Kommt es im Rahmen der Penetration zu erfolgreichen Exploiting-Vorgängen, werden die betroffenen Systeme rot markiert, sind dadurch sofort erkennbar und lassen sich in der grafischen Oberfläche weiter analysieren.

Abb. 2–13 *Erfolgreiche Übernahme eines Systems*

Die dargestellte Oberfläche macht einen Pentest mit Metasploit in vielen Fällen transparenter und anschaulicher. Einige Features wie die durchzuführenden Port- und Service-Scans lassen sich nahezu automatisch und oftmals erheblich einfacher als manuell auf der Kommandozeile durchführen. Trotz der scheinbar einfachen Bedienung und dem intuitiven Handling dieser grafischen Oberfläche sollte jeder Anwender umfangreiches Metasploit-Know-how mitbringen.

Wurde für einen Pentest in erster Linie die Metasploit-Konsole mit Datenbankanbindung eingesetzt, ist es möglich, die ermittelten Informationen in Armitage zu laden und weiterzuverwenden. Beispielsweise lässt sich die grafische Aufbereitung der Scanergebnisse für die abschließende Reporterstellung nutzen.

2.5.3 Metasploit Community Edition

Die Metasploit-Produktreihe umfasst mittlerweile vier unterschiedliche Produkte mit speziellen Features, die auf den jeweiligen Einsatz hin optimiert bzw. angepasst sind. Aufbauend auf der freien Open-Source-Version hat Rapid7 die Metasploit-Express- und die Metasploit-Pro-Version für den Unternehmenseinsatz erstellt. Folgende Abbildung zeigt die unterschiedlichen Versionen mit den Feature-Highlights der jeweiligen Versionen.

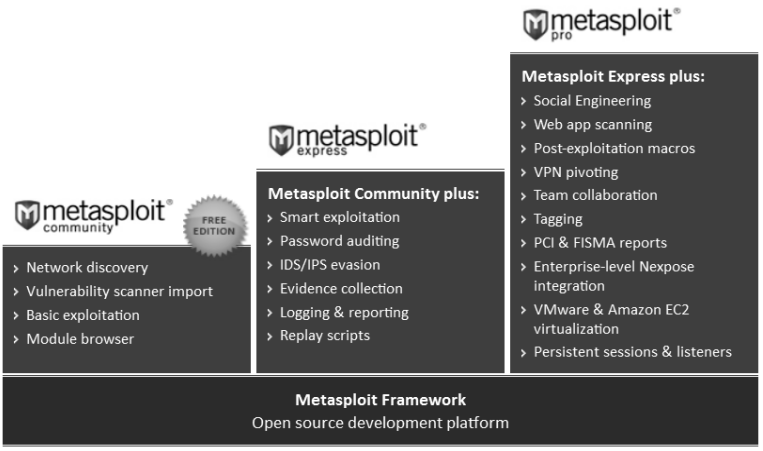

Abb. 2–14 *Die unterschiedlichen Metasploit-Produkte*

Bei der Metasploit Community Edition handelt es sich um die kostenlos verfügbare Version der von Rapid7 vertriebenen kommerziellen Metasploit-Varianten. Diese bringen unterschiedliche Vorzüge gegenüber der Open-Source-Version mit. Beispielsweise vereinfacht die grafische Oberfläche den Überblick über den Penetration-Test, und die wöchentlichen Updates im Zyklus der Metasploit-Pro-Version sorgen durch den Qualitätssicherungsprozess von Rapid7 dafür, dass das eingesetzte System immer funktionsfähig ist und nicht durch einen Fehler oder durch eine massive Änderung nur eingeschränkt oder gar nicht nutzbar ist.

Wird der typische Metasploit-Installer von der Metasploit-Webseite genutzt, ist neben der Open-Source-Variante des Frameworks automatisch auch die kommerzielle Version installiert. Je nach aktivierter Lizenz lässt sich eine der möglichen Versionen nutzen:

- Metasploit Pro
- Metasploit Express
- Metasploit Community Edition

Im Anschluss an die Installation des Metasploit-Frameworks ist die integrierte freie Version in folgendem Verzeichnis zu finden:

```
<MSF-Install-PAth>/apps/pro/vendor/bundle/ruby/<VERSION>gems/metasploit-
framework-<VERSION>/
```

Auf der Konsole lässt sich die zugehörige Metasploit-Konsole mit dem Kommando `msfpro` starten.

```
m1k3@ubuntu:~$ which msfpro
/usr/local/bin/msfpro

m1k3@ubuntu:~$ ls -l /usr/local/bin/msfpro
lrwxrwxrwx 1 root root 22 Jun 26 10:21 /usr/local/bin/msfpro ->
/opt/metasploit/msfpro
[*] Starting Metasploit Console...
<snip>
[*] Successfully loaded plugin: pro

m1k3@ubuntu:~$ sudo /etc/init.d/metasploit start

m1k3@ubuntu:~$ sudo msfpro
```

