# Advent of cyber 2022

## DAY1

Objectives:

Attack cycles :

1. IN
2. Through
3. OUT

## DAY2

Objectives:

* Learn what log files are and why they’re useful.
  + Login attempts or failures.
  + Traffic on a network
  + Things (website URLs, files, etc.) that have been accessed.
  + Password changes
  + Application errors (used in debugging)
  + and many, many more
* Understand what valuable information log files can contain.
* What has happened?
* When has it happened?
* Where has it happened?
* Who did it? Were they successful?
* What is the result of the action?
* Understand some common locations these logs file can be found.
  + windows logs
  + Linux logs
* Use some basic Linux commands to start analyzing log files for valuable information.
  + GREP
  + SIEM

## DAY3

Learning Objectives

* What is OSINT, and what techniques can extract useful information against a website or target?
* Using dorks to find specific information on the Google search engine
* Extracting hidden directories through the Robots.txt file
* Domain owner information through WHOIS lookup
* Searching data from hacked databasesTools
* Acquiring sensitive information from publicly available GitHub repositories

Tools:

* **Google Dorks**
* **inurl**
* **filetype**
* **site**
* **cache**
* **WHOIS Lookup**
* **Robots.txt**
* **Breached Database Search**
  + <https://haveibeenpwned.com/>
  + **Searching GitHub Repos**

## Day4

Learning Objectives

* What is Scanning?
* Scanning types
  + Passive
  + Active
* Scanning techniques
  + Network Scanning
  + Port Scanning
  + Vulnerability Scanning
* Scanning tools
* NMAP
* Nikto

## Day5

Learning Objectives

* Learn about common remote access services.
* SSH
* RDP
* VNC
* Recognize a listening VNC port in a port scan.
* Learn about authentication. (This process is usually achieved by one, or more, of the following)
  + **Something you know**
  + **Something you have**
  + **Something you are**

## Attacking Passwords

* Shoulder Surfing
* Password Guessing
* Dictionary Attack
* Brute Force Attack
* Use a tool to find the VNC server’s password.
* Hydra
* Connect to the VNC server using a VNC client.
* Remmina

## Day6

Learning Objectives

* Learn what email analysis is and why it still matters.
* Learn the email header sections.
  + X-Mailer
  + X-Spam Status
  + X-Received
  + X-Headers
  + MIME-Version
  + Message-ID
  + SPF
  + …
* Learn the essential questions to ask in email analysis.
* Do the "From", "To", and "CC" fields contain valid addresses?
  + Having invalid addresses is a red flag.
* Are the "From" and "To" fields the same?
  + Having the same sender and recipient is a red flag.
* Are the "From" and "Return-Path" fields the same?
  + Having different values in these sections is a red flag.
* Was the email sent from the correct server?
  + Email should have come from the official mail servers of the sender.
* Does the "Message-ID" field exist, and is it valid?
  + Empty and malformed values are red flags.
* Do the hyperlinks redirect to suspicious/abnormal sites?
  + Suspicious links and redirections are red flags.
* Do the attachments consist of or contain malware?
  + Suspicious attachments are a red flag.
  + File hashes marked as suspicious/malicious by sandboxes are a red flag.

Tools

* emlAnalyzer
* VirusTotal
  + A service that provides a cloud-based detection toolset and sandbox environment.
* InQuest
  + A service provides network and file analysis by using threat analytics.
* IPinfo.io
  + A service that provides detailed information about an IP address by focusing on geolocation data and service provider.
* Talos Reputation
  + An IP reputation check service is provided by Cisco Talos.
* Urlscan.io
  + A service that analyses websites by simulating regular user behaviour.
* Browserling
  + A browser sandbox is used to test suspicious/malicious links.
* Wannabrowser
  + A browser sandbox is used to test suspicious/malicious links.

## Day7

Learning ObjectivesCyberchef logo

* What is CyberChef
* What are the capabilities of CyberChef
* How to leverage CyberChef to analyze a malicious document
* How to deobfuscate, filter and parse the data.
  + Add the File to CyberChef
  + Extract strings
  + Remove Pattern
  + Drop Bytes
  + Decode base64.
  + Decode UTF-16
  + Find and Remove Common Patterns
  + Find and Replace
  + Extract URLs
  + Split URLs with @
  + Defang URL

## Day8

Learning Objectives

* Explain what smart contracts are, how they relate to the blockchain, and why they are important.
* Understand how contracts are related, what they are built upon, and standard core functions.
* Understand and exploit a common smart contract vulnerability.

