REPORT

SW보안개론

(3번과제: [Metasploit을 활용한 Pen Testing)



**과목명 :SW보안개론**

**분반 : 1분반**

**교수명 :조성제**

**학 과 : 소프트웨어학과**

**학 번 : 32162566**

**이 름 : 안찬웅**

**2022년 6월 3일**

EMB0000356c3453

<목 차>

I. 과제 진행 과정을 순차적으로 보고서에 작성

A. exploit 명령과 ‘id’명령어 수행 후 자신의 학번과 함께 root권한 획득 내용 캡쳐 3

B. NIST Four-Stage Penetration Testing Methodology 각 단계에 맞게 보고서를 작성 4

C. 해당 pentesting을 통해 Target System에서 발생한 공격을 방어 및 완화 기법 논의 11

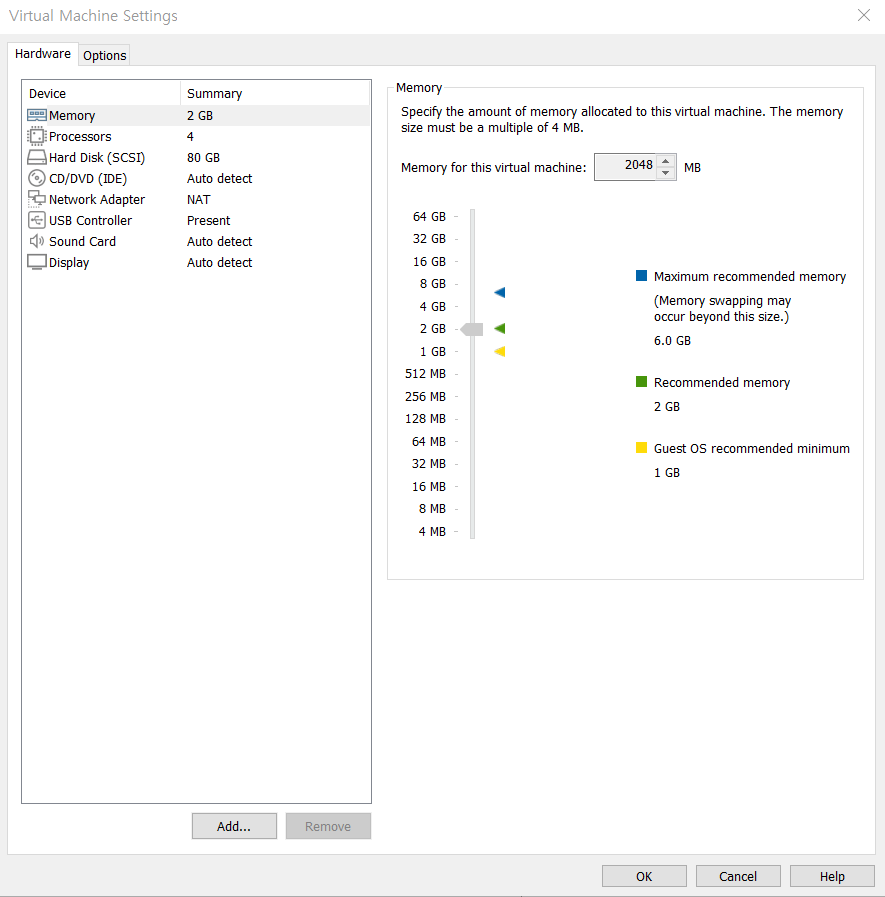
**A**.

