Segurança em Ambiente Linux

Uma visão geral das tecnologias, ferramentas e abordagens utilizadas na área de segurança do Sistema Operacional Linux

Parte II:

Cenários de ataque e principais ferramentas de segurança

Ademar de Souza Reis Jr.
<ademar@conectiva.com.br>
http://www.ademar.org

XII Congresso C. Computação Bolívia
Tarija – Bolívia – Outubro 2005

última versão atualizada disponível em
http://www.ademar.org/

Conteúdo

- Cenários e ferramentas de ataque
  - Portscans
  - Sniffers
- Principais tecnologias e ferramentas de segurança
  - Segurança física
  - Criptografia
  - Autenticação e login (PAM, Kerberos)
  - POSIX ACLs
  - Filtro de pacotes (firewall)
  - Detecção de vulnerabilidades, vírus e intrusões
  - Logs
- Dicas para (man)ter um sistema seguro

Portscan: Nmap

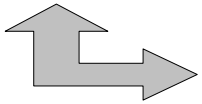
- Poderosa ferramenta de varredura de portas
- Detecção de SO e uptime (TCP/IP Fingerprinting)
- Detecção de versão de serviços (Service Fingerprinting)
- Varredura “stealth” (invisível ou com origens falsas)
- **Cuidado:** sua utilização, mesmo que para testes, geralmente é recebida como uma tentativa de ataque se detectada pela máquina alvo

Portscan: Nmap

Exemplos de uso

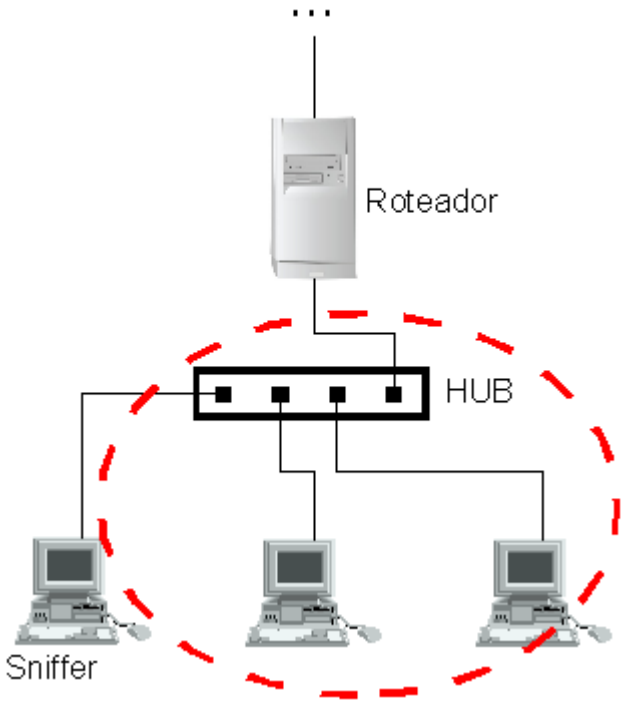
```
[root@optimus64 root]# nmap -sV -O localhost

Starting nmap 3.93 ( http://www.insecure.org/nmap/ ) at 2005-10-18 22:35 UTC
Interesting ports on localhost.localdomain (127.0.0.1):
(The 1655 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE  VERSION
21/tcp   open  ftp      ProFTPD 1.2.9
22/tcp   open  ssh      OpenSSH 3.8.1p1 (protocol 1.99)
80/tcp   open  http     Apache httpd 2.0.49 ((Unix) mod_ssl/2.0.49 OpenSSL/0.9.7c DAV/2)
111/tcp  open  rpcbind  2 (rpc #100000)
443/tcp  open  ssl/http Apache httpd 2.0.49 ((Unix) mod_ssl/2.0.49 OpenSSL/0.9.7c DAV/2)
633/tcp  open  rquotad  1-2 (rpc #100011)
670/tcp  open  mountd   1-3 (rpc #100005)
2049/tcp open  nfs      2-4 (rpc #100003)
Device type: general purpose
Running: Linux 2.4.X|2.5.X|2.6.X
OS details: Linux 2.5.25 - 2.6.3 or Gentoo 1.2 Linux 2.4.19 rc1-rc7), Linux 2.6.3 – 2.6.8
Uptime 0.045 days (since Sat Oct 15 19:06:57 2005)

Nmap run completed -- 1 IP address (1 host up) scanned in 14.995 seconds
[root@optimus64 root]#
```

