SYLLABUS

THREAT HUNTING PROFESSIONAL
VERSION 1

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

eLearnSecurity has been chosen by students in over 140 countries in the world and by leading organizations such as:
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 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 and IOCs to hunt for known threats
- Comfortably inspect network traffic and identify malicious traffic
- Perform memory analysis using Redline and Volatility to identify malware
- Use tools such as Sysmon and ELK to analyze Windows events and detect attack patterns
- Use tools such as PowerShell, Microsoft ATP and ATA to detect attacks, and more

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
INTRODUCTION

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, TCP/IP, typical network applications such as DNS, HTTPS, SMTP, etc. (Recommended)
- Intermediate understanding of IT security matters
- Intermediate to advanced understanding of penetration testing tools and methods. (Recommendation: PTP 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
- Penetration testers/Red team members
- Network security engineers
- Incident response team members
- Information security consultants and IT auditors
- Managers who want to understand how to create threat hunting teams and intelligence capabilities
- Anyone who is interested in threat hunting and threat intelligence

WILL I GET A CERTIFICATE?

The Threat Hunting Professional (THP) course will prepare you for the eLearnSecurity Certified Threat Hunter Professional (eCTHP) certification exam.
ORIENTATION OF CONTENTS

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

THREAT HUNTING

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

HUNTING THE NETWORK: NETWORK ANALYSIS

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

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. Threat Hunting
   1.1. Introduction
      1.1.1. Introduction to Threat Hunting
      1.1.1.1. What is threat hunting & the need for threat hunting?
      1.1.2. Incident Response
      1.1.2.1. Incident Response Process
      1.1.2.2. Incident Response & Hunting
      1.1.3. Risk Assessment
      1.1.3.1. What are risk assessments?
      1.1.3.2. Risk Assessments & Hunting
      1.1.4. Hunting mindset: Threat Intelligence
      1.1.4.1. What is threat intelligence?
      1.1.4.2. Using threat intelligence to hunt
      1.1.5. Hunter mindset: Forensics
      1.1.5.1. What is digital forensics?
      1.1.5.2. Using digital forensics to hunt
      1.1.6. Threat Hunting/Intelligence Simulation
      1.1.6.1. Continually testing the hunter(s)

1.2. Threat Hunting Terminology
   1.2.1. APT (Advanced Persistent Threat)
   1.2.2. TTP (Tools, Tactics, and Procedures)
   1.2.3. Pyramid of Pain
   1.2.4. The Cyber Kill Chain Model
   1.2.5. The Diamond Model

1.3. Threat Intelligence
   1.3.1. Threat Reports & Research
   1.3.2. Threat Sharing & Exchanges
      1.3.2.1. ISACs (Information Sharing and Analysis Centers)
      1.3.2.2. Government-sponsored threat sharing
      1.3.2.3. US-CERT (US Computer Emergency Readiness Team)
1.3.2.4. DHS/CISCP (Department of Homeland Security / Cyber Information Sharing and Collaboration Program)
1.3.2.5. Alien Vault OTX (Open Threat Exchange)
1.3.2.6. Threat Connect
1.3.2.7. MISP (Malware Information Sharing Platform)
1.3.2.8. CRITs (Collaborative Research Into Threats)

1.3.3. IOCs (Indicators of Compromise)
  1.3.3.1. IOC Editor
  1.3.3.2. OpenIOC
  1.3.3.3. STIX (Structured Threat Information Expression)
  1.3.3.4. CyBOX (Cyber Observable Expression)
  1.3.3.5. TAXII (Trusted Automated Exchange of Indicator)

1.4. Threat Hunting Methodology
  1.4.1. Methodology
    1.4.1.1. Report Writing
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.

2. Network Analysis
   2.1. Introduction to Network Hunting
      2.1.1. Introduction
      2.1.2. TCP/IP & Networking Primer
      2.1.3. Tools

   2.2. Suspicious Traffic Hunting
      2.2.1. ARP
      2.2.2. ICMP
      2.2.3. TCP
      2.2.4. DHCP
      2.2.5. DNS
      2.2.6. HTTP/HTTPS
      2.2.7. Unknown
      2.2.8. Tools

   2.3. Hunting Web Shells
      2.3.1. Introduction
      2.3.2. Hunting Tools
      2.3.3. Hunting Web Shells
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.

3. Endpoint Analysis
   3.1. Introduction to Endpoint Hunting
      3.1.1. Introduction
      3.1.2. Windows Processes
      3.1.3. Endpoint Baselines
   
   3.2. Malware Overview
      3.2.1. Introduction
      3.2.2. Malware Classifications
      3.2.3. Malware Delivery
      3.2.4. Malware Evasion Techniques
      3.2.5. Malware Persistence
   
   3.3. Hunting Malware
      3.3.1. Introduction
      3.3.2. Detection Tools
      3.3.3. Detection Techniques
      3.3.4. Memory Analysis
   
   3.4. Event IDs, Logging and SIEMs
      3.4.1. Windows Event Logs
      3.4.2. Windows Event IDs
         3.4.2.1. Suspicious Account Usage & Creation
         3.4.2.2. Passwords
         3.4.2.3. Hashes (PTH)
         3.4.2.4. Forged Kerberos Tickets
         3.4.2.5. RDP
         3.4.2.6. PsExec
         3.4.2.7. WMIX
3.4.2.8. Scheduled Tasks
3.4.2.9. Service Creation
3.4.2.10. Admin Shares
3.4.2.11. Lateral Movement
3.4.3. Windows Event Forwarding
3.4.4. Log Rotation & Log Clearing
3.4.5. PowerShell Logging
3.4.6. Tools
   3.4.6.1. Sysmon
   3.4.6.2. SIEMs (ELK & Splunk)

3.5. Hunting with PowerShell
3.5.1. Kansa
   3.5.1.1. Invoke-IR
3.5.2. Microsoft ATP & ATA
We are eLearnSecurity.

Based in Santa Clara, California, with offices in Pisa, Italy and Dubai, UAE, Caendra Inc. is a trusted source of IT security skills for IT professionals and corporations of all sizes. Caendra Inc. is the Silicon Valley-based company behind the eLearnSecurity brand.

eLearnSecurity has proven to be a leading innovator in the field of practical security training, with best of breed virtualization technology, in-house projects such as Coliseum Web Application Security Framework and Hera Network Security Lab, which has changed the way students learn and practice new skills.

Contact details:

[www.elearnsecurity.com](http://www.elearnsecurity.com)
[contactus@elearnsecurity.com](mailto:contactus@elearnsecurity.com)