RAPID7

PRODUKTBESCHREIBUNG

metasploit®

Stellen Sie Ihre Abwehrmaßnahmen auf den Prüfstand

Metasploit, die Penetration Testing-Lösung von Rapid7 erhöht die Produktivität, validiert Schwachstellen und schafft ein Phishing-Bewusstsein.

DIE ANTIZIPATION GEGNERISCHER VERHALTENSWEISEN, HILFT IHNEN, IHRE VERTEIDIGUNG BESSER VORZUBEREITEN.

Metasploit, unterstützt von einer Community aus 200.000 Benutzern und Mitwirkenden, verschafft Ihnen diese Einblicke. Es ist die wirkungsvollste Penetration Testing-Lösung, die es aktuell zu kaufen gibt. Mit ihr entdecken Sie Schwachstellen in Ihrer Abwehr, konzentrieren sich auf die größten Gefahren und verbessern Ihre IT-Sicherheit.

Die eigenen Schwachpunkte kennen

Simulieren Sie realitätsnahe Angriffe, um Ihre Schwachpunkte zu ermitteln, bevor dies ein böswilliger Angreifer tut. Metasploit lässt sich nahtlos mit dem Metasploit Open-Source-Framework integrieren - es ermöglicht den Zugriff auf Module zur Erkundung und Auswertung, um die Tests zu beschleunigen. Verwenden Sie die Techniken der Angreifer, um Anti-Viren-Software zu entgehen, schwache Anmeldedaten zu finden und durch das gesamte Netzwerk zu navigieren.

Machen Sie sich die weltweit größte Exploit-Code-Review-Datenbank zunutze

Die Leitung des Metasploit OpenSource-Projekts gewährt Rapid7 wichtige Einblicke in die neuesten Methoden der Angreifer und deren Denkweise. Rapid7 arbeitet eng mit der User-Community zusammen, um im Durchschnitt pro Tag 1 neuen Exploit zu den derzeit mehr als 1.300 Exploits sowie über 2.000 Modulen hinzuzufügen.

Simuliert realitätsnahe Angriffe auf Ihre Abwehr

Metasploit umgeht führende Anti-Virus-Lösungen in 90% der Fälle und ermöglicht Ihnen, mittels 200 Modulen ein kompromittiertes Gerät vollständig zu übernehmen. Navigieren Sie durch Ihr Netzwerk, um herauszufinden, wie weit ein Angreifer kommen kann.

Entdecken Sie schwache und wiederverwendete Anmeldeinformationen

Testen Sie Ihr Netzwerk auf schwache und wiederverwendete Passwörter. Indem es über das einfache „Knacken" von Betriebssystemkonten hinausgeht, kann Metasploit Brute-Force-Angriffe gegen mehr als 20 Kontotypen initiieren, einschließlich Datenbanken, Webserver und Remote-Administrationslösungen.

Metasploit umgeht in 90% der Fälle Anti-Virus-Lösungen, und fügt im Durchschnitt pro Tag 1 neuen Exploit hinzu.

PRIORISIEREN SIE, WAS ENTSCHEIDEND IST

Ihre Schwachpunkte zu identifizieren, ist nur die halbe Miete. Als Penetration-Tester, ist es Ihre Aufgabe, eine gründliche Bewertung durchzuführen und zu kommunizieren, was getan werden muss, um das Risiko einer Datenschutzverletzung zu verringern. Ermitteln Sie die schwachen Glieder in der Angriffskette und validieren und priorisieren Sie Schwachstellen durch die nahtlose Integration mit Nexpose und Top Remediation Reports.

Lokalisieren Sie die schwachen Glieder in der Angriffskette präzise

Die Angriffe werden immer raffinierter; der Gegner bündelt verschiedene Techniken, um damit Ihre Systeme schneller als je zuvor zu umgehen. Mit Metasploit können Sie Angriffe so simulieren, wie sie vom Gegner ausgeführt werden und damit problemlos die größten Sicherheitsrisiken melden.

Nahtlose Integration mit Rapid7 Nexpose® für Remediation

Wenn andere Abteilungen die Stichhaltigkeit der Scan-Ergebnisse in Frage stellen, zeigen Sie auf, dass eine Schwachstelle die Systeme und Daten dem Risiko eines Angriffs aussetzt. Sie werden von den Beteiligten rasche Zustimmung für Wiederherstellungsmaßnahmen erhalten und Glaubwürdigkeit schaffen. Metasploit und Nexpose stellen die einzige Validierungslösung aus einer Hand dar, die Schwachstellenpriorisierung und Remediation-Berichte vereinfacht.

VERBESSERN SIE DIE ERGEBNISSE

Die Zeit drängt. Als Penetration-Tester können Sie sich nicht, wie der Gegner, den Luxus erlauben, zu warten. Metasploit ermöglicht Ihnen, Verbesserungen voranzutreiben, indem es im großen Umfang Penetration-Tests ausführt und Compliance-Programme rascher zum Abschluss bringt. Darüber hinaus können Sie Phishing-Kampagnen simulieren. Damit schärfen Sie das Sicherheitsbewusstsein, indem Sie Benutzer zur Schulung weiterleiten, nachdem diese eine gefährliche Maßnahme getroffen haben.

Führen Sie Penetration-Testing-Programme im großen Stil aus

Die Durchführung von Assessments und das Daten-Management in Netzwerken mit über 100 Hosts kann herausfordernd sein. Metasploit führt Skalierungen durch, um pro Projekt tausende Hosts sowie mehrerer Penetration-Tester gleichzeitig zu unterstützen. Automatisieren Sie die Penetration-Test-Schritte mithilfe von Aufgabenketten und Metamodulen, um die Produktivität zu verbessern.

Reduzieren Sie das Benutzerrisiko, indem Sie Phishing-Kampagnen und Schulungen durchführen

Senden und verfolgen Sie die E-Mails an Tausende von Benutzer mit Metasploit Pros skalierbaren Phishing-Kampagnen. Klonen Sie die Anmeldeseiten von Web-Anwendung mit nur einem Klick, um die Anmeldeinformationen abzugreifen. Messen Sie die Conversion-Rates bei jeder Stufe der Phishing-Kampagne. Wenn Benutzer eine gefährliche Maßnahme ergreifen, können sie an Ort und Stelle zu einer Schulung geleitet werden.

Erfüllen Sie Compliance-Programme schneller

Erstellen Sie Berichte, um Ihre Ergebnisse darzustellen und sie nach Regularien wie PCI DSS und FISMA zu ordnen. Überprüfen Sie, ob Wiederherstellung oder kompensierende Controls implementiert sind, um die Betriebsfähigkeit und Wirksamkeit der Systeme zu schützen. Erstellen Sie Schwachstellenausnahmen auf Basis fundierter Beweise, die Ihr nächstes Audit problemlos bestehen. Zeichnen Sie Maßnahmen und Resultate der Beurteilung Ihres Netzwerks und der Anwendungsebene automatisch auf, um wertvolle Zeit zu sparen, die Sie sonst durch Ausschneiden und Einfügen vergeuden würden.

„Was uns wirklich an die Spitze brachte, waren die Phishing-Fähigkeiten, die Metasploit beinhaltet... Das war für uns der geschäftsentscheidende Faktor."

- Tim Pospisil, IT Security Supervisor
Nebraska Public Power District

SIND SIE BEREIT, LOSZULEGEN?

Tel.: 866.7.RAPID7

E-Mail: sales@rapid7.com

Schulung: www.rapid7.com/services/teaching-you-to-use-it.jsp