APT 시나리오 분석 문제

Target : <https://blog.naver.com/sk_shieldus/222704110870>

1. 각 스텝별로 MITRE ATT&CK Matrix 의 어느 분류에 속하는지 정의하시오

( 분류 : Reconnaissance / Resource Development / Initial Access / Execution / Persistence / Privilege Escalation / Defense Evasion / Credential Access / Discovery / Lateral Movement Collection / Command and Control / Exfiltration / Impact )

1. 2022년 북한 해킹조직 김수키는 FTP관련 1-day 취약점을 사용하였다. 해당 취약점의 CVE 번호와 대상 소프트웨어의 이름을 서술하시오

(2-1) 이미 패치 버전이 배포된 소프트웨어의 취약점을 이용한 공격임에도 파급력이 존재하는 이유와 해결 방안을 서술하시오