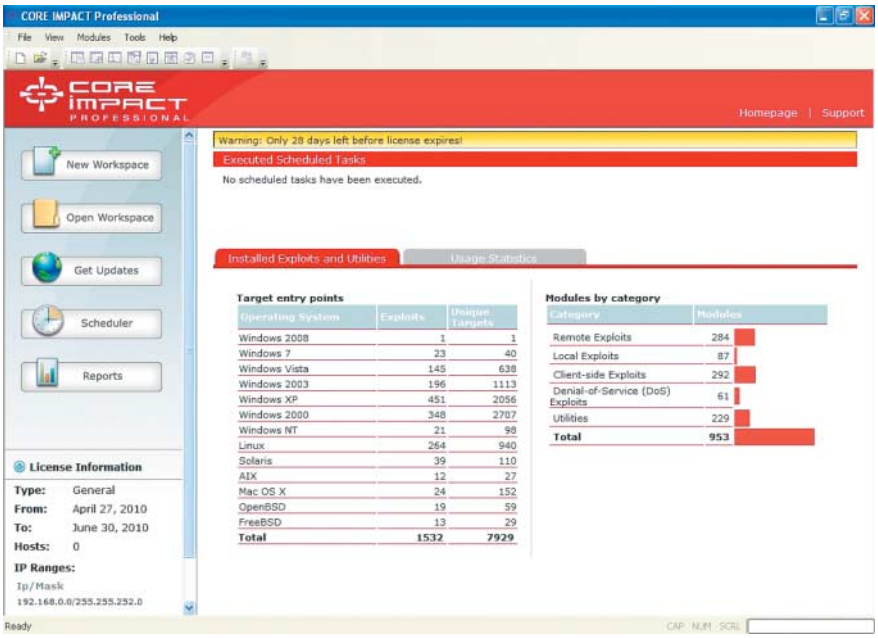

Sicherheitslücken automatisiert finden

Hack à la carte

Christoph Puppe, Oliver Schill-Lübben

Seit Kurzem bietet Core Security die Version 10.5 von Core Impact an. Ein Praxiseinsatz des Sicherheits-Analysewerkzeugs zeigt, was sich im vergangenen halben Jahrzehnt des langen Werdegangs getan hat.

Core Impact, eine integrierte Arbeitsumgebung für technische Sicherheitsüberprüfungen von IT-Systemen, hatte schon im Jahr 2004 einen gründlichen Test in der *iX* durchlaufen [1]. Das Prinzip der Software blieb seitdem unverändert: Von der ersten Informationsgewinnung über das Aufdecken von Sicherheitslücken und das Einbrechen in dieselben bis hin zum Erstellen eines Berichts bildet sie alle Arbeitsschritte eines Penetrationstests ab.

Die Praxistauglichkeit musste Core Impact in einer Testumgebung mit insgesamt acht Zielen unter Beweis stellen: Windows 2003 SP2 (englisch) sowie 2008, XP und Windows 7, dazu Damn Vulnerable Linux, SUSE Enterprise Server 9, Solaris 10 und FreeBSD 6.1. Realisiert war diese Serverfarm auf einer VMware Workstation.

Einen Paketfilter gab es nicht. Auf dem Arbeitsplatzrechner des Prüfers lief ein Windows XP. Core Impact setzt das Service-Pack 3 voraus und installiert .Net, GraphViz und den Embedded-SQL-Server zur Datenhaltung.

Jeder Test läuft in einer eigenen, passwortgeschützten Arbeitsumgebung („Workspace“). Der Schlüssel dient später der Kommunikation mit den Modulen. Seit dem letzten Test neu hinzugekommen ist die Aufteilung, welche Art von Angriff stattfinden soll. Zur Auswahl stehen Netz, Client und Web. Der erste Typus umfasst direkte Zugriffe auf Systeme, die per IP erreichbar sind, etwa Server. Client-Angriffe finden per Datenträger und E-Mails statt – also über den Benutzer, sei es, weil er einen präparierten USB-Stick findet oder eine verseuchte E-Mail empfängt. Die dritte Angriffsvariante obliegt einem Werkzeug zur automatisierten Fehlersuche auf Webseiten.

Bei jeder Variante stehen die Arbeitsschritte im linken Teil des Workspace als Wizards zur Verfügung. Sie sind gemäß der Vorgehensweise „richtiger“ Angreifer organisiert: „Informationen sammeln“, „Angriff und Penetration“, „lokales Sammeln von Informationen“, „Rechte erweitern“, „Aufräumen“ – gefolgt von „Bericht erstellen“.

