Introdução a Canais Dissimulados e Backdoors

Carlos H. P. Caetano Chaves[2], Luiz Otávio Duarte[1 3], Antonio Montes[1 3]

[1]Divisão de Segurança de Sistemas de Informação
Centro de Pesquisas Renato Archer
Ministério da Ciência e Tecnologia

[2]Segurança de Dados no EC
Visanet

[3]Laboratório Associado de Computação e Matemática Aplicada
Instituto Nacional de Pesquisas Espaciais
Ministério da Ciência e Tecnologia

GTS.07

Objetivos

Apresentar e discutir conceitos relacionados à backdoors e canais dissimulados, baseando-se em exemplos e observações práticas dos problemas causados por artefatos que utilizam estes mecanismos.

Motivação

- Grande tendência de ataques que se utilizam de novas técnicas para tentar ocultar a presença do atacante e aumentar sua permanência para periodos grandes de tempo.
- Dissertação de mestrado desenvolvida por Carlos Henrique para o curso de Computação Aplicada do INPE/MCT.

Roteiro

- Conceitos Inicias;
- Backdoors;
- Evolução de Backdoors;
- Canais Dissimulados.

Conceitos Iniciais

Esta apresentação trata de dois mecanismos muito utilizados por atacantes para manter o acesso a um dado computador sem que uma vulnerabilidade precise ser explorada.

- Backdoors;
- Canais Dissimulados (Cover Channels).

- Possuem o objetivo de prover acesso aos computadores previamente comprometidos sem que uma vulnerabilidade necessite ser explorada novamente.
- Normalmente estes backdoors inserem novos processos no sistema comprometido. Mas podem ser inseridos em códigos-fonte, arquivos de configuração de aplicações legítmas e etc...
- Muitas vezes estes backdoors podem ser detectados por sistemas de detecção de intrusão, antivírus, anti-spyware e etc...

Backdoors: Exemplos.

- Binários isolados que esperam por conexão em uma dada porta, retornando um shell a quem se conectar;
- Configurações específicas em ”daemons” como inetd ou xinetd;
- Modificações em códigos-fonte;
- Utilização de binários do sistema;
- Shellcodes com chamadas específicas de sistema. (Necessita nova exploração.)

Backdoors: Binários Isolados.

- Win32.BackOrifice;
- Win32.SubSeven;
- Win32.Kuang2;
- Variantes de implementações de SSH.

Backdoors: Configurações de Aplicações.

inetd

```
1  echo "1010 stream tcp nowait root \
2  /usr/sbin/tcpd /bin/sh" >> /etc/inetd.conf
```

xinetd

```
1  cat >> /etc/xinetd.conf << EOF
2  service ftp
3  {
4          protocol                = tcp
5          wait                    = no
6          only_from               = 0.0.0.0/0
7          user                    = root
8          server                  = /bin/sh
9  }
10 EOF
```

Backdoors: Modificações Código-fonte.

Libpcap: (Original)

```
1 MD5 Sum 0597c23e3496a5c108097b2a0f1bd0c7 libpcap-0.7.1.tar.gz
2 MD5 Sum 6bc8da35f9eed4e675bfdf04ce312248 tcpdump-3.6.2.tar.gz
3 MD5 Sum 03e5eac68c65b7e6ce8da03b0b0b225e tcpdump-3.7.1.tar.gz
```

Libpcap: (Com Backdoor)

```
1 MD5 Sum 73ba7af963aff7c9e23fa1308a793dca libpcap-0.7.1.tar.gz
2 MD5 Sum 3a1c2dd3471486f9c7df87029bf2f1e9 tcpdump-3.6.2.tar.gz
3 MD5 Sum 3c410d8434e63fb3931fe77328e4dd88 tcpdump-3.7.1.tar.gz
```

Backdoors: Modificações Libpcap.

- Inserção do bpf ”not port 1963”;
- Conexão na porta 1963 de um determinado host;
- Abertura de um **shell reverso**.
- http://www.hlug.org/trojan/

Evolução de Backdoors

- Os backdoors surgiram de necessidade de **atacantes que precisavam voltar ao sistema comprometido** sem necessitar explora-los novamente.
- Com isso, o atacante poderia **eliminar a vulnerabilidade utilizada** na primeira exploração. Desta forma não permitindo que novos atacantes entrassem no sistema pela mesma vulnerabilidade.
- Entretanto, a difusão de sistemas de filtragem de pacotes de entrada dificultaram a utilização destes backdoors.

Evolução de Backdoors

- Com filtragem de pacotes de entrada, duas possibilidades eram possíveis:
  - Modificar o serviço legítmo por um backdoor;
  - Fazer o backdoor acessar o host externo em uma dada porta. Assim, a máquina comprometida seria cliente da máquina invasora. Esta técnica é chamada de ”shell reverso”.
- Entretanto, usuários perceberiam a troca do serviço e filtragem de pacotes de saída poderiam não permitir que a máquina atacada acessasse qualquer host em qualquer porta.

Evolução de Backdoors

- Os sistemas de filtragem de saída (outbound) aliados a proxies de saída de aplicação, fizeram com que os backdoors precisassem de características peculiares como respeitar um determinado protocolo de troca de dados.
- Surgem os softwares capazes de utilizar canais dissimulados.

- São mecanismos capazes de, utilizando-se **canais de comunicação legítmos**, trafegar **informações ilícitas**;
- Por exemplo, fazer com que um protocolo de P2P, proibido segundo a política de segurança de uma empresa, seja encapsulado sobre um outro protocolo permitido;
- Os canais dissimulados geralmente são criados sobre protocolos como **ICMP**, **HTTP**, **HTTPS** e **DNS**.

Canais Dissimulados: Ferramentas

- rwwwshell;
- CCTT;
- Wsh;
- Firepass;
- Httptunnel;
- Your Freedom;
- LogMeIn.

Canais Dissimulados: rwwwshell

- *The Reverse WWW Shell* é composto por scripts Perl que permitem que o cliente se conecte no servidor requisitanto por comandos;
- O modo de atuação é por shell reverso;
- Pode funcionar através de qualquer filtro de pacotes que permita que usuários acessem servidores Web de forma irrestrita;
- Os comandos são enviados através de mensagens do tipo GET ou POST.

Canais Dissimulados: cctt

- O *covert channel tunneling tool* permite a criação de canais dissimulados para protocolo HTTP;
- Pode atual também como um backdoor em qualquer porta UDP ou TCP;
- Atua por iniciativa do cliente que disponibiliza um shell reverso;
- Permite a troca de dados utilizando criptografia.

Canais Dissimulados: cctt

- As requisições de clientes são realizadas através de POST.
- Pode ser utilizado em comunicações onde exista proxy HTTP.
- Permite a criação de túneis para outros protocolos:
  - Cliente ssh - cliente cctt - Internet - servidor cctt - servidorssh.

Canais Dissimulados: Wsh

- Permite a criação de canais dissimulados em HTTP/HTTPS;
- O cliente executa scripts Perl. Já o servidor possui um servidor web com um CGI instalado;
- Neste caso o cliente possui o controle de requisições no servidor;
- Os comandos wshget e wshput permitem baixar ou enviar arquivos do ou para o servidor.

Canais Dissimulados: Firepass

- Desenvolvido para que seja possível encapsular outros protocolos de aplicação;
- Dois scripts, sendo um CGI que executa em um servidor Web;
- Pode funcionar mesmo através de um proxy;
- Muito utilizado para fazer com que o cliente acesse aplicações externas;

Canais Dissimulados: Httptunnel

- Possui o mesmo objetivo do Firepass;
- Dois scripts htc (cliente), hts (servidor);

```
1  server# htps -F 192.168.0.1:1010 80
2  client# htpc -F 10000 192.168.0.1:80
```

Canais Dissimulados: Your Freedom

- Trabalha em três métodos: Local port forward, Socks 4/5, Proxy HTTP;
- Implementa canais dissimulados sobre HTTP/HTTPs com os seguintes objetivos:
  - Contornar firewalls, proxies, e filtros de conteúdo.
  - Manter o anonimato do usuário.

Canais Dissimulados: Your Freedom

- O Your Freedom, instalado na máquina do cliente, conecta a servidores Freedom externos para estabeleçer canais dissimulados e encapsular dados de:
  - HTTP;
  - IM (MSN, Y!, ICQ, IRC, Skype, Teamspeak 2);
  - P2P (eMule, Kazaa, Bittorrent, ...)
  - Jogos;
  - E-mail (Thunderbird);
  - Multimedia (Realplayer, Winamp 5);
  - FTP;
  - SSH;
  - ....

Referências Bibliográficas


Rik Farrow
Musings.
;login: The Usenix Magazine, out. 2004


Mudge
Insider Threat.
;login: The Usenix Magazine, dez. 2003


Van Hauser.
The Reverse WWW Shell. The Hacker's Choice.
http://www.thc.org/download.php?t=r&d=rwwwshell-2.0.pl.gz

Referências Bibliográficas

Van Hauser

Placing Backdoors Through Firewalls. The Hacker's Choice.

http://www.thc.org/download.php?t=p&d=fw-backd.htm

Simon Castro

CCTT - Cover Channel Tunneling Tool

http://www.gray-world.net/pr_cctt.shtml

Alex Dyatlov and Simon Castro

Wsh - Web Shell. Gray World.net Team.

http://www.gray-world.net/pr_wsh.shtml

Referências Bibliográficas

Alex Dyatlov
Firepass. Gray World.net Team.
http://www.gray-world.net/pr_firepass.shtml

Lars Brinkhoff
Httptunnel. NoGrew.org.
http://www.nocrew.org/software/httptunnel.html

Craig H. Rowland
Covert Channels in the TCP/IP Protocol Suite. First Monday.
http://www.firstmonday.dk/issues/issue2_5/rowland/

Referências Bibliográficas

Carlos Henrique Peixoto Caetano Chaves and Antonio Montes
Backdoors e Canais Dissimulados: uma metodologia para detecção.
Simpósio sobre Segurança em Informárica (SSI'2004)

Contatos

Luiz Otávio Duarte
loduarte@cenpra.gov.br
duarte@lac.inpe.br

Carlos Henrique Peixoto Caetano Chaves
ccaetano@visanet.com.br

Antonio Montes
antonio.montes@cenpra.gov.br