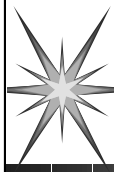


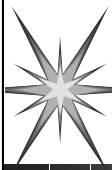
Curso de Segurança de Sistemas Unix e Redes

Marcos Aguinaldo Forquesato
Equipe de Segurança em Sistemas e Redes
Centro de Computação
UNICAMP

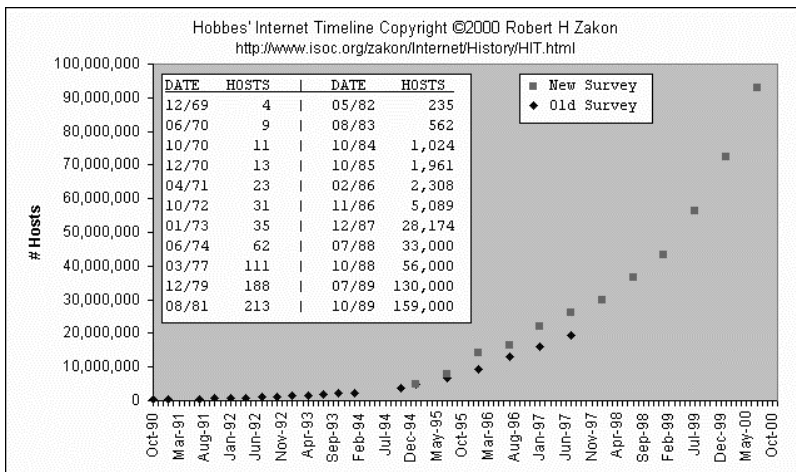


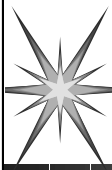
Tópicos

- Introdução
- Políticas de segurança
- Segurança Física
- Hardening
- Vulnerability Scanners
- Criptografia **
- Autenticação
- PKI: Public Key Infrastructure
- Verificação de Integridade
- Monitoramento de logs
- Firewalls **
- IDS: Intrusion Detection Systems
- Arquitetura de rede
- Incidentes de Segurança
- Análise Forense



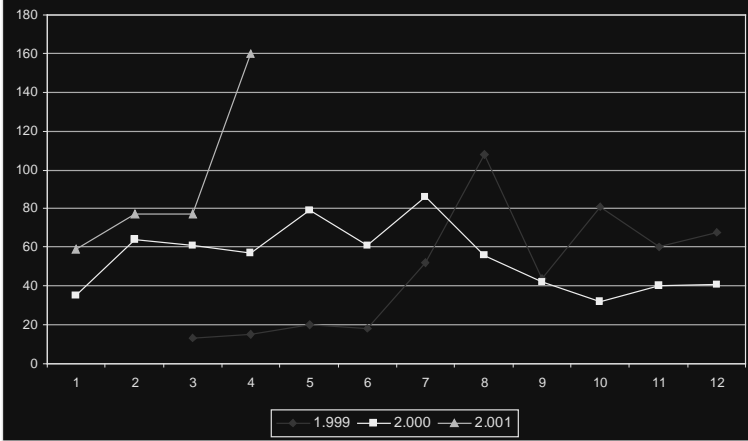
Por que você precisa de segurança?

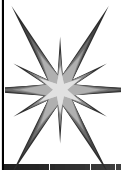




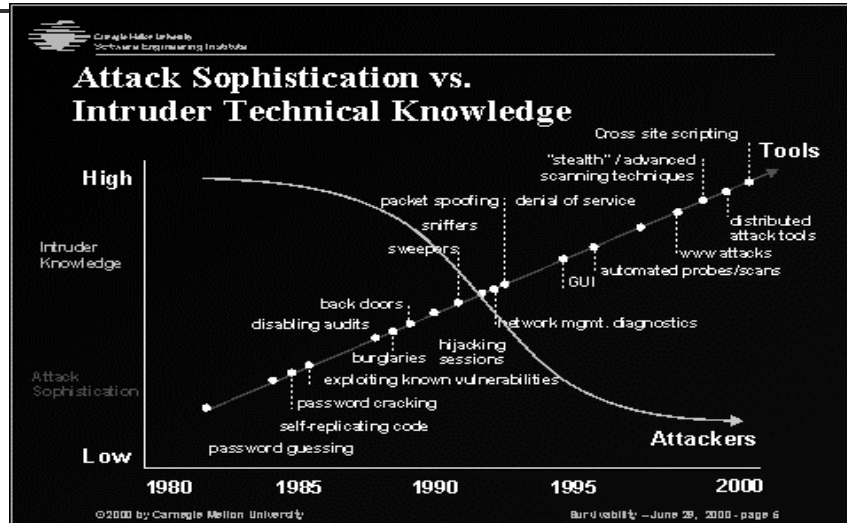
Incidentes envolvendo a UNICAMP

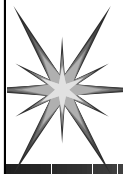
Incidentes de segurança (comparativo)





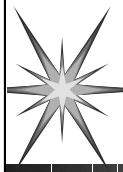
Attack vs. Knowledge





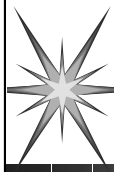
O que você está tentando proteger?

- ▶ Seus dados
 - ▶ Integridade
 - ▶ Privacidade
 - ▶ Disponibilidade
- ▶ Seus recursos
- ▶ Sua reputação



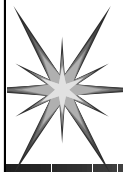
Contra o que você está tentando se proteger?

- ▶ Classes de Ataques
 - ▶ Roubo de senhas
 - ▶ Engenharia Social
 - ▶ BUG & Backdoors
 - ▶ Falha de autenticação
 - ▶ Falha de protocolo
 - ▶ Obtendo Informações
 - ▶ Negando serviços



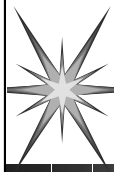
Por que nossos sistemas são vulneráveis?

