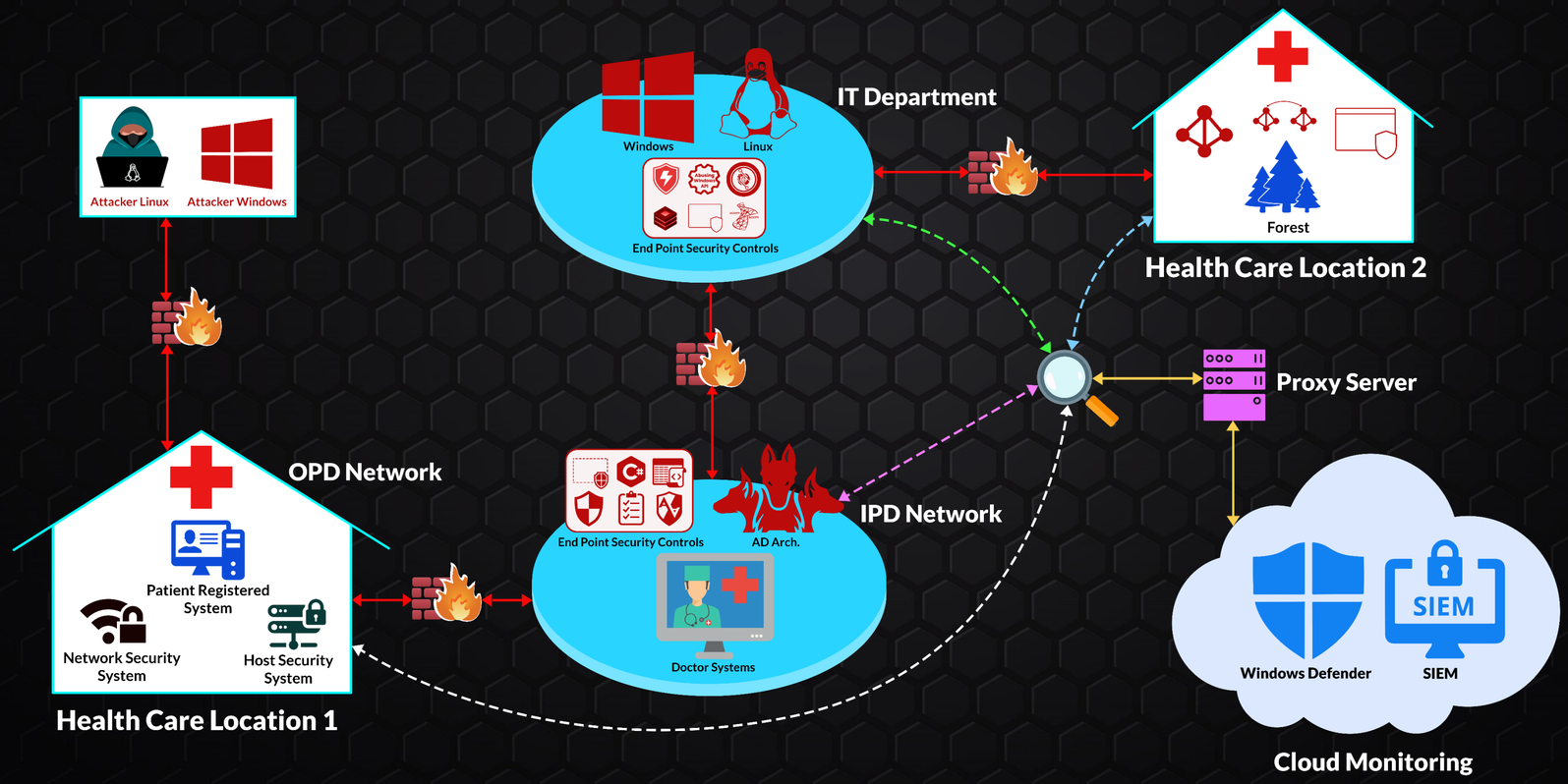
CWL
CyberWarFare Labs

Certified Enterprise Security Controls Attack Specialist [CESC-AS]

