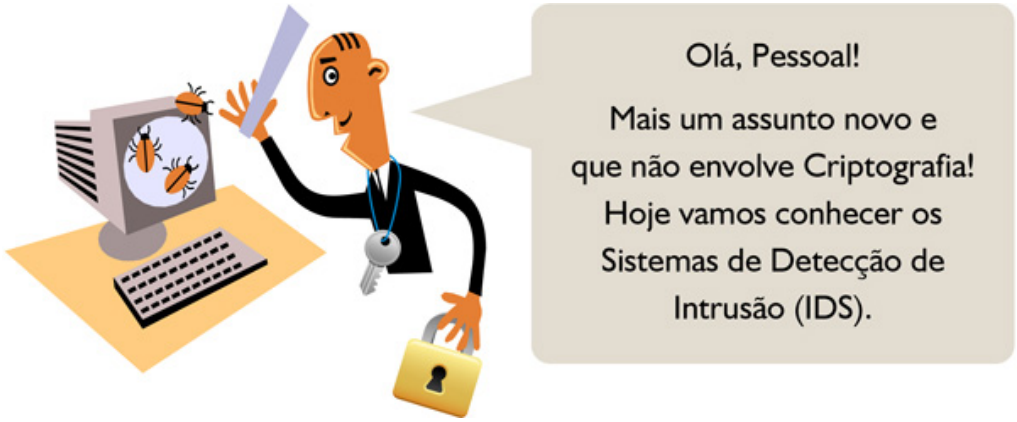
Segurança em Redes

Aula 09 - Sistemas de Detecção de Intrusão e Auditoria

Apresentação



Nesta aula, você estudará mais uma maneira de adicionar segurança aos sistemas computacionais, os sistemas de detecção de intrusão (IDS — *Intrusion Detection System*s). Também vai conhecer o que são *honeypots* (potes de mel). Além disso, estudaremos um pouco um dos IDS mais conhecidos, o Snort. Por fim, estudaremos algumas noções de auditoria de segurança de sistemas.

Vídeo 01 - Apresentação

Objetivos

Ao final desta aula, você será capaz de:

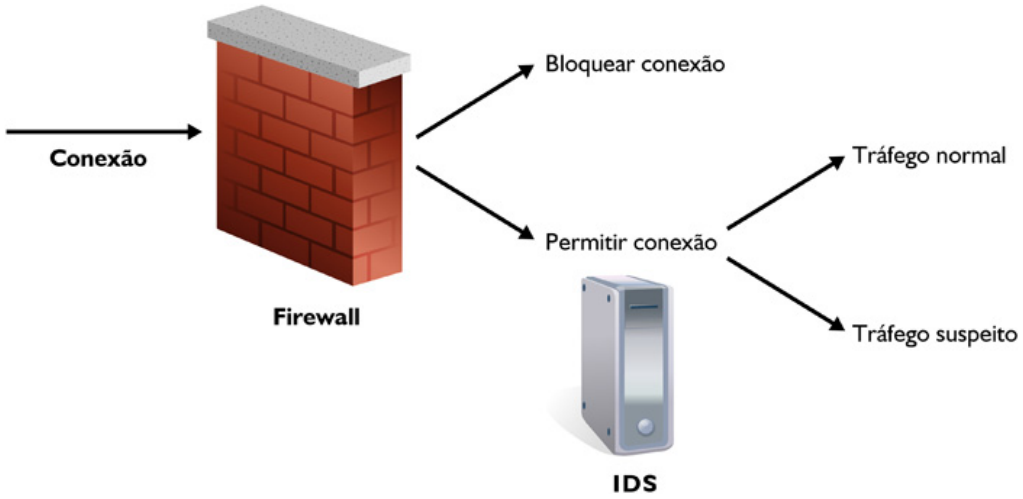
- Reconhecer os sistemas de detecção de intrusão (IDS).
- Conhecer os tipos de IDS.
- Compreender o que são os *honeypots*.
- Saber como *honeypots* podem contribuir para a segurança.
- Entender o que faz a auditoria de segurança.

