

---

# Hands-on Learning Experiences for Cyber Threat Hunting Education

---

Jinpeng Wei, Bei-Tseng “Bill” Chu  
University of North Carolina at Charlotte  
Deanne Cranford-Wesley  
Forsyth Technical Community College





# Overview

- Introduce Cyber Hunting
  - Skills needed for Cyber Hunting
    - Community College
    - 4-year programs
    - Advanced (competition)
  - Cyber Hunting Labs We Built
  - Demos
-



# Cyber Hunting

- Cyber threat hunting has emerged as a critical part of cyber security practice. However,
  - there is a **severe shortage** of cybersecurity professionals with **advanced analysis skills** for cyber threat hunting
- We have developed **freely-available, hands-on** learning materials (**labs**) for cyber threat hunting
- Our lab environment contains real threats (e.g., malware) against real software (e.g., Operating Systems and applications), and real security datasets, covering two important skill sets
  - **Threat analysis**: how to detect active and dormant malware, analyze its activities, and assess its impact
  - **Security data analytics**: how to search and probe for anomalies in a variety of datasets using multiple analytical skills, such as statistical analysis, machine learning, and data visualization



# Cyber Hunting

- Cyber Hunting
    - Find unknown threats (e.g. malware, insider threats)
  - Contrast with other cybersecurity activities
    - Cyber Defense
      - Harden systems (e.g. IDS, IPS, Patching)
    - Penetration Testing
      - Discover unknown vulnerabilities
    - Forensics
      - Part of incidence response: collect evidence, understand the scope of damage
-

# Threat Detection and Analysis Labs

- Objective: help a student learn how to detect active and dormant malware (either on disk or in memory), analyze its activities, assess its impact, and minimize its damage
  
  - Covered Threat Hunting Skill Set
    - ❑ Incident detection
    - ❑ Malicious code analysis
    - ❑ Memory forensic analysis
    - ❑ Security data analysis
-



# Design of the Hands-on Labs

- Each hands-on exercise covers a set of threat hunting skills that are needed to deal with a representative, real-world malware
- Labs are at various difficulty levels
- The exercise is created by installing representative malware into a lab environment and then taking a snapshot of the virtual machine
- The student's task is to use the snapshot to uncover what is happening, without any pre-knowledge of the particular malware installed
- Necessary analysis and development tools are installed in the lab environment for the student's use
- The student will submit a report of discoveries for each lab. The report will be graded based on the completeness and clarity of the submission
- Each lab exercise is packaged in one or more virtual machine snapshots



# Representative Lab Difficulty Levels

- Easy Labs
    - Malware does not try to hide (e.g., by choosing common names)
    - Malware has persistent networking activities
    - Malware behavior does not depend on an external server
  - Intermediate Labs
    - Malware runs as a service
    - Malware persists over reboot
    - Malware behavior is triggered by commands from an external server
  - Difficult Lab
    - Malware is fileless
    - Malware has a rootkit component that hides malicious processes, files, or network connections from user-level analysis tools
    - Malware employs obfuscation and/or anti-disassembly to thwart static analysis
    - Malware employs anti-debugging and/or anti-VM techniques to thwart dynamic analysis
-



# Tools Available in the Labs

- **Debuggers** (e.g., OllyDbg and Windbg)
- **Disassemblers** (e.g., IDA)
- **Basic static analysis tools** (e.g., CFF Explorer, Dependency Walker, PEiD, PEview, UPX, Resource Hacker),
- **Basic dynamic analysis tools** (e.g., Process Monitor, Process Explorer, System Monitor, Regshot, WinObj Object Manager, Sysinternals, ApateDNS, Netcat, iNetSim, and NtTrace)
- **Packet sniffers** (e.g., Wireshark)
- **Forensic analysis tools** (e.g., FTK, EnCase, Volatility, Memoryze)
- **Memory dump analysis tools** (e.g., Rekall, Redline, and Comae Windows Memory Toolkit)





# Security Data Analytics Labs

- Objective: help a student learn how to search and probe for anomalies in a variety of datasets (e.g., event logs, packet captures, and IDS/IPS alerts)
  
  - Covered Threat Hunting Skill Set
    - Basic search
    - Statistical analysis
    - Machine learning
    - Data visualization
-



# Insider Threat Hunting

## Overview of C0mp@ny:

C0mp@ny is an IT solutions company headquartered in Charlotte.

