2022년 중부대학교 정보보호학과 졸업 작품 전시회

침투 테스팅 시뮬레이션 개발

Breach Attack Simulation Development

*김진수, 김대원, 오원재, 여수한, 양환석

중부대학교 정보보호학과, 중부대학교 정보보호학과 교수

목차

01. 서론

02. 이론적 배경

03. 시스템 요약

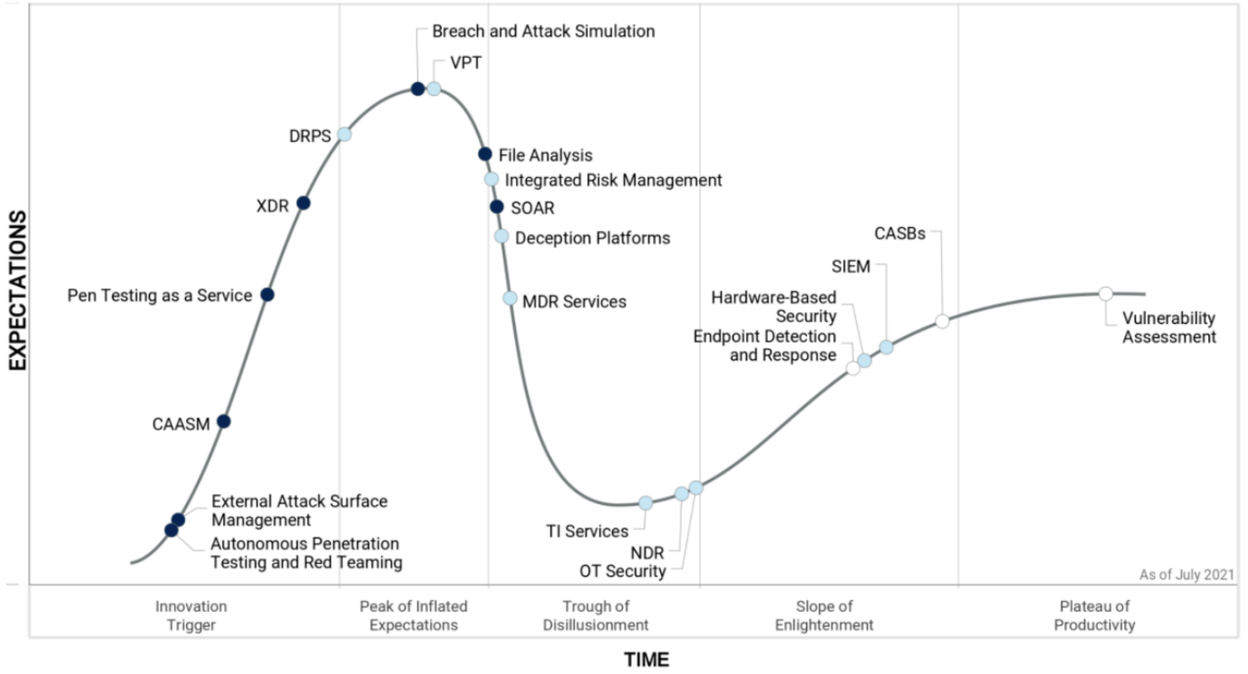
04. 시스템 상세

05. 시연

06. 결론 및 성과

07. Q&A

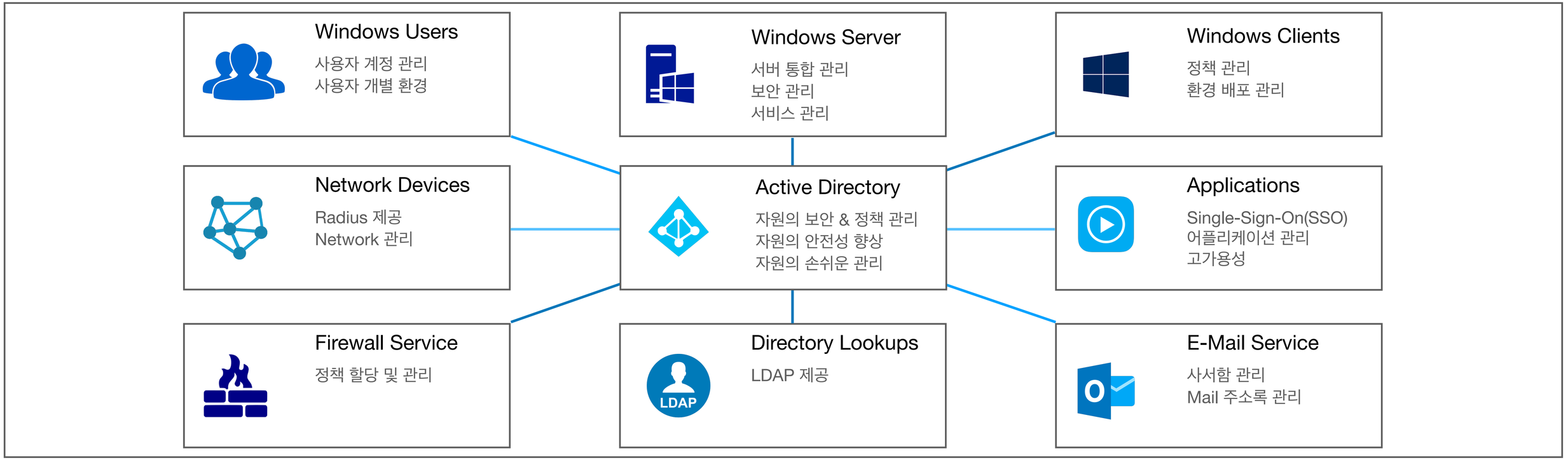
01. 서론



- 사이버 보안 위협이 심각한 수준으로 확산되며 BAS에 대한 관심으로 인해 성장세가 매우 빠르다
- Active Directory에 대한 공격이 증가하지만 Blue Team 활동에만 초점이 맞추어진 기업의 보안팀
- Active Directory 환경에서 MITRE ATT&CK 단계별 완전히 자동화되어 작동하는 BAS를 개발했음

