SYLLABUS

THREAT HUNTING
VERSION 2

A must have for any blue or red teamer's skill arsenal

eLearn Security
AN INE COMPANY

eLearnSecurity has been chosen by students in 140 countries in the world
and by leading organizations such as:

hp Microsoft intel cisco AT&T verizon U.S. AIR FORCE pwc gemalto security to be free

COURSE DESCRIPTION

Regardless of which side you are on, blue or red, good understanding of Threat Hunting and Threat Intelligence is vital if you want to be a complete IT Security professional. You cannot be a professional defender without good knowledge of attacking techniques. The same goes for penetration testers.

The Threat Hunting Professional (THP) course was designed to provide IT security professionals with the skills necessary not only to proactively hunt for threats, but also to become a stealthier penetration tester.

As a blue team member, you would use the techniques covered in the Threat Hunting Professional (THP) course to:

- Establish a proactive defense mentality and start your own threat hunting program/procedure
- Proactively hunt for threats in your organization's network, endpoints or perimeter and be several steps ahead of forthcoming adversaries
- Constantly fine tune your organization's defenses based on the latest attacker Techniques, Tactics and Procedures
- Use threat intelligence or hypotheses to hunt for known and unknown threats
- Inspect network traffic and identify abnormal activity in it
- Perform memory forensics using Redline, Volatility and a variety of tools to identify in-memory malware
- Use tools such as Sysmon and SilkETW to collect event logs
- Detect advanced hacking techniques such as AMSI bypasses, COM Hijacking and sophisticated/evasive malware
- Use tools such as PowerShell, ELK and Splunk to analyze Windows events and detect attacks such as DCSync, Kerberoasting and obfuscated PowerShell commands

As a red team member, you would use the techniques covered in the Threat Hunting Professional (THP) course to:

- Get familiar with the detection techniques being used by mature organizations
- Identify how an attack looks like in the wire and in memory
- Identify the most common events that are analyzed, in order to avoid triggering them
- Fine tune your attack strategy, attack vectors, and infrastructure, so that you remain under the radar
- Understand how you could leverage Threat Intelligence to upgrade your arsenal and deliver advanced adversary simulations, and more

WILL I GET A CERTIFICATE?

The Threat Hunting Professional (THP) course will also prepare you for the eLearnSecurity Certified Threat Hunter (eCTHPv2) certification exam.

PREREQUISITES

This course covers the foundational topics for threat hunting and threat intelligence; however, a good working knowledge coupled with experience in information technology, with a focus on security, prior to the class will be needed to help aid you in your learning. You should have:

- A solid understanding of computer networks: switches, routing, security devices, common network protocols, etc. (Recommended)
- Intermediate understanding of IT security matters
- Intermediate to advanced understanding of penetration testing tools and methods. (Recommendation: IHRP course)

WHO SHOULD TAKE THIS COURSE?

This training course is primarily intended for SOC/IT Security analysts that would like to proactively detect attacks and/or possible malware behavior in their environments.

The target audience of this course are:

- Security Operations Center analysts and engineers
- Incident response team members
- Penetration testers/Red team members
- Network security engineers
- Information security consultants and IT auditors
- Managers who want to understand how to create threat hunting teams and intelligence capabilities

ORGANIZATION OF CONTENTS

The student is provided with a suggested learning path to ensure the maximum success rate and the minimum effort.

SECTION 01: THREAT HUNTING

- Module 1: Introduction to Threat Hunting
- Module 2: Threat Hunting Terminology
- Module 3: Threat Intelligence
- Module 4: Threat Hunting Hypothesis

SECTION 02: HUNTING THE NETWORK - NETWORK ANALYSIS

- Module 1: Introduction to Network Hunting
- Module 2: Suspicious Traffic Hunting
- Module 3: Hunting Webshells

SECTION 03: HUNTING THE ENDPOINT - ENDPOINT ANALYSIS

- Module 1: Introduction to Endpoint Hunting
- Module 2: Malware Overview
- Module 3: Hunting Malware
- Module 4: Event IDs, Logging, and SIEMs
- Module 5: Hunting with PowerShell

THREAT HUNTING

This section will introduce you to the world of threat hunting, which will include a brief overview of what threat hunting is and why companies are seeking to establish this capability within their organization. Certain industry terms will be discussed, as well as having the hunter mindset and whether it will lean towards threat intel or DFIR.