Jeder Wizard besteht aus mehreren Python-Modulen. Sie sind einzeln ausführbar, sowohl manuell als auch per Makro zeitgesteuert. Core Impact vergleicht die Ergebnisse wiederholter Tests miteinander und berichtet Veränderungen. Für eine Software unter einer Closed-Source-Lizenz lässt sich Core Impact überaus flexibel konfigurieren: Anwender können nicht nur eigene Module schreiben, sondern auch vorhandene verändern. Der Hersteller bietet darüber hinaus die Dienstleistung an, Module nach Vorgaben des Kunden zu erstellen.

Die Arbeit mit den Wizards und den Modulen ist komplett über die grafische Oberfläche zu erledigen, die im Vergleich zu der des Vorgängers übersichtlicher geworden ist. Protokolle, Status, nächste Schritte und aktuelle Ergebnisse sind in Fenstern dargestellt, die der Benutzer frei anordnen kann. Nach dem Zuordnen eines Wizard zu einem Ziel per Drag & Drop erhebt eine Abfragemaske die Details. Schließlich arbeitet Core Impact die Schritte automatisiert ab und protokolliert alle Aktionen in einem Fenster und in der Datenbank. Das gewährleistet jederzeit den Nachweis, was zu welchem Zeitpunkt geschah.

Geheimagenten schwärmen aus

Eine besondere Stärke von Core Impact sind die Agenten. Die kleinen Programme laufen bei erfolgreichem Angriff entweder im Speicher des Ziels oder landen auf dessen Festplatte. Um auch einen Systemstart überstehen zu können, starten sie zum Beispiel unter Windows einen Dienst. Die Agenten können das Ziel lokal auf weitere Schwachstellen untersuchen und als Ausgangspunkt für weitere Angriffe nutzen. So kann der Tester einen Netzbereich prüfen, der gar nicht direkt erreichbar wäre, etwa von einem Webserver in einer mit dem Internet verbundenen DMZ aus, der wiederum Datenbankserver in einer eigentlich internen DMZ anspricht.

Der erste Reiter dient der Auswahl des Angriffstyps gegen Systeme, die

über eine feste IP-Adresse verfügen. Vom ersten Portscan mit Identifikation des Betriebssystems bis zum aktiven Angriff decken die Wizards alles ab. Core Impact konnte im Test gegen die erste Version der Ziele nur auf zwei Systemen, dem Windows 2003 und dem Windows 2008 Server – jeweils in der englischen Version – erfolgreich einen Agenten installieren. Hier zeigt sich eine Schwachstelle der Software, die bereits vor fünf Jahren aufgefallen war. Die immerhin 1532 Exploits mit insgesamt 7929 Targets (angreifbare Versionen der verwundbaren Software) eignen sich hauptsächlich für englische Versionen der getesteten Software. Es fehlen jedoch wichtige Parameter, etwa Sprungadressen, für Versionen anderer Sprachen. Um diese Zahl zu vergrößern, legt der Hersteller seit Kurzem das Open-Source-Exploit-Framework Metasploit bei. Es ist in die grafische Benutzeroberfläche eingebettet und wird von Core Impact bei einem Angriff auf Wunsch mit ausgeführt.

Angriff aufs Netz

Der auf den genannten Systemen von Core Impact installierte Agent ließ sich für weitere Angriffe gegen das hinter diesem System liegende Netz nutzen. Core Impact identifizierte den im simulierten Intranet untergebrachten XP-Client zwar, konnte aber keinen Angriff ausführen. Windows 7 wurde nicht erkannt. In einem früheren Versuch gelang Core Impact der Angriff auf einen neu hinzugefügten Windows 2000 Server über den MS SQL Server. Core Impact konnte keines der weiteren Betriebssysteme erfolgreich angreifen, obwohl auf allen Systemen sämtliche standardmäßig installierten Dienste gestartet waren. Ein Portscan mit *nmap* ergab immerhin 75 offene TCP-Ports, von denen fast alle Zugang zu einem Serverdienst gewährten. Manche hatte *inetd* allerdings geöffnet, ohne dass der dazugehörige Dienst installiert gewesen wäre.

Für den Vergleich mit einem Verwundbarkeits-Scanner kam Nessus zum Scannen aller Ziele zum Einsatz, in der Version 3.2.1 mit Plug-ins vom 8. Februar 2010. Insgesamt konnte Nessus auf 24 schwerwiegende Verwundbarkeiten hinweisen, unter anderem von alten PHP- und Joomla-Versionen. Schwerwiegend auch, dass Core Impact eine bekannte Schwachstelle im Telnet auf Solaris nicht identifizierte: Mit *telnet -l ,-fbin' sol10* kann sich jeder ohne Passwortabfrage als Benutzer „bin" anmelden. Darüber hinaus meldete Nessus 36 Sicherheitswarnungen.

