

Sicherheitsrisiken überzeugend darstellen: Das Metasploit – Framework

Autoren: Sebastian Schreiber, Stefan Arbeiter

Oft fehlt das Verständnis dafür, beliebige Sicherheitsmaßnahmen, auch ein banales Patch-Management zu finanzieren, das Risiko besteht ja nur theoretisch, solange man nicht bereits einen entsprechenden Vorfall, z.B. Wurmbefall hatte.

Mittlerweile haben Administratoren aber ein Werkzeug zur Hand mit dem die klassischen Hackerangriffe eindrucksvoll demonstriert werden können, das Metasploit-Framework¹. Es verfügt über eine graphische Oberfläche und eignet sich damit auch zur Sensibilisierung und Schulung von nicht-technischen Personal. Ursprünglich ein Netzwerkspiel wurde es von seinen Autoren mittlerweile zu einem formidablen Werkzeug weiterentwickelt.

Das Framework bietet für eine Reihe von Code, der Sicherheitslücken ausnutzen kann („exploits“) eine gemeinsame Oberfläche, sowohl unter Windows als auch Linux/Unix.

Das Innovative an dem Framework ist, das die Exploits nicht jeweils nur eine Wirkung (Z.B. Shellzugriff) haben, sondern beliebig mit einer Reihe von weiteren Werkzeugen beliebig kombiniert werden können, der Einsatz folgt damit immer zwei Schritten:

Nachdem Start von „msfweb“ kann man über <http://127.0.0.1:55555> das Interface von Metasploit aufrufen und den gewünschten Exploit aufrufen: Verfügbar sind hier die durch Würmer bekannten RPC-Verwundbarkeiten, SAMBA- und Internet Explorer-Sicherheitslücken aber auch Nischenprodukte wie der SAMBAR-Proxy für Windows.

Zusätzlich werden Links zu Beschreibung der Sicherheitslücke (und damit den Patches) angegeben, anschliessend kann aus der Menge der verfügbaren Payloads ein passender Teil ausgewählt werden: Nachdem ein Buffer Overflow ausgelöst wurde, muss schliesslich der Angreifer dafür sorgen, das für ihn interessanter Code ausgeführt, ansonsten löst der Angriff eventuell nur einen Absturz eines bestimmten Dienstes (D.o.S, Denial of Service) aus. Das Framework bietet solchen Code in der Form von Shellcodes an, diese reichen vom Öffnen einer Shell mit Administrator-Rechten über das anlegen lokaler Benutzer (Windows RCP Exploit) bis zum laden und ausführen von Exe-Dateien.

Im Falle des öffnen einer Shell kann man wählen, welchen Port Metasploit auf dem Zielsystem für die Kommunikation verwenden soll, bequemerweise wird die Verbindung über einen eigenen, lokalen Port ermöglicht.

Im Falle des Windows-RPC-Exploits sind zwei Payloads für Demonstrationen besonders interessant: Zum einen die zum öffnen einer Shell, zum anderen die zum Ausführen einer eigenen Datei.

Die ersteren (Z.B. winbind_stg und winreverse) demonstrieren deutlich den klassischen Hacker-Angriff. Auf einem ungepatchten Windows-System erhält man eine Shell mit Administrationsrechten, und kann anschliessend über ftp weitere Software nachladen, und mit dem net-Kommando weitere Benutzer und Freigaben anlegen.

Mit dem Payload winbind_stg_upexec kann eine Datei, z.B. ein selbst zusammengestellter Trojaner, auf dem Zielsystem direkt ausgeführt werden, was ein weiteres bekanntes Angriffsmuster darstellt.

Zusammenfassend kann gesagt werden, das Framework ein ideales Werkzeug ist, um darzustellen, wie einfach ungenügend administrierte, da ungepatchte Systeme angegriffen und übernommen werden können.

1 <http://www.metasploit.org>, mit vielen Links zu weiterer Dokumentation