Chkrootkit
10 anos de rootkits

Nelson Murilo
<nelson@pangeia.com.br>

Rootkit

Definição

Código ou conjunto de códigos usados, após uma invasão, para ocultar a presença do invasor na máquina da vítima

Rootkit
histórico

1989 – Publicação na Phrack Magazine de códigos para esconder a presença de invasores

1994 – Rootkits são mencionados em alertas do CERT

1995 – Pacote denominado *RootKit* torna-se popular entre invasores

1997 – Referências a LKM maliciosos

– Criação do Chkrootkit

Rootkit

1ª geração:

- Sistemas alvo
  - `SunOS e Linux`
- Substituição de comandos básicos
  - `ls, ps, login, find, etc.`
- Retirada das entradas do invasor do *wtmp*
- Uso de arquivos de configuração

Rootkit

2ª geração:

- Sistemas alvo
  - SunOS, Linux, *BSD e Mac OS X
- Inclusão de comandos próprios
  - backdoors, ataques a terceiros (DoS, enumeração, varredura, exploração)
- Manipulação do inetd ou xinit
  - binário e arquivos de configuração

Rootkit

3ª geração:

- 1ª e 2ª geração
- Uso de LKMs maliciosos
- Propagação via Worms

Rootkit

Características gerais

- Código fonte geralmente disponível
- Usualmente roda com opções *default*
- Objetivos
  - Ataques a terceiros
  - Bots de IRC
  - Armazenamento de arquivos

Chkrootkit

Motivações:

- Em 1997 diversos servidores analisados apresentavam os mesmos sinais de invasão
- Então os mesmo comandos eram constantemente repetidos
- E então o processo foi sendo automatizado

Chkrootkit

Premissas para desenvolvimento:

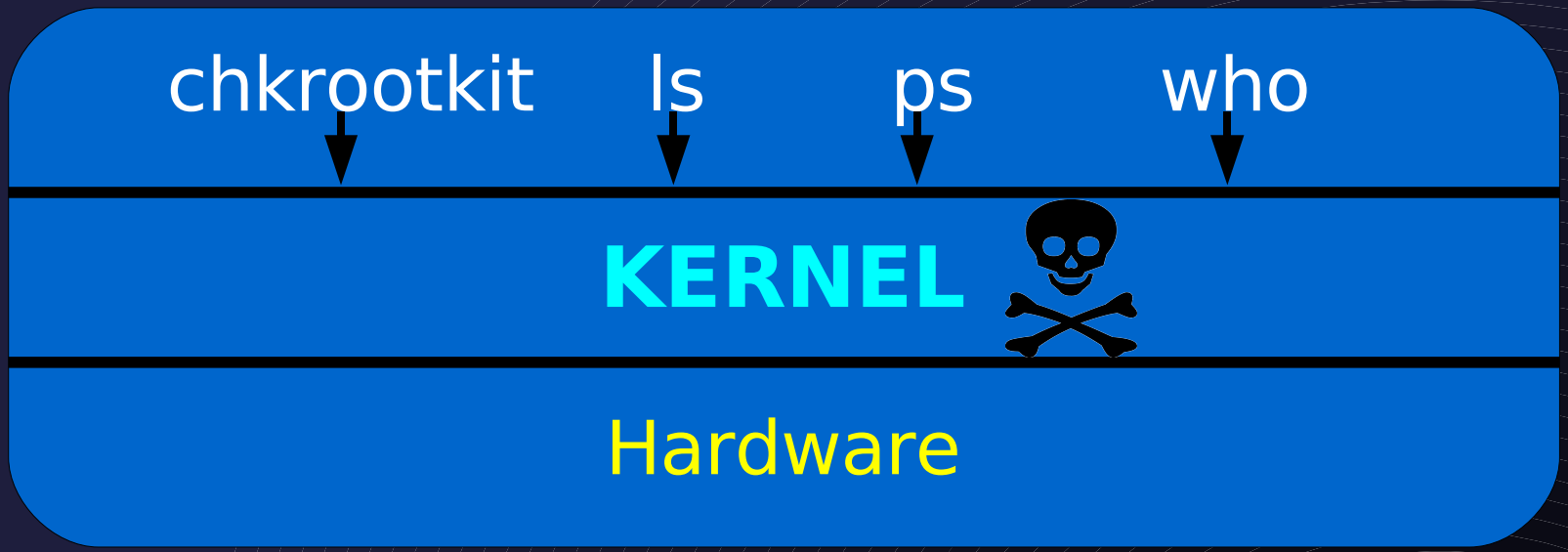
- Fácil de instalar e utilizar
- De fácil entendimento p/ facilitar contribuições
- Menor número de dependencias possível
- Alta portabilidade
- Escrito em linguagens de fácil portabilidade
  - Posix Shell
  - C Ansi