Listing 2–15 *Kommerzielle Metasploit-Konsole*

Um die Weboberfläche nutzen zu können, muss erst ein Benutzer angelegt werden und es sollte zudem sichergestellt sein, dass die entsprechenden Dienste laufen. Der Benutzer lässt sich wahlweise auf der Konsole oder per Webbrowser auf dem lokalen System einrichten. Im Normalfall startet der grafische Installer automatisch einen Browser, der zu den weiteren Schritten führt. Ist allerdings nur SSH-Zugriff auf dem System möglich, lässt sich der Benutzer mit folgendem Kommando einrichten. Bevor kein Benutzer eingerichtet ist, lässt sich die grafische Weboberfläche nicht nutzen.

```
m1k3@ubuntu:~$ sudo /opt/metasploit/createuser
[*] Please enter a username: m1k3
[*] Creating user 'm1k3' with password ')eRQc^pc,`u8' ...

m1k3@ubuntu:~$ sudo /etc/init.d/metasploit status
metasploit is running
postgresql already running
prosvc is running
nginx is running
```

Listing 2–16 *Metasploit-Startskript*

Alternativ zum vorhandenen Init-Skript lässt sich auch das mitgelieferte Control-Skript im Metasploit-Verzeichnis (`/opt/metasploit/ctlscript.sh`) zur Steuerung der Dienste nutzen.

Wurde der Benutzer für das Webinterface erfolgreich angelegt und laufen alle Services wie erwartet, kann man sich mit dem Webbrowser per HTTPS über Port 3790 auf das Webinterface verbinden.

Bevor die Weboberfläche uneingeschränkt nutzbar ist, muss zudem die benötigte Version des Frameworks online aktiviert werden. Der Registrierungsprozess der Community Edition ist kostenlos. Zudem ist es möglich, die Metasploit Pro mit allen Features zu testen. Im Anschluss an eine erfolgreiche Aktivierung sollten im ersten Schritt alle verfügbaren Updates eingespielt werden.

Hinweis: Die kommerziellen Versionen von Metasploit werden wöchentlich mit Aktualisierungen versorgt.

Nach der erfolgreichen Aktualisierung lässt sich die grafische Oberfläche erstmals nutzen. Hierfür sollte ein neues Projekt erstellt werden, und ein erster Discovery-Vorgang füllt die Datenbank mit Informationen zu den vorhandenen Systemen. Folgende Abbildung stellt die Ergebnisse eines ersten Discovery-Vorgangs dar:

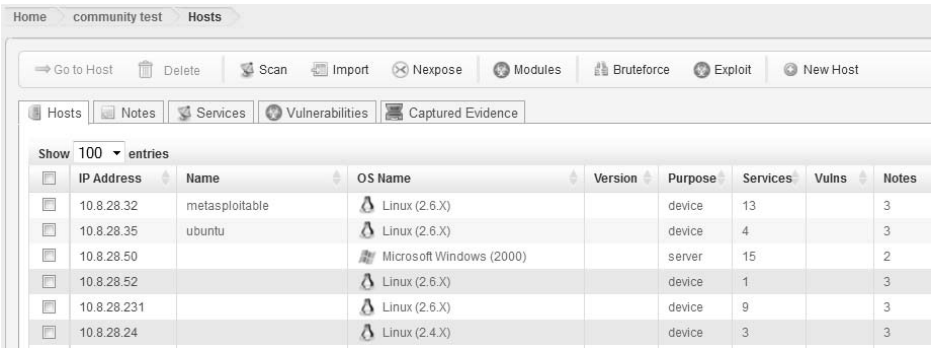

Abb. 2–15 *Übersicht der erkannten Hosts*

Dieser Discovery-Vorgang ist analog zu dem von Metasploit Pro und nutzt neben dem Nmap-Portscanner auch unterschiedliche Metasploit-Module, um möglichst schnell einen überaus umfangreichen Überblick des zu analysierenden Netzwerkes aufzubauen.

Ein sehr angenehmes Feature der kommerziellen Metasploit-Versionen ist der Einsatz derselben Datenbank von `msfpro` auf der Konsole und auf dem Webinterface. Dementsprechend ist es auf einfache Weise möglich, alle bekannten Features des Konsoleninterfaces, zu nutzen und mit den Vorteilen der grafischen Aufbereitung, die die Weboberfläche bietet, zu kombinieren. Speziell durch die Übersichtlichkeit der Datenaufbereitung ist die Kombination beider Oberflächen überaus hilfreich und ermöglicht dementsprechend effektivere Analysen der zu untersuchenden Umgebung.

Eine Vielzahl der erweiterten Features sind weiterhin den kommerziellen Versionen vorbehalten. Möchte man auf diese in der Weboberfläche zugreifen, wird man mit einem entsprechenden Hinweis auf die Pro-Version verwiesen.

Weitere Features der kommerziellen Versionen werden in Kapitel 12 zum Unternehmenseinsatz von Metasploit Pro betrachtet.