- ▶ Pessoas destreinadas ou sem tempo para aprender e fazer as atividades
 - ▶ Conflito de demandas
 - ▶ “Quando o sistema estará no ar?”
 - ▶ “Mantenha o sistema funcionando!”
- ▶ Segurança Física X Seg. da Informação
- ▶ Falha em aspectos operacionais
 - ▶ “Você aplicou todos os patches?”
 - ▶ “Quando eu tiver tempo...”
- ▶ Qual é o preço de sua informação?



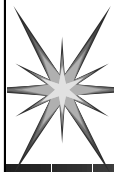
Por que os ataques tem sucesso? Top 10 by SANS

- ▶ Servidores conectados a internet antes de aprimorar a segurança
 - ▶ Remover os serviços desnecessários, aplicar os patches, etc.
- ▶ Default accounts/passwords
- ▶ Falta de atualização dos sistemas operacionais e produtos
- ▶ Uso de serviços não cifrados (telnet, ftp, etc)



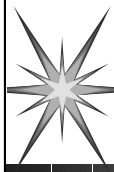
Por que os ataques tem sucesso? Top 10 by SANS (cont.)

- ▶ Envio de senhas via telefone ou email
- ▶ Falha nos backups (Teste os backups!)
- ▶ Execução de serviços desnecessários
- ▶ Erro de configuração de sistemas operacionais, produtos e Firewalls
- ▶ Falha na implementação de Antivirus
- ▶ Falha na educação dos usuários sobre o que fazer e quem procurar no caso de incidentes



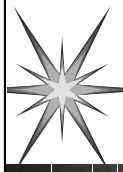
Políticas de segurança

- ▶ Estar ciente que o uso do parque computacional é regido por normas e portarias divulgadas e periodicamente atualizadas em <http://www.unicamp.br/cgi/portarias.html>.
- ▶ Assumir pessoalmente a responsabilidade por qualquer uso do parque computacional da Unicamp em discordância com tais normas ou portarias ou qualquer outra lei maior externa à Unicamp.



Segurança Física

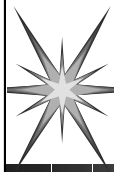
- ▶ Backups
- ▶ Plano de contingência
- ▶ Cadeados (xlock)



Hardening

- ▶ Atualizar sistema operacional e softwares
- ▶ Aplicar todos os patches
- ▶ Remover os serviços desnecessários
- ▶ Configurar softwares de segurança
- ▶ Instalar e atualizar antivírus
- ▶ Monitorar as logs diariamente **
- ▶ Segurança das senhas (senhas default)

Uma das maneiras mais fáceis de um intruso acessar um sistema é descobrindo a senha de algum usuário. Isto ocorre facilmente, visto que muitas instituições não verificam a segurança das senhas.



Hardening (cont.)

- ▶ Remova os suids desnecessários dos filesystems (locais e remotos)
- ▶ umask (027 ou 077)
- ▶ Montar filesystems read-only
- ▶ Network File System (NFS)
 - ▶ /etc/exports (-access)
 - ▶ Restrição de acesso para o root
 - ▶ nosuid/nodev

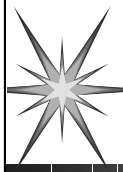
Normalmente o diretório /tmp possui acesso universal para gravação, permitindo que qualquer usuário remova arquivos pertencentes a qualquer outro usuário. Ativando o sticky bit no diretório /tmp, os usuários podem remover apenas seus próprios arquivos. Para ativar o sticky bit em um diretório, use o comando:

```
chmod o+t diretório
```

Ao criar um arquivo, normalmente todas as permissões são ativadas. Como isto raramente é o desejado, o valor do umask é usado para modificar o grupo de permissões com as quais um arquivo é criado. Ou seja, da mesma forma com que o comando chmod especifica quais bits devem ser ligados, o comando umask especifica quais bits devem ser desligados.

Para impedir a criação acidental de arquivos com permissão 777, deve-se usar o seguinte comando nos arquivos .login ou .profile:

```
umask 027
```



Hardening (cont.)

- Checklists diários
 - /etc/passwd (formato/conteúdo)
 - arquivos suid/sgid
 - arquivos sem dono
 - .rhosts
- Ativar o account

A segurança de dispositivos é uma questão importante em sistemas Unix. Arquivos de dispositivo são usados por vários programas para acessar dados nos discos rígidos ou na memória. Se estes dispositivos não estão devidamente protegidos, o sistema está vulnerável a ataques. A lista completa de dispositivos é muito grande e varia de sistema para sistema. Em linhas gerais, as seguintes normas se aplicam:

Os arquivos /dev/kmem, /dev/mem e /dev/drum não devem ter permissão de leitura universal.

Os dispositivos de disco, tais como /dev/sd0a, /dev/rx1b, etc., devem pertencer ao usuário root e grupo operator, e devem possuir modo 640.

Com raras exceções, todos os outros dispositivos devem pertencer ao usuário root.

Uma destas exceções são os terminais, que pertencem ao usuário que o estiver utilizando no momento. Ao desconectar-se, o terminal volta a pertencer ao root.

O comando *showmount* pode ser usado em um servidor NFS para exibir o nome de todas as máquinas que estão montando alguns de seus diretórios. Se executado sem opções o programa simplesmente exibe uma lista de todos os computadores.