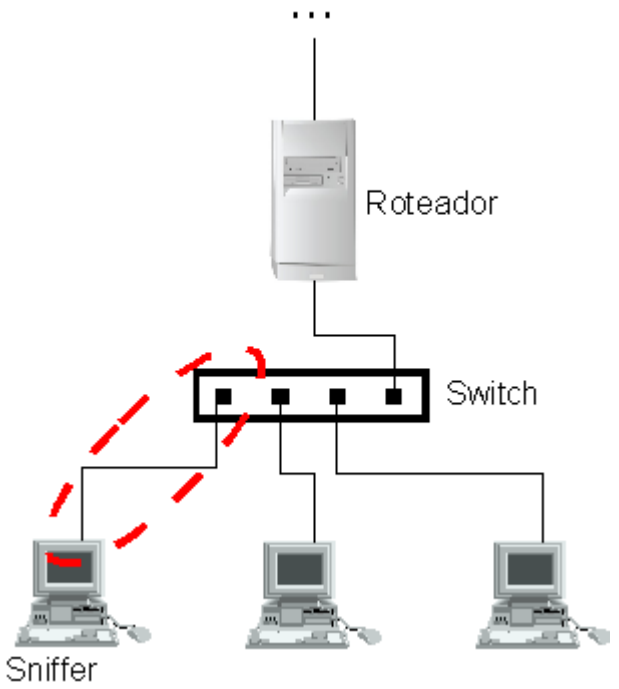
```
[root@optimus64 root]# nmap -sX localhost -p 22 -D 192.168.100.1,ademar.org,conectiva.com.br
```



Nos logs, aparecerão quatro origens do portscan. Reação automática --> “tiro no pé”

Sniffers: cenários



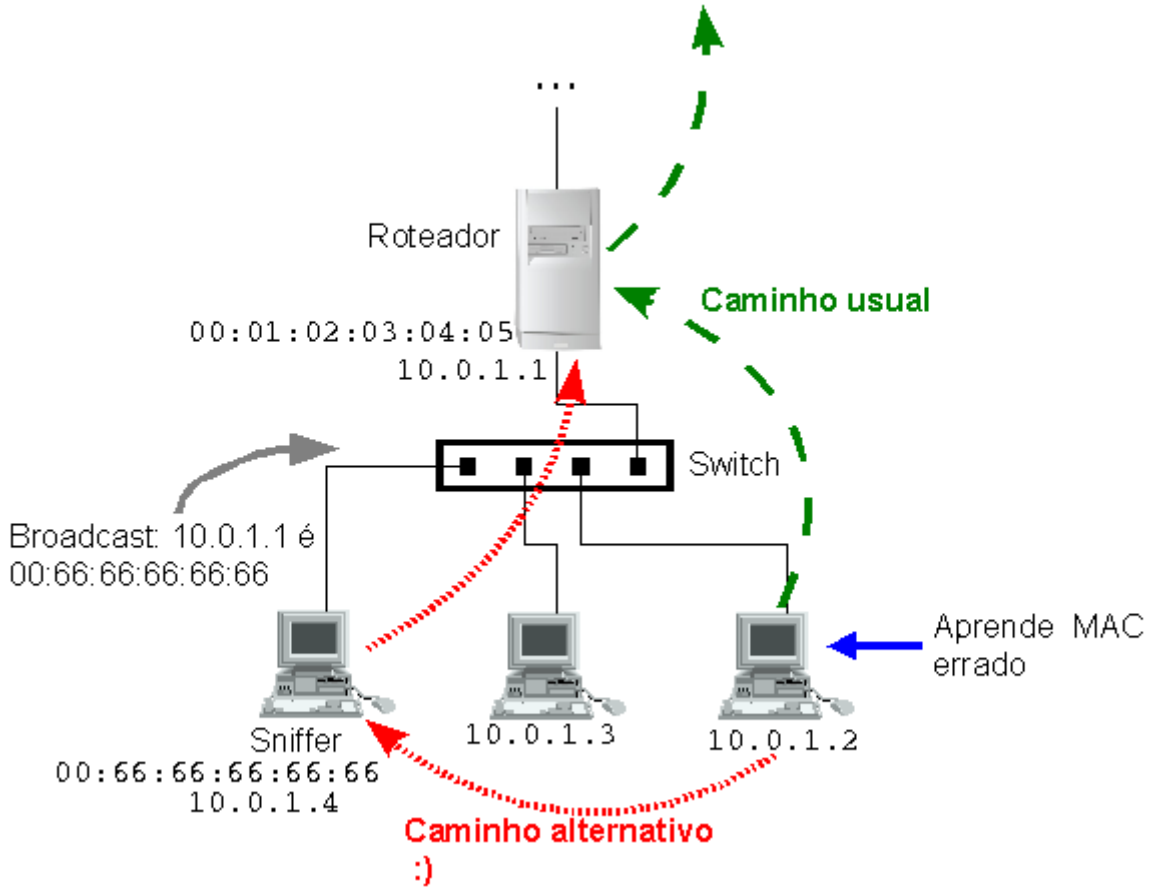


- **HUB:** todo o tráfego da rede é visível
- **Switch:** a visibilidade do tráfego é limitada a própria máquina

