Um pouco sobre “MetaSploit”.

O Metasploit é uma plataforma de testes de penetração que permite encontrar, explorar e validar vulnerabilidades. Ele fornece a infra-estrutura, o conteúdo e as ferramentas para realizar testes de penetração e auditoria de segurança extensiva e, graças à comunidade de código aberto e à própria equipe de conteúdo de trabalho duro da Rapid7, novos módulos são adicionados regularmente, o que significa
que o último recurso está disponível para Você assim que for publicado.

O projeto foi criado pelo Hacker HD Moore, iniciado em 2003 e lançada oficialmente
no ano seguinte, o mesmo já contava com alguns exploits escritos em linguagens de programação como C, Perl e Assembly. O projeto teve de ser reescrito em 2007 com o lançamento da versão 3.x da linguagem Ruby, o acontecido possibilitou o ampliamento de novos desenvolvedores e exploits para o framework.

No ano de 2009 a Rapid7 comprou o Metasploit e em alguns anos projetaram uma versão Pro para comercialização.

O projeto foi se tornando popular pela eficiência em seus módulos auxiliares
e exploits, sendo mesmo implementado em diversas distribuições GNU/Linux por padrão para facilitar utilização por Pentesters, Hackers, Administradores de Redes e entusiastas de segurança.

As atuais versões do projeto possuem mais de 1573 exploits, 906 módulos auxiliares, 270 módulos post, 8 Módulos Nop, 455 Payloads, e 39 Encoders.

Abaixo as ferramentas do Metasploit Framework:

º Msfconsole - Metasploit em modo console;

° Msfbinscan - Permite procurar em executáveis instruções de salto, instruções POP;

° Msfpescan - Usado para análisar e descompilar executáveis e DLLs;

° Msfvenom - União de msfencode e msfpayload, permite criar Payloads e encriptar para evasão de AV, Firewall ou IDS;

° Msfupdate - Usado para atualização do Framework;

°Msfd - Fornece uma instância do msfconsole que os clientes remotos podem se conectar;

° Msfrpc - Conecta a uma instância RPC do Metasploit;

° Msfrpcd - Fornece uma interface RPC para Metasploit.

- Existem diversos livros e cursos baseados no Metasploit, devido sua enorme eficácia em exploração de sistemas.

Certamente é uma das melhores ferramentas de Hacking existentes, por isso recomendamos uma leitura de sua
documentação e testes em sua rede local.

Abaixo links com informações adicionais:

Documentação: https://community.rapid7.com/docs/DOC-1567

Site: https://metasploit.com/

- Créditos: Merces Letifer Security

- Auto corrigido por: Loock Underwood

- Implementações de: Loock Underwood