A opção *-a* faz com que o comando *showmount* liste todos as combinações de computadores e diretórios:

```
% showmount -a
```

```
apoio.unicamp.br:/pub/pub6/linux/slackware/slakware
```

```
aracati.unicamp.br:/home
```

```
atlanta.unicamp.br:/usr/local
```

A opção *-d* faz com que seja exibida uma lista de todos os diretórios que estão montados por alguma máquina. Deve ser verificado que apenas máquinas locais montem os diretórios exportados e que apenas diretórios normais estejam sendo montados.

```
% showmount -d
```

```
/home
```

```
/pub/pub6/linux/slackware/slakware
```

```
/usr/local
```

Verificar falhas de segurança no sistema de arquivos é outra tarefa importante do administrador. Primeiramente devem ser identificados os arquivos que podem ser alterados por usuários não autorizados, arquivos que podem involuntariamente dar permissões excessivas e arquivos que possam fornecer acesso a invasores. É importante também monitorar modificações no sistema de arquivos e possuir mecanismos que permitam a volta do sistema ao estado original.

O comando find tem como propósito geral pesquisar o sistema de arquivos. O comando

```
# find / -type f -a \( -perm 04000 -o -perm 02000 \) -print
```

localiza todos os arquivos do sistema com os bits setuid ou setgid ligados. A saída deste comando deve ser analisada para determinar se não existe algum arquivo suspeito na lista.

O comando

```
# find / -perm -2 -print
```

identifica todos os arquivos com permissão de escrita universal.

O comando

```
# find / -nouser -o nogroup -print
```

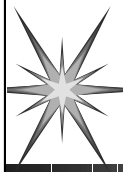
identifica arquivos que não pertencem a nenhum usuário ou a nenhum grupo. Imediatamente após a instalação de um sistema, deve-se gerar um arquivo que liste a configuração inicial dos arquivos do sistema:

```
# ls -aslgR /bin /etc /usr >> MasterChecklist
```

Este arquivo contém uma lista completa de todos os arquivos nestes diretórios. As linhas referentes a arquivos que mudem freqüentemente devem ser removidas do arquivo. O masterchecklist deve ser guardado em um local seguro para evitar adulterações. Para pesquisar alterações no sistema de arquivos, execute o comando acima novamente e compare-o com o arquivo mestre:

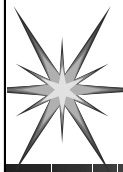
```
# diff MasterChecklist Currentlist
```

Outro aspecto muito importante é a realização de backups freqüentes do sistema de arquivos. Backups não apenas protegem contra falhas de hardware como contra deleções acidentais.



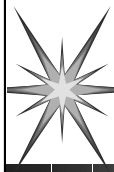
Hardening (cont.)

- ▶ Serviços
 - ▶ "r" commands -> SSH
 - ▶ lpd -> LPRng
 - ▶ NIS -> NIS+
 - ▶ NFS -> DFS
 - ▶ POP/IMAP -> POP/IMAP com SSL
 - ▶ Webmail -> Webmail com SSL



Ferramentas de Hardening

- TITAN - www.fish.com/~brad/titan/
- YASSP - www.yassp.org/
- Amoring -
www.enteract.com/~lspitz/linux.html
- TrustedBSD - www.trustedbsd.org/
- LIDS - www.lids.org
- Openwall - www.openwall.com
- SELinux - www.nsa.gov/selinux/

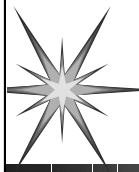


Sincronização de horários via NTP

► www.eecis.udel.edu/~ntp/

Network Time Protocol (NTP) é usado para sincronizar relógios de computadores e outros equipamento de rede a partir do padrão UTC (Universal Time Coordinated).

O UTC é baseado na rotação da Terra sobre seu eixo e no Calendário Gregoriano que é baseado na rotação da Terra em torno do Sol e possui um mecanismo de ajuste com o TAI ("International Atomic Time") pela inserção de segundos em intervalos de aproximadamente 18 meses.



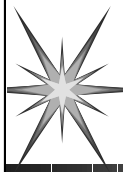
Vulnerability Scanners Host-Based

- ▶ Tripwire
- ▶ COPS/Tiger

COPS (Computer Oracle and Password System): Identifica riscos de segurança em sistema Unix. Verifica se o arquivo de senhas (/etc/passwd) está vazio, se existem arquivos com permissão de escrita para world, se o servidor de FTP anônimo está mal configurado, dentre outros.

Disponível em: <ftp://ftp.cert.org>

Tiger: Verifica vulnerabilidades de segurança em sistemas Unix. É muito parecido com o COPS porém possui mais recursos.



Vulnerability Scanners Network-Based

- ▶ SATAN (Security Administrator Tool for Analyzing Networks)
- ▶ ISS (Internet Security Scanner)
- ▶ Strobe
- ▶ Nmap
- ▶ Nessus **

Nessus: Audita remotamente uma rede, obtendo informações (tipo de máquinas, serviços oferecidos, etc), verificando suas vulnerabilidades e determinando se ela pode ser invadida.

Disponível em: <http://www.nessus.org>

ISS (Internet Security Scanner)

Disponível em: <http://www.iss.net>

SATAN (Security Administrator Toll for Analyzing Networks)

Disponível em: <ftp://ftp.win.tue.nl>

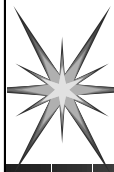
Strobe: Lista todas as portas ativas de um computador remoto.

Disponível em: <ftp://minnie.cs.adfa.oz.au>

Nmap: Ferramenta de varredura de portas de alta performance que além de mostrar os serviço disponíveis possui muitas outras características, tais como detecção remota do sistema operacional via impressão digital TCP (TCP fingerprint) e vários tipos e velocidades de varreduras.