텍스트이(가) 표시된 사진

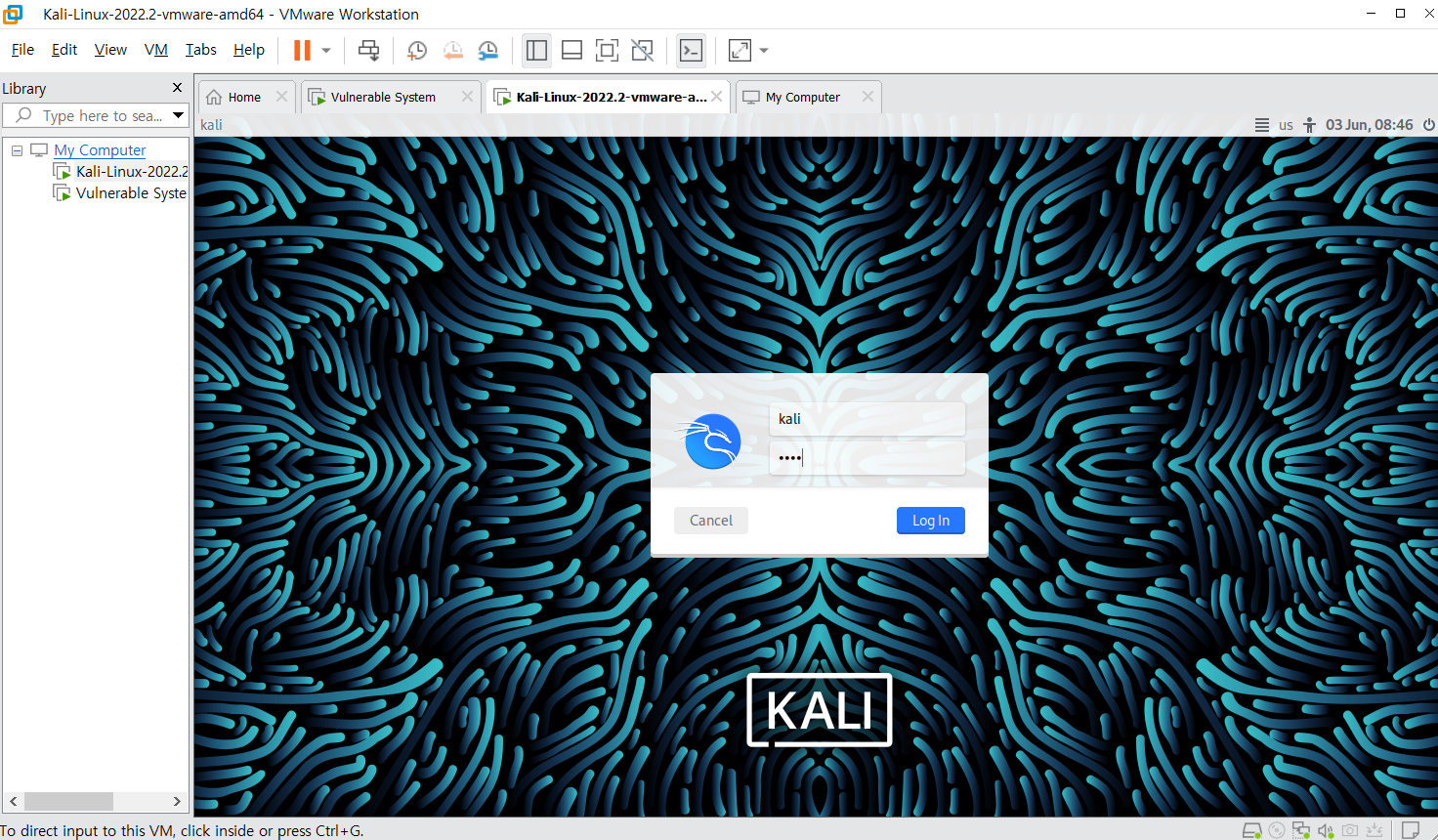
자동 생성된 설명

B

**Planning : 성공적인 침투 테스트를 위한 토대 마련**



Network adaptor -> net 설정



Kali-Linux

Id: kali pw: kali 설정

텍스트, 모니터, 스크린샷, 실내이(가) 표시된 사진

자동 생성된 설명

‘ifconfig’ 명령어 실행

자신의 ip확인

**Discovery**

텍스트, 모니터, 스크린샷, 전자기기이(가) 표시된 사진

자동 생성된 설명

Netdiscover 명령어 실행

텍스트이(가) 표시된 사진

자동 생성된 설명

Nmap을 통해 시스템 포트 스캐닝

텍스트, 스크린샷, 모니터, 검은색이(가) 표시된 사진

자동 생성된 설명

Searchsploit proftpd 명렁어 수행

ProFTPD 1.3.3c – Backdoor Command Execution(Metasploit) 확인

텍스트이(가) 표시된 사진

자동 생성된 설명

Msfconsole 명령어 수행

텍스트, 실내, 스크린샷이(가) 표시된 사진

자동 생성된 설명search proftpd 수행

Use /exploit/unix/ftp/proftpd\_133c\_backdoor 입력

텍스트이(가) 표시된 사진

자동 생성된 설명

Show options 명령어를 통해 입력해야 할 옵션 확인

RHOSTS 옵션 값 입력

텍스트이(가) 표시된 사진

자동 생성된 설명

Show payloads 명령어를 통해 사용 가능한 payload확인

Set payload cmd/unix/reverse 명령어 입력

텍스트, 스크린샷, 모니터, 화면이(가) 표시된 사진

자동 생성된 설명

Show options 명령어를 통해 payload의 옵션 확인

LHOST 옵션 값 입력

텍스트이(가) 표시된 사진

자동 생성된 설명

Show options명령어를 통해 옵션 값이 잘 설정 되었는지 확인

**Attack**

텍스트이(가) 표시된 사진

자동 생성된 설명

Exploit 명령어로 공격 수행

**Reporting**

텍스트이(가) 표시된 사진

자동 생성된 설명

공격 성공 확인

**C.**

해당 pentesting을 통해 Target System에서 발생한 공격을 방어 및 완화 하는 기법으로 Rapid7의 솔루션의 보안 취약점을 자동화된 방식으로 분석/검증/대응 하여 기업 내 자산을 보호하는 제품 방식입니다. 최근 증가하는 보안사고 형태에 많은 부분 내부 시스템 및 소프트웨어 취약점을 통해서 이루어지고 있으며 지금 이 순간에도 계속 새로운 취약점들이 발견되고 있습니다. 기업의 보안 담당자는 내부 자산이 이런 보안 취약점에 노출되어 있는지 관리하고 지속적인 보안 업데이트를 통해 보안 사고를 방지해야 하지만, 수많은 시스템과 어플리케이션을 수동적인 방법으로 관리 하기는 불가능에 가깝습니다. Rapid7의 솔루션은 기업 자산의 보안 취약점을 자동으로 탐지하고 위험 순위에 따른 조치 사항을 제시하며, 실제 침투 테스트를 통한 검증을 통해 최소한의 비용과 시간으로 내부 자산을 보호하고 관리할 수 있는 방안입니다.