Finalidade de um Sistema de Detecção de Intrusão

Como você viu nas aulas anteriores, há várias formas de melhorar a segurança de uma rede. Os firewalls, por exemplo, filtram os pacotes, autorizando ou não a sua entrada na rede. Os sistemas de detecção de intrusão (IDS) também contribuem para a segurança de uma rede. Como o nome já diz, um IDS tem como finalidade detectar tentativas de invasão (ou intrusão), direcionadas à rede, e se houve comprometimento de algum elemento dessa rede. Em caso positivo, o IDS deve alertar o administrador.

A diferença do firewall para o IDS está ilustrada na **Figura 1**. O firewall analisa os pacotes que chegam ou saem da rede, autorizando ou não sua passagem. Contudo, nem todos os pacotes autorizados a passar são completamente confiáveis. Então, o IDS serve para analisar os pacotes que passam pelo firewall e identificar os que são normais ou suspeitos.

Figura 01 - Diferença de firewall e IDS.



Funções de um IDS

O funcionamento de um IDS é semelhante a um sistema de detecção de ladrões, usado em residências. Esse sistema é configurado para especificar o que monitorar (janelas, portas, movimento) e para quem deve ser direcionado o alerta (polícia, donos da casa, central de segurança eletrônica) em caso de entrada de um ladrão.

No ambiente computacional, é necessário especificar o que monitorar (redes ou endereços IP, serviços etc.) e para quem devem ser direcionados os alarmes ou relatórios.

Para realizar seu trabalho, um IDS deve capturar e analisar, por exemplo, o tráfego a ser monitorado. Informações sobre atividades suspeitas detectadas devem ser armazenadas. Atualmente, os IDS, além de simplesmente gerarem alertas, também podem ter um comportamento reativo. Dessa forma, ele passa a, além de detectar, reagir à intrusão. Por exemplo, um IDS pode determinar o fechamento de uma conexão ou a inserção de uma nova regra no firewall.

Vídeo 02 - O Que é um IDS?

Atividade 01

1. Quais as vantagens de utilizar um IDS?
2. Por que o firewall não substitui um IDS?

Tipos de IDS

IDS podem ser instalados em diferentes locais de uma rede, e isso caracteriza seu tipo e as ações que ele desempenhará. Nesta seção, iremos apresentar os três tipos mais comuns de IDS.

IDS baseado em host (HIDS)

Esse tipo de IDS procura por indícios de intrusão na máquina onde está instalado. Em geral, com base em informações de arquivos de log do sistema operacional, eles procuram por atividades que não são comuns, como tentativas de

login ou tentativas de alteração em privilégios do sistema. Por exemplo, se algum usuário tentar logar como administrador no Linux usando o comando su, o sistema vai gravar tal tentativa em um log de ações e incluir o login do usuário que fez a tentativa com o horário. A Figura 2 mostra algumas informações do sistema que podem ser analisadas por um HIDS.

Figura 02 - Exemplos de informações analisadas por um HIDS.

Dentre as vantagens de um HIDS, vale destacar:

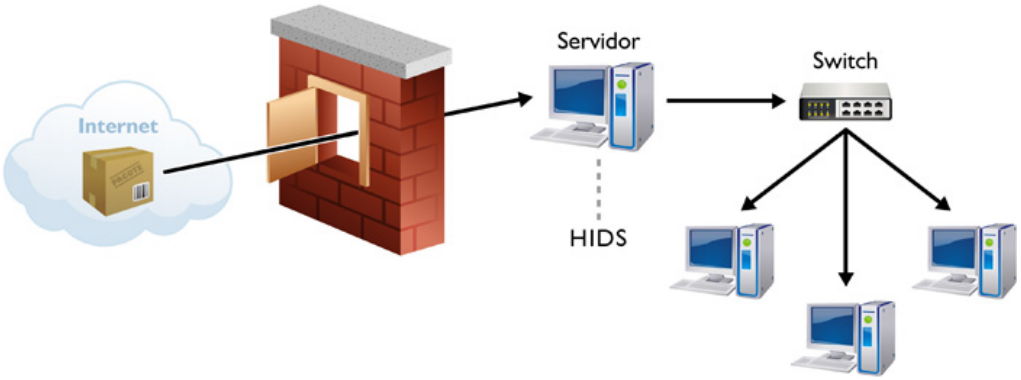
- A capacidade de monitorar atividades do sistema tais como acesso a arquivos, modificação de permissões, login e logout de usuários etc;
- A dependência da topologia da rede;
- Não necessidade de hardware adicional.