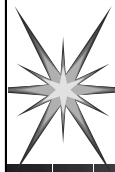
Disponível em : <http://www.insecure.org/nmap/>

Man : http://www.insecure.org/nmap/nmap_manpage-pt.html

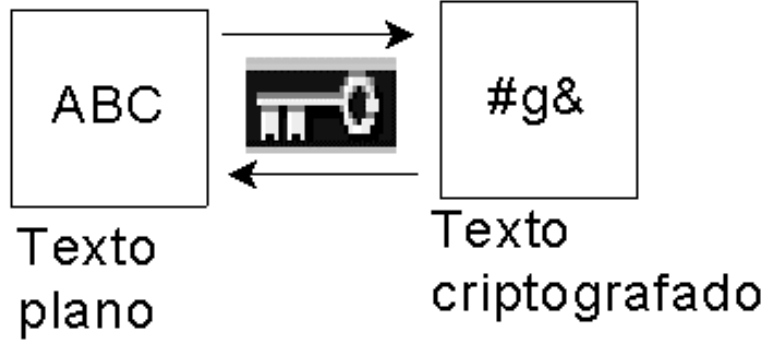


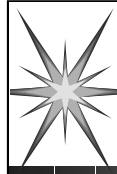
Conceitos de Criptografia

- ▶ Criptografia Simétrica
- ▶ Criptografia Assimétrica
- ▶ Certificação
- ▶ Assinatura Digital

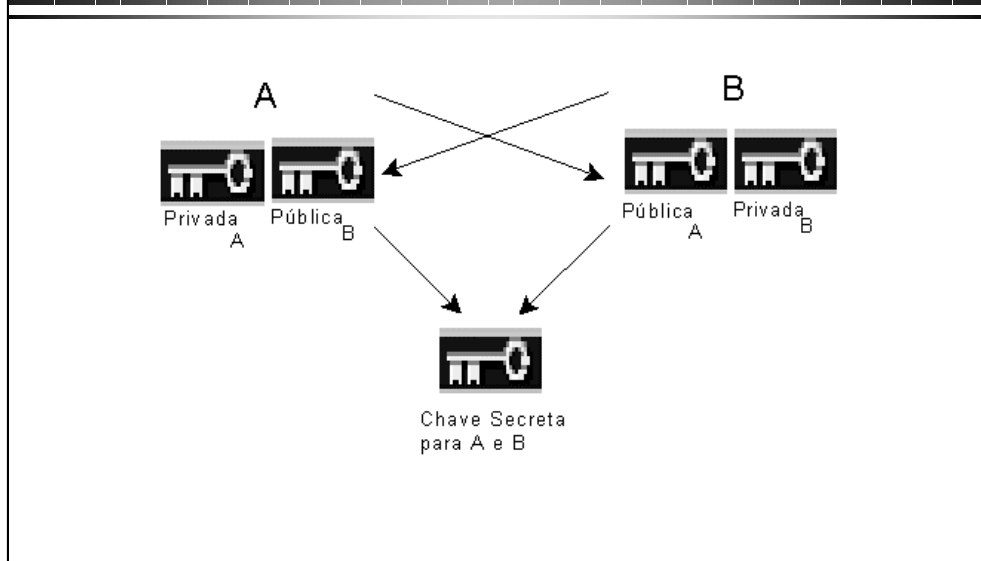


Criptografía Simétrica

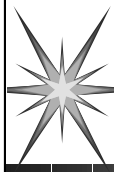




Criptografia Assimétrica



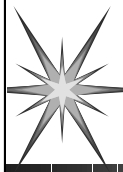
Os sistemas assimétricos e simétricos são complementares, o primeiro é empregado no processo de autenticação e ciframento de chaves de sessão, que são usadas por algoritmos simétricos para cifrar o fluxo de dados.



Certificação

- ▶ Verifica a chave pública
- ▶ Necessita de um terceiro elemento , conhecido como Autoridade Certificadora (CA)

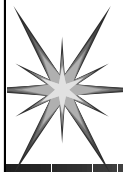
O Certificado de Identidade Digital é a versão eletrônica de sua cédula de identidade. Ele pode ser apresentado eletronicamente como prova de sua identidade.



Assinatura Digital

- ▶ Garante a autenticidade de um documento
- ▶ A chave pública pode usada para validar a assinatura digital

A Assinatura Digital é a versão digital da assinatura de punho em documentos físicos.



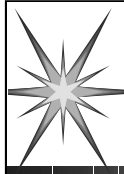
Ferramentas de criptografia

- ▶ SSH (Secure Shell) - www.freessh.org
- ▶ SSL (Secure Socket Layer) -
SSLtelnet/SSLftp
- ▶ PGP (Pretty Good Privacy) - gnupg

SSL (Secure Socket Layer) é um protocolo desenvolvido pela Netscape Communications para transferir informações de modo seguro na internet. Permitirá que o computador cliente se conecte ao servidor Web e, de forma transparente, será criado um canal de comunicação seguro entre o Site e o Cliente. Uma vez que esta conexão é feita, informações, como o número de cartões de crédito, poderão ser fornecidas sem que alguma outra pessoa possa interceptar os dados.

SSH (Secure Shell) é um programa para login remoto, execução de comandos remotamente e cópia de arquivos de uma máquina para a outra; com autenticação forte e comunicação segura.

PGP (Pretty Good Privacy) é um programa de criptografia de chave pública, amplamente usado na criptografia de correio eletrônico (email).



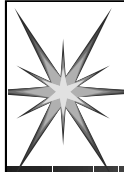
VPN (Virtual Private Networks)

- ▶ IPsec
- ▶ SKIP

IPsec: O principal objetivo é agregar conceitos de segurança (autenticação e privacidade) na camada IP. Uma das principais características desta arquitetura é manter a independência e modularidade entre os protocolos.