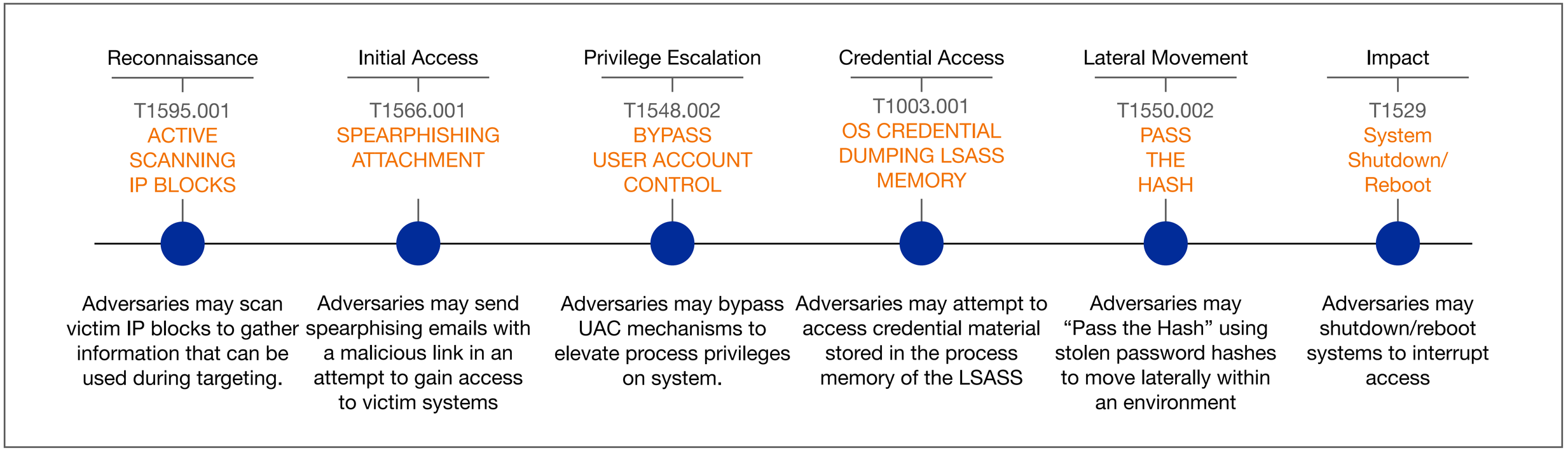
02. 이론적 배경(1/2)

- **ACTIVE DIRECTORY**
  - Mircosoft社 의 Windows Server에서 제공하는 Directory Service이다.
  - 디렉토리 내 관리자가 네트워크 자원의 접근과 권한을 관리할 수 있도록 한 서비스다.



02. 이론적 배경(2/2)

- **MITRE ATT&CK FRAMEWORK**
  - MITRE社 에서 제공하는 프레임워크
  - 실제 사이버 공격을 기반으로 공격을 14단계로 상세하게 나눈 프레임워크



03. 시스템 요약

Attackme .exe

Main module

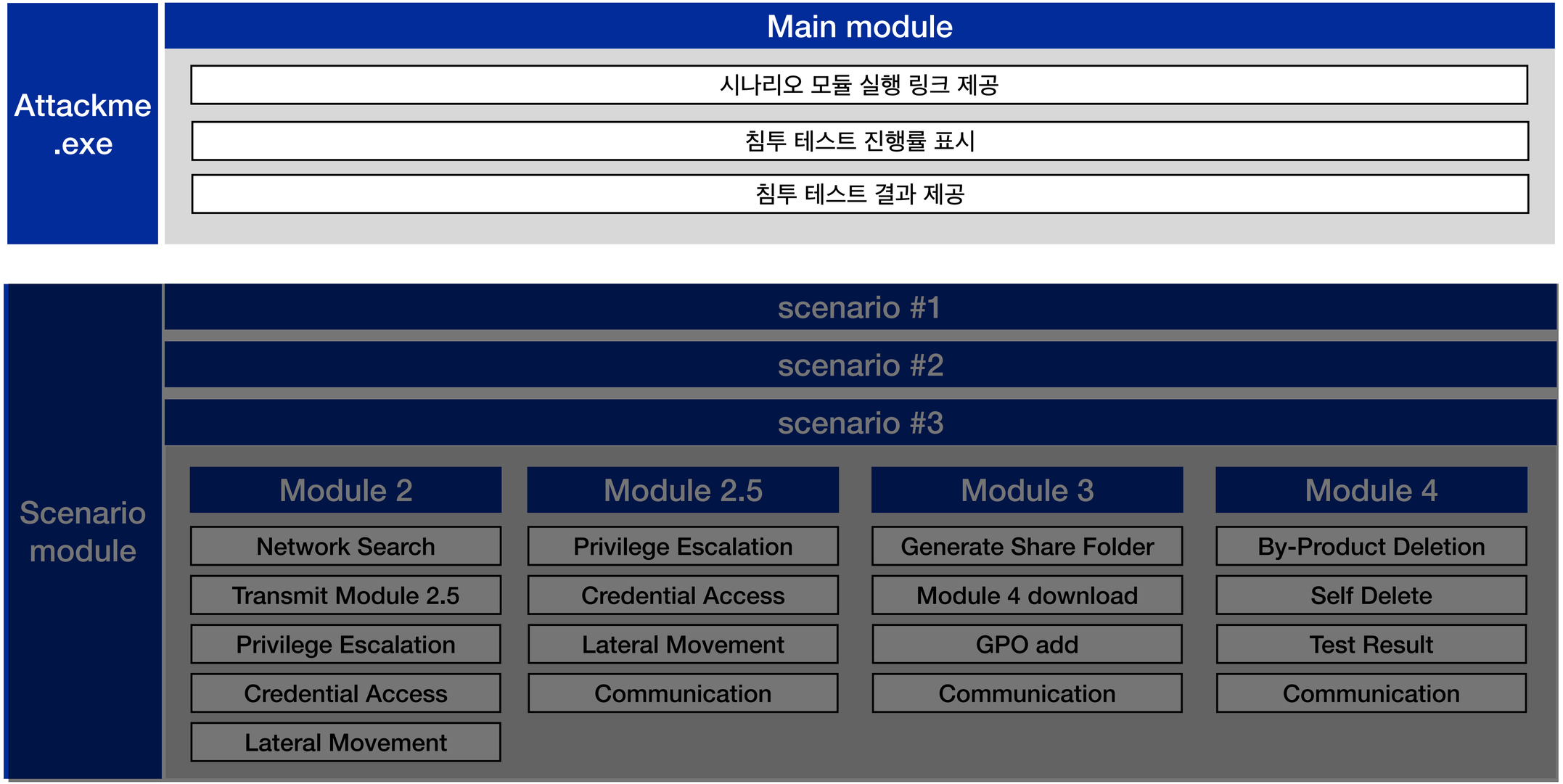
- 시나리오 모듈 실행 링크 제공
- 침투 테스트 진행률 표시
- 침투 테스트 결과 제공

