- Focus your analysis
- Virtual machine safety and configuration
- Lab