Algumas de suas desvantagens são:

- Escalabilidade (dificuldade de gerenciar e configurar todos os hosts que devem ser monitorados);
- Dependência do Sistema Operacional (um HIDS que funciona no Windows é diferente de um para o Linux ou para Mac OS X);
- Capacidade de comprometer o desempenho do host monitorado.

Perceba que a **Figura 3** ilustra a arquitetura típica de uma rede com um HIDS.

Figura 03 - HIDS.



IDS baseado em rede (NIDS)

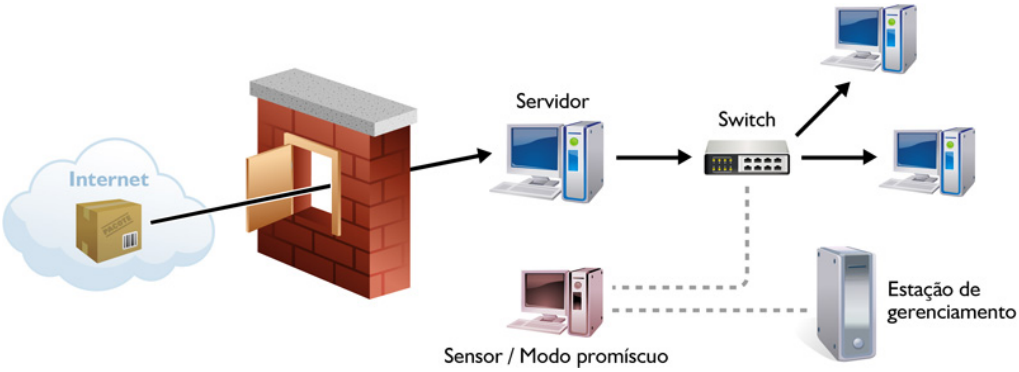
Esse tipo de IDS monitora o tráfego de uma rede ou segmento dela. Em geral, sua operação exige que a interface de rede do IDS opere em modo promíscuo — como também ocorre nos *sniffers*. No modo promíscuo, todos os pacotes "avistados" pela interface de rede de uma máquina serão recebidos, mesmo que não sejam destinados a ela.

Normalmente, o NIDS captura os cabeçalhos e, opcionalmente, parte do conteúdo dos pacotes e os compara com uma série de padrões conhecidos característicos de ataques. Atualmente, o NIDS mais utilizado no mundo é o Snort. Esse tipo de IDS em geral é dividido em duas partes, as quais veremos a seguir.

- **Sensores**: são posicionados nos segmentos de rede que se deseja monitorar. Realizam a captura e análise do tráfego de rede. Os sensores são instalados em uma máquina específica, mas, por atuarem em modo promíscuo, um único sensor tem a capacidade de detectar tentativas de intrusão destinadas a todas as máquinas da rede monitorada (ou originadas nelas).

- **Estação de gerenciamento**: é uma estação que gerencia os sensores. Em geral, o software da estação de gerenciamento possui uma boa interface gráfica que permite a configuração dos sensores e visualização dos alarmes por eles gerados.

Figura 04 - NIDS.



A **Figura 4** ilustra a arquitetura de uma rede com um NIDS. Vale salientar que, muitas vezes, a comunicação entre sensores e o console usa criptografia. Dentre as vantagens de um NIDS, podemos destacar:

- Possibilidade de monitorar estações de trabalho e servidores com sistemas operacionais e aplicações bastante distintas;
- Possibilidade de detectar diversos tipos de ataques;
- Detecção de ataques em tempo real;
- Ausência de impacto no desempenho da rede ou hosts monitorados.