Scenario module

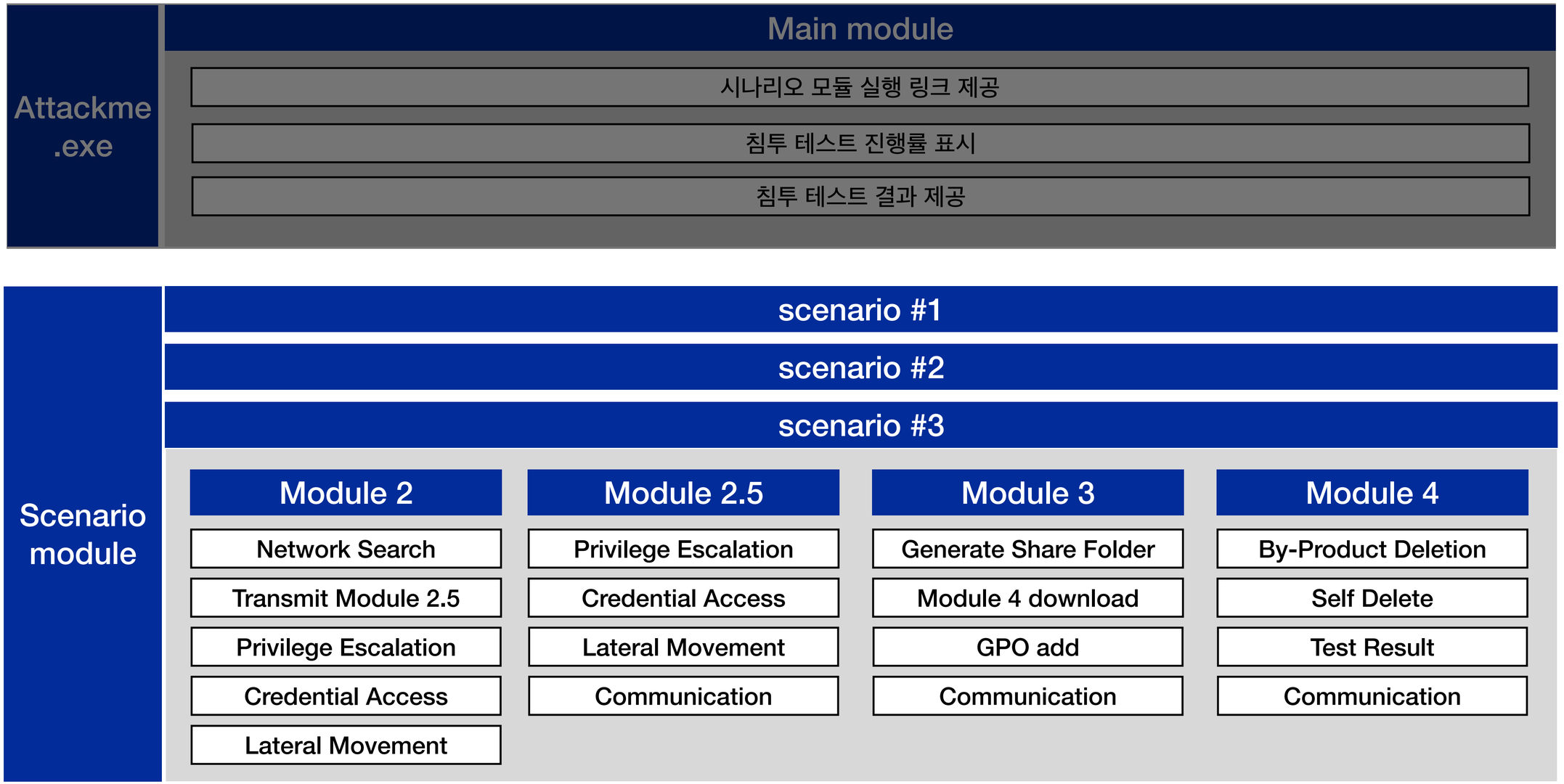
- scenario #1
- scenario #2
- scenario #3