1. MODULE 01 – INTRODUCTION TO THREAT HUNTING

- **1.1. Introduction**
- **1.2. Incident Response**
  - 1.2.1. Incident Response Process
  - 1.2.2. Incident Response & Hunting
- **1.3. Risk Assessments**
- **1.4. Threat Hunting Teams**
  - 1.4.1. Ad-hoc Hunter
  - 1.4.2. Analyst and Hunter
  - 1.4.3. Dedicated Hunting Team

2. MODULE 02 – THREAT HUNTING TERMINOLOGY

- **2.1. Threat Hunting Terms**
  - 2.1.1. Advanced Persistent Threat
  - 2.1.2. Tactics, Techniques & Procedures
    - 2.1.2.1. TTPs – IOCs
  - 2.1.3. Pyramid of Pain
    - 2.1.3.1. Hash Values
    - 2.1.3.2. IP Addresses
    - 2.1.3.3. Domain Names
    - 2.1.3.4. Network/Host Artifacts
    - 2.1.3.5. Tools
    - 2.1.3.6. TTPs
  - 2.1.4. Cyber Kill Chain Model
  - 2.1.5. The Diamond Model

MODULE 02 – THREAT HUNTING TERMINOLOGY (cont.)

- **2.2. Threat Hunting Mindset: Threat Intelligence**
  - 2.2.1. The 3 Types of Threat Intelligence
    - 2.2.1.1. Strategic
    - 2.2.1.2. Tactical
    - 2.2.1.3. Operational
- **2.3. Threat Hunting Mindset: Digital Forensics**
  - 2.3.1. Attack Based Hunting
  - 2.3.2. Analytics Based Hunting
  - 2.3.3. Hunting Periods
    - 2.3.3.1. Point in Time
    - 2.3.3.2. Real Time
    - 2.3.3.3. Historic
  - 2.3.4. Reverse Engineering Binaries
- **2.4. Threat Hunting Simulations**

3. MODULE 03 – THREAT INTELLIGENCE

- **3.1. Introduction**
- **3.2. Threat Intelligence Reports & Research**
  - 3.2.1. Threat Intelligence Reports - FireEye
  - 3.2.2. Threat Intelligence Research
- **3.3. Threat Sharing and Exchanges**
  - 3.3.1. ISACs (Information Sharing and Analysis Centers)
  - 3.3.2. US-CERT (US Computer Emergency Readiness Team)
  - 3.3.3. Alien Vault OTX (Open Threat Exchange)
    - 3.3.3.1. VIDEO: OTX & IOCs
  - 3.3.4. Threat Connect
  - 3.3.5. MISP (Malware Information Sharing Platform)
- **3.4. IOCs (Indicators of Compromise)**
  - 3.4.1. OpenIOC
  - 3.4.2. IOC Editor
    - 3.4.2.1. VIDEO: Creating IOCs with IOC Editor
  - 3.4.3. Redline
    - 3.4.3.1. VIDEO: Redline and IOCs
  - 3.4.4. YARA
    - 3.4.4.1. VIDEO: YARA and YARA Rules
  - 3.4.5. HERA LAB: Hunting with IOCs

4. MODULE 04 – THREAT HUNTING HYPOTHESIS

NETWORK ANALYSIS

In this section, we'll go over the TCP/IP stack and learn how to recognize normal network traffic. We will then use that foundation and attempt to detect suspicious network traffic patterns. Additionally, we will also look at how to detect web shells hiding in our environment using various tools. During web shell hunting, we will also cover how you can combine threat intelligence with statistical analysis to hunt for threats.

1. MODULE 01 – INTRODUCTION TO NETWORK HUNTING

- **1.1. Introduction**
- **1.2. TCP/IP & Networking Primer**
  - 1.2.1. OSI & TCP/IP Model
  - 1.2.2. TCP/IP Model
  - 1.2.3. Routers
  - 1.2.4. Switches
  - 1.2.5. ARP Traffic
  - 1.2.6. TCP Traffic
    - 1.2.6.1. TCP Header
  - 1.2.7. UDP Header
  - 1.2.8. Common Ports
- **1.3. Packet Analysis & Tools**
  - 1.3.1. Live Network Captures
    - 1.3.1.1. Port Mirroring
    - 1.3.1.2. Network Tap
    - 1.3.1.3. MAC Floods
    - 1.3.1.4. ARP Poisoning
  - 1.3.2. Libpcap
  - 1.3.3. Wireshark
  - 1.3.4. Dumpcap
  - 1.3.5. Tcpdump
  - 1.3.6. Berkley Packet Filter