VPN: Se sua organização tem mais de um firewall em redes fisicamente isoladas através da Internet, você pode fazer uso de criptografia para criar um túnel IP cifrado entre as redes, criando uma rede de perímetro virtual (VPN)

SKIP (Simple Key Management for Internet Protocols): estrutura de gerenciamento de chaves, projetada para protocolos orientados a datagramas IP



IPSec (IP Security)

- ▶ AH (Authentication Header)
- ▶ ESP (IP Encapsulating Security Payload)
 - ▶ Mode de tunelamento (túnel IP) **

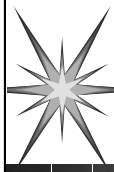


- ▶ Modo de transporte



O objetivo do AH (Authentication Header) é oferecer autenticação e integridade aos datagramas IP, a fim de obter o não repúdio da informação.

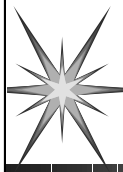
O objetivo do ESP (IP Encapsulating Security Payload) é oferecer privacidade ao conteúdo dos dados encapsulados em um datagrama IP, podendo oferecer também autenticação e integridade dependendo do algoritmo e do seu modo de operação.



Ferramentas de autenticação

- ▶ One-time passwords
 - ▶ Programa/Calculadora - Ex: S/Key (jotp)
 - ▶ Lista de senhas
- ▶ Smart Card - Ex : SecurID
- ▶ Biometria
 - ▶ impressão digital, geometria da mão, retina, íris, voz ou perfil da face, impressão vascular da mão, odores do corpo, etc.

SmartCard é um cartão com dimensões físicas de um cartão de crédito, equipado com um circuito eletrônico de um microcomputador mais um dispositivo anti-fraude.



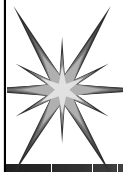
Ferramentas de autenticação

- ▶ Kerberos
- ▶ DCE
- ▶ PAM (Pluggable Authentication Modules)
 - ▶ pam_cracklib
 - ▶ pam_ldap
 - ▶ pam_mysql
 - ▶ pam_smb

Kerberos foi desenvolvido primordialmente visando a autenticação de requisições para acesso a recursos de rede. Fornece autenticação em tempo real num ambiente distribuído. Disponível em:
<ftp://ftp.ua.pt/pub/kerberos>

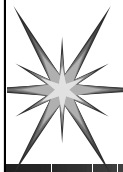
DCE (Distributed Computing Environment) é um ambiente integrado e modular que prove vários serviços, incluindo autenticação de usuários, remote procedure call, compartilhamento de arquivos e gerenciamento de sistemas (configuração).

PAM (Pluggable Authentication Modules) é um conjunto de bibliotecas que permitem ao administrador escolher como autenticar os usuários.



MAC times

- ▶ mtime = modification time
- ▶ atime = access time
- ▶ ctime = status change time
- ▶ dtime = deletion time (Linux)

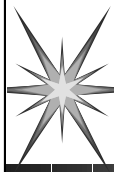


Ferramentas para verificação de integridade dos dados

- ▶ Tripwire - www.tripwire.com
- ▶ AIDE - www.cs.tut.fi/~rammer/aide.html

Tripwire: Checa a integridade de arquivos e diretórios, comparando os arquivos e diretórios atuais com a informação armazenada previamente em banco de dados.

Homepage : <http://www.tripwire.com>

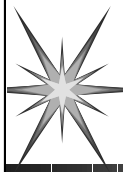


Diretórios

- ▶ Armazenar
 - ▶ contas
 - ▶ chaves
 - ▶ certificados
- ▶ LDAP (Lightweight Directory Access Protocol) - www.openldap.org **

O LDAP (Lightweight Directory Access Protocol) é um subconjunto do X.500 DAP.

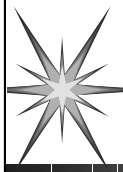
Um serviço de diretório é uma aplicação de base de dados distribuída, projetada para gerenciar atributos e disponibiliza-los através de uma rede TCP/IP.



Public Key Infrastructure (PKI)

- ▶ Autoridade certificadora
- ▶ Repositório de certificados
- ▶ Software cliente
- ▶ Links:
 - ▶ www.openca.org
 - ▶ oscar.dstc.qut.edu.au

Infra-estrutura de Chaves Públicas consiste de serviços, protocolos e aplicações utilizados para o gerenciamento de chaves públicas e certificados.



Ferramentas para monitoramento de logs

- ▶ Logcheck
- ▶ Logsurf
- ▶ swatch

Uma das tarefas do administrador de sistemas é a monitoração da segurança. Esta tarefa envolve o exame de arquivos de log para detectar acessos não autorizados, bem como a monitoração de falhas de segurança.

As contas devem ser monitoradas periodicamente de modo a verificar dois eventos: usuários que logam quando não devem (por exemplo, tarde da noite ou quando estão de férias) e usuários executando comandos que normalmente não deveriam usar.

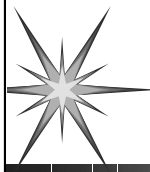
O arquivo `/usr/adm/lastlog` registra o login mais recente de cada usuário do sistema. A mensagem impressa no terminal a cada vez que um usuário loga

```
Last login: Sat Mar 10 10:50:48 from host.unicamp.br
```

utiliza a data armazenada no arquivo `lastlog`. A data do último login relatada pelo comando *finger* também usa estes dados. Os usuários devem ser alertados a inspecionar esta data para certificarem-se de que não foi efetuado nenhum acesso não autorizado às suas contas e, caso positivo, alertar o administrador de sistemas para o ocorrido.

O arquivo `/etc/utmp` é usado para registrar quem está logado no sistema no momento.

Para cada usuário é exibido o `userid`, o terminal sendo utilizado e o computador remoto (se o login foi efetuado via rede). O arquivo `/usr/adm/wtmp` registra as datas de login e logout de cada usuário.