@CyberWarFare Labs

Certified Enterprise Security Controls Attack Specialist Architeture



CWL
CyberWarFare Labs

INTRODUCTION TO CERTIFIED ENTERPRISE SECURITY CONTROLS ATTACK SPECIALIST

CWL
CyberWarFare Labs

Module 1
Introduction to Security Controls & Solutions

1. Introduction to Security Controls & Solutions:
    - 1.1 Anti-Virus
    - 1.2 End-Point Detection and Response (EDR)
    - 1.3 AV vs EDR
    - 1.4 Microsoft Security Solutions
    - 1.4.1 Windows Resources & Defender Features
        - A. Windows Security Components :
            - A.1 Windows Defender (AMSI, CLM) & User Access Control (UAC)
            - A.2 Windows Defender Application Control (WDAC), AppLocker
            - A.3 Microsoft Defender Application Guard (formerly WDAG)
            - A.4 Windows Defender Exploit Guard (Attack Surface Reduction (ASR) Feature)
            - A.5 Windows Sandbox

1.4.2 Directory-Level Controls Setup

A. Just Enough Administration (JEA) & Just in Time Administration (JIT)

B. Privileged Access Workstations (PAW) & Privileged Access Management (PAM) Trust

C. Credential Guard / Remote Credential Guard

D. Local Administrator Password Solution (LAPS)

E. Resource Based Constrained Delegation (RBCD)

1.5 Linux Environment

1.5.1 Application Restriction

A. AppArmor

1.6 Playing with EDR

1.6.1 Attempt to Access Credentials (T1003.001) to incident discovery in Endpoint Portal

1.6.2 Attempt to Modify ATP Service to incident discovery in Endpoint Portal

1.6.3 Collecting artifacts using Live Response Session

1.6.4 Advanced Hunting

Module 2
Implementation of Security Controls and Solutions

2.1 Virtual Environment Setup and Configuration

2.2 Host-Level Controls Setup

- 2.2.1 Enabling End-Point Defences
  - A. Enabling AMSI, Script Block Logging and System-wide Transcript
- 2.2.2 Enabling Constrained Language Mode (CLM)
- 2.2.3 Windows Defender Exploit Guard (ASR Implementation)
- 2.2.4 Windows Defender Application Guard (WDAG)
- 2.2.5 Application Control for Windows
  - A. Windows Defender Application Control (WDAC)
  - B. Windows AppLocker
- 2.2.6 Setting-Up and Installing Windows Based Features
  - A. PowerShell Remoting & Web-Based PowerShell Remoting
  - B. Windows Subsystem for Linux (WSL & WSLv2)
  - C. Windows Credential Guard
  - D. Windows Sandbox

2.3 Network-Level Controls Setup

2.3.1 Just enough Administration (JEA)

2.3.2 Resource Based Constrained Delegation (RBCD)

2.3.3 Implementing LAPS

2.3.4 Implementing Privileged Access Management (PAM)

2.4 Implementing AppArmor

Module 3
Offensive C# Tradecraft

3.1 Introduction to C#

- Why Learn C# from a Red Team Perspective ?
- Common Language Runtime (CLR)
- Managed VS Un-Managed Code
- P/Invoke & D/Invoke
- Setting Up Environment

3.2 C# Basics [Labs]

3.2.1 Utilizing .NET class for stdin / stdout operations

3.2.2 Identifying the process architecture (32-bit or 64-bit)

3.2.3 Identifying the state of a process (Hard-Coded Process Name)

3.2.4 Identifying all Processes Status

3.2.5 Hidden command prompt

3.2.6 Domain Environment SID Enumeration 8

3.2.7 Utilizing Platform Invoke to call Unmanaged Function Calls

– Hello using P/Invoke

3.2.8 Create & Instantiate a class from a separate library

3.2.9 Calling our own .NET Assembly (Externally)

3.2.10 Hijacking AppDomain Manager

3.3 Offensive C# Trade-Craft [Labs]

3.3.1 Custom Meterpreter Magic

3.3.2 Invoking PowerShell without Powershell.exe Binary

3.3.3 Writing Custom Obfuscated C# Reverse Shell

3.3.4 Weaponizing AppDomain Manager

3.3.5 Case Study of an Initial Access TTP (Utilizing C# Trade Craft)

Module 4
Windows API

4.1 Introduction to API

4.2 Windows API Components

- 4.2.1 Process
- 4.2.2 Thread
- 4.2.3 Process Token
- 4.2.4 Handle
- 4.2.5 Windows Structure