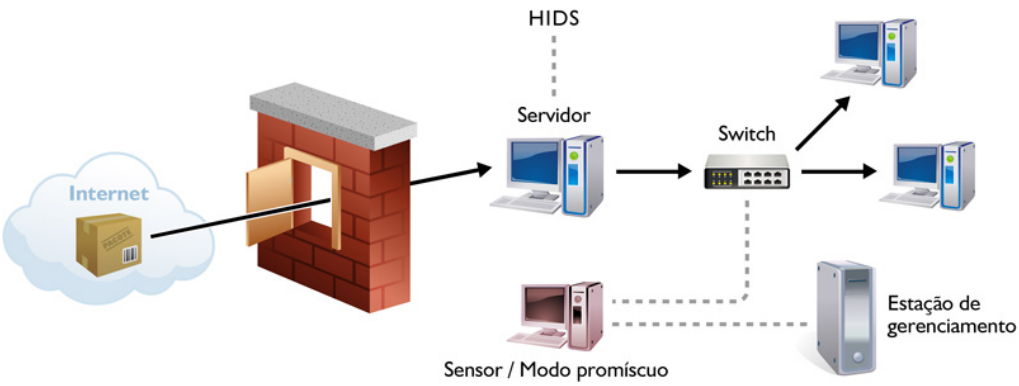
Dentre suas desvantagens, temos:

- Perda de pacotes em redes saturadas;
- Impossibilidade de monitorar tráfego criptografado;
- Dificuldade de uso em redes que utilizam switches.

IDS híbrido

Os dois tipos de IDS apresentados anteriormente podem se complementar, uma vez que os HDIS atuam em estações e o NIDS analisa o tráfego de rede. Dessa forma, podemos utilizar um NIDS para detectar ataques destinados às estações clientes da rede local (ou que partem delas), e um HIDS em cada um dos servidores da rede. A **Figura 5** mostra uma rede que utiliza este tipo de solução.

Figura 05 - Solução híbrida.



Atividade 02

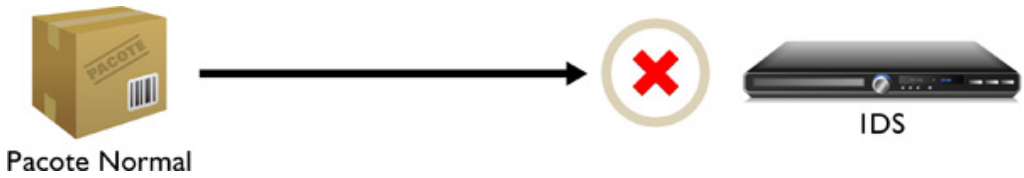
1. Quais as vantagens de se utilizar uma solução híbrida?
2. Por que os HIDS não precisam usar a interface de rede no modo promíscuo?

Problemas de IDS

Os principais problemas de IDS são os falsos positivos e os falsos negativos.

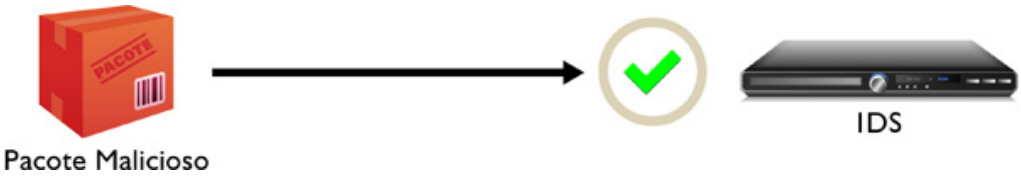
Falsos positivos acontecem quando pacotes normais são identificados como tentativas de ataque. Para que isso não ocorra, é necessário que o IDS seja bem configurado e tenha um sistema de gerenciamento que facilite sua configuração e a análise dos logs. A **Figura 6** ilustra um falso positivo.

Figura 06 - Falso positivo.



Falsos negativos acontecem quando um IDS não identifica os verdadeiros ataques. A **Figura 7** ilustra o falso negativo.

Figura 07 - Falso negativo.



