Desenvolvimento de módulos para o Metasploit

Projeto de Informática

Bruno Miguel Rebelo Ramos Nº 1010906

Docente orientador: José Carlos Fonseca

Engenharia Informática 2015/2016
Instituto Politécnico da Guarda
Escola Superior de Tecnologia e Gestão

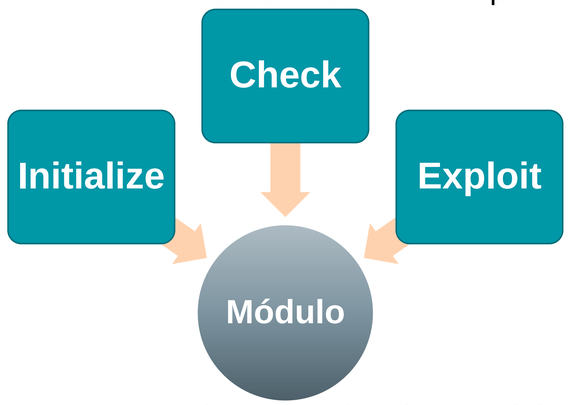
1. Introdução

Este trabalho insere-se na área da segurança informática, com enfoque no ciclo de vida de três das vulnerabilidades mais comuns existentes nas aplicações: *SQL Injection (*SQLi), *Cross-Site Scripting* (XSS) e *Buffer Overflow (BO)*.
Este projeto visa mostrar o ciclo de vida destes três tipos de vulnerabilidades, desde a criação das aplicações vulneráveis, passando pela sua exploração manual, para finalmente se automatizar essa exploração através da criação de módulos para o Metasploit. Também são analisadas correções para estas vulnerabilidades. Para o Metasploit foram criados módulos que exploram XSS, SQLi, BO em Linux e BO em Windows.

XSS	SQLi	BO no Linux	BO no Windows
Este modulo possui várias opções como inserir um *keylogger*, redirecionar para uma página à escolha do utilizador ou então roubar as *cookies* de sessão.	A execução deste modulo permite descobrir informações como o nome da base de dados, o nome das tabelas, o seu conteúdo, entre outras.	Este modulo explora o BO presente num servidor de FTP do sistema operativo Linux.	O modulo BO no Windows, permite explorar um BO muito conhecido numa aplicação chamada FTP FreeFloat Server.

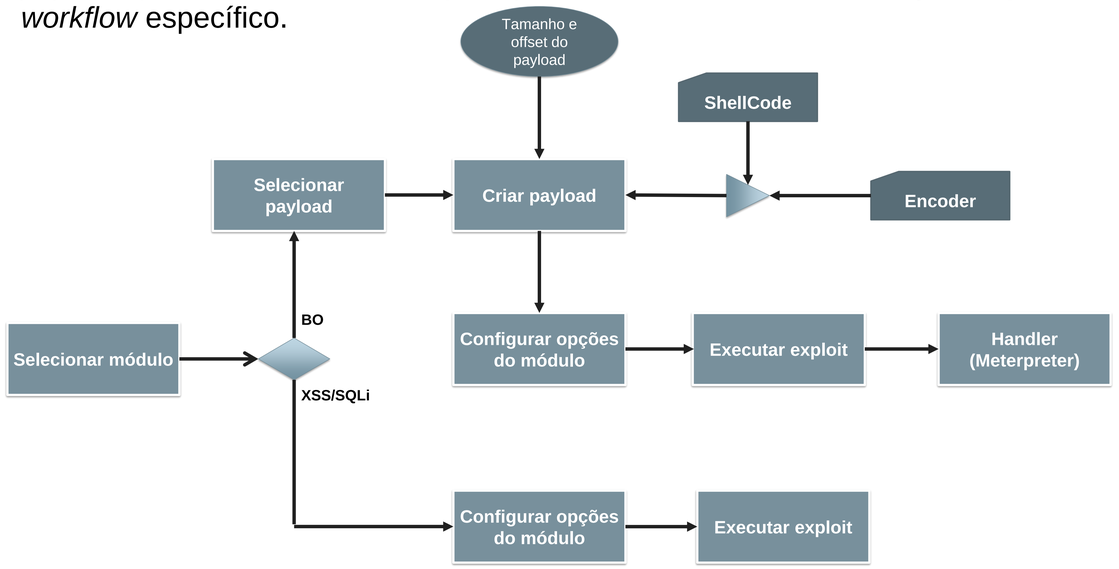
2. Desenvolvimento de modulos para o Metasploit

O Metasploit é uma *framework open source* para testes de penetração que é utilizada tanto por profissionais de segurança como por *hackers*. É extensível através da criação de novos módulos cuja programação é feita na linguagem Ruby. São estes módulos que contêm os programas (*exploits*) que têm como objetivo explorar vulnerabilidades encontradas em *software* e sistemas operativos, através das potencialidades do Metasploit. Internamente, os módulos estão organizados em três partes: Initialize, Check e Exploit. Apesar da complexidade do BO, foi o desenvolvimento dos módulos para XSS e SQLi que protagonizaram o maior desafio, dada a praticamente inexistente informação relativa ao desenvolvimento deste tipo de módulos.



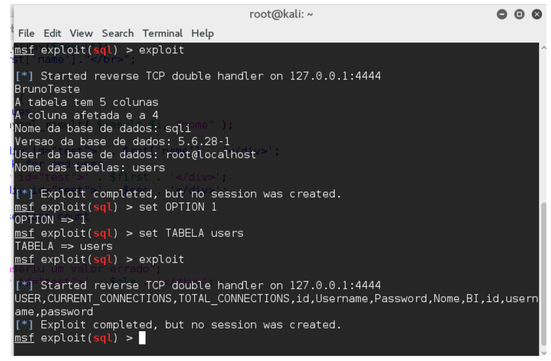
Initialize	Check	Exploit
Contém toda a informação do módulo, tal como o nome, descrição e *payload*	Função utilizada para verificar se a aplicação alvo é vulnerável ou não	Código para explorar a vulnerabilidade

O processo de execução dos módulos, depende destes utilizarem ou não *payload (*como é o caso do BO). Dependendo disso, a sua execução segue um *workflow* específico.



3. Resultados

Os quatro módulos desenvolvidos (XSS, SQLi, BO Linux e BO Windows) foram testados extensivamente, tendo conseguido sempre explorar com sucesso, e de forma automática, as respetivas vulnerabilidades.



Após correção das vulnerabilidades, a execução dos módulos deixou de conseguir realizar a exploração, como seria de esperar.

4. Conclusões

Este trabalho mostra como um atacante pode desenvolver, com relativa facilidade, módulos novos para o Metasploit, tendo em vista as vulnerabilidades mais comuns. Para os atuais e futuros engenheiros informáticos este é mais um alerta acerca da importância do desenvolvimento de software seguro. De facto, a falta de uma simples validação pode colocar em risco toda uma organização.
A explicação de como podem ser criados módulos para XSS, SQLi e BO, vem colmatar a falta de documentação neste campo, levando a que este trabalho também possa ser uma importante ferramenta de aprendizagem nesta área.