Alguns arquivos importantes

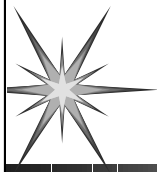
- ▶ `syslog`
- ▶ `messages`
- ▶ `suolog`
- ▶ `xferlog`
- ▶ `pacct`

O arquivo *wtmp* pode também ser examinado manualmente através do comando *last*. Este comando ordena as entradas no arquivo, relacionando os tempos de login e logout. Se invocado sem argumentos, o comando *last* exibe toda a informação contida no arquivo.

O arquivo *pacct* registra a execução de cada comando no sistema, quem o executou, quando e quanto tempo gastou. Esta informação é registrada cada vez que um comando é completado.

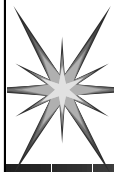
O arquivo *pacct* pode ser examinado através do comando *lastcomm*. Se invocado sem argumentos toda a informação do arquivo é exibida. O comando *lastcomm* aceita como argumentos o nome de um comando, de um usuário ou de um terminal.

O *syslog* é um mecanismo que permite que qualquer comando registre mensagens de erro e informativas na console do sistema e/ou em um arquivo. Normalmente mensagens de erro são gravadas no arquivo `/var/adm/messages` juntamente com a data e hora em que foram gravadas.



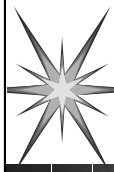
Conceitos de Internet Firewalls

Para proteger uma rede contra invasões , dois enfoques são necessários: a segurança de sistemas, redes e serviços; e isolar a rede interna, restringindo o acesso externo através de um firewall.



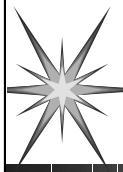
O que é um Internet Firewall?

- ▶ Restringe acessos a um local cuidadosamente controlado
- ▶ Impede que invasores alcancem suas demais defesas
- ▶ Restringe saídas de um local cuidadosamente controlado



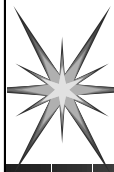
O que um Firewall pode fazer?

- ▶ Forçar a política de segurança
- ▶ Registrar todo tráfego
- ▶ Limitar riscos
- ▶ Um firewall é um foco de decisões



O que um Firewall não pode fazer?

- ▶ Proteger contra pessoas internas
- ▶ Proteger contra conexões que não passam por ele
- ▶ Proteger completamente contra novos caminhos

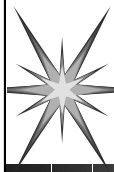


Definições

- ▶ Filtros de pacotes
- ▶ Proxy / Aplicação Gateway

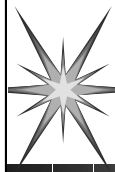
A filtragem é efetuada com base nos seguintes critérios : protocolo (UDP, TCP, etc), endereço IP e portas de origem e destino, além dos campos de controle.

Os proxies são programas específicos que propiciam controle de acesso (inclusive no nível de usuários) e geram logs do tráfego.

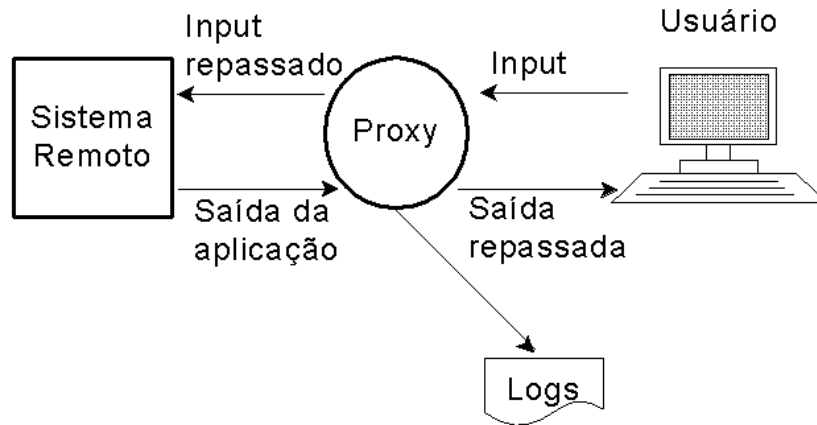


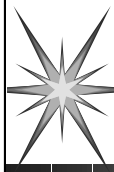
Filtros de pacotes

- Controle de acesso
 - Endereço de origem e destino
 - Protocolo (TCP, UDP ou ICMP)
 - Porta de origem e destino (TCP ou UDP)
 - Tipo de mensagem ICMP
 - Interface de rede de entrada e saída
 - TCP flags
 - Fragmentos



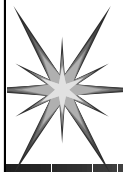
Proxy / Aplicação Gateway





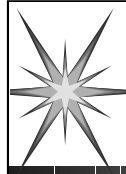
Proxy / Aplicação Gateway

- ▶ Recebe as conexões e repassa a entrada de dados (input) para o sistema remoto. A aplicação responde aos proxies que repassam a saída (output) para o usuário.
- ▶ Controle de acesso
- ▶ Verifica o protocolo de cada aplicação
- ▶ Registra o tráfego
- ▶ Pode possuir mecanismos anti-virus

