Texas Tech University
Spring 2017
Digital Forensics
Lab Settings and The Installation of Required Open-Source Tools

Introduction

Digital forensics and cybersecurity are emerging fields in desperate need of trained professionals. In response, Texas Tech began offering a digital forensics class (CS5332) in the spring of 2017. One challenge discovered in the first offering of digital forensics was an insufficient amount of time for the depth of study. Students spent more time setting up environments and tools and less time actually using the tools for a hands-on learning experience.

In an attempt to address this issue we are setting up a lab with pre-built virtual machines so students can spend more time analyzing and learning and less time setting up environments. This is not a lab with many computers but more of a "virtual" lab where students can access pre-configured virtual machines from their own computers.

Goals

- Texas Tech to become a leader in cybersecurity education
- Save students' time by providing baseline environments for lab exercises
- Maintain university network security while providing students with a place to use industry tools and analyze real-world threats to gain skills necessary for cybersecurity jobs

Research

Security considerations:

Digital forensics includes the analysis of malware and other potentially harmful data. Data samples and software tools required for the lab require access to the internet to download. Additionally, students will benefit from the ability to monitor network traffic.

Access to the internet raises the concern of spreading malware over the network. To mitigate risk, the structure of the lab is important. The goal is always to keep the host free of malware and keep specimens contained in the virtual machines. However, network connections to and from the lab should be treated as "potentially dangerous".

Provided below is a simple risk assessment that acknowledges threats along with mitigating controls.

Threat	Mitigating Controls
Host (server) becomes infected	● Install antivirus software ● Keep samples confined to virtual machines ● Create a baseline from which the original, clean environment can be easily restored
Malware propagates the network	● Keep server free of malware ● Isolate the network from the main university network ● Harden the server to prevent unnecessary open ports

	● Use the firewall capabilities of the router that separates the university network ● Work with the university IT department to create a comfortable setup ● Study executables on a computer that is not connected to the network

There are a variety of ways to configure a digital forensics lab based on the needs and resources of the university and digital forensics course. Some common, adaptable, setups are outlined below:

Server Virtualization without network boundary
Benefits
- Less worries about commercial licenses
- Easy for students

Disadvantages
- Forensic investigation is limited in order to limit risk to the main network

Server Virtualization with Network Boundary
Benefits
- Less worries about commercial licenses
- Potential damage to university is mitigated by network isolation
- The network environment is customizable and allows students to do network analysis they may not be able to do on the main university network because of restrictions

Disadvantages
- Expensive
- Must be able to support the potential network flood

Server Virtualization - hybrid approach
Benefits
- Little worry about commercial licenses

Disadvantages
- Expensive

Desktop Virtualization
Benefits
- Students can do work on their own computers
- Inexpensive

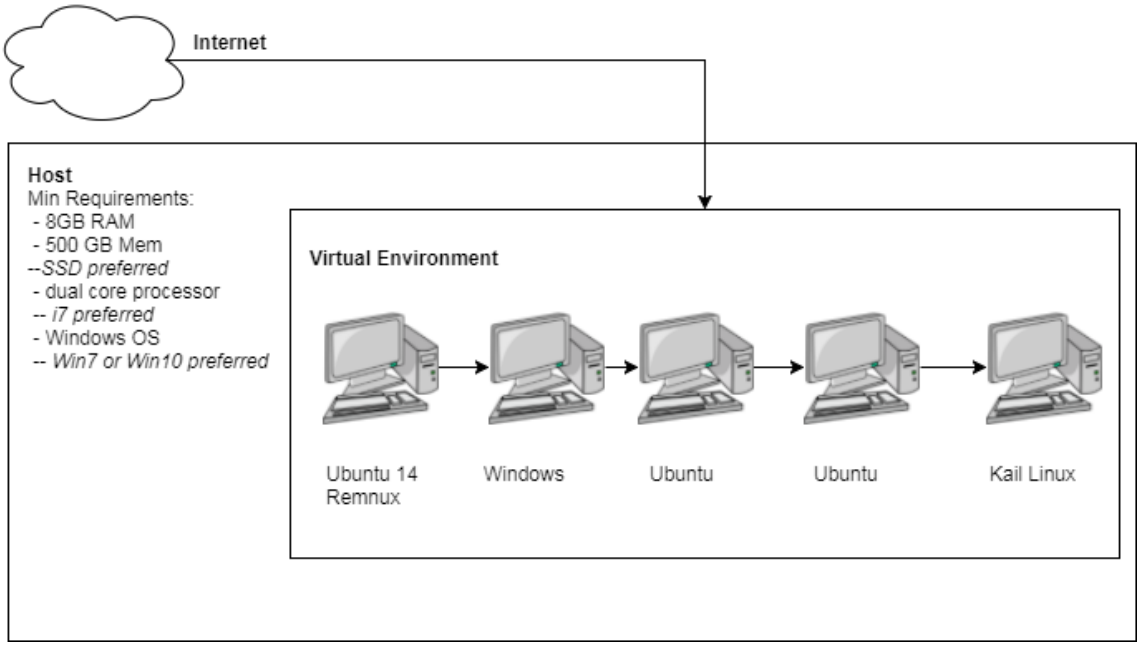
Disadvantages
- More difficult to standardize
- Not all students have the ability to run virtual machines on their computers
- Commercial license limitations

Texas Tech University
Spring 2017
Digital Forensics
Lab Settings and The Installation of Required Open-Source Tools

Care should be taken during setup and configuration to assure safety. There are potentially malicious files that students of the course analyze. Because of this, all of their work should be conducted inside of virtual machines. Even then, some malware can detect that it is being run in a virtual machine and try to escape to infect the host machine. Network traffic to and from the lab should be treated as potentially dangerous.

Procedure

Due to limited space and hardware we decided to take a hybrid approach to the lab. If students cannot remote into the lab or if something else happens, detailed instructions have been developed for students to install the environments on home computers.



Tools by Topic:

	Virtual Machines	Tools
Disk Forensics	Kali Windows	Autopsy (Windows)
Memory Analysis	Kali	
Network Analysis	Kali Windows	Network Miner (Windows) Wireshark (Kali)
Reverse Engineering	Remnux	
File System Analysis	Kali Windows	Autopsy (Windows)

Create an isolated network from the main university network.

Conclusion

Hopefully students will be able to use this digital forensics lab to complete their assignments. Although it is valuable to know how to set up an environment for forensics, the lab's goal is to save students' time so they can focus more on content and less on setup and tools. In addition to the lab, detailed instructions about how to setup the different environments have been documented in order to walk students through the process, making it easier if they do want to run the lab on their own home computers.

Texas Tech University
Spring 2017
Digital Forensics
Lab Settings and The Installation of Required Open-Source Tools

Sources

Son, Joon, Chinedum Irrechukwu, and Patrick Fitzgibbons. "Virtual Lab for Online Cyber Security Education." *Communications of the IIMA* 12.4 (2012): 5.

Bardas, Alexandru G., and Xinming Ou. "Setting up and using a cyber security lab for education purposes." *Journal of Computing Sciences in Colleges* 28.5 (2013): 191-197.

Al Falayleh, Mousa. "Building a digital forensic laboratory for an educational institute." *The International Conference on Computing, Networking and Digital Technologies (ICCNDT2012)*. The Society of Digital Information and Wireless Communication, 2012.

Malware sample : https://null0x4d5a.blogspot.com/2017/05/memory-analsyis-of-wannacry-ransomware.html

https://www.cfreds.nist.gov/dfrws/Rhino_Hunt.html