## Day9

Learning Objectives

* Using Metasploit modules and Meterpreter to compromise systems
* Network Pivoting
* Post exploitation
* view sessions
* upgrade the last opened session to Meterpreter
* interact with a session
* Background the currently interactive session, and go back to the Metasploit prompt
* Get information about the remote system, such as OS
* Upload a file or directory
* Display interfaces
* Resolve a set of host names on the target to IP addresses - useful for pivoting

## Day10

Learning Objectives

* Learn how data is stored in memory in games or other applications.
* Use simple tools to find and alter data in memory.
* Cetus
* Explore the effects of changing data in memory on a running game.

## Day11

Learning Objectives

* See what Operating System the memory dump is from
* See what processes were running at the time of capture
* See what connections were being made at the time of capture
* memory forensics
* Volatility
  + an open-source memory forensics

## Day12

Learning Objectives

* Learn the fundamentals of analyzing malware samples without relying on automated sandbox scanners.
  + Static analyzes.
  + Dynamic analyzes.
* Learn and understand typical malware behavior and its importance in the incident investigation pipeline.
  + **Network connections**
  + **Registry key modifications**
  + **File manipulations**

Tools:

* Detect It Easy
* CAPA
* Process Monitor Filter

## Day13

Learning Objectives

* Learn what traffic analysis is and why it still matters.
* Learn the fundamentals of traffic analysis.
* Which addresses are communicated?
* Is there any resource share event between addresses?
* If there is a file share event, which addresses hosts which files?
* Do the user-agent fields look unusual, suspicious or malformed?
* Learn the essential Wireshark features used in case investigation.
* HTTP GET requests
* Requested URIs
* HTTP requests host addresses
* Used user-agents
* Learn how to assess the patterns and identify anomalies on the network.
* Learn to use additional tools to identify malicious addresses and conduct further analysis.
* What are shared files?
* Does the hash reputation marked as suspicious or malicious?
* Which domain hosts the suspicious/malicious file?

## Day14

Learning Objectives

* Web Applications
* The Open Web Application Security Project (OWASP) Top 10
* IDOR

## Day15

Learning Objectives

* Input validation of file upload funtionality
* Unrestricted file upload vulnerabilities
* Phishing through file uploads
* metasploit create reverseshell for windows
* How to properly secure file upload functionality
* File Extension Validation
* File Renaming
* Malware Scanning

## Day16

Learning Objectives

* SQL Refresher
* Sending SQL Queries from PHP
* SQL Injection (SQLi)
* Fixing SQLi

## Day17

Learning Objectives

* Input Validation Foundations
* REGEX

## Day18

Learning Objectives

* Threat Detection
* Sigma Rule Syntax
* Windows events

## Day19

Learning Objectives

* How data is sent via electrical wires in low-level hardware
* Hardware communication protocols
* **USART**
* **SPI**
* **I2C**
* How to analyze hardware communication protocols
* Reading USART data from a logic capture

Tools:

* Saleae

## Day20

Learning Objectives

* What is firmware reverse engineering.
* Techniques for extracting code from the firmware
  + Static Analysis
  + Dynamic Analysis
* Extracting hidden keys from an encrypted firmware
* Modifying and rebuilding a firmware

Tools:

* Binwalk
* Qemu
* extract-firmware.sh

## Day21

Learning Objectives

* Explain the Internet of Things, why it is important, and if we should be concerned about their danger.
* Understand the difference between an IoT-specific protocol and other network service protocols.
* MQTT
* HTTP
* CoAP
* AMQP
* DDS
* Understand what a publish/subscribe model is and how it interacts with IoT devices.
* Broker
* Publish/Subscribe Model
* Analyze and exploit the behavior of a vulnerable IoT device.

Tools:

* Mosquito
* Rtsp

## Day22

Learning Objectives

* Understand what an attack vector is.
* Understand the concept of the attack surface.
* Some practical examples of attack surface reduction techniques

# Day23

* Core Mindset
* levels of defense
  + detection
  + prevention
  + logging
  + privileged access
  + network segmentation