In den letzten Jahren haben Angriffe gegen Clients, etwa Drive-by Downloads und Phishing, stark zugenommen. Dieser Entwicklung trägt Core Impact in der aktuellen Version Rechnung. Der Angriffstypus „Client Side" nutzt keine Scans, sondern erzeugt aus den Exploits Dateien, die per E-Mail zum Client gelangen. Wenn der Exploit dort erfolgreich ist, baut der damit gestartete Agent eine Verbindung zum Core Impact des Testers auf. Sobald der Agent läuft, starten darüber Angriffe gegen die internen Server. Immerhin 225 Exploits befinden sich zu diesem Zweck im Lieferumfang.

Ein Großteil der Angriffe gegen Firmen und Institutionen hat Websites zum Ziel. Eine Automatisierung ist teilweise möglich, sofern es um bestimmte, gut bekannte Schwachstellen auf vielen Sites geht. Wer Exotischeres untersuchen will, muss bekannte Fehlertypen in den Formularen der Site identifizieren. Core Impact löst diese Aufgabe nicht schlecht. Dass sich etwa mittels SQL-Injektion wieder ein Agent starten lässt, fällt positiv auf.

Im Test wurde unter anderem die Oberfläche von WebGoat untersucht. Die Cross-Site-Scripting-Angriffe wurden zum größten Teil gefunden. Die weiteren in dieser Anwendung enthaltenen Verwundbarkeiten leider nicht. Zumindest bei den SQL-Injektionen wäre zu erwarten gewesen, dass Core Impact diese findet. Der Crawler hatte diese Seite nicht entdeckt, ein neuer Test unter direkter Angabe dieser URL brachte allerdings auch kein anderes Ergebnis.

Fazit

Core Impact tritt in zwei Märkten an: Gegen Angriffs-Frameworks wie Metasploit und gegen Verwundbarkeits-Scanner. Als Ersatz für Letztere erscheint es nicht geeignet, da sie wesentlich mehr Tests ausführen und dadurch eine sehr viel größere Palette von Schwachstellen finden können. Zwar berichten sie auch oft Schwachstellen, die es nicht gibt, aber dafür greifen sie die IT-Systeme nicht an. Core Impact ist präziser, da es nur Lücken aufzeigt, die es erfolgreich angreifen kann. Die gute Tiefe des Tests geht jedoch zulasten der Breite. Immerhin ist Metasploit nun integriert, was die Tiefe weiter erhöhen sollte, davon war in diesem Test leider nichts zu spüren.

Daten und Preise

Core Impact 10.5

Hersteller: Core Security

Firmen-Website: www.coresecurity.com

Preise: auf Anfrage; kostenlose 30-Tage-Testlizenz

iX-Wertung

⊕ flexibles Framework für automatisierte Einbruchstests

⊕ einfach zu bedienen

⊕ Agenten zur Schwachstellenanalyse

⊖ keine deutsche Version

⊖ wenig Exploits für deutsche Betriebssystemversionen

Die direkte Konkurrenz ist eher bei den Frameworks zu suchen. Die gute Strukturierung, eine große Zahl von Exploits und die drei unterschiedlichen Angriffstypen machen Core Impact zu einer interessanten Alternative zu Open-Source-Produkten. Leider trübt wieder das Fehlen der Exploits für nicht englische und unübliche Betriebssysteme, etwa FreeBSD und AIX, das Bild.

Wer in einer englischen Umgebung arbeitet und Exploits auch selbst schreiben (lassen) kann, dem bietet Core Impact eine Arbeitsumgebung mit hohem Automatisierungsgrad. Für Anwender, die in deutschsprachigen Umgebungen Sicherheitstests durchführen wollen, eignet sich Core Impact derzeit nur eingeschränkt. Allerdings hat der Hersteller in diese Richtung einiges unternommen und zumindest wichtigen Exploits auch Targets für nicht englische Betriebssystemversionen mitgegeben. Die Methoden, Webserver anzugreifen, sind im Gesamtpaket eine gute Ergänzung, bei manchen Funktionen auch mit Alleinstellungsmerkmalen. Wer hauptsächlich Webseiten testen will, ist gut beraten, sich auch die darauf spezialisierte Software anzusehen. (un)

CHRISTOPH PUPPE UND OLIVER SCHILL-LÜBBEN

sind Sicherheitsberater bei der HiSolutions AG, Berlin.

Literatur

[1] Christoph Puppe; Systemsicherheit; Hack-O-Mat: Automatisierte Einbruchstests; *iX* 10/2004; S. 72