- ❖ It has 100 employees.
  - ❖ The C0mp@ny has offices in Charlotte NC, Paris, London, and Luxembourg worldwide.
  - ❖ There are 4 departments (HR, Research, IT, Finance), and each employee is associated with only a single department.
  - ❖ Each department has different allocated resources.
  - ❖ The employees are allowed to work from the office or from home.
  - ❖ Some employees get to also travel to visit other worldwide office locations.
  - ❖ The general working hours are from 8am to 5pm. However, some employees work from home and also access the company resources outside the regular working hours.
-



# Logs Used

- ❖ **Datalogs-** Contains access and authentication logs for 100 employees over 12 months (October 2015 To September 2016) period.
  - ❖ **Employee Info-** Contains employee ID, name, home address (latitude, longitude), department, start date, end date.
  - ❖ **Resource Info-** Contains mapping of resources to departments.
  - ❖ **Office Locations-** Contains latitude and longitude of 4 office locations.
-



# Insider Threat Hunting Activities

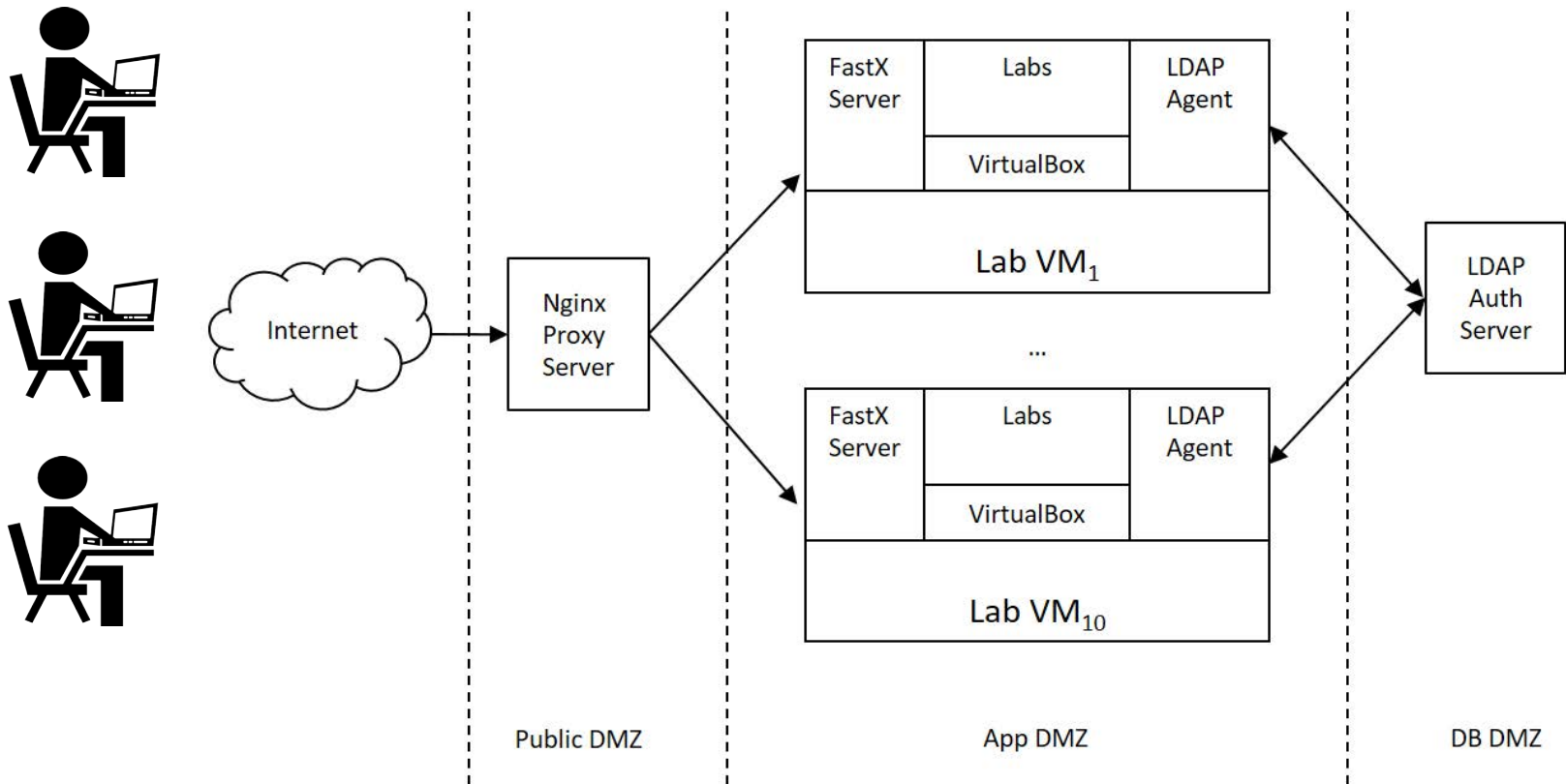
- Access before login
  - Access location other than home or office
  - Access resources outside of department
  - Access after leaving the company
  - Invalid employee ids
  - Failed attempts over a "short" period.
  - Print command to non-printers
  - More than one user accounts, same IP, same time
  - Time access pattern
-



