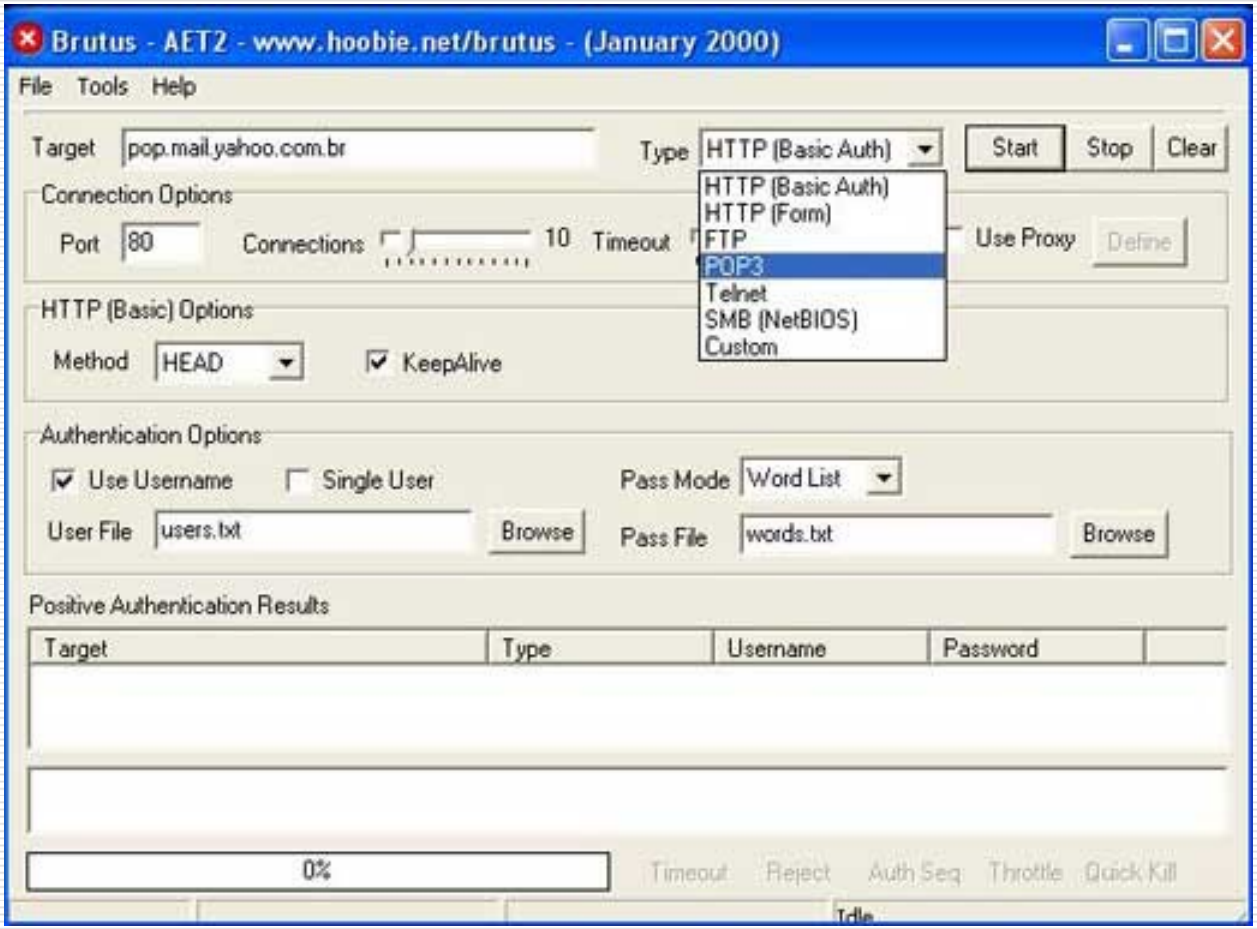
Força Bruta em Serviços

Força Bruta em Serviços

- Técnicas clássicas e “barulhentas”.
- A maioria dos sistemas gera *logs* de tentativas de conexão.
- Ferramentas:
  - Sdi.brutus.pl (Melo, S. 2004 p.130)
  - Blaster (Melo, S. 2004 p.130)
  - **Hydra** (Melo, S. 2004 p.131)

Brutus


Brutus - AET2 - www.hoobie.net/brutus - (January 2000)
File Tools Help
Target pop.mail.yahoo.com.br
Type HTTP (Basic Auth)
Start Stop Clear
HTTP (Basic Auth)
HTTP (Form)
FTP
POP3
Telnet
SMB (NetBIOS)
Custom
Connection Options
Port 80
Connections 10
Timeout
Use Proxy
Define
HTTP (Basic) Options
Method HEAD
KeepAlive
Authentication Options
Use Username
Single User
Pass Mode Word List
User File users.txt
Browse
Pass File words.txt
Browse
Positive Authentication Results
Target
Type
Username
Password
0%
Timeout
Reject
Auth Seq
Throttle
Quick Kill
Idle

Hydra

- Escrita na linguagem C.
- Desenvolvida para ambientes POSIX.
- Objetivo: descobrir ***username*** e/ou ***password*** a partir de um serviço.
- Arquivos: **`userlist.txt`**
  `passwd.txt`

Hydra

- Front End **Xhydra** em GTK.
- Linux, UNIX BSD, Solaris, Mac OS/X e outros UNIX-like.
- Windows com Cygwin, com suporte a IPV4 e IPV6.
- Sistemas móveis baseados em processadores ARM (Zaurus, Ipaq).

Hydra

- **Prova o conceito de recursos de segurança**, com a possibilidade de mostrar a facilidade de se **obter acesso não-autorizado** a um sistema remoto, ...
- ... dentro de um cenário em que o administrador mantém **configurações padrões de contas** e **senhas fracas** nos serviços disponíveis.

Hydra

- É possível testar os seguintes serviços:

  Telnet, FTP, HTTP, HTTPS, HTTP-Proxy, LDAP, SMB, SMBNT, MS-SQL, MySQL, POP3, IMAP, NNTP, ICQ, PCNFS, VNC, SOCKS5, REXEC, SAP/R3, Cisco Auth, Cisco Enable, Cisco AAA.

Hydra

- SSH e Oracle.
- Pode usar a técnica de *Bounce* para força-bruta em aplicação Web utilizando um Proxy-Web mal configurado.

Hydra

- Compilando Hydra:
  ```
  >./configure
  >make
  >make install
  ```

- Compilando o Front End GTK
  ```
  >cd hydra-gtk
  >./configure && make && make
   install
  ```

Hydra

- Compilando em Palm Pilot e Mobiles baseados em processadores ARM:
  >./configure-palm
  >./configure-arm

- Por padrão, o Hydra será instalado em /usr/local/bin/...
  Seu binário é “hydra” e o binário do Front End é “xhydra”.

Hydra

- **`hydra <ip-alvo> <def-serviço> <opções>`**

- Opções Especiais:

  opção “-m”

  Alguns serviços requerem técnicas de força-bruta com a opção “-m”.

  WWW, SSL, HTTP, HTTPS,

Hydra

- Restaurando uma sessão abortada ou travada.
  - CTRL + C
  - hydra.restore (arquivo)
  - > ???

- Performance no uso do Hydra
  - opção “-t”
  - desempenho depende do protocolo.
  - o mais rápido, é geralmente, o POP3.

Hydra

- Outras opções em serviços como:

  SMBNT, LDAP, serviços Cisco, SAP/R3

- O aplicativo **PW-INSPECTOR**:

  Utilitário para manipular wordlist, extraindo de uma wordlist uma segunda wordlist seguindo padrão pré-definido pelos seus parâmetros.

PW-INSPECTOR

- Serve para criar outras *wordlists*, quando o atacante sabe o perfil de senha que o alvo utiliza, resultando assim numa redução da lista de senhas (*wordlist*).

  Por exemplo: senhas com o mínimo de 6 caracteres.

PW-INSPECTOR

- Seja uma wordlist com vários tipos de senhas: `words.txt`

- Ordenando words.txt
```
>cat words.txt | sort | uniq >
 dictionary.txt
```

- Extraindo de `dictionary.txt` apenas as senhas que atendam ao padrão:
```
>cat dictionary.txt | pw-inspector –m
 –c 2 –n > passlist.txt
```