

MetaSploit 3 mit eigenen Tests erweitern

Ivan Bütler – 2. September 2009



MetaSploit Framework

Um bei einem Penetration Test einen Exploit anzuwenden verwendet Compass ab und zu das MetaSploit Framework 3. Manch ein Exploit ist jedoch nicht im offiziellen MetaSploit Programm enthalten, so dass man manuell nachladen möchte. Dieser Artikel beschreibt die Ergänzung von MetaSploit 3 mit weiteren Tests/Exploits.

Prüfung der Anzahl MetaSploit Exploits

Bevor man mit der Ergänzung beginnt, sollte man die Anzahl Exploits in der Status Meldung von der MetaSploit Console ablesen

```
./msfconsole
      =[ msf v3.2-release
+ -- ---[ 320 exploits - 217 payloads
+ -- ---[ 20 encoders - 6 nops
      =[ 99 aux
```

Lokation der eigenen MetaSploit Tests

Die eigenen MetaSploit Tests gehören ins \$HOME/.msf3 Verzeichnis – und nicht wie möglicherweise angenommen ins Original Verzeichnis von MetaSploit. Dort muss man die Metasploit Struktur nachbauen. Am besten mit folgenden Befehlen:

```
cd .msf3/
mkdir -p ./modules/exploits/windows/http/
cp /tmp/apache-mod-rewrite.rb modules/exploits/windows/http/apache-mod-rewrite.rb
```

Löschen von "modcache"

Danach im \$HOME/.msf3 den Ordner modcache löschen. Beim nächsten Start von MetaSploit wird dieser Ordner automatisch wieder generiert und die neuen Module im \$HOME/.msf3 indexiert.

Neustarten MetaSploit

Nach einem Neustart sollten die MetaSploit Module/Exploits geladen werden – und in der Status Meldung ersichtlich sein. Vorher hatten wir 320 Exploits. Der neue Screen sieht wie folgt aus

```
./msfconsole
      =[ msf v3.2-release
+ -- --=[ 321 exploits - 217 payloads
+ -- --=[ 20 encoders - 6 nops
      =[ 99 aux
```

MetaSploit (www.metasploit.org)

Metasploit provides useful information to people who perform penetration testing, IDS signature development, and exploit research. This project was created to provide information on exploit techniques and to create a useful resource for exploit developers and security professionals. The tools and information on this site are provided for legal security research and testing purposes only. Metasploit is a community project managed by Metasploit LLC.

Thank You

Vielen Dank für das Lesen dieses Tutorial

Grüsse

Ivan Bütler, E1
Compass Security AG