2. MODULE 02 - SUSPICIOUS TRAFFIC HUNTING

- **2.1. Introduction**
- **2.2. ARP Traffic**
  - 2.2.1. ARP
    - 2.2.1.1. Normal ARP
    - 2.2.1.2. Suspicious ARP
  - 2.2.2. Wireshark Tip
- **2.3. ICMP Traffic**
  - 2.3.1. ICMP
    - 2.3.1.1. Normal ICMP
    - 2.3.1.2. Suspicious ICMP
  - 2.3.2. Wireshark Tip
- **2.4. TCP Traffic**
  - 2.4.1. TCP
    - 2.4.1.1. Normal TCP
    - 2.4.1.2. Suspicious TCP
  - 2.4.2. UDP
  - 2.4.3. Wireshark Tip
- **2.5. DHCP Traffic**
  - 2.5.1. DHCP
    - 2.5.1.1. Normal DHCP Traffic
    - 2.5.1.2. Suspicious DHCP
  - 2.5.2. Wireshark Tip
- **2.6. DNS Traffic**
  - 2.6.1. DNS
    - 2.6.1.1. Normal DNS
    - 2.6.1.2. Suspicious DNS
  - 2.6.2. Wireshark Tip
- **2.7. HTTP/HTTPS Traffic**
  - 2.7.1. HTTP
    - 2.7.1.1. Normal HTTP
      - Protocol Hierarchy Statistics
      - Export HTTP Object
    - 2.7.1.2. Suspicious HTTP
  - 2.7.2. HTTPS
    - 2.7.2.1. Normal HTTPS
    - 2.7.2.2. Suspicious HTTPS
  - 2.7.3. Wireshark Tip
- **2.8. Unknown Traffic**
  - 2.8.1. VIDEO: Wireshark

MODULE 02 - SUSPICIOUS TRAFFIC HUNTING (cont.)

- **2.9. More Hunting Tools**
  - 2.9.1. NetworkMiner
    - 2.9.1.1. VIDEO: Network Miner
  - 2.9.2. RSA NetWitness Investigator
    - 2.9.2.1. VIDEO: RSA Witness Investigator
  - 2.9.3. VIDEO: Packet Hunting
  - 2.9.4. HERA LAB: Hunting Insider Threats Part 1
  - 2.9.5. HERA LAB: Hunting Insider Threats Part 2
  - 2.9.6. HERA LAB: Network Hunting & Forensics

3. MODULE 03 – HUNTING WEB SHELLS

- **3.1. Introduction**
  - 3.1.1. C99
  - 3.1.2. B347K
  - 3.1.3. R57
- **3.2. Hunting Tools**
  - 3.2.1. LOKI Simple IOC Scanner
  - 3.2.2. NeoPI
  - 3.2.3. BackdoorMan
  - 3.2.4. PHP-Malware-Finder
  - 3.2.5. unPHP
  - 3.2.6. Web Shell Detector
  - 3.2.7. Linux Malware Detect
  - 3.2.8. Invoke-ExchangeWebShellHunter
  - 3.2.9. NPROCWATCH
- **3.3. Hunting Web Shells**
  - 3.3.1. Linux Commands
  - 3.3.2. Windows Commands
  - 3.3.3. LOKI Simple IOC Scanner
  - 3.3.4. NeoPI
  - 3.3.5. BackdoorMan
  - 3.3.6. File Stacking
  - 3.3.7. Baselines
  - 3.3.8. Statistical Analysis
    - 3.3.8.1. VIDEO: Log Parser Studio
  - 3.3.9. PHP in Exif Data
  - 3.3.10. W3WP Parent-Child Detection
  - 3.3.11. HERA LAB: Hunting Webshells Part 1
  - 3.3.12. HERA LAB: Hunting Webshells Part 2

ENDPOINT ANALYSIS

In this section, you will dive into the workstation. You will be introduced to the Windows OS where you will learn how to detect what's in plain sight, and whether it is normal or potentially malicious. Also introduced are techniques on how to track malicious behavior on the endpoint/s through lateral movement and how to use certain tools to assist you with this task across thousands of endpoints. You will learn to detect Mimikatz, malicious macros, code injection, and more, using various detection methods. Finally, you will also get familiar with how malware operates and how you can detect their operations in memory.

