Como efetuar ataque de Brute Force com Hydra e como se proteger

20 de setembro de 201520 de setembro de 2015 / s0ph0s

O método de ataque conhecido como *bruteforce* (ou "força bruta") é um dos métodos de ataque mais usado e questionado em relação na sua eficiência nos dias de hoje, criando um certo preconceito nesse método. Abordaremos detalhes sobre o método de ataque, demonstrando o uso da ferramenta ***THC Hydra***, que explicaremos como utilizar seus recursos e configurar seu ataque. Essa será um das series de artigo relacionado a ferramenta, já que ela possui muitos mais recursos de configuração de ataque, ainda abordaremos aqui proteção desse ataque, utilizando métodos simples de segurança em servidores e nas criações de suas senhas.

O que é *BruteForce*?

O ataque de bruteforce consiste em tentativas consecutivas de verificação de *strings* sobre um serviço de um alvo, a qual utiliza-se uma *wordlist* (banco de palavras) para verificação dos dados. Dando exemplo mais simples, ele pega palavras dessa wordlist (como exemplo de uma senha) e faz uma série de verificações com cada palavra até ser equivalente a real senha.

Conhecendo a ferramenta THC Hydra.

O *THC Hydra* é uma das dezenas de ferramentas que utilizam esse método de ataque de *bruteforce*, suportando diversos tipos de serviços que podemos tentar invadir, como:

- AFP
- Cisco AAA
- Cisco auth
- Cisco enable
- CVS
- Firebird
- FTP
- HTTP-FORM-GET
- HTTP-FORM-POST
- HTTP-GET
- HTTP-HEAD
- HTTP-PROXY
- ICQ
- IMAP
- IRC
- LDAP2
- LDAP3
- MS-SQL
- MYSQL
- NCP
- NNTP
- Oracle
- Oracle-Listener
- Oracle-SID
- PC-Anywhere
- PCNFS
- POP3
- POSTGRES
- RDP
- REXEC
- RLOGIN
- RSH
- SAP/R3
- SIP
- SMB
- SMTP
- SMTP-Enum
- SNMP
- SOCKS5
- SSH(v1 and v2)
- Subversion

- Teamspeak (TS2)
- Telnet (Protocolo que iremos utilizar)
- VMware-Auth
- VNC and XMPP

Ela vem instalada por padrão nas distribuições de PenTest como o *Kali Linux*. Caso não tenha em sua distro, utilize nossa ferramenta *Organon* para realizar a instalação dela. Mas se quiser instalar manualmente, siga as instruções abaixo.

Instalando o THC Hydra

Baixe a ferramenta com o comando abaixo.

wget http://www.thc.org/releases/hydra-7.2-src.tar.gz

Entre na pasta da ferramenta.

cd hydra-7.2-src

E dê os comandos abaixo para realizar a instalação dela.

./configure
make
make install

Configurando e realizando o ataque com THC Hydra.

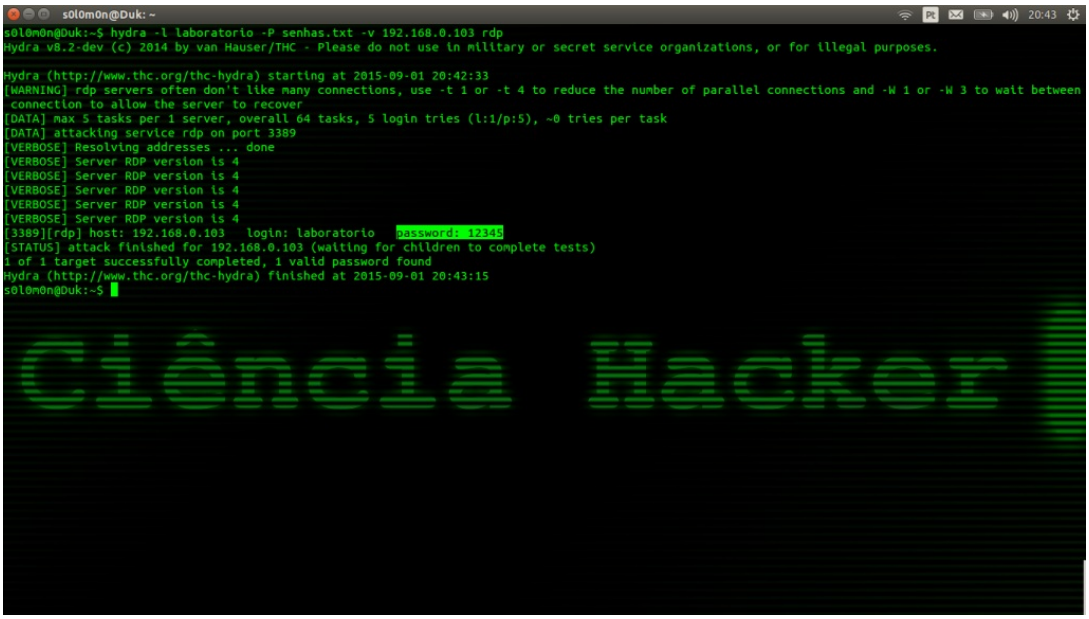
Antes de iniciar o ataque, precisamos ter uma Wordlist em mão, baixe uma ou crie uma com o *Crunch* (apresentado aqui em nossos tutoriais). Para entendermos melhor os comandos e todos os recursos do THC Hydra, aqui estão algumas opções:

