AWSF
: Windows Server 취약점 분석

팀 명 BoBs

팀 원 김동준, 김종성, 홍성흔

지도교수 손태식

2025-1 AJOU SOFTCON

개발동기 및 목적

전 세계적으로 Windows Server는 기업, 기관 등에서 광범위하게 사용되고 있다. 기업을 운영할 때 필요한 Windows Exchange Server, MSSQL Server 등이 모두 Windows Server에서 제공되기 때문이다. 이로 인해 기업을 노리는 해커들의 타겟이 되어왔고, 서버에서 취약점이 발생할 경우 전 세계 기업들에 큰 타격이 갈 수 있다. 특히 다양한 네트워크 서비스, COM, RPC 등의 통신 프로토콜이 존재하여 공격자가 노릴 수 있는 표면이 매우 넓다. BoBs 팀은 이러한 흐름 속에서 취약점 분석을 도와주는 도구를 개발하여 선제적으로 Windows Server에 존재하는 취약점을 발견하여 제보를 수행, Windows 보안 생태계에 기여하는 것을 목표로 시작하였다.

개발내용

개요

먼저 효과적으로 취약점을 찾기 위해 자동화된 도구 개발이 필요하였다. 기존에도 kAFL, WTF, Jackalope 등과 같은 다양한 자동화 취약점 탐지 도구가 연구되어 있었지만, 아래 표와 같은 기능의 한계가 있었다. 이 이유로 AWSF(Semi-Automatic Windows Server Fuzzing Framework)를 개발하여 Windows Server 취약점 분석에 활용하였다.

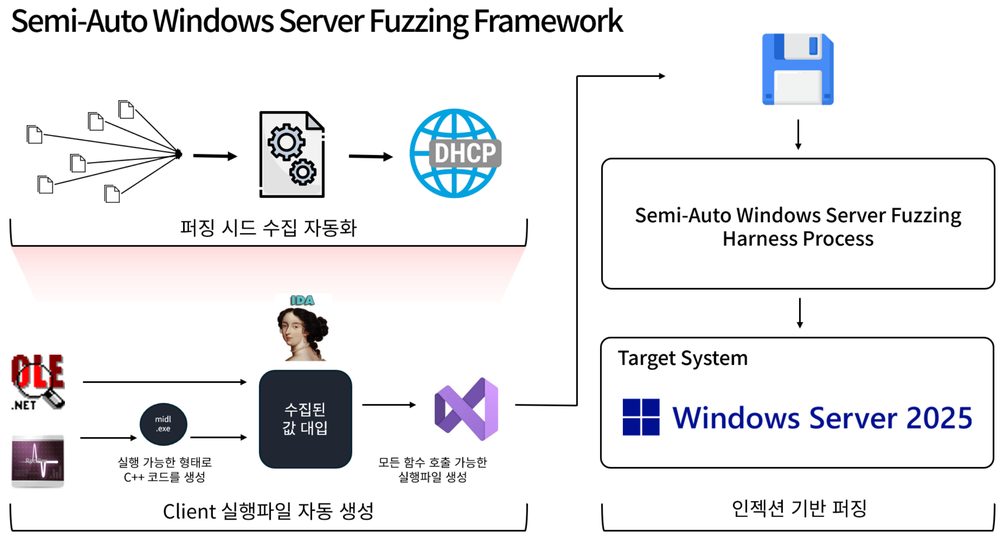
Feature \ Name	kAFL (USENIX Security)	what the fuzz	IRPT	Capstone Project
Fuzzing Remote Process	△	X	X	O
Automatic Fuzzing Seed Collection	X	X	O	O
Automatic Harness Generation	X	X	X	O

AWSF는 원격 프로세스에서 발생할 수 있는 취약점을 자동으로 탐지하고, 탐지에 필요한 초기 값 또한 자동으로 설정한다. 또한, 발견된 취약점을 재현할 수 있도록 스켈레톤 코드까지 생성해주는 기능을 포함하고 있다.

