뭉치서버 Brute Force 분석 결과

□ 개요

○ 2025. 05. 29. (목)에 신원 미상의 해커가 쇼핑몰 서버(뭉치 시스템)를 대상으로 사이버 공격을 시도, 사용자 정보가 유출되는 사고 발생하여 분석하였음.

□ 피해서버 정보

○ 서버정보

구분	시스템명	IP	호스트명	OS	OS 설치일
내용	뭉치 시스템	192.168.0.39	attack	Ubuntu 20.04	2025.04.28

○운영중인 서버계정:Administrator, attack 등 5개 계정

```
drwxr-xr-x  2 root   root   4096 2025-05-28 23:53 Administrator
drwxr-xr-x 23 attack attack 4096 2025-05-28 21:22 attack
drwxr-xr-x  2 root   root   4096 2025-05-28 23:54 Guest
drwxr-xr-x  2 root   root   4096 2025-05-28 23:53 public
drwxr-xr-x  2 root   root   4096 2025-05-28 23:53 Supervisor
```

□ 공격자 정보

구분	IP	국가	최초공격일시	공격성공일시
내용	192.168.0.133	대한민국	2025.05.29. 오후 11:47	2025.05.29. 오후 11:47

□ 사고경위

○ 2025.05.29(목).11:47 대한민국 국적 IP에서 attack 서버로 공격 시도가 발생함

○ 2025.05.29.(목).11:47 Brute-Force를 이용한 로그인 시도가 다수 확인됨

○ 2025.05.29.(목).11:47 공격 시도에 동일한 User-Agent 값이 지속으로 확인됨

○ 2025.05.29.(목).11:47 Password 리스트 기반 반복 로그인 시도가 탐지됨

○ 2025.05.29.(목).11:47 7여 개 계정이 비정상 로그인 성공 처리 확인됨

○ 2025.05.29.(목).11:47 attack 서버에 admin 및 로그인 가능한 계정의 ID, Password가 탈취됨

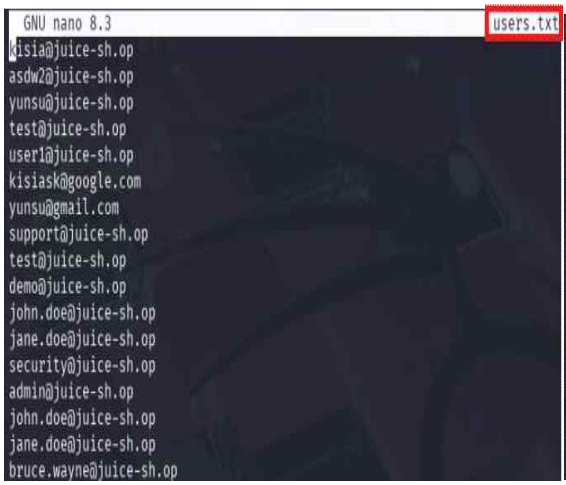
○ 2025.05.29.(목).11:47 attack 서버에 Brute Force로 다수의 유저 정보가 탈취됨

□ 공격내용

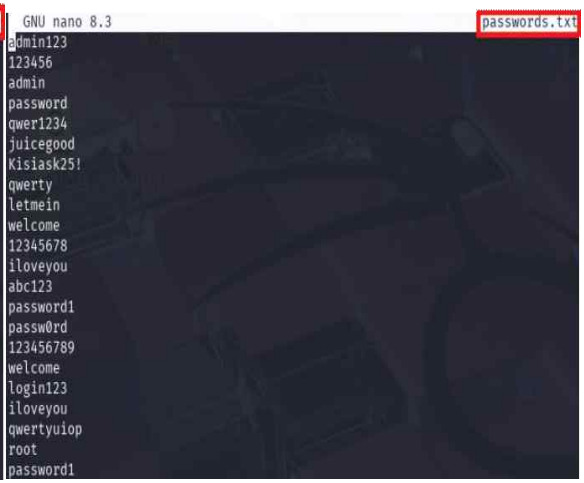
○ Splunk에서 특정 IP(192.168.0.133)로부터 192.168.0.39 서버로 245건의 연속 로그인 실패가 탐지되어 Brute-Force 공격이 의심됨

※ Splunk 모니터링을 통해 홈페이지 로그인 시도가 과다하다는 것을 확인한 후, Brute-Force 공격 도구를 자체 제작하여 테스트를 수행함.

