Tipos de Payloads

windows/x64/meterpreter/reverse_tcp
windows/shell_bind_tcp
windows/adduser
linux/x86/adduser
linux/x86/shell/reverse_tcp
bsd/x64/shell_bind_ipv6_tcp
android/meterpreter/reverse_https
php/meterpreter/reverse_tcp
windows/x64/vncinject/reverse_tcp

+ A primeira parte do nome explicita informações sobre a arquitetura do host que estamos atacando
Windows, Linux, etc

+ A parte do meio diz mais ou menos os protocolos usados

+ O fim diz os métodos (direto, reverso, etc)

+ Se for usar o método da reverse shell, devemos lembrar de habilitar a abertura da porta que irá ser utilizada e isso pode dar problema de acordo com a configuração do roteador ou firewall de cada um
→ Por isso é normal que se use uma VPS para esse tipo de serviço

+ Esse de adicionar usuário pode ser bom pro caso de querermos infectar a máquina com algum arquivo que já tenhamos pronto. Para isso, adicionamos um usuário, baixamos o arquivo e iniciamos o que queremos.

Staged x Inline

windows/x64/meterpreter_reverse_tcp – Inline / non_staged

windows/x64/meterpreter/reverse_tcp - Staged

windows/shell_bind_tcp - Inline / non_staged

windows/shell/bind_tcp - Staged

windows/adduser - Inline / non_staged
linux/x86/adduser - Inline / non_staged

linux/x86/shell/reverse_tcp – Staged

linux/x86/shell_reverse_tcp - Inline / non_staged

+ Nos payloads do tipo inline (_), todas as funções são executadas de uma única vez, o que necessita de mais espaço
+No staged (/), o exploit vai carregando vários estágios ou pedaços de código