Capturando Informações Sobre Ataques de Força Bruta SSH

Rede Nacional de Ensino e Pesquisa - RNP
Centro de Atendimento a Incidentes de Segurança - CAIS
Dezembro de 2005

Ivo de Carvalho Peixinho
ivocarv@cais.rnp.br

RNP/PAL/0198

Sumário

- Motivação
- Desenvolvimento da ferramenta
- Dados capturados
- Tratamento de incidentes
- Análise de ferramenta brutessh
- Conclusões
- Recomendações
- Próximos passos

CAIS

Motivação

- Registros de ataques a partir de Agosto de 2004 – SANS ISC.

- Servidores SSH muito utilizados para acesso remoto em sistemas UNIX e equipamentos de rede.

- Inexistência de ferramentas para captura de informações – *Standalone e Honeypots.*

- Serviço Criptografado – Dificuldades na captura de informação "em trânsito" (ex: tcpdump, snort).

- *Logs* do próprio servidor SSH e assinaturas do *snort* (bleeding snort) como única forma de detecção atualmente.

- Registros de ataques bem-sucedidos – Existência de senhas "fracas".

- **SSH Remote Root password Brute Force Cracker Utility - 20/08/2004: http://www.frsirt.com/exploits/08202004.brutessh2.c.php**

Motivação (2)

- Responder algumas perguntas:
  - De onde vem os ataques?
  - Qual a média de ataques por dia?
  - Quantas tentativas de autenticação por IP?
  - Quais os usuários e senhas mais atacados/utilizados?
  - Existem ferramentas automatizadas (*worm*)?
  - Quais os passos do atacante após conseguir um *shell*?
  - Qual o nível de "inteligência" dos dicionários utilizados?

CAIS

Ferramenta de Captura

- Modificação do próprio servidor SSH
- 1a versão – Autenticação desabilitada
  - Funcionamento *inetd (honeyd)* ou *standalone*
    - *add default tcp port 22 "fakesshd -i -f fakesshd_config -w $sport -z $ipsrc"*
  - **Registro em *log* à parte das informações coletadas:**
    - **Tue Jun 14 06:39:41 2005: Connection from XXX.XXX.XXX.XXX port YYYY**
    - **Tue Jun 14 09:31:14 2005: Authentication attempt (SSHv2) ! User: XXXXXX Password: XXXXXXX**

CAIS

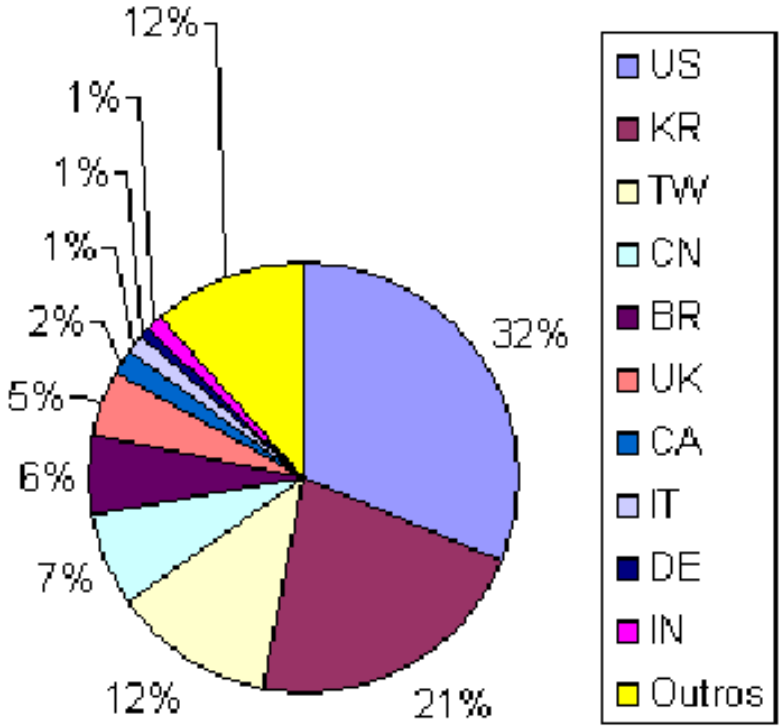
Ferramenta de Captura

- 2a versão – Captura de comandos
  - Autenticação aleatória baseado em probabilidade
  - Especificação de um *shell* alternativo independente do *shell* definido no sistema
  - Registro em log:
    - **Thu Aug 11 00:31:14 2005: Authentication attempt (SSHv2) ! User: XXXXXX Password: YYYYYYYY**
    - **Thu Aug 11 00:31:14 2005: User authenticated ! Dice: 15.213012 Probability: 40**
  - Log de sessões de comandos em arquivo independente

Capturando Informações Sobre Ataques de Força Bruta SSH

Captura de Dados

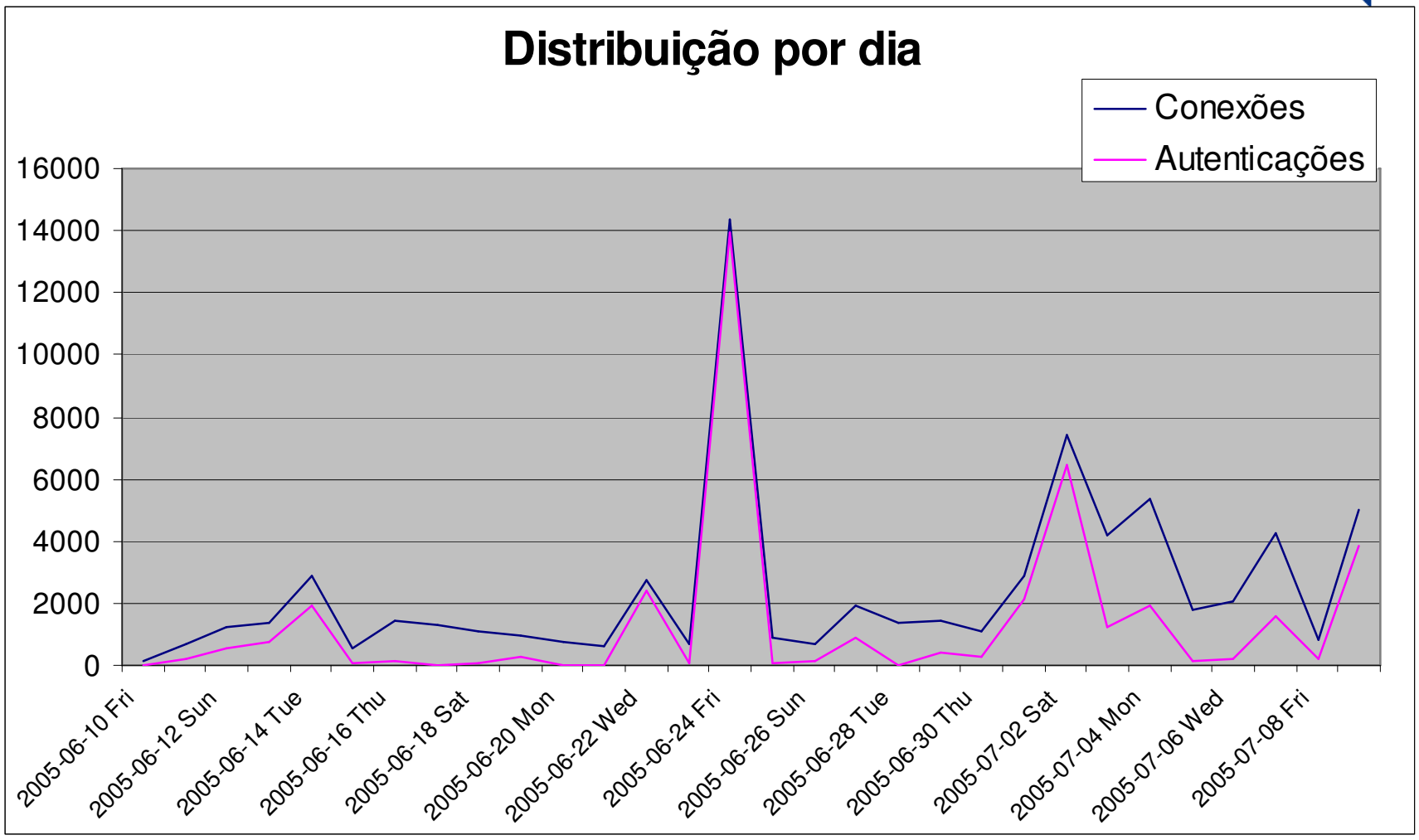
- Janela de Captura: 10/06/2005 a 09/07/2005
- Coleta através de dois *honeypots* (duas classes C)
- Autenticação desabilitada (1a versão)
- Estatísticas:
  - **. 71992 conexões**
  - **. 132 endereços IP distintos**
  - **. 39949 tentativas de autenticação**



Capturando Informações Sobre Ataques de Força Bruta SSH

CAIS

Captura de Dados



Capturando Informações Sobre Ataques de Força Bruta SSH

Captura de Dados

- Usuários mais atacados

root	10733
apache	2226
test	1261
admin	758
guest	353
webmaster	272
aaron	242
aakarshan	236
mysql	212
oracle	210

- Senhas mais usadas

admin	913
root	884
test	743
123456	732
server	591
password	467
administrator	385
apache	346
qwerty	282
webadmin	279

Captura de Dados

- Pares (usuario/senha) mais usados

root	root	829
test	test	655
root	server	566
root	admin	418
admin	admin	360
root	123456	288
root	root1	261
root	qwerty	259
guest	guest	254
root	administrator	251

Captura de Dados

- Curiosidades
  - Tentativas de usuários e senhas em português, espanhol e japonês
  - Tentativas de senhas com nomes de *software* e jogos, como *debian, fedora, counterstrike, frozenthrone, worldofwarcraft*.
  - Tentativas de senhas "de teste" como *123456, password, qwerty, q1w2e3r4, 1q2w3e, !@#$%, $changeme$, test123.*
  - Tentativas de acesso usando um usuário: "#" e uma senha: ":::::: Scanner of SSH Service Brute Force - 2005 Version! ::::: #"
  - Maior parte das senhas em minúsculas
  - Presença de diversos *scans* em uma classe C inteira
  - Maioria dos ataques proveniente dos EUA

CAIS

Tratamento de Incidentes

- Obtenção diária de dados referentes a tentativas de conexão e de autenticação
  - Endereço IP do atacante
  - AS correspondente
  - *Timestamp* da primeira tentativa no dia
- Obtenção diária das senhas usadas e a quantidade
- Repasse dos incidentes referentes ao backbone da RNP para o sistema de tratamento de incidentes
- Repasse dos incidentes restantes para as entidades externas responsáveis
- Dicionário de senhas utilizadas em ataques brute force

Tratamento de Incidentes

Senhas em japonês

Japanese First Name (male)

ryuu ryouta kenichi katsuro
akira kenji ken kazuo jiro goro kazuya
takumi daiki naoki jun hanzo kenta
hachiro katsuo kazuki daisuke hiroshi
hideaki kichiro naoto kouhei katsu takuya
isamu souta ichiro kenshin takahiro daichi
hotaka

Japanese First Name (female)

aki ayame saki kiku shiori ai hotaru miho
akiko junko hitomi natsumi keiko mai
chikako misaki kasumi aiko chika
etsuko mil kazuko nanami hiroko hanako
monoko miki haruka hikari haruko
hikaru akio akemi
kaede izumi momoko emi aya

Estatísticas até 2/12/2005:

- **10261 usuários distintos**
- **13646 senhas distintas**
- **17906 pares distintos**

CAIS

Análise de ferramenta brutessh

```
tc-vmware:~# ./sc
Usage: ./sc <classe-a> <porta> [classe-b] [classe-c]

tc-vmware:~# ./sc 172 22 16 203
[+] found 172.16.203.128
[+] continuing scan ...
[+] found 172.16.203.130
[+] continuing scan ...
[+] found 172.16.203.136
[+] continuing scan ...

tc-vmware:~# more ipfile
172.16.203.128
172.16.203.130
172.16.203.136
```

Análise de ferramenta brutessh

tc-vmware:~# ./usf1 -help

SSHBrute v1.4 - Tal0n [cyber_talon@hotmail.com] on 09-04-04

SSHBrute is a SSH Daemon login brute forcer (-brute), supports a SSHd banner
grabber (-grab), and of course this message (-help). Need more info? USE THE SOURCE!

