Hands-on Learning Experiences for Cyber Threat Hunting Education

Bill Chu, Jinpeng Wei, Trevon Williams
University of North Carolina at Charlotte
Dr. Deanne Cranford-Wesley
Forsyth Technical Community College

UNC CHARLOTTE

ForsythTech
Education For Life

Overview

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

UNC CHARLOTTE

ForsythTech
Education For Life

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 are developing 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

UNC CHARLOTTE

ForsythTech
Education For Life

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

UNC CHARLOTTE

ForsythTech
Education For Life

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

UNC CHARLOTTE

ForsythTech
Education For Life

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

UNC CHARLOTTE

ForsythTech
Education For Life

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

UNC CHARLOTTE

ForsythTech
Education For Life

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)

UNC CHARLOTTE

ForsythTech
Education For Life

Implementation

- Lab environment is hosted on dedicated servers; a web portal will be created for remote access
- Once a student authenticates to our server, he/she can view the list of available labs, read lab manuals, choose and log into lab virtual machines to finish the exercises, and upload his/her analysis reports
- Malware samples used in the labs are selected from real-world repositories such as VirusSign or other reputed sources
- We choose VirtualBox as the virtualization tool
- We will provide a student manual and an instructor manual for each lab

UNC CHARLOTTE

ForsythTech
Education For Life

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 worlwide.
- 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.

UNC CHARLOTTE

ForsythTech
Education For Life

Logs

- **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.

UNC CHARLOTTE

ForsythTech
Education For Life

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

UNC CHARLOTTE

ForsythTech
Education For Life

Demo Lab: Backdoor Discovery

- The malware process constantly tries to connect to the domain www.uncc-cyber-huntingforfun.com on port 9999 and establishes a reverse shell once the connection is accepted

UNC CHARLOTTE

ForsythTech
Education For Life

Analysis Steps

Tool	Student Action	Observation
Process Explorer		No process with a suspicious name
Wireshark	Capture traffic	Periodic DNS requests to resolve www.uncc-cyber-huntingforfun.com, with no response
ApateDNS	Configure the tool to resolve any domain name to the host's IP address	Periodic requests for domain www.uncc-cyber-huntingforfun.com
Wireshark	Continue to capture traffic	TCP SYN packets to the host's IP address on port 9999, without TCP SYN-ACK packets from the host
Netcat on the host	Listen on port 9999	A Windows command prompt displayed by netcat, which can accept commands like "dir" and respond like a shell
Wireshark	Continue to capture traffic and follow TCP stream	Successful TCP three-way handshake and data exchange over the connection
System Monitor (sysmon)	Enable network monitoring	One process makes a network connection to the host IP address on port 9999; that is the malware process

UNC CHARLOTTE

ForsythTech
Education For Life

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
  - Receives and acts upon several commands
    - One command is to exfiltrate the recorded keystrokes
  - Persists over reboot

UNC CHARLOTTE

ForsythTech
Education For Life

Analysis Steps

Tool	Student Action	Observation
Process Explorer	Inspect process names	No process with a suspicious name
ApateDNS	Configure the tool to resolve any domain name to the host's IP address	Periodic requests for domain total-updates.com
Wireshark	Capture traffic	Periodic TCP SYN packets to the host's IP address on port 80, without TCP SYN-ACK packets from the host
Netcat on the host	Listen on port 80	A HTTP POST message is received, which includes the username, hostname, and group name of the analysis VM
System Monitor (sysmon)	Enable network monitoring	One process makes a network connection to the host IP address on port 80, and the process name is javaw.exe
Process Explorer	Find the start location of javaw.exe	At the location there is another file named Log.txt, and its content is logged keystrokes, such as "dir [enter]"

UNC CHARLOTTE

ForsythTech
Education For Life

Analysis Steps (cont.)

Tool	Student Action	Observation
Process Monitor (procmon)	Trace the API calls made by javaw.exe	Confirm that javaw.exe invokes WriteFile (“Log.txt”)
OllyDbg	Attach to javaw.exe, and set breakpoint at WriteFile, and use the call stack to locate malware code that makes such calls	Confirm how javaw.exe logs keystrokes and saves them in Log.txt
OllyDbg	Set breakpoint at InternetOpenA and use the call stack to figure out where in the malware such APIs are invoked	Confirm how javaw.exe contacts the host at port 80 and how the reply from the host affects its execution, and find out the commands that the malware understands, such as “Update”, “Upload KeyLogs”
Python scripts on the host	Develop a Python based web server that responds with “Update”, “Upload KeyLogs”, etc	Confirm that when the server replies “Upload KeyLogs”, the malware sends encoded content of Log.txt. Confirm effects of other commands

UNC CHARLOTTE

ForsythTech
Education For Life

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
  - Entry-level NetFlow 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

UNC CHARLOTTE

ForsythTech
Education For Life

Implementation

- Labs accessible through web portal:
  - 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

UNC CHARLOTTE

ForsythTech
Education For Life

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
- Mai Moftha
- Trevon Williams
- Michael Johnson
- Crystal Baldwin