metasploit®
pro

Metasploit Pro for Federal Government

Industry Product Brief

Cyber-attacks on Federal government networks and systems are increasingly sophisticated, frequent, and dynamic. Federal departments and agencies need a way to assess the overall effectiveness of their defenses against real-world attacks.

Overview

Rapid7 Metasploit® Pro improves penetration testers' productivity, validates vulnerability exploitability, and manages phishing campaigns. With Metasploit Pro, you can automatically document your actions and findings, significantly reducing time spent writing reports. Backed by a community 200,000 users and contributors, Metasploit is the world's most impactful penetration testing solution.

Know Your Weak Points

Simulate real-world attacks to find your agency's weak points before a malicious attacker does. Metasploit gives your Red Team access to reconnaissance, exploitation and post-exploitation modules, with advanced automation features to accelerate testing.

Utilize world's largest code-reviewed exploit database

Leverage the Metasploit open-source project to gain insight into the latest attacker methods and techniques. Rapid7 works with the user community to add an average of 1 new exploit per day, currently counting more than 1,300 exploits and more than 2,000 modules.

Simulate real-world attacks against your agency's defenses

Use Metasploit to create dynamic payloads to evade leading anti-virus solutions 90% of the time, and get past firewall and IPS using traffic-level techniques. Control machines you have compromised with over 200 modules, and get local network access with VPN pivoting.

Test your network for weak and reused credentials

Go beyond just cracking operating system accounts. Metasploit can run brute-force attacks against over 20 account types, including databases, web servers and remote admin tools. Automate credentials re-use to see how far an attacker can get in the network.

Prioritize What Matters Most

Penetration testers need to perform a thorough assessment to pinpoint the weak links in the attack chain and prioritize the most critical risks across the agency. Scanning tools can identify vulnerabilities on your network but not whether it poses actual risk in the context of your environment.

Validate vulnerabilities with Rapid7 Nexpose® integration

Metaploit integrates seamlessly with Nexpose to provide the only closed-loop vulnerability validation solution for determining which vulnerabilities can be exploited. Uncover risks with Nexpose, automatically test for exploit-ability with Metasploit, and return results to Nexpose for prioritization and remediation.

Simulate phishing campaigns to improve security awareness

Users are often targeted by attackers to gain access to your network. Create automated, scalable user awareness campaigns with Metasploit. Clone web application login pages with one click, send and track emails to thousands of users, and measure conversion rates at every step. Users can be redirected to a training site on the spot.

Improve Your Outcomes

Test your agency's security defenses more efficiently. Writing reports is often the most time-consuming and frustrating part of the job, taking up to weeks of man-hours. Metasploit allows Red Teams to accelerate improvement by running penetration tests at scale and automating key tasks.

Save time with powerful and flexible reporting engine

Metasploit automatically records actions and findings from your penetration test to save valuable time otherwise spent on cutting and pasting. Use the built-in reporting templates or upload your own custom templates, with the ability to sort by regulations such as FISMA, then export to add more contextual information.

Run agency-wide penetration testing programs at scale

Conducting an assessment and managing data in networks over 100 hosts can be challenging. Metasploit scales to support thousands of hosts per project on engagements and multiple simultaneous penetration testers. Automate repetitive steps with Task Chains and MetaModules to complete assessments faster.

Simplify Compliance

Metasploit can help Federal departments and agencies comply with the following programs:

NIST 800-53 – Verify that security controls implemented to protect Federal information systems are operational and effective.

FedRAMP – Use Metasploit to conduct penetration tests, including phishing attacks, on cloud services as part of the FedRAMP assessment process.

Federal Information Security Management Act (FISMA) – Metasploit can be used to test security controls and validate vulnerabilities as required for FISMA compliance.