Potes de mel (*honeypots*)

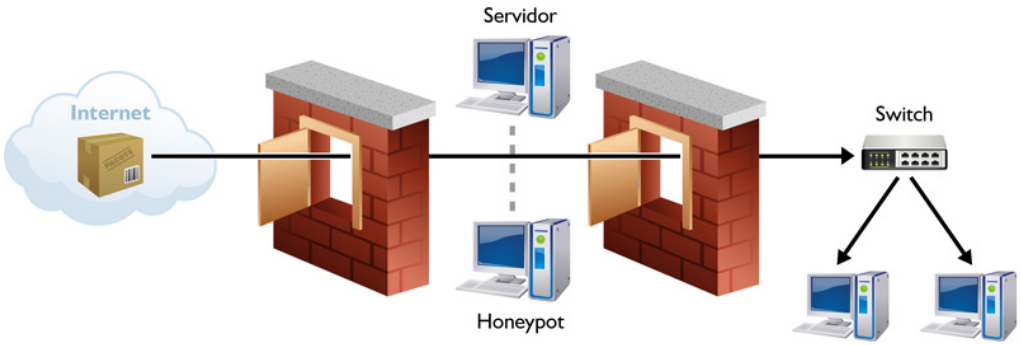
Os potes de mel não são IDS, mas os auxiliam muito. O termo é usado para referir-se a algo tentador, como uma armadilha. Em segurança, os *honeypots* são armadilhas para atrair invasores de redes.

Em geral, são máquinas que vão servir como iscas para os invasores que irão atacá-la. As informações sobre a invasão são guardadas em outro local para identificar quem foi o invasor e como ele conseguiu realizar o ataque.

Como os potes de mel não incluem funções de segurança, eles, em si, não realizam a melhoria da segurança da rede. Servem para captar informações importantes de como são feitas invasões à rede e de como serviços são atacados. Além disso, ajudam a identificar os invasores. Portanto, os potes de mel são úteis em termos de segurança porque quando se tem informações de como as invasões foram realizadas, pode-se criar medidas e segurança para evitá-las. Pode-se configurar novas regras no firewall e no IDS, por exemplo.

Como a máquina que faz papel de pote de mel está ligada à rede, é importante isolar o acesso direto dessa máquina às outras máquinas da rede através de um firewall, conforme ilustra a **Figura 8**.

Figura 08 - *Honeypots*.

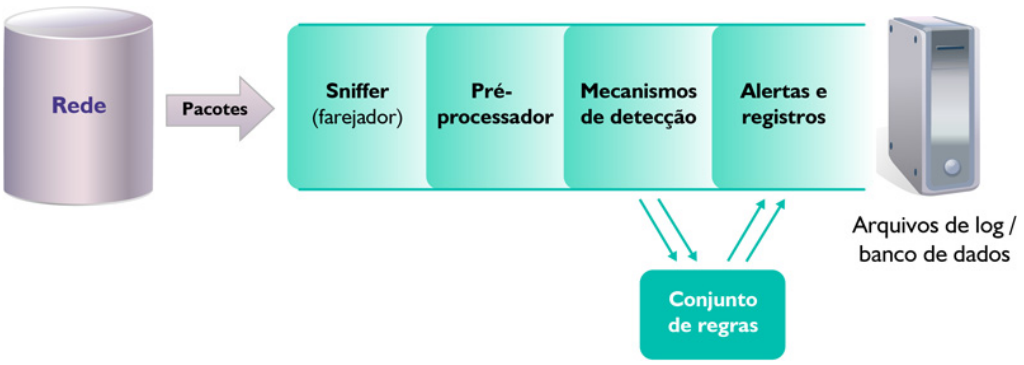


Vídeo 03 - *Honeypots*

Snort

O Snort é um dos NIDS mais utilizados no mundo. Ele realiza a análise de tráfego em tempo real, identificando ataques direcionados a uma rede (ou host). Sua ação é baseada na análise de protocolos e comparação com padrões característicos de ataques. O Snort, segundo Caswell et. al. (2003), possui quatro módulos principais: sniffer; pré-processador; detector de intrusão e gerador de alertas e registros. A **Figura 9** mostra a arquitetura do Snort.

Figura 09 - Arquitetura Snort.



O sniffer realiza a captura dos pacotes. Os pré-processadores são responsáveis por classