Advanced Windows Logic Bug Hunting

Yongil Lee

본 트레이닝은 **한국어**로 진행됩니다.
This training is taught in **Korean**.

INTRODUCTION

소개

Windows 논리 취약점(비-메모리코럽션) 특히 권한상승이나 샌드박스 이스케이프에 이용되는 논리 취약점이란 무엇이고 어떻게 찾을 수 있는지를 가르쳐드리는 트레이닝 코스입니다. 우선 Windows 보안 개념, 샌드박스 구현 방식, COM/RPC 내부 동작 이해 등 Windows 취약점을 이해하는데 필요한 필수 배경 지식을 상세히 설명할 예정이고 이 후 Windows 논리 취약점들이 가지는 공통적인 패턴들을 기존 취약점들 분석을 통해 알아볼 것입니다. 마지막으로 이러한 패턴을 이용해 새로운 Windows 취약점을 발견할 수 있음을 단계별 실습을 통해 보여드리겠습니다.

BIO

최근 사이버보안회사 *Diffense*를 설립하여 취약점 연구와 제품 개발에 집중하고 있습니다.
이전에는 대한민국 정보기관에서 수 년간 취약점 연구를 하였습니다.

연세대학교 컴퓨터과학과를 졸업하고, 최근에는 Windows EoP 취약점을 여럿 발견하여 벤더사에 제보하였습니다.

INTRODUCTION

Day1

* Widows Security Fundamentals
  * Security concepts의 오용으로 인한 EoP 취약점 케이스 분석
* Sandbox Implementation in Windows
  * Restricted Token, Job Object, Integrity Level 등을 이용한 샌드박스 구현 방법
  * 웹 브라우저의 샌드박스 구현 살펴보기
  * 브라우저 샌드박스 취약점 케이스 분석

Day2~3

* Understanding of Windows COM/RPC Internals
  * Writing COM/RPC Client and Server
  * Communicating with COM/RPC Endpoints
  * Enumerating COM/RPC Attack Surfaces
* 기존 취약점 케이스 분석하여 버그 패턴 식별
* 패턴 적용하여 새로운 윈도우즈 취약점 헌팅 실습

INTRODUCTION

기간
3일

수강대상

①취약점 리서처: Windows 권한상승 제로데이를 발견할 수 있는 능력을 갖추게 될 것이고,
②디펜더: 권한상승 취약점 분석 및 대응 능력을 갖추게 될 것입니다.

제공되는 것

- 트레이닝 슬라이드
- VM Image
- Scripts and code samples

PREREQUISITES

- Be Comfortable with C/C++ and Visual Studio
- Bring a laptop running any host OS
    - (Vm Image를 담을 수 있는 충분한 디스크 필요)
- Have Vmware installed