Module 2	Module 2.5	Module 3	Module 4
Network Search	Privilege Escalation	Generate Share Folder	By-Product Deletion
Transmit Module 2.5	Credential Access	Module 4 download	Self Delete
Privilege Escalation	Lateral Movement	GPO add	Test Result
Credential Access	Communication	Communication	Communication
Lateral Movement			

03. 시스템 요약

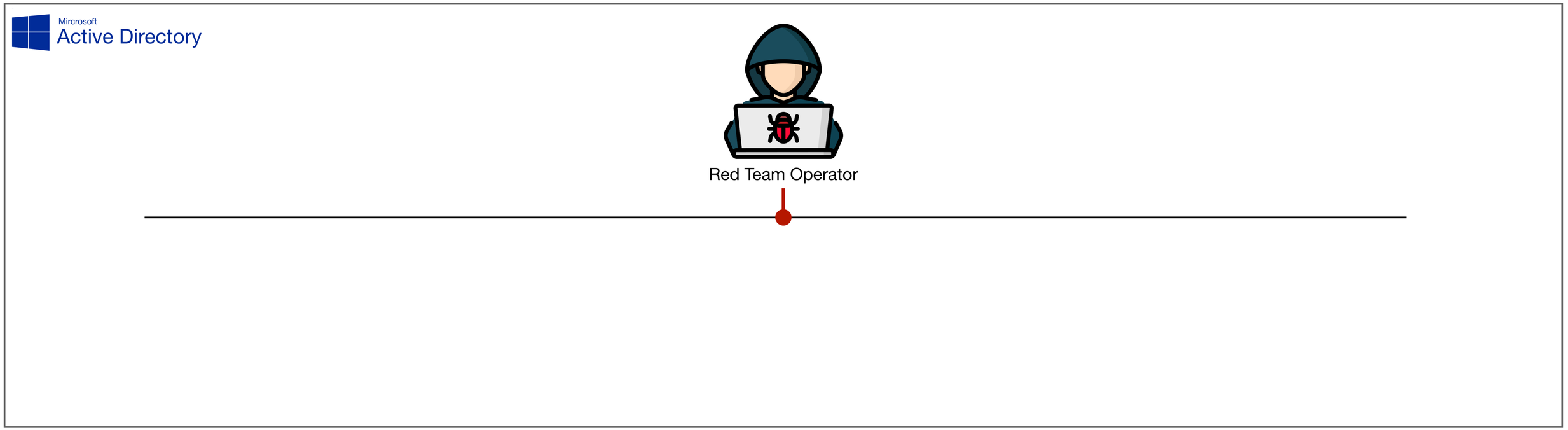


03. 시스템 요약



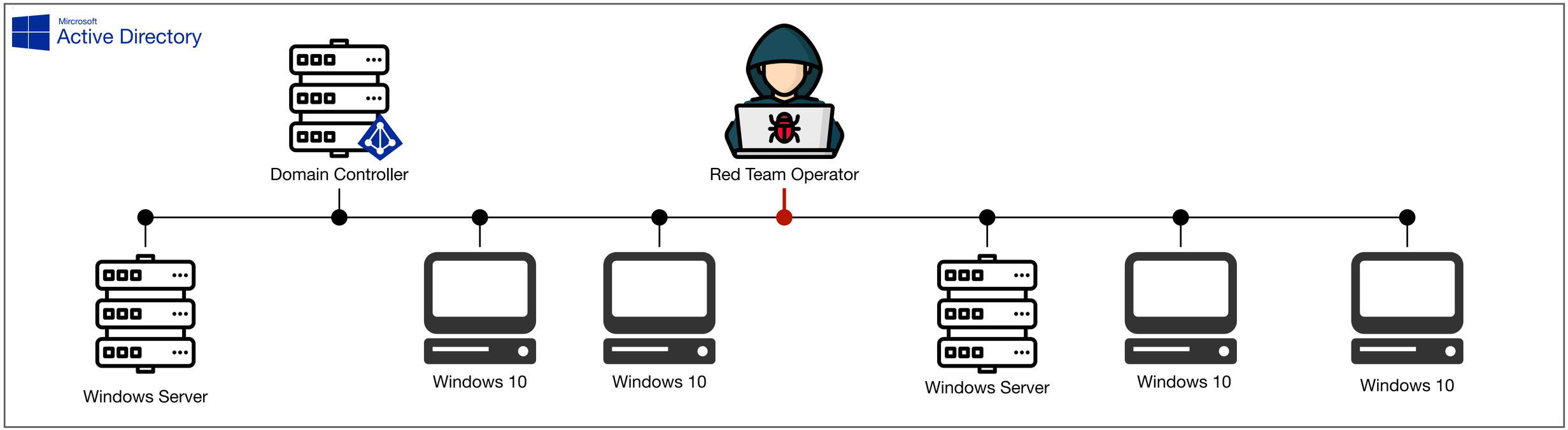
04. 시스템 상세(1/6)

- **Module 1**
  - 레드팀 오퍼레이터가 테스트 하고자 하는 네트워크에 연결합니다.
  - 사용자는 침투 테스트의 시작점을 선택합니다.
  - 선택한 시작점에서 Module 2가 실행되고, 네트워크에 대한 스캔을 시작합니다.