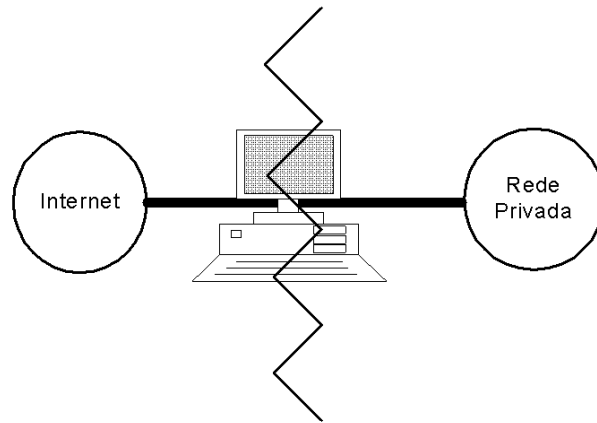


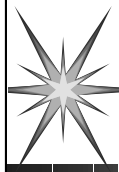
Arquiteturas de Firewall

- Dual-Homed Host
- Screened Host
 - Bastion Host
- Screened Subnet
 - Rede perimetral (Zona desmilitarizada)
 - Bastion Host
 - Roteador interno
 - Roteador externo

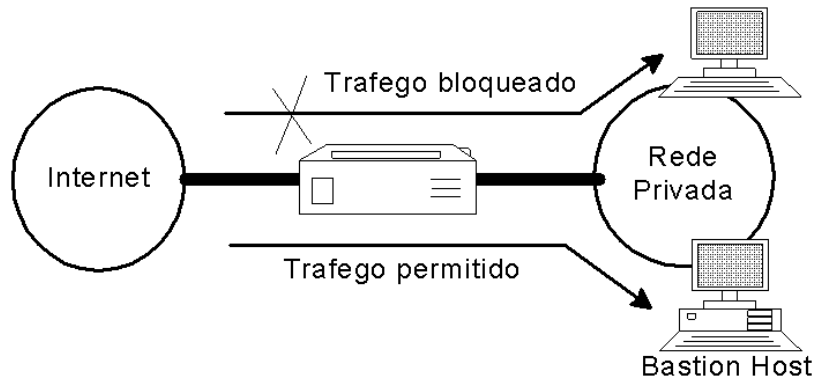


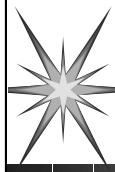
Dual-Homed Gateway



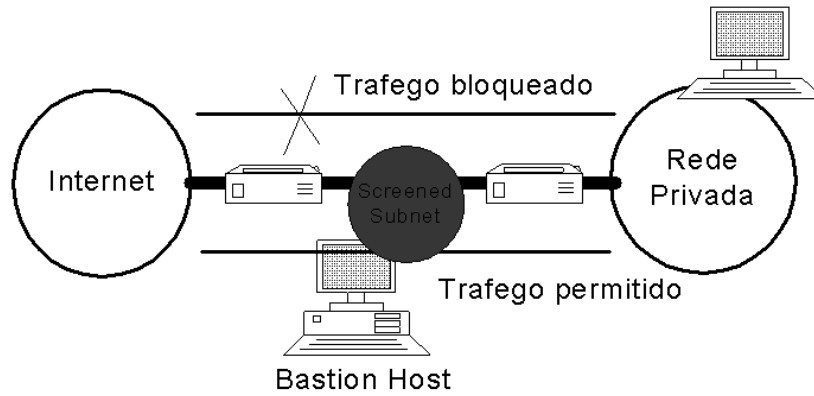


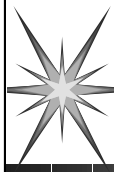
Screened Host





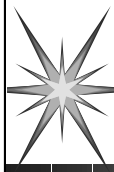
Screened Subnet





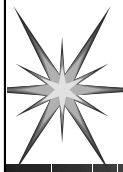
Zona desmilitarizada (DMZ)

- ▶ Subrede localizada entre a rede externa (Internet) e a rede interna (rede privada)
- ▶ Pode ser a terceira interface de um gateway



Variações sobre as arquiteturas

- ▶ Múltiplos bastion hosts
- ▶ Juntar o roteador externo e interno
- ▶ Múltiplos roteadores externos
- ▶ Múltiplas redes perimetrais
- ▶ Usar Dual-Homed Hosts e Screened Subnet



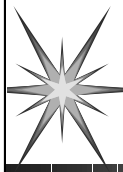
Network Address Translation (NAT)

- ▶ Mecanismo que troca o endereço IP de máquinas da rede interna para o endereço do firewall (ou um range de endereços)
- ▶ Os IPs internos não são de conhecimento público

Exemplo de regras para o ipfilter (ipnat):

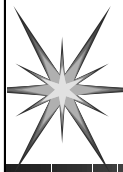
```
map ed1 10.1.0.0/16 -> 240.1.0.1/32 portmap tcp 10000:20000
```

```
map ed1 10.1.0.0/16 -> 240.1.0.0/24
```



Administração do Firewall

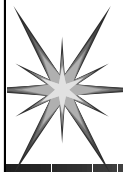
- ▶ Alertas
- ▶ Auditoria
- ▶ Atendimento a emergências de segurança



Firewalls baseados em filtros de pacotes

- IPfilter
- IPFW

Filtragem de pacotes é um mecanismo dos roteadores que controla os pacotes que passam de uma rede para a outra, comparando cada pacote com uma lista de regras antes de decidir se esse pacote deve ser repassado ou não.



Firewalls baseados em proxies

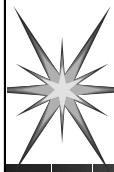
- SOCKS
- TIS Internet Firewall Toolki
- Aplicações proxies
 - UDP Packet Relay
 - Rinetd
 - Stunnel

SOCKS: Protocolo de proxies que permite converter um programa TCP padrão em uma versão do mesmo programa com proxy.

UDP Packet Relay: Sistema de proxies que fornece para aplicações UDP a mesma funcionalidade que o SOCKS fornece para aplicações TCP.

Rinetd: Programa que redireciona conexões TCP para uma máquina.

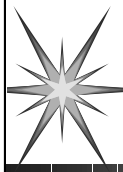
Stunnel: Programa que cria um canal seguro entre cliente e servidor, através de um túnel de criptografia.