1. MODULE 01 – INTRODUCTION TO ENDPOINT HUNTING

- **1.1. Introduction**
- **1.2. Windows Processes**
  - 1.2.1. smss.exe
  - 1.2.2. csrss.exe
  - 1.2.3. winlogon.exe
  - 1.2.4. wininit.exe
  - 1.2.5. lsm.exe
  - 1.2.6. services.exe
  - 1.2.7. lsass.exe
  - 1.2.8. svchost.exe
  - 1.2.9. taskhost.exe
  - 1.2.10. explorer.exe
- **1.3. Endpoint Baselines**
  - 1.3.1. System Center Configuration Manager
  - 1.3.2. PowerShell Desired State Configuration
  - 1.3.3. Microsoft Security Compliance Manager
  - 1.3.4. Microsoft Security Compliance Toolkit
  - 1.3.5. Services Baseline
  - 1.3.6. Processes Baseline

2. MODULE 02 – MALWARE OVERVIEW

- **2.1. Introduction**
- **2.2. Malware Classifications**
  - 2.2.1. Viruses
  - 2.2.2. Worm
  - 2.2.3. Rootkits
  - 2.2.4. Bootkits
  - 2.2.5. Trojans
  - 2.2.6. Backdoors
  - 2.2.7. Remote Access Trojans
  - 2.2.8. Spyware
  - 2.2.9. Botnets
  - 2.2.10. Ransomware
  - 2.2.11. Information Stealers
- **2.3. Malware Delivery**
  - 2.3.1. Physical Media
  - 2.3.2. Email
  - 2.3.3. URL Links
  - 2.3.4. Drive-by Downloads
  - 2.3.5. Web Advertising
  - 2.3.6. Social Media
  - 2.3.7. Software Vulnerabilities
- **2.4. Malware Evasion Techniques**
  - 2.4.1. Alternate Data Streams
  - 2.4.2. Injections
    - 2.4.2.1. DLL Injections
    - 2.4.2.2. Reflective DLL Injection
    - 2.4.2.3. Thread Hijacking
    - 2.4.2.4. PE Injection
    - 2.4.2.5. Process Hollowing
    - 2.4.2.6. Hook Injection
    - 2.4.2.7. KernelMode Rootkits: SSDT Hooks
    - 2.4.2.8. KernelMode Rootkits: IRP Hooks
    - 2.4.2.9. Userland Rootkits: IAT Hooks
    - 2.4.2.10. Userland Rootkits: EAT Hooks
    - 2.4.2.11. Userland Rootkits: Inline Hooks
    - 2.4.2.12. Rootkits: Process Hiding
  - 2.4.3. Masquerading
  - 2.4.4. Packing / Compression

MODULE 02 – MALWARE OVERVIEW (cont.)

- 2.4.5. Recompiling
- 2.4.6. Obfuscation
- 2.4.7. Anti-Reversing Techniques

2.5. Malware Persistence

- 2.5.1. Autostart Locations
- 2.5.2. Scheduled Task
- 2.5.3. COM Hijacking
- 2.5.4. DLL Hijacking: Search Order
- 2.5.5. DLL Hijacking: Phantom DLL
- 2.5.6. DLL Hijacking: Side Loading
- 2.5.7. Windows Services: Service Creation
- 2.5.8. Windows Services: Service Replacement
- 2.5.9. Windows Services: Service Recovery

3. MODULE 03 – HUNTING MALWARE

- **3.1. Introduction**
- **3.2. Detection Tools**
  - 3.2.1. PE Capture
  - 3.2.2. ProcScan.rb
  - 3.2.3. Meterpreter Payload Detection
  - 3.2.4. Reflective Injection Detection
  - 3.2.5. Powershell Arsenal
  - 3.2.6. Get-InjectedThread.ps1
- **3.3. Detection Techniques**
  - 3.3.1. Fuzzy Hashing
  - 3.3.2. Import Hashing
  - 3.3.3. Execution Tracing
- **3.4. Malware Analysis**
  - 3.4.1. Redline
    - 3.4.1.1. VIDEO: Redline – Create Standard Collector
    - 3.4.1.2. VIDEO: Redline – Basic Usage
    - 3.4.1.3. VIDEO: Redline – Create Analysis File
    - 3.4.1.4. VIDEO: Redline – Detecting Code Injection
  - 3.4.2. Volatility
    - 3.4.2.1. HERA LAB: Hunting in Memory
  - 3.4.3. Live System Memory Hunting
    - 3.4.3.1. Get-InjectedThread
    - 3.4.3.2. Memhunter
    - 3.4.3.3. Captain
  - 3.4.4. HERA LAB: Hunting for Process Injection & Proactive API Monitoring
  - 3.4.5. HERA LAB: Advanced Endpoint Hunting
- **3.5. Malware Analysis**
  - 3.5.1. HERA LAB: Hunting in Malware Part 1
  - 3.5.2. HERA LAB: Hunting in Malware Part 2
  - 3.5.3. HERA LAB: Hunting Empire