tc-vmware:~# ./usf1

SSHBrute v1.4 - Tal0n [cyber_talon@hotmail.com] on 09-04-04
Usage: ./usf1 -brute <hosts.txt> || -grab <ip> || -help

Encontrados 127 binários usf#!
Código fonte disponível em http://www.flowsecurity.org/tools/flow-sshbrute.c

CAIS

Análise de ferramenta brutessh

tc-vmware:~# strings usf1
[useless stuff]
SSHBrute Started (File = %s, PID = %d).
Error: fork()
root
root1
root12
root123
root1234
123456
12345678
Password
password
passwd
(etc..)
SSHBrute Complete (File = %s, PID = %d).
[more useless stuff]

CAIS

Análise de ferramenta brutessh

tc-vmware:~# ./usf1 -grab 172.16.203.137

SSHd Banner: SSH-1.99-OpenSSH_4.1

tc-vmware:~# ./usf1 -brute ipfile
SSHBrute Started (File = ipfile, PID = 18969).
SSHBrute Complete (File = ipfile, PID = 18969).

tc-vmware:~# more brutessh.log
Tue Sep 27 21:19:18 2005: Authentication attempt (SSHv2) ! User: root Password: root1
Tue Sep 27 21:19:18 2005: User authenticated ! Dice: 38.984818 Probability: 100
Tue Sep 27 21:19:24 2005: Connection from 172.16.203.137 port 37890
Tue Sep 27 21:19:24 2005: Authentication attempt (SSHv2) ! User: root Password: root12
Tue Sep 27 21:19:24 2005: User authenticated ! Dice: 4.477194 Probability: 100
Tue Sep 27 21:19:36 2005: Authentication attempt (SSHv2) ! User: root Password: root1234
Tue Sep 27 21:19:36 2005: User authenticated ! Dice: 34.335648 Probability: 100
(etc…)

Não foram encontrados registros no *log* de comandos

CAIS

Análise de ferramenta brutessh

tc-vmware:~# more all

./usf1 -brute $1;
./usf2 -brute $1;
./usf3 -brute $1;
(etc… até ./usf127 –brute $1;)

tc-vmware:~# more vuln.shell
[root/root 172.16.203.137]
[root/root1 172.16.203.137]
[root/root12 172.16.203.137]
[root/root123 172.16.203.137]
[root/root1234 172.16.203.137]
[root/123 172.16.203.137]
[root/123456 172.16.203.137]
[root/12345678 172.16.203.137]
[root/root 172.16.203.137]
[root/password 172.16.203.137]

CAIS

Conclusões

- **Ataques de força bruta a servidores SSH ocorrendo em larga escala**
- **Dicionários sendo utilizados com senhas em diversas línguas e senhas óbvias**
- **Muitas tentativas de ataque ao usuário root**
- **Aparente inexistência de *worms* realizando este tipo de ataque**
- **Ataques manuais:**
  - **Scan de classes e geração de listas de IP com servidores SSH**
  - **Tentativa de autenticação nos servidores da lista**
  - **Acesso aos servidores comprometidos**

Recomendações

- **Mudar o servidor SSH de porta**
- **Utilizar métodos de autenticação mais fortes (RSA)**
- **Auditar senhas dos usuários**
- **Utilizar regras para impedir utilização de senhas fracas**
- **Utilizar filtros de pacotes (*firewall*)**
- **PermitRootLogins = no**
- **Monitorar as conexões ao servidor SSH (logs)**

CAIS

Próximos passos

- **Realizar captura de comandos**
- **"Implementar" alguns comandos mais utilizados no *shell* falso (w, uptime, wget, cd, ls, pwd)**
- **Utilizar implementação falsa de *wget* e *ftp* para obter cópia de programas baixados pelos atacantes**
- **Simular outros servidores SSH (roteadores, etc)**
- **Sensores em honeypots acadêmicos**
- **Gerar uma base de senhas utilizadas neste tipo de ataque**
- **Notificar os envolvidos**

Capturando Informações Sobre Ataques de Força Bruta SSH

CAIS

Perguntas?

Informações de Contato

Centro de Atendimento a Incidentes de Segurança – CAIS

cais@cais.rnp.br - http://www.rnp.br/cais

Ivo de Carvalho Peixinho – ivocarv@cais.rnp.br