

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

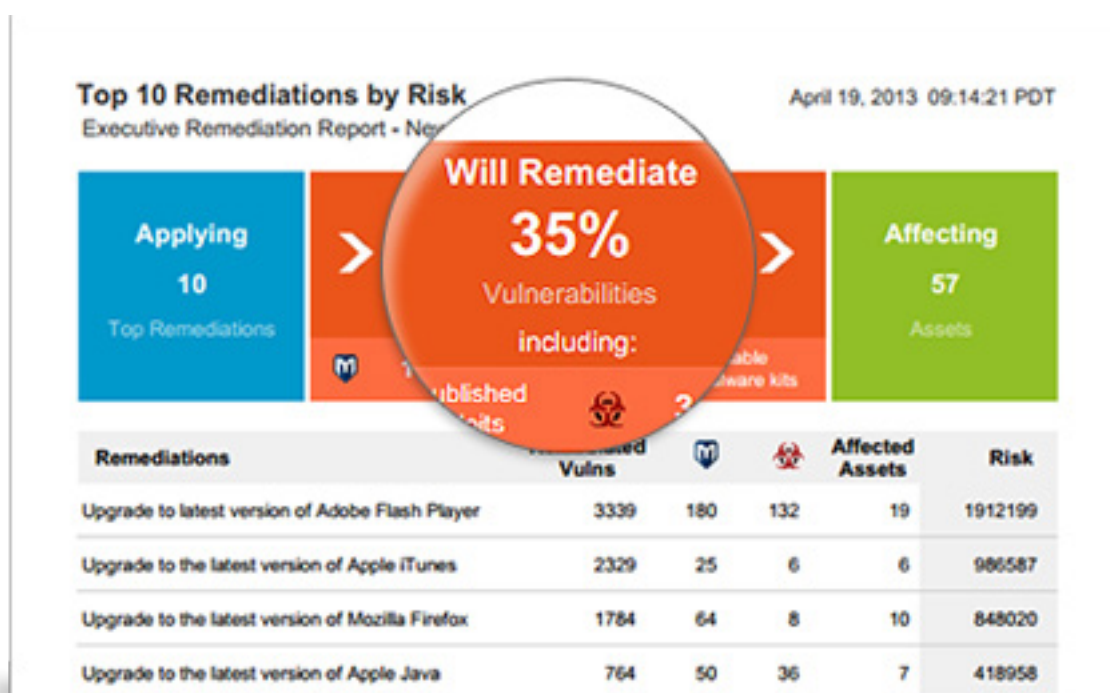
Rapid7 Metasploit

Rapid7 Metasploit решение для тестирования проникновения угроз, которое позволяет оценивать риски и меры их устранения, чтобы предотвращать утечки данных и иные последствия нарушения безопасности IT-инфраструктуры.

Благодаря Rapid7 Metasploit IT-специалисты получают наглядное представление о том, какие уязвимости в инфраструктуре предприятия могут использовать вредоносные компоненты и сконцентрироваться на наиболее критичных и важных рисках.

«После восьми месяцев использования Metasploit и Nexrose мы смогли уменьшить риск на 98%. Это впечатляюще. Сейчас мы используем Metasploit ежеквартально на всех хостах»

Scott Erven, Специалист по информационной безопасности Essentia Health



ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

- Полностью автоматизированный процесс
- Полная видимость всех возможных угроз
- Возможность работы с большими сетями
- Обход систем защиты для полноценного тестирования на проникновение
- Сбор доказательств проникновения
- Автоматическая отчетность

ВАЛИДАЦИЯ УЯЗВИМОСТЕЙ

- Подтверждение уязвимостей, най-

денных сторонними решениями

- Приоритизация угроз на основе реальности их осуществления
- Оптимизация плана устранения уязвимостей

ФИШИНГ КАМПАНИИ

- Оценка человеческого фактора в информационной безопасности
- Отслеживание действия пользователей с фишинговыми письмами
- Контроль подготовленности сотрудников к фишинг атакам

Softprom - официальный дистрибьютор компании Rapid7 на территории стран СНГ

ТЕСТИРОВАНИЕ НА ПРОНИКНОВЕНИЕ

Rapid7 Metasploit

ВОЗМОЖНОСТИ METASPLOIT:

- Осуществляет симуляцию атаки на сеть и выявляет проблемы ее безопасности
- Интегрируется с системой управления уязвимостями Nexpose для анализа существующих рисков
- Выполняет оценку доступных способов защиты от атак и инструментов контроля вторжений
- Определяет незащищенность перед фишингом и утечками конфиденциальных данных
- Снижение затрат времени тестирования на проникновение на 45%
- Наибольшая база эксплойтов с предоставлением исходного кода
- Легкое оперирование большими массивами данных
- Встроенные механизмы обхода систем безопасности, таких как anti malware, IPS
- Сбор доказательств при успешном проникновении на хост
- Автоматическая генерация отчетов

Air Train
At&T
Best Buy
Capital One
Carnegie Mellon
CPS
Money Gram
International
Petco
United Health Group
US Cellular

«Metasploit Pro действительно помогает оптимально распределить время, это та причина, почему для нас это наилучшее решение»

Jim O'Gorman, Президент Offensive Security

СРАВНЕНИЕ РЕДАКЦИЙ Rapid7 Metasploit

Характеристики	Metasploit Express	Metasploit Pro
Тестирование на проникновение Windows/Linux систем, баз данных и сетевого оборудования	✓	✓
Тестирование на проникновение Web приложений		✓
Применение эксплойтов	✓	✓
Комбинирование эксплойтов		✓
Сбор подтверждений успешной реализации эксплойтов	✓	✓
Подбор паролей к учетным записям	✓	✓
Эмуляция фишинговых атак		✓
Обход системы IDS/IPS antimalware		✓
Получение доступа через скомпрометированные узлы к другим узлам сети		✓
Расширенная отчетность		✓
Дополнительные модули проверок		✓
Совместная работа нескольких пентестеров		✓
Импорт данных со сторонних систем управления уязвимостями	✓	✓
Web консоль	✓	✓
Управление с помощью консольных команд		✓