
Cyber Hunting Exercise Development

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



Overview

- Introduce Cyber Hunting
- Cyber Hunting activities
 - Big data analysis of logs (cyber analytics)
 - In depth threat analysis
- Demo

Cyber Hunting

- Cyber Hunting
 - Find unknown threats (e.g. malware, insider threats)
 - Academy need to catch up with industry demands
 - 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
 - Working with current systems (no XP!) and real malware with strong safe guards
 - ❑ VM
-

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, PView, 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, ProDiscover, Volatility, OSForencis, Memoryze)
 - **Memory dump analysis tools** (e.g., Rekall, Redline, and Comae Windows Memory Toolkit)
-

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

- ❖ **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
-

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
-

Demo overview

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

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.
 - Eg (Workforce Framework) Defend and Protect
 - <https://niccs.us-cert.gov/workforce-development/cyber-security-workforce-framework?category=Analyze>
 - Contribute input to Knowledge Units for CAE2Y
 - KU's (Cyber Threats)
- 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



UNC CHARLOTTE

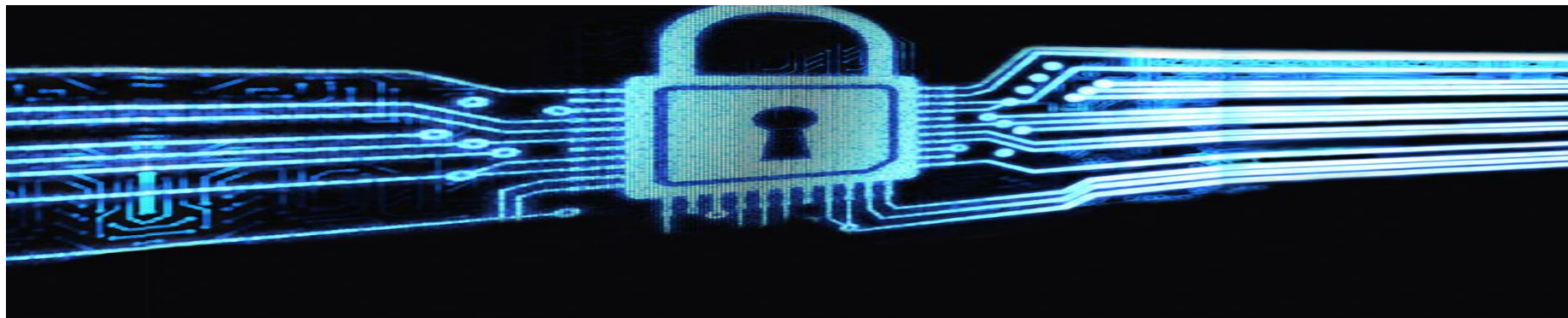
ForsythTech
Education For Life

Cyber Hunting Activities

1. Introduce and document the use in a community college setting of new instructional material developed by the UNCC team.
2. Provide other expertise and resources as available through Forsyth Tech's designation as a CAE Regional Resource Center.

CYBER HUNT

[This Photo](#) by Unknown Author is licensed under [CC BY-SA](#)



[This Photo](#) by Unknown Author is licensed under [CC BY-NC](#)

Responsibilities of CAE Regional Resource Center

- Cultivation of collaboration and support to designated schools in the region, faculty professional development for all designated CAEs
 - Program development support to schools in the candidates program. Host events and workshops, collaborate with the other CRRCs and CNRCs to minimize program duplication and share resources
 - Manage development of the Candidates in their region.
-

Acknowledgement

- NSA funding under S-004-2017 CAE-C
 - Mohammed Shehab
 - Ehab Al-Shaer
 - Michael Johnson
 - Trevon Williams
-



UNC CHARLOTTE



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)