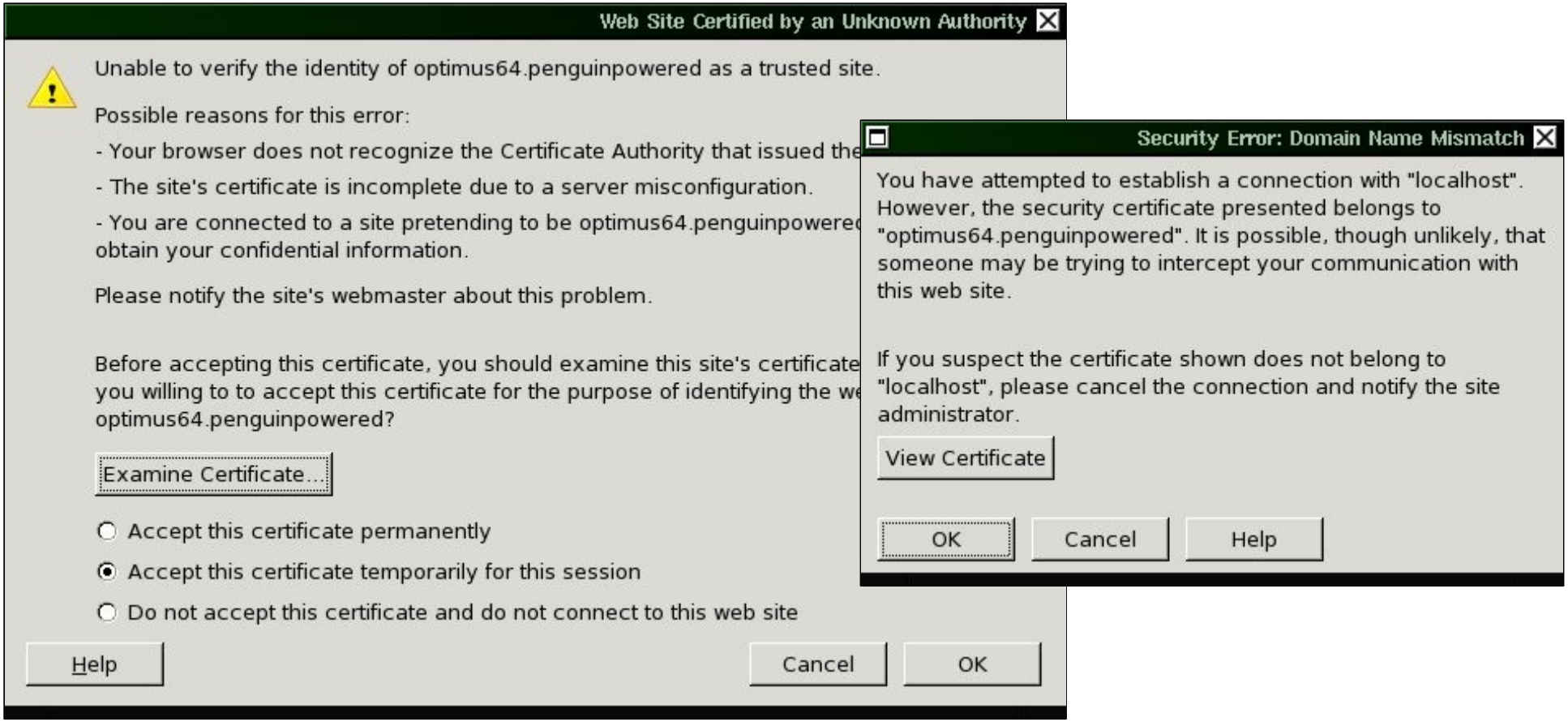
Estou protegido usando switches?