4.2.6 API Calls

4.3 Utilizing Windows API for Red Team Profit [Labs]

- 4.3.1 Process Injection Basics
  - Listing DLLs loaded by a Process
  - Writing Data to a Process in Memory
  - DLL Injection

4.4 Alternative Code Execution Techniques [Labs]

4.4.1 Alternative Shellcode Execution Techniques

– Via EnumSystemGeoID() Function API

– Shell Back via CreateThreadPoolWait() Function API – AV Bypass

4.5 Process Injection Techniques [Labs]

4.5.1 Process Hollowing

– Create, Suspend & Resume a Process

– Reverse Shell via Process Hollowing

4.5.2 Process DoppleGanging

4.5.3 Process Herpaderping

– Reverse Shell via Process Herpaderping - AV Bypass

4.5.4 Process Ghosting

4.6 Bullet-Proof AV Evasion [Lab]

– Magic of a project file - AV Bypass

Module 5
Abusing / Evading Security Controls

5.1 Host-Level Security Controls

5.1.1 Host-Level & Network-Level Security Controls

A. Bypassing Host-Level Defences

A.1 Numerous ways of Bypassing / Disarming AMSI [Custom Ways]

A.2 Bypassing CLM

A.3 Evading Script Block Logging

B. Bypassing ASR Rules

B.1 Impede JavaScript and VBScript to launch executables

B.2 Block execution of potentially obfuscated scripts

B.3 Block Office Applications from Creating Child Process

B.4 Block Win32 API Calls from Office Macro

B.5 Block Process Creation Originating from WMI / PSEXEC

C. Bypassing Windows Application Whitelisting

C.1 Mis-Configured WDAC

C.2 Mis-Configured AppLocker

– Abusing LOLBINS

– Bypass Applocker in an Advanced Initial Access TTP

– Via installed 3rd Party Applications

– Via Alternate Data Streams (ADS)

CWL
CyberWarFare Labs

D. Abusing Windows Features (or bug?) :

D.1 PowerShell

D.2 Interesting Payload Deliver Techniques

- Via Windows Defender
- MS Paint as LOLBAS

D.3 Windows Subsystem for Linux (WSL & WSLv2)

D.4 UAC (You see me?)

– Custom File-less UAC Bypass (Macro) – AV, ASR Bypass

D.5 Weaponizing Windows Sandbox – AV Bypass

5.2 Network-Level Security Controls

5.2.1 Network Security Controls

A. Abusing Resource Based Constrained Delegation (RBCD)

– With & without adding computer account

B. Abusing Microsoft Monitoring & Patching Solutions :

– Leveraging SCCM

– Leveraging SCOM

C. Abusing Mis-Configured :

– Local Administration Password Solution (LAPS)

– Group Policy Objects (GPO)

D. Credential Access :

D.1 PowerShell PS-ReadLine Module

D.2 Credential Guard Bypass

- Via Custom SSP
- WDigest.dll Memory Patching

D.3 Interesting ways of LSASS Dumping

- Via comsvcs.dll
- Via WerFault.exe
- Custom C# LSASS Dumper

D.4 Kerberos with Linux

- SSSD, LDAP, DNS in Linux
- Discovery - Kerberos in Linux
- Various ways of credential extraction
- From Linux server to Domain Controller

D.5 Cross Forest Abuse Techniques

- Kerberoasting
- Cross-Forest ACL Abuse
- Foreign Security Principal (FSP) Abuse
- Trust Key
- Abusing PAM Trust

D.6 EDR Bypass

- Advanced Threat Protection (MS ATP Bypass)
- Techniques to identify EDR Bypass

CWL
CyberWarFare Labs

Thank You

Cyberwarfare.live