BRUTE FORCE

# O que e?:

brute force e uma técnica usada por invasores e crackers (mal intencionados) na qual eles utilizam ferramentas para tentar quebrar geralmente um usuário e uma senha(login), e umas das técnicas mais eficazes que existem no cenário de web hacking, porem e umas das técnicas que mais podem demorar, dependendo a complexidade da senha ou mesmo do hash (criptografia da senha). Outra definição de brute force também pode ser aplicada em algumas ferramentas de pentestes que realizam a numeração ou a listagem de diretórios, esse método apesar de ser considerado como de brute force ele e considerado mesmo invasivo quando comparado ao brute force autentication por exemplo.

### Ferramentas:

Algumas das ferramentas listadas abaixo já veem padrão no KALI LINUX (sistema operacional muito usado na área de pentestes) por esta razão não necessita da instalação ou configuração:

* JOHN DE RIPPER
* HYDRA
* CAIN & ABEL
* OPHCRACK
* HASHCAT

### Como Evitar:

* Bloquear o acesso após um numero x de tentativas de requisições ao site, muitos sites e sistemas são criados em WORDPRESS uma plataforma de CMS muito popular hoje em dia, com a simples instalação de um plugin para limitar as requisições em uma pagina ou mesmo a programação de um algoritmo próprio. Outra forma de evitar esse tipo de ataque seria a utilização de um WAF (web application firewall) um firewall configurado para bloquear o IP ou ate mesmo de bloquear IPs vindo de uma determinada região geográfica, muitos WAF hoje em dia também utilizam até mesmo padrões de ataques para bloquear outras ferramentas que utilizam o mesmo tipo de requisição como porta e protocolos utilizados para realizar o brute force.
* Use CAPTCHA são uma das formas mais eficazes de se proteger de um ataque de brute force, pois para realizar uma determinada requisição ao sistema faz necessário a resolução do “quebra cabeça” criado pelo CAPTCHA, além disso o sistema pode analisar a resolução do mesmo para identificar se quem está realizando a ação e uma maquina ou uma pessoa o que o torna mais difícil a resolução por BOTS ou SPAMS.
* Autenticação de Dois Fatores outra forma muito eficiente de se proteger de um brute force e a utilização de uma autenticação em dois fatores, ou seja, além das credenciais como: USARIO e SENHA e aplicado uma verificação onde é enviado geralmente via SMS ou e-mail um PIN (código complementar) na qual o usuário do sistema deve digitar para poder finalmente realizar o acesso ao mesmo, além de evitar redundâncias esse processo evita também ataques por BOTS ou MAQUINAS.
* Bloquear o acesso por SSH como anteriormente o brute force e um ataque usado contra uma variedade de protocolos e serviços em suas respectivas portas, portanto bloquear o SSH na porta 22 pode reduzir significativamente as chances de um invasor obter sucesso em seu ataque de brute force.
* Outra técnica bem eficaz e a utilização de senhas fortes e seguras, ou seja, evite usar suas informações pessoais como data de nascimento, cpf, número de telefone etc. além disso evite a utilização simultânea de uma senha em vários cadastros ou contas online, crie combinações forte de senha com letras e números letras maiúsculas e minúsculas e complemente com caracteres especiais como por exemplo: @, #, $, \_ etc. quanto mais caracteres combinados mais forte será sua senha.