Sniffers: spoofing

Sniffers com poderes Jedi



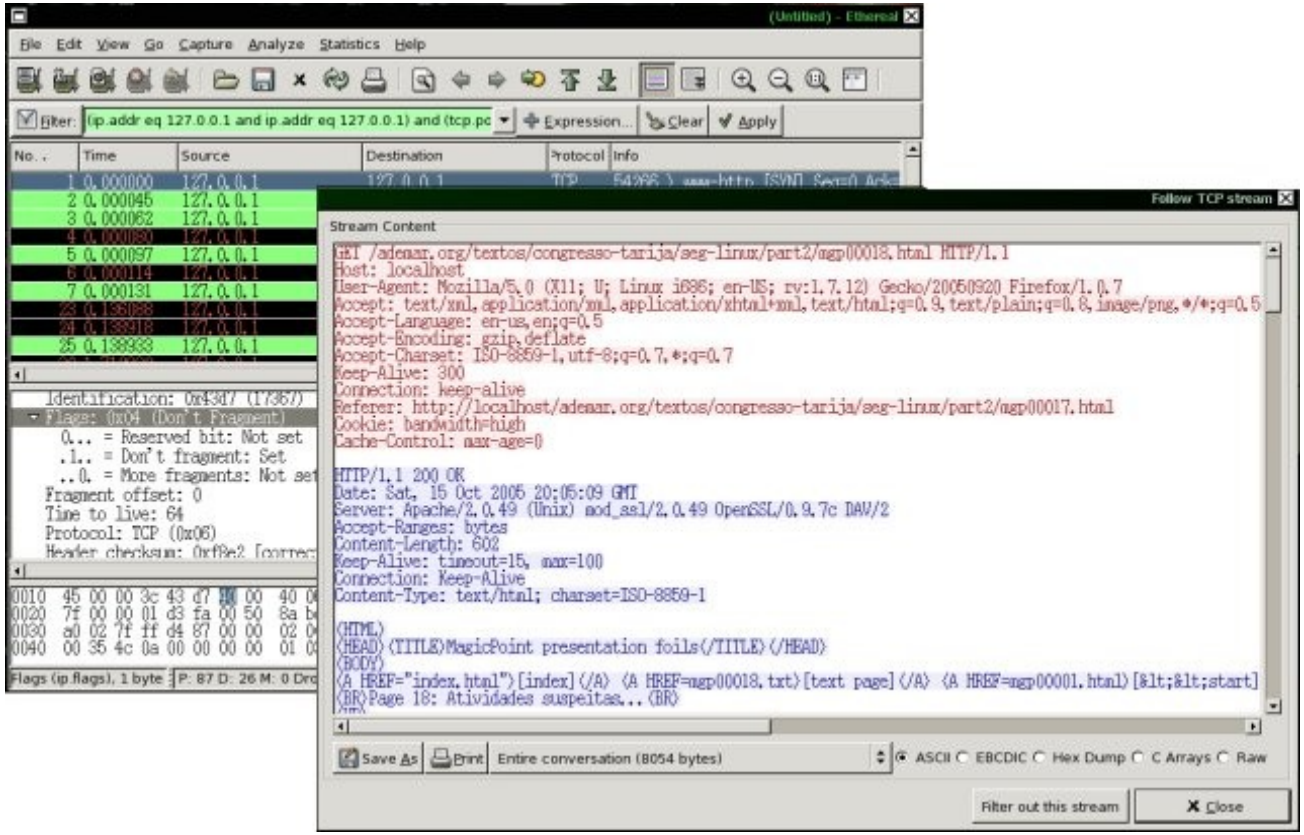
Sniffers: spoofing



Jedi do lado negro da força não é páreo para uma verificação de um certificado SSL

Sniffers: Ethereal

Sniffer gráfico, muito utilizado como ferramenta de desenvolvimento, depuração e testes



Sniffers: dsniff

Coleção de ferramentas que implementam diversas técnicas de sniffing

- dsniff
- webspy
- tcpkill
- arpspoof
- dnsspoof
- webmitm
- ...

```
WEBSPY(8)                                                       WEBSPY(8)

NAME
       webspy - display sniffed URLs in Netscape in real-time

SYNOPSIS
       webspy [-i interface] host

DESCRIPTION
       webspy  sends URLs sniffed from a client to your local Netscape browser
       for display, updated in real-time (as the target  surfs,  your  browser
       surfs along with them, automagically). Netscape must be running on your
       local X display ahead of time.

OPTIONS
       -i interface     Specify the interface to listen on.

       host             Specify the web client to spy on.

SEE ALSO
       dsniff(8)

AUTHOR
       Dug Song <dugsong@monkey.org>
```

Segurança física

Se o atacante tem acesso físico à máquina, o controle total é uma **questão de tempo**

Uma boa configuração causará um **atraso** no ataque

- **BIOS**
  - Habilitar boot apenas pelo disco principal
  - Senha
- **Bootloader (grub, lilo)**
  - Senha de boot
  - Senha para edição de opções
- **Criptografia no sistema de arquivos**
  - Por partição
  - Lento (overhead de leitura/escrita)
  - E o swap?