-l = Nome/login da vítima;
-L = Carrega uma lista contendo nomes/logins de vítimas (1 por linha);
-p = Especifica senha única;
-P = Carrega uma lista com senhas (1 por linha);
-e = Adiciona ‘n’, testa senha em branco ou adicional ‘s’ testa user como pass;
-C = Usado para carregar um arquivo contendo usuário:senha. Formato usuário:senha equivale a -L/-P;
-M = Carrega lista de servidores alvos (1 por linha);
-o = Salva as senhas encontradas dentro do arquivo que você especificar;
-f = Faz o programa parar de trabalhar quando a senha ou usuário for encontradao;
-t = Limita o número de solicitações por vez (default: 16);
-w = Define o tempo máximo em segundos para esperar resposta do servidor (default: 30s);
-v / -V = Modo verbose do programa. ‘V’ mostra todas tentativas

Agora vemos alguns comandos que podem ser usados para atacar, que explicaremos logo abaixo:

hydra -l laboratorio -P senhas.txt 192.168.0.102 rdp
hydra -L wordlist.txt -P wordlist.txt -v cienciahacker.com.br ftp

No exemplo (1) o ataque IP do nosso alvo é *192.168.0.102,* a qual o ataque é direcionado no serviço *RDP (Remote Desktop Protocol).* Na configuração do ataque setamos o *login* como “laboratorio” devido termos conhecimento do usuário (como exemplo muitos serviços usam logins padrões como “admin” ou “root” que economiza o tempo de nosso ataque) e a *senha* é introduzida através da nossa *wordlist.* Veja o exemplo abaixo:



Note que ele pega a versão do RDP que é 4, e tenta realizar a sequência de ataques revelando a senha *12345*. Descoberta a senha agora só basta iniciar o serviço e efetuar o login.

No exemplo (2) é um exemplo bem simples de ataque, onde atacamos o alvo com a utilização de uma *wordlist* para tentar descobrir *login* e *senha*, sendo nosso alvo o *www.cienciahacker.com.br* (ou pode substituir pelo endereço IP do site) rodando no alvo o serviço de FTP. Uma opção desse ataque é a opção *-v* que envia requisições pausadamente para que evite que um firewall ou mecanismo de segurança do alvo bloqueie seu ataque, usado muito como ataque a "cegas" por não saber nem o login e senha do site.

Isso são apenas demonstrações de exemplo de ataques que podem ser utilizados, uma vez analisado o serviço do alvo você deve fazer as configurações corretas no ataque de acordo com o alvo. Para saber todas essas informações, existem técnicas de varreduras e scan que algumas ferramentas realizam, como já apresenta aqui o tutorial do Nmap.

Um recurso interessante do *THC Hydra* é o fato de que caso você sofra uma interrupção durante o ataque, seja pela queda da conexão ou bloqueio, você pode retornar ao ponto que você parou e continuar o ataque. Lembrando que durante o PenTest o ataque de *bruteforce* é visto como o último recurso de ataque devido não existir nenhum esforço para realizar tal prática.

A eficiência do ataque é relacionada a fraqueza da senha criada no serviço, existem diversos serviços privados ou governamentais que utilizam senhas padrões nos logins, ou muitos *administradores* desses serviços criam uma senha frágil a qual pode ser facilmente quebrada pelo processo de *bruteforce*.

Como se proteger do ataque?

Como dito, para que o método de ataque seja eficiente requer que a senha/login do serviço esteja numa Wordlist cujo muitos "Hackers" criam esse banco de palavras a partir de informações pessoais da vítima, senhas *default,* nome de pessoas ou palavras comuns usadas como sequências de letras ou números. Para evitar que seu serviço seja atacado, seja sua conta pessoal de e-mail (Gmail, Hotmail, entre outros) ou serviços rodando no seu servidor (FTP, SSH..), recomendamos que crie uma senha segura com os seguintes critérios:

- Letras maiúsculas e minúsculas (a-A).
- Números (0-9).
- Caracteres especiais (@#$%&*).

Outras dicas de segurança muito importantes para ajudar a ter maior segurança são:

- Nunca utilizar a mesma senha em vários serviços.
- Não usar na senha informações pessoais.
- A cada determinado período de tempo troque a senha.
- Cuidado onde se faz backup da senha.

Para quem lida com serviços em servidores, recomendamos a instalação de um patch de segurança que evite ataque sequenciais de um determinado endereço IP. Como exemplo da ferramenta Block Hostname Mikrotik e plugins em CMS como LimiteLoginAttempt (WordPress), Jsecure (Joomla).

,,,