Chkrootkit

LEMBRETE

Chkrootkit roda em ***userspace***

Chkrootkit



Chkrootkit

O que é

- Verifica localmente sinais de rootkit instalado
- Roda em tempo real
  - Assim como a maior parte dos HIDS
- Roda em modo “*port mortem*”
  - Uso em forense computacional

Chkrootkit

verificações

- Módulos de kernel maliciosos
- Binários comprometidos
- Arquivos e diretórios suspeitos
- Portas e serviços suspeitos
- Processos suspeitos

Chkrootkit

Verificações

Processos

- portas suspeitas já conhecidas
- processo associado a um tty, mas não presente no arquivo wtmp
- Dono e grupo diferentes do esperado para um determinado processo

Chkrootkit

Verificações

Binários

- Assinaturas de rootkits conhecidos
- Existência de executáveis ou permissão não esperada
- Dono do programa que está rodando (limitado ao inetd.conf)

Chkrootkit

Verificação

LKM

- Limitado ao Linux e FreeBSD (<6.x)
- Examina */dev/kmem*
- Compara saída do *ps* e as entradas em */proc* (chkproc.c)
- Discrepância entre o contador de links e o número de diretórios visíveis (chkdirs.c)
- Verifica serviços e portas suspeitas

Chkrootkit

Uso em tempo real

Vantagens

- Pode verificar programas em uso
- Pode verificar portas e servidos ativos
- Pode verificar alguns LKMs em ação

Chkrootkit

Uso em tempo real

Principal desvantagem

- Alguns LKMs e códigos maliciosos em área de kernel podem passar desapercebidos

Chkrootkit

Utilização em modo *post morten*

Vantagem

Detecta mais facilmente LKMs e códigos maciliosos que rodam em área de kernel

Desvantagem

Naturalmente são perdidas as informações sobre processos e conexões ativas

Chkrootkit

Versão atual (0.47) detecta:

- 42 tipos de Rootkits e variações
- 13 Worms
- 5 LKM maliciosos

Chkrootkit

Versão 0.47

```
$ wc -l chkrootkit *.c
  2684 chkrootkit
   206 check_wtmpx.c
   258 chkdirs.c
   292 chklastlog.c
   370 chkproc.c
   210 chkutmp.c
    96 chkwtmp.c
   373 ifpromisc.c
   115 strings.c
  4604 total
```

#63 chkrootkit : Locally checks for signs of a rootkit

chkrootkit is a flexible, portable tool that can check for many signs of rootkit intrusion on Unix-based systems. Its features include detecting binary modification, utmp/wtmp/lastlog modifications, promiscuous interfaces, and malicious kernel modules.

See all rootkit detectors

#64 SPIKE Proxy : HTTP Hacking

↓15

Spike Proxy is an open source HTTP proxy for finding security flaws in web sites. It is part of the Spike Application Testing Suite and supports automated SQL injection detection, web site crawling, login form brute forcing, overflow detection, and directory traversal detection.

See all application-specific scanners

#65 OpenBSD : The Proactively Secure Operating System

↓14

OpenBSD is one of the only operating systems to treat security as their very highest priority. Even higher than usability in some cases. But their enviable security record speaks for itself. They also focus on stability and fight to obtain documentation for the hardware they wish to support. Perhaps their greatest achievement was creating OpenSSH. OpenBSD users also love [pf], their firewall tool.

See all security-oriented operating systems

Chkrootkit

O que está por vir?

- Manter atualização em relação à evolução dos sistemas e dos ataques
- Porte para outros sistemas baseados em Unix (AIX, por exemplo)
- Reformulação do projeto (baseado em arquivos de configuração)
- Estudo de novos ambientes (PDA, celular?)

Chkrootkit

Chkrootkit em ação!

Chkrootkit

10 anos de rootkits

http://www.chkrootkit.org

Nelson Murilo
<nelson@pangeia.com.br>