AWSF 프레임워크

1. 퍼징 시드 수집 자동화 : 더 효과적인 퍼징을 수행하기 위해 실제 프로세스에서 사용되는 값을 수집하여 입력 값으로 활용한다. 이 실제 값을 활용하여 퍼징을 수행하는 하네스의 실행 흐름을 안정적으로, 더 많은 코드를 실행할 수 있게 한다.
2. COM/RPC 기반 client code 자동화 : COM과 RPC를 통한 프로세스 호출을 위해 함수 원형(IDL)을 적절히 해석하여 취약점을 재현할 수 있도록 호출 가능한 C++ 코드와 이에 필요한 Client, Server, header stub을 자동으로 생성한다.
3. Server Service 대상 kAFL 퍼징 하네스 : VM기반의 기존 퍼저인 kAFL 개선하여, 실행되고 있는 원격 프로세스에서의 실행 상태를 파악하기 위해 해당 프로세스에 인젝션을 하여 퍼징을 수행하는 새로운 하네스를 제시한다.

주요기술



AWSF Core Architecture

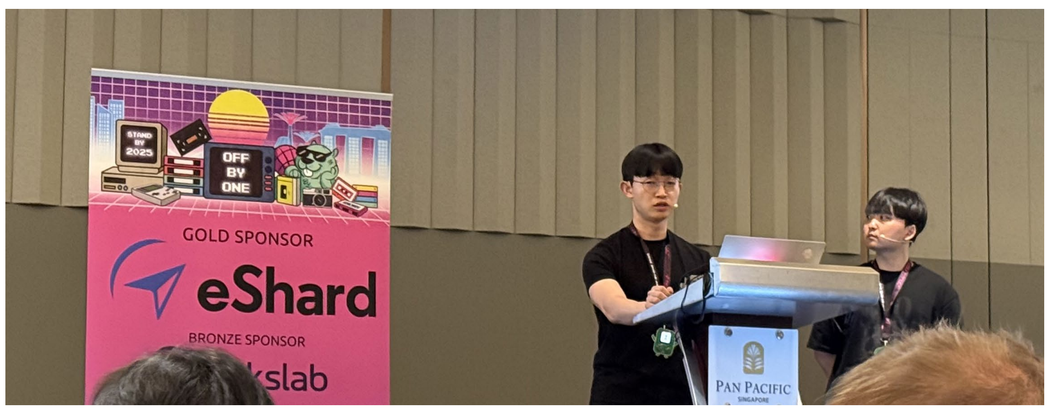
주요 기술적 구현 사항은 위 그림과 같다.

결과 및 분석

AWSF를 적극적으로 활용하여 Windows Server 환경에서 취약점 분석을 수행하였고, 총 8건의 심각한 권한 상승 취약점을 발견하였다. 모든 취약점은 Microsoft에 제보하였으며, 이 중 6건은 모든 심사가 완료, 2건은 금액 평가 단계에 있다. 최종적으로 학기 종료 전까지 총 65,000$ 상당의 버그 바운티를 받을 예정이다.

자체적인 분석 방법론과 도구 개발 경험을 바탕으로 싱가포르에서 진행되는 'Off-by-One 2025' 해외 해킹 컨퍼런스에 제출하였고, 발표자로 선정되어 직접 발표하는 성과도 이루었다. 이를 통해 본 프로젝트가 학문적, 기술적으로도 충분한 인정과 주목을 받았음을 확인할 수 있다.

Target	Vulnerability	Bounty
* NDA *	* 취약점 종류 1 *	30,000$
* NDA *	* 취약점 종류 2 *	5,000$
* NDA *	* 취약점 종류 2 *	5,000$
* NDA *	* 취약점 종류 2 *	5,000$
* NDA *	* 취약점 종류 2 *	5,000$
* NDA *	* 취약점 종류 2 *	5,000$
* NDA *	* 취약점 종류 3 *	5,000$
* NDA *	* 취약점 종류 4 *	5,000$



활용방안 및 기대효과

AWSF는 Windows Server에 대한 연구 공백을 보완하며, Server 환경에서 취약점을 탐지하고 분석하는 데 실질적인 도움을 줄 수 있는 기능을 갖추고 있다.

또한, Microsoft에 제보한 취약점에 대한 보상까지 확정된 성과는 기술의 유효성과 실전 적용 가능성을 입증하는 사례로, 향후 Windows 기반 보안 연구의 기반 도구로 활용될 수 있음을 보여준다.