# Implementation

- Lab environment is hosted on dedicated servers
  - We choose VirtualBox as the virtualization tool
  - Malware samples used in the labs are selected from real-world repositories such as VirusSign or other reputed sources
  - We provide a manual for each lab
  
  - A student first requests an account to our servers at the project page: <https://sites.google.com/uncc.edu/cyberthreathunting/home>
  - Then the student can log in to our servers, view the list of available labs, choose and start labs to finish the exercises, and upload his/her analysis reports
-

# The Topology of Our Lab Environment



# The Threat Hunting Project Page

<https://sites.google.com/uncc.edu/cyberthreathunting/labs>



## [Malware Analysis](#)

This lab will give you hands on experience for the Malware Analysis

[\*Click here to register the access to lab\*](#)



## [Login Location Anomaly Detection](#)

This lab will give you hands on experience to identify the access of an application by the employee from locations other than the home or office.

# The Threat Hunting Project Page (cont.)

<https://sites.google.com/uncc.edu/cyberthreat hunting/labs>



## [Resource Anomaly Detection](#)

This lab will give you an experience to identify the access of any company resources by an employee outside their department.



## [Employee Activity Anomaly Detection](#)

This lab will give you an experience to identify the unauthorized access of any company resources by an employee who has already resigned.





UNC CHARLOTTE

ForsythTech

Education For Life

# New User Registration Page



## Registration Form

Sign up using this form to access the lab.

\* Required

Email address \*

Your email

First Name \*

Your answer

Last Name \*

Your answer

Organization \*



# Demo Lab: Keylogger Discovery and Analysis

- Prominent behavior of the malware
  - ❑ Disguises under an innocuous name: javaw.exe
  - ❑ Records keystrokes and saves them in a file
  - ❑ Contacts a C&C server at [total-updates.com](http://total-updates.com)
  - ❑ Receives and acts upon several commands
    - One command is to exfiltrate the recorded keystrokes
  - ❑ Persists over reboot

[Demo video](#)

---



## Introduce Cyber Hunting in Community College

- Incorporate cyber threat hunting into the curriculum for community college students
    - Identify skill sets for cyber threat hunting appropriate for community college instruction
    - Contribute input to Knowledge Units for CAE2Y
  - Design cyber hunting instructional material suitable for community college students
    - Entry-level firewall configuration lab
    - Intermediate-level firewall configuration lab
    - Entry-level Wireshark lab
    - Intermediate-level Wireshark lab
  - Introduce and document the use in a community college setting of new instructional material developed by the UNCC team
  - Provide other expertise and resources as available through Forsyth Tech's designation as Central Eastern Regional Resource Center for Academic Excellence in Cyber Defense
-



# Implementation

- Labs accessible through web portal:
    - [netlab.forsythtech.edu](http://netlab.forsythtech.edu)
  - Netlab+ interface grants students access to lab topology, lab documentation, and VMs.
  - Instructor and student resources available
  - Currently implemented:
    - Entry-level Wireshark lab
    - Intermediate-level Wireshark lab
-



## Intermediate-level Wireshark lab

### ■ Backdoor Discovery

- Accessed through Netlab+ web portal
- Shows how an attacker/hacker makes an open connection to a host PC.
- Similar to previously mentioned Keylogger Discovery



UNC CHARLOTTE

**ForsythTech**

*Education For Life*

# Acknowledgement

- NSA funding under S-004-2017 CAE-C
- Mohammed Shehab
- Ehab Al-Shaer
- Md Rabbi Alam
- Trevon Williams
- Mai Moftha
- Chandni B. Jivani
- Michael Johnson
- James Brown
- Crystal Baldwin

# Thank You!



Dr. Jinpeng Wei<sup>1</sup>, Dr. Bei-Tseng “Bill” Chu<sup>2</sup>  
University of North Carolina at Charlotte  
[1jwei8@uncc.edu](mailto:jwei8@uncc.edu), [2billchu@uncc.edu](mailto:billchu@uncc.edu)

Dr. Deanne Cranford-Wesley  
Forsyth Technical Community College  
[dwesley@forsythtech.edu](mailto:dwesley@forsythtech.edu)