Criptografia

- **Tecnologias**
  - OpenSSL implementa dezenas de algoritmos
  - O tamanho da chave não é o mais importante
  - Não confie em algoritmos fechados
  - Descobertas de ataques recentes: estamos em perigo?
- **No Sistema de Arquivos**
  - Linux Crypto HOWTO (chapter 4)
  - Cryptoloop HOWTO
- **Arquivos e e-mail**
  - GNUPG (gpg)
  - Há inúmeros frontends para o gpg
- **Rede**
  - **VPNs:** OpenVPN, stunnel, FreeSwan
  - Preferir https para serviços web

Autenticação: PAM

Pluggable Authentication Modules

- Aplicação desconhece a forma de autenticação usada (LDAP, Samba, /etc/passwd, etc)
- Atualmente PAM é amplamente utilizado no Linux, mas ainda existem programas sem o devido suporte
- Módulos são configurados em `/etc/security/`
- Programas são configurados em `/etc/pam.d/`

Autenticação: PAM

Exemplo de configuração

```
#/etc/pam.d/login
#%PAM-1.0
auth       required    /lib/security/pam_nologin.so
auth       required    /lib/security/pam_securetty.so
auth       sufficient  /lib/security/pam_unix.so shadow nullok
auth       required    /lib/security/pam_ldap.so use_first_pass
account    sufficient  /lib/security/pam_unix.so
account    required    /lib/security/pam_ldap.so
password   required    /lib/security/pam_cracklib.so
password   sufficient  /lib/security/pam_unix.so nullok use_authtok md5 shadow
password   required    /lib/security/pam_ldap.so use_first_pass
session    optional    /lib/security/pam_console.so
session    sufficient  /lib/security/pam_unix.so
session    required    /lib/security/pam_ldap.so
session    required    /lib/security/pam_limits.so
```

Teste prático com pam_limits

Autenticação: Kerberos

- **Single Sign On**

  “quero informar minha senha apenas uma vez”

- **Interoperabilidade com dezenas de serviços**
  - OpenSSH
  - Samba
  - Clientes de e-mail
  - Web
  - etc

Firewall: iptables

- **Stateful Packet Filtering**

  “só quero que entrem respostas a algo que eu pedi”

- **Dezenas de módulos/extensões**
  - **owner:** regras com base no usuário que gerou o pacote
  - **limit:** regras com base na quantidade/frequência de pacotes

- **Dezenas de frontends**
  - Tecnologia madura, inúmeros frontends
  - Integração com diversos programas

Anti-virus

“Não existe vírus pra linux”
Mito ou realidade?

- **Clam Anti-Virus (Clamav)**
  - Fácil integração com postfix (MTA/servidor de e-mail)
  - Banco de dados livre, atualizado com frequência
- **Soluções proprietárias**

Detecção de intrusão

- **Snort**
  - Leve e poderoso NIDS (Network Intrusion Detection System)
  - Base dinâmica disponível na internet
  - Geralmente exige um tempo de ajuste para evitar falsos-positivos
  - Principal frontend: ACID
- **AIDE**
  - Verificação de integridade do sistema de arquivos
- **ARPwatch**
  - Detecta alterações na tabela ARP

Cuidado com falsos positivos e reação automática

Logs do sistema

- **`/var/log`**
  - Praticamente todos os programas geram logs
  - `/var/log/messages`: principal log do sistema
- **Servidor de logs**
  - Logs em outra máquina ou mesmo impressora
  - Conexão via IP, serial, porta paralela, etc
  - Máquina deve ser 100% dedicada, nenhum outro serviço
- **Cuidados**
  - Flood de mensagens falsas
  - Consumo de CPU
  - Dificuldade em analisar muitos logs

Dicas e receitas

Tecnologias e cuidados para (man)ter um sistema seguro

- Desabilite serviços não essenciais
- Isole as redes com múltiplos firewalls
- Mantenha tudo sempre atualizado
- Proteja o sistema em múltiplos níveis (redundância)
- Comece com tudo bloqueado, liberando apenas o necessário
- Utilize detectores de intrusão
- Lembre-se de outros fatores de segurança, principalmente o humano

Para saber mais...

- Projetos: Nmap, dsniff, Ethereal, Snort, Nesus, Iptables, OpenSSH, OpenSSL, OpenVPN, Kerberos 5 (MIT), SASL, PAM, AIDE.
- Simson Garfinkel and Gene Spafford. Practical Unix and Internet Security (Second Edition). ISBN 1-56592-148-8.
- Phrack: http://www.phrack.org
- CERT: http://www.cert.org
- Google: http://www.google.com :-)