○ users.txt, passwords.txt 임의로 작성하여 Brute-Force 실행함

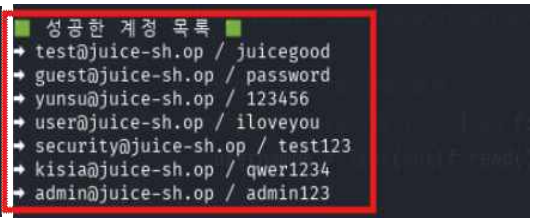


※ python코드 users.txt



※ python코드 passwords.txt

※ Brute-force공격 실행 구문임



※ 공격 실행 후 성공 계정 목록임

○ 로그인 실패 시 서버 응답에 "Invalid email or password"가 포함되며, 이를 기준으로 Brute-Force 공격 성공 여부를 판단함.

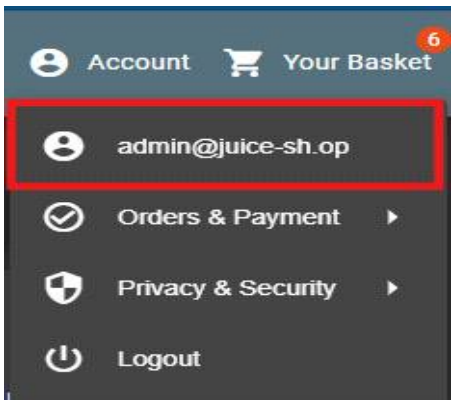
※ 로그인 실패 시, 화면과 개발자 도구(Network > Preview) 응답에서 “Invalid email or password” 메시지를 통해 실패 여부를 확인할 수 있음

※ 로그인 성공한 화면으로 성공 시 응답에 포함된 token 값을 획득함.

○ 응답 결과에 토큰(token)을 획득하면, 해당 계정의 로그인 성공 및 계정 탈취로 판단됨

※ 성공한 계정으로 로그인 후 token값 획득한 화면임

○ 공격 목적은 관리자 포함 사용자 인증 정보 탈취 및 로그인 성공임



※ 성공한 계정 중 관리자 계정으로 로그인 성공한 모습임

○ 공격 발생지 IP 192.168.0.133로 확인됨

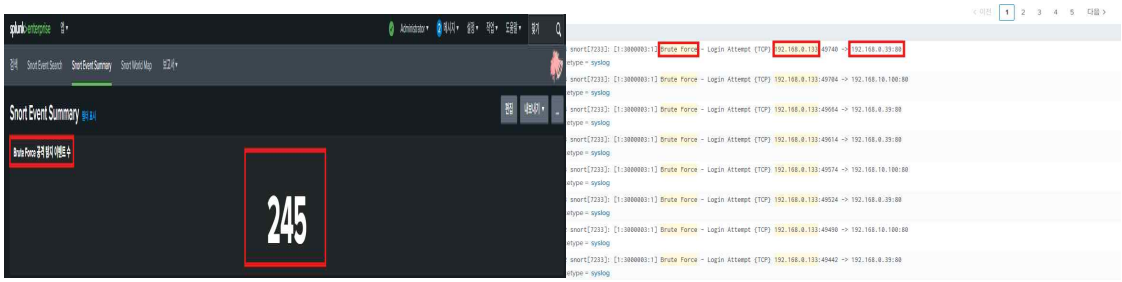
□ 피해내용

○ 2025.05.29.(목) 11:47 ~ 11:48경 Brute-Force 공격이 발생함

○ 총 7건(관리자 1건, 일반 사용자 6건) 계정 정보 탈취됨

○ 로그인 성공 후 인증 토큰 발급되어 서비스 접근 가능 상태로 확인됨

○ /rest/user/login API 대상 자동화 로그인 시도 245건 이상 탐지됨



○ 공격 IP : 내부 테스트망 (192.168.0.133)으로 확인됨

○ 탈취된 정보는 이메일(ID), 패스워드 조합으로 확인됨

□ 보안대책

○ 비밀번호는 9자리 이상으로 숫자, 영문 대소문자, 특수문자를 포함하도록 정책을 강화함
○ 일정 횟수 로그인 실패 시 일정 시간 계정 잠금 처리 정책 적용함
○ 자동화된 공격 방지를 위해 CAPTCHA 기능 도입함
○ 비정상 로그인 패턴 및 과도한 요청 탐지를 위한 WAF 정책 강화함
○ 인증 응답 메시지는 실패 원인을 노출하지 않도록 일반적인 오류 오류 메시지로 통일함
○ 관리자 계정 등 주요 계정에 대해 2차 인증(MFA) 적용함
○ 관리자 계정 로그인은 허용된 IP 대역에서만 접속 가능하도록 제한함
○ 정보시스템 취약점 점검을 정기적으로 수행함