Intrusion Detection Host-Based

- ▶ chkrootkit - www.chkrootkit.org
- ▶ ISS - www.iss.net
- ▶ Tripwire - www.tripwire.com

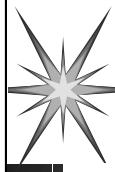
Host-based intrusion system é um software que monitora acessos não autorizados a dados, arquivos ou serviços, alertando o administrador sobre essas violações.



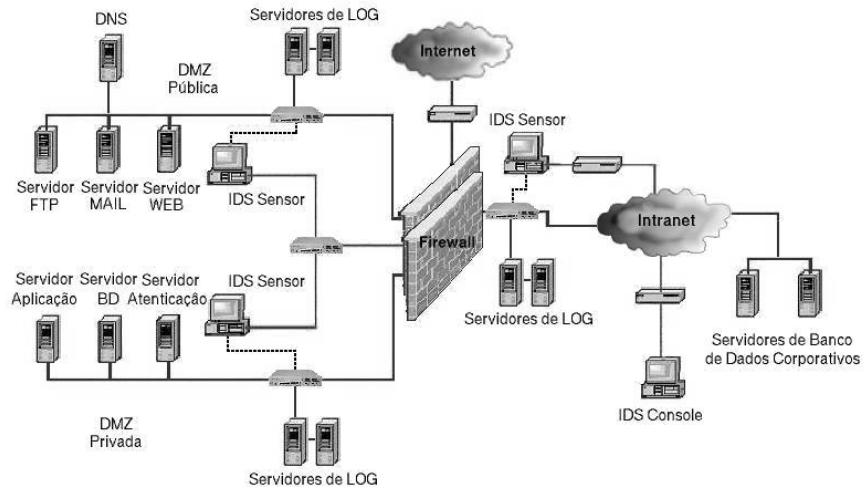
Intrusion Detection Network-Based

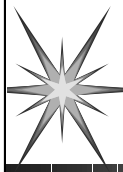
- ▶ Shadow - www.nswc.navy.mil/ISSEC
- ▶ Snort - www.snort.org
- ▶ LIDS - www.lids.org
- ▶ ACME - www.acme-ids.org

Network-based intrusion system monitora o tráfego de rede e alerta o administrador quando detecta anomalias ou tráfego que case com sua base de assinaturas de ataques (buffer overflows, portscans, ataque a CGIs e outros).



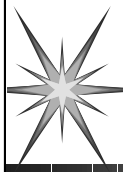
Proposta de arquitetura de rede





Como tratar incidentes de segurança?

- ▶ Mantenha a calma (tire o dedo do teclado)
- ▶ Siga as políticas da instituição
- ▶ Documente todas as suas ações
- ▶ Faça backups
- ▶ Não trabalhe com os dados originais
- ▶ Peça ajuda!



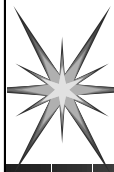
Ferramentas de análise forense

- ▶ The Coroner's Toolkit (TCT)
 - ▶ <http://www.porcupine.org/forensics/tct.html>

Definição de Análise Forense:

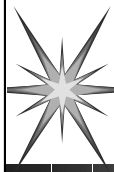
“Trata-se da captura e análise de evidências, tanto quanto possível livres de estarem distorcidas ou tendenciosas, de tal forma a reconstruir determinados dados ou o que aconteceu num sistema no passado”

- Dan Farmer



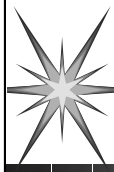
Quem procurar na UNICAMP?

- ▶ O administrador de rede da sua unidade
- ▶ A equipe de segurança
 - ▶ www.security.unicamp.br
 - ▶ [mailto: security@unicamp.br](mailto:security@unicamp.br)



Quem procurar no Brasil?

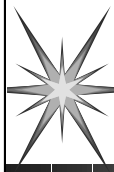
- A equipe de segurança de sua organização
- NIC BR Security Office
 - www.nic.br/nbso.html
 - [mailto: nbso@nic.br](mailto:nbso@nic.br)
- Polícia Civil de São Paulo
 - [mailto: webpol@policia-civ.sp.gov.br](mailto:webpol@policia-civ.sp.gov.br)
- Polícia Federal
 - [mailto: saac@nic.br](mailto:saac@nic.br)



Referências

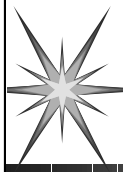
► Livros :

- Firewalls and Internet Security
- Building Internet Firewalls
- Practical Unix & Internet Security
- Computer Crime
- Hacker Proof
- Web Security



Referências

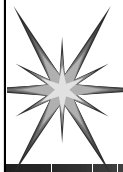
- ▶ Livros :
 - ▶ Network Intrusion Detection: an analyst's handbook
 - ▶ Implement Virtual Private Networks
 - ▶ Applied Cryptography: Protocols, Algorithms, and Source Code in C
 - ▶ Understanding the Public-Key Infrastructure



Referências

► Links

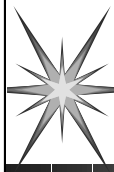
- SANS - www.sans.org
- Securityfocus - www.securityfocus.com
- CERT Coordination Center - www.cert.org
- Dan Farmer e Wietse Venema -
www.porcupine.org / www.fish.com
- NIC-BR - www.nic.br
- Pangéia - www.pangeia.com.br
- CAIS - www.rnp.br/cais



Referências

► Links

- Instituto de Computação - www.ic.unicamp.br
- ACME - www.acme-ids.org
- ISS - www.iss.net



Listas

- ▶ security-l@unicamp.br
- ▶ gts-l@unesp.br
- ▶ BUGTRAQ@NETSPACE.ORG