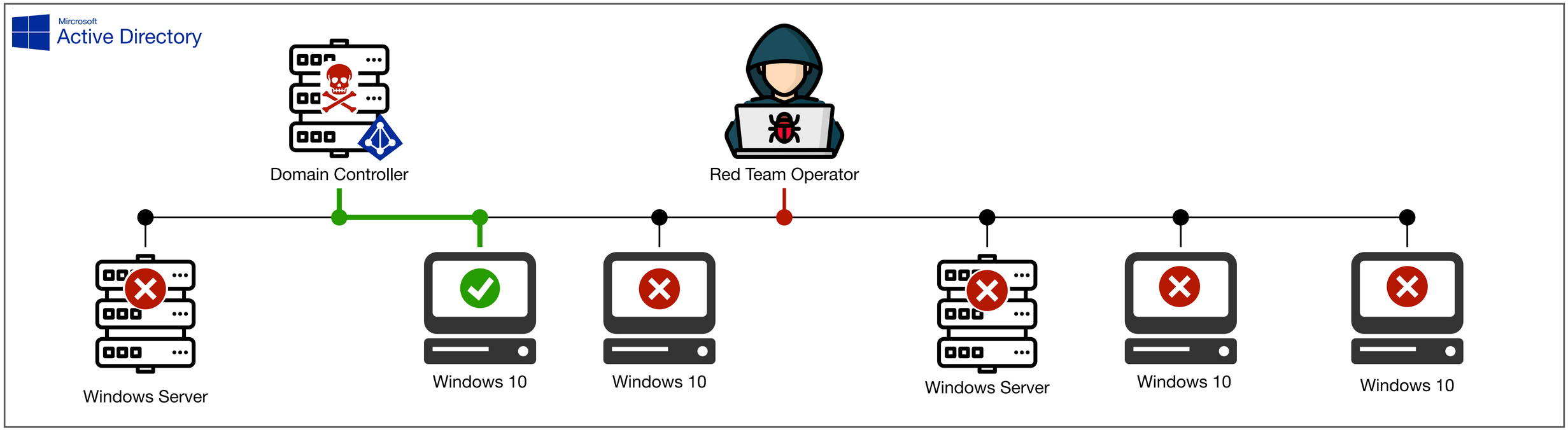
04. 시스템 상세(2/6)

- **Module 2**
  - 네트워크 스캔을 통해 얻은 도메인 노드에 Module 2.5를 Injection & Execute 합니다.
  - 공격 도구를 이용하기 위해 로컬 권한 상승을 합니다.
  - Mimikatz 등의 도구를 이용해 Domain Admin 수준의 Credential을 탐색합니다.



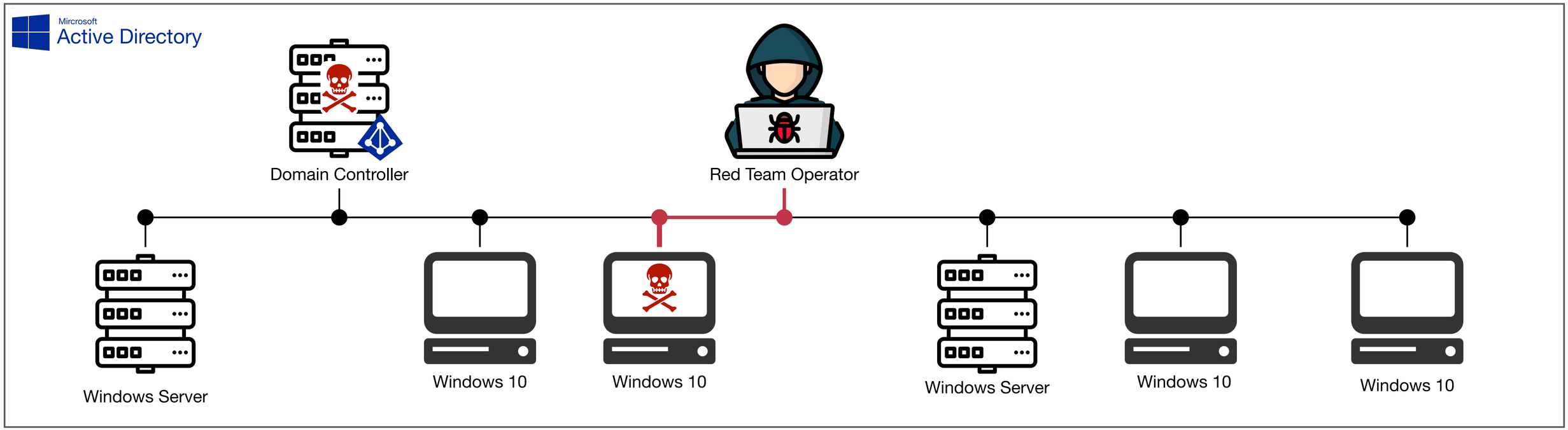
04. 시스템 상세(3/6)

- **Module 2.5**
  - 공격 도구를 이용하기 위해 로컬 권한 상승을 합니다.
  - Mimikatz 등의 도구를 이용해 Domain Admin 수준의 Credential을 탐색합니다.
  - 탈취한 Credential을 이용해 Domain Controller에 접근하여 Module 3를 다운로드 및 실행합니다.



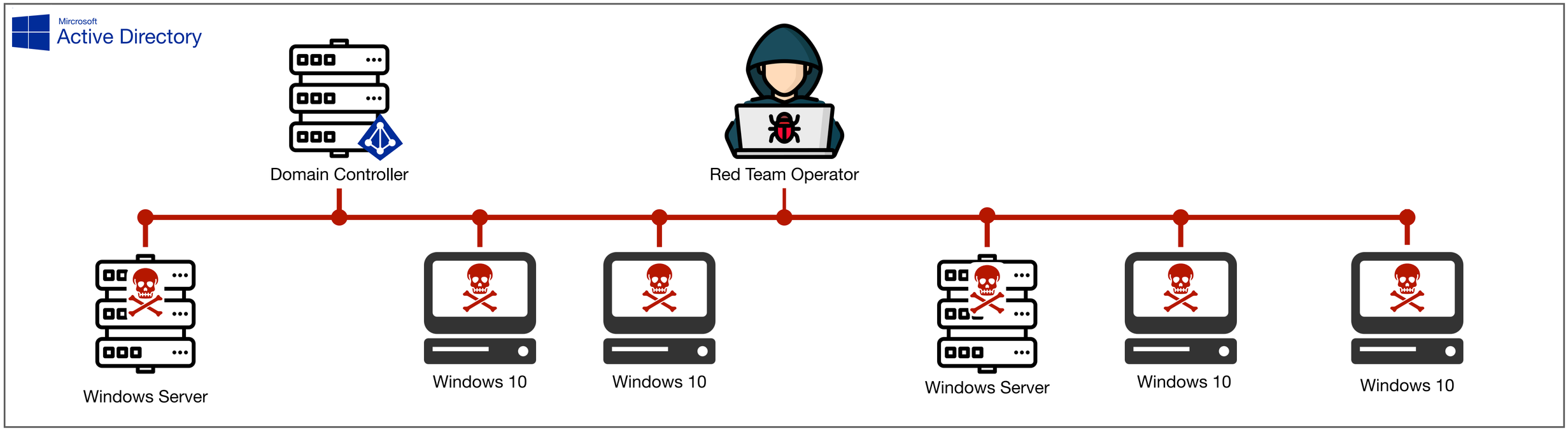
04. 시스템 상세(4/6)

- **Module 3**
  - 도메인 내에서 사용할 수 있는 권한의 공유 폴더를 생성합니다.
  - 그룹 정책을 통해 AD Site에서 실행될 Module 4를 공유 폴더에 다운로드 합니다.
  - 그룹 정책 생성을 통해 도메인 내 모든 노드가 Module 4를 실행하도록 정책 설정합니다.



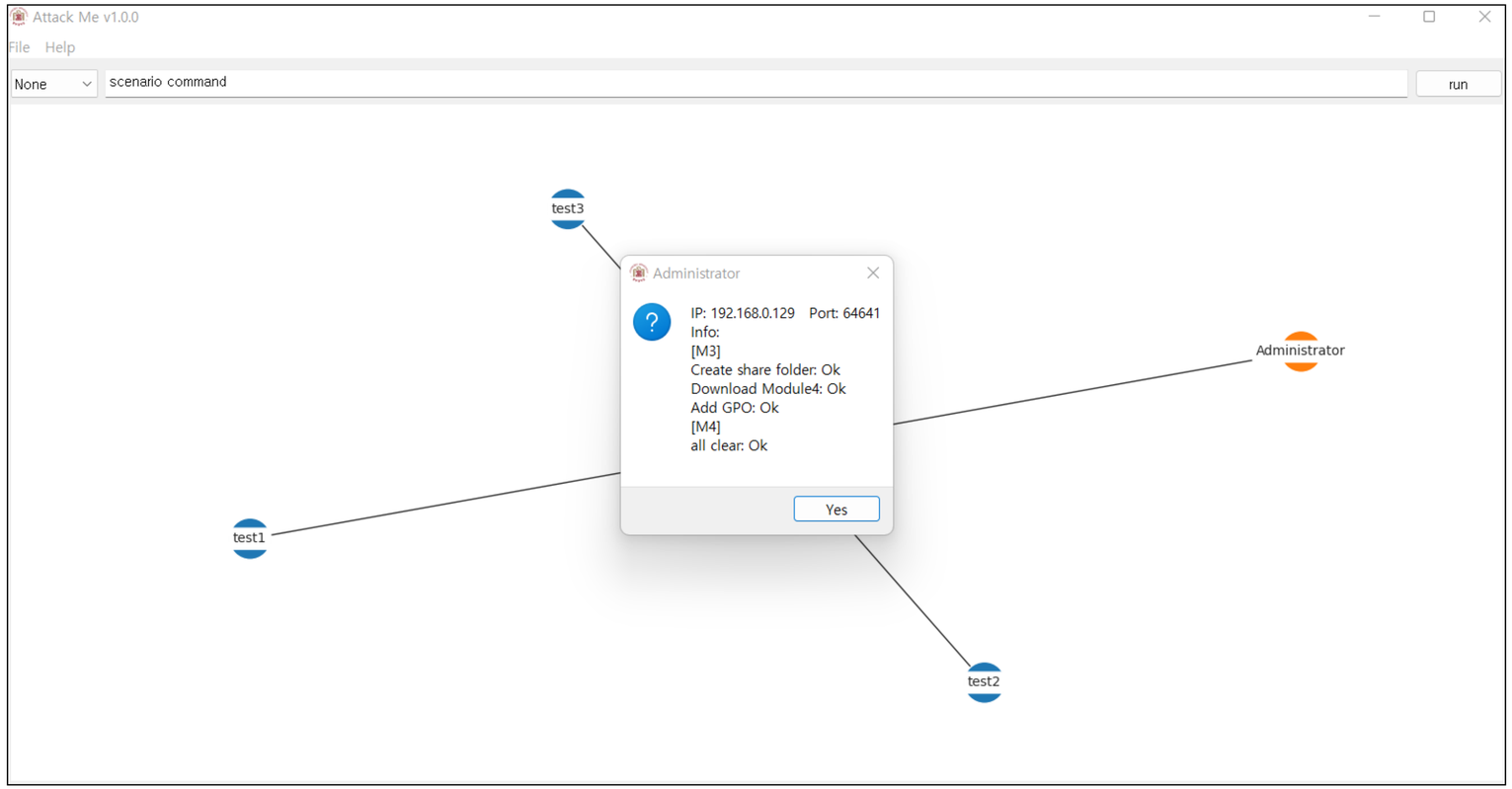
04. 시스템 상세(5/6)

- **Module 4**
  - Module4의 실행은 곧 테스트 종료를 뜻합니다.
  - 모듈 2,3 행위 중 나온 모든 부산물을 삭제하고 마지막으로 자가 삭제까지 합니다.
  - 실행 직후, 자가 삭제 직전 모듈 1과 모든 상황을 공유합니다.

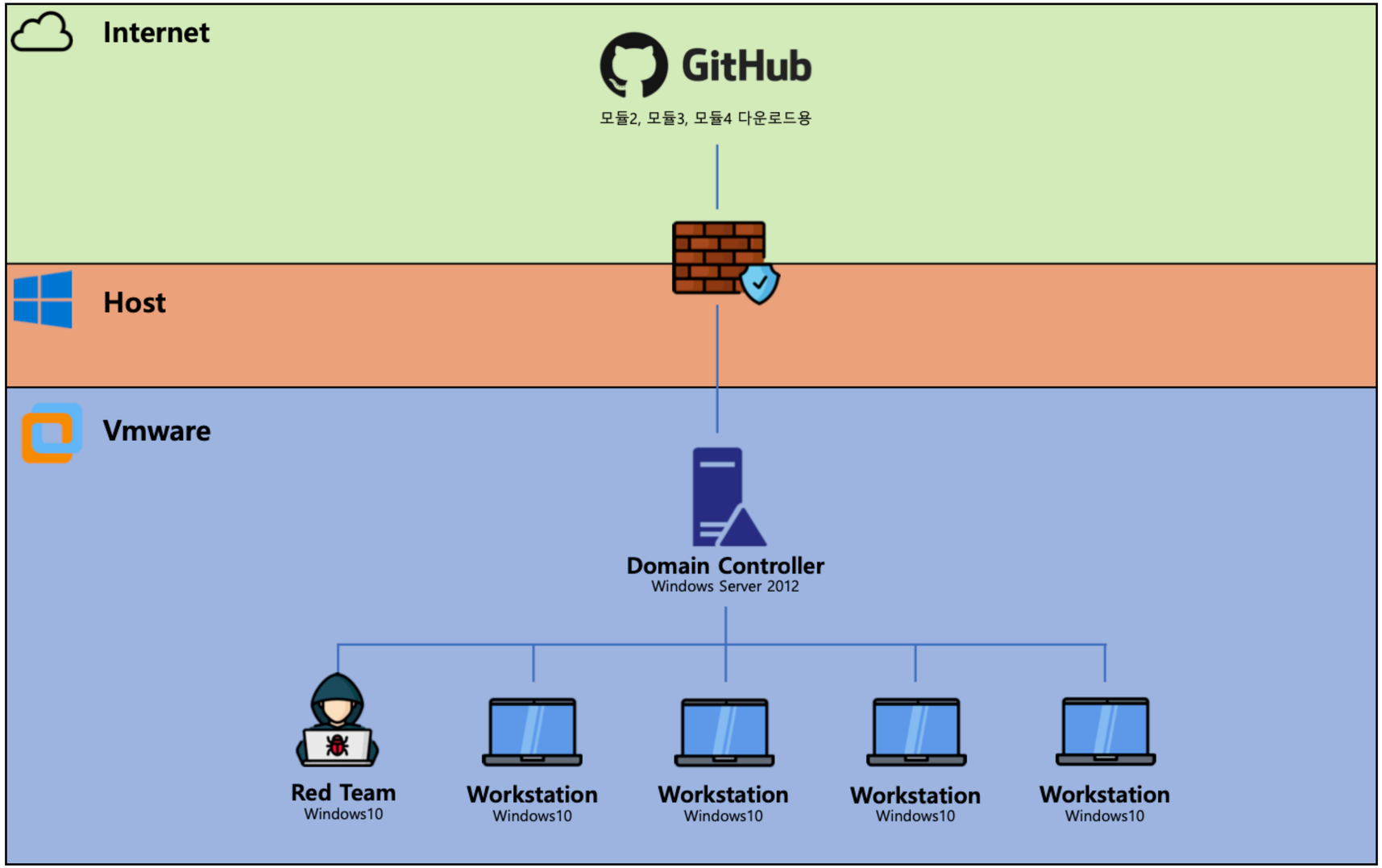


04. 시스템 상세(6/6)