4. MODULE 04 – EVENT IDS, LOGGING AND SIEMS HUNTING

MODULE 04 – EVENT IDS, LOGGING AND SIEMS HUNTING (cont.)

- 4.7.5. COM Hijacking
- 4.7.6. VIDEO: Threat Hunting with ELK
- 4.7.7. HERA LAB: Hunting for WMI Abuse, Parent Process Spoofing & Access Token Theft
- 4.7.8. HERA LAB: Hunting with ELK
- 4.7.9. HERA LAB: Hunting with SPLUNK

5. MODULE 05 – HUNTING WITH POWERSHELL

- **5.1. Introduction**
- **5.2. PowerShell Hunting Tools**
  - 5.2.1. Kansa
  - 5.2.2. PSHunt
  - 5.2.3. NOAH
  - 5.2.4. HERA LAB: Hunting at Scale with Osquery
- **5.3. Windows Advanced Threat Protection**
- **5.4. Microsoft Advanced Threat Analytics**
  - 5.4.1. Microsoft Advanced Threat Analytics
  - 5.4.2. Azure Advanced Threat Protection
- **5.5. PowerShell Defenses**
  - 5.5.1. System-Wide Transcript File
  - 5.5.2. Constrained Language Mode
  - 5.5.3. Anti-Malware Scan Interface

LABS

The THP course is a practice-based curriculum **containing 27 hands-on labs**. Being integrated with Hera Lab, the most sophisticated virtual lab in IT Security, it offers an unmatched practical learning experience. Hera is the only virtual lab that provides fully isolated per-student access to each of the real-world network scenarios available on the platform. Students can access Hera Lab from anywhere through VPN.

Modules will be accompanied by many hands-on labs.

- Lab 1: Hunting with IoCs
- Lab 2: Hunting Insider Threats Part 1
- Lab 3: Hunting Insider Threats Part 2
- Lab 4: Network Hunting & Forensics
- Lab 5: Hunting Web Shells Part 1
- Lab 6: Hunting Web Shells Part 2
- Lab 7: Hunting in Memory (2 Labs)
- Lab 8: Hunting for Process Injection & Proactive API Monitoring
- Lab 9: Advanced Endpoint Hunting (2 Labs)
- Lab 10: Hunting Malware Part 1
- Lab 11: Hunting Malware Part 2
- Lab 12: Hunting Empire
- Lab 13: Hunting Responder
- Lab 14: Hunting .Net Malware (2 Labs)
- Lab 15: Hunting for WMI Abuse, Parent Process Spoofing & Access Token Theft
- Lab 16: Hunting with ELK (3 Labs)
- Lab 17: Hunting with Splunk (5 Labs)
- Lab 18: Hunting at Scale with Osquery

ABOUT US

We are eLearnSecurity.

eLearnSecurity was founded with the simple mission of revolutionizing the way IT professionals develop their information security skills. Now based in Cary, North Carolina with offices and employees around the United States and Europe, eLearnSecurity is a worldwide leader in cyber security training.

Through a blend of in-depth content and real-world simulations, our detailed courses, training paths, and certifications equip businesses and individuals with the skills needed to take on the cyber security challenges of today and tomorrow.

Whether you are interested in brushing up on specific ethical hacking techniques or following a comprehensive training path, eLearnSecurity provides a unique opportunity for security professionals to enhance their knowledge of the industry. We train red, blue, and purple teams in the latest cyber security techniques with classes ranging from beginner to expert levels.

eLearnSecurity's Hera Labs is an industry-leading virtual lab that offers our clients practical penetration testing and ethical hacking experience, changing the way students and businesses take on the future of cyber security.

Contact details:

www.elearnsecurity.com
contactus@elearnsecurity.com

Via Gian Battista Queirolo 15
Pisa, Italy

575 New Waverly Place #201
Cary, NC, USA