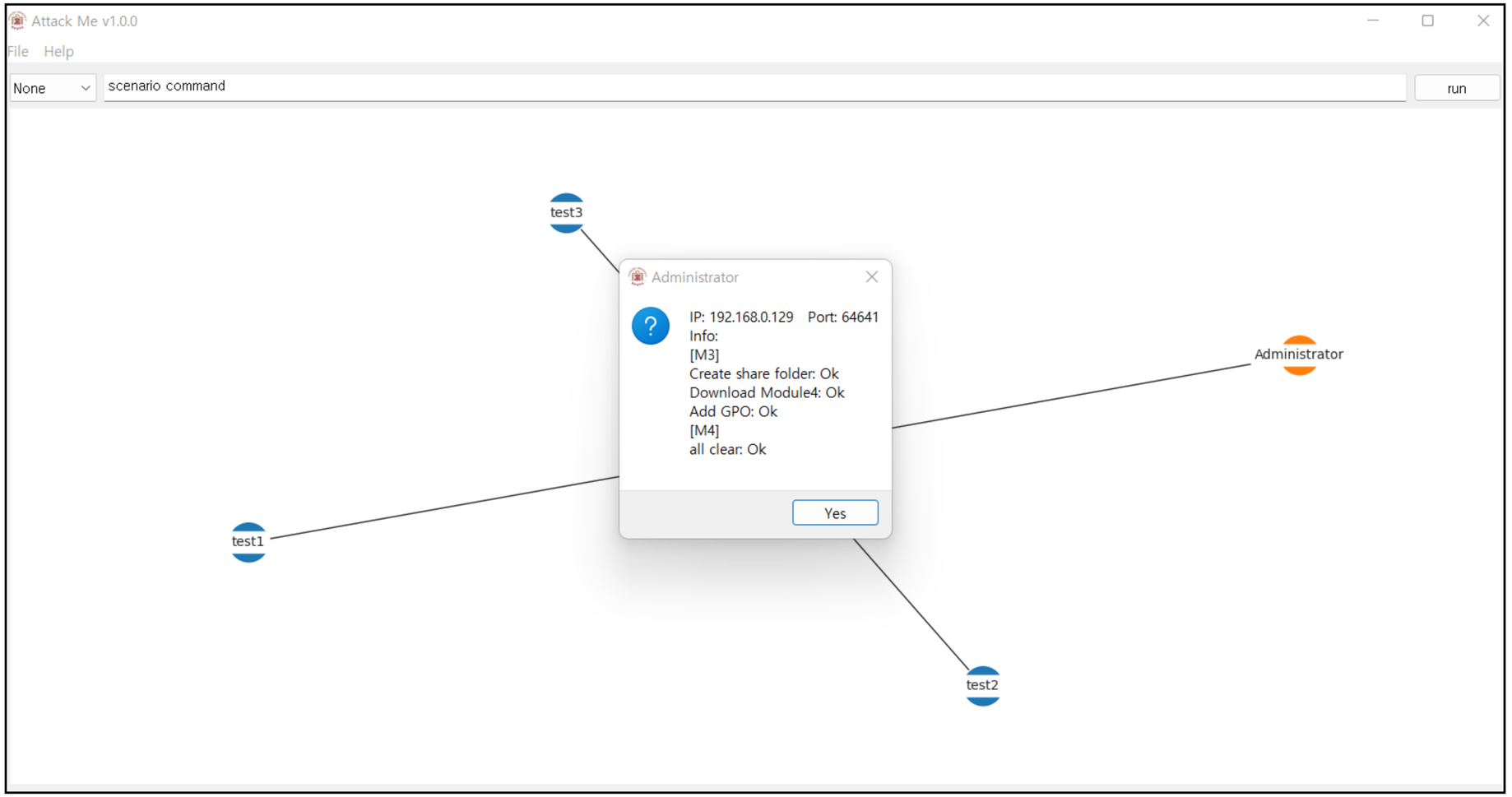
- **Module 1**
  - 획득하는 정보 종류 아래와 같습니다.



05. 시연(1/2)



05. 시연(2/2)



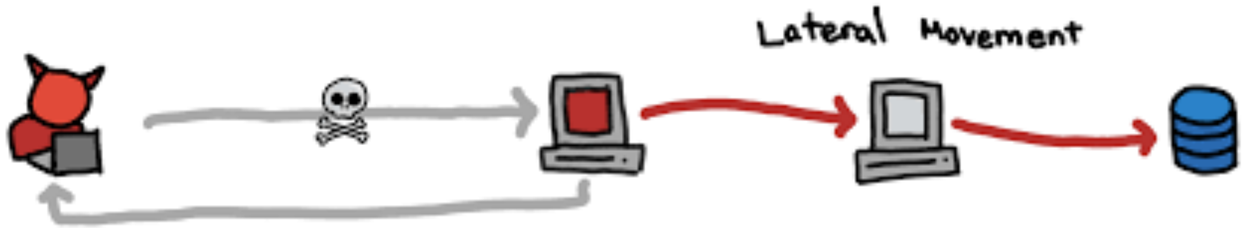
06. 결론 및 향후 계획(1/2)

- **결론**
  - Active Directory 환경을 대상으로 침투 테스팅하는 BAS 프로그램을 개발했다.
  - APT 공격 시나리오를 MITRE ATT&CK 단계로 분류하고 해당 공격을 완전히 자동화했다.
  - 운용자가 침투 테스트 진행사항과 결과를 시각적으로 확인할 수 있다.

- **기대효과**
  - 보안 정책의 취약점을 확인하거나 보안 솔루션 등에 탐지 되는지를 확인할 수 있다.
  - Blue Team 위주인 기업 보안 팀의 Red Team 활동을 장려할 수 있다.

06. 결론 및 향후 계획(2/2)

- **다양한 시나리오 추가**
  - APT 기반의 공격 시나리오 추가 뿐만 아니라 WAF 등 네트워크 솔루션에 대한 시나리오도 추가 예정.
- **분석 보고서 및 보완 대책 제공**
  - 결과에 대한 분석 보고서, 취약점에 대한 보안대책 등의 편의 기능을 추가로 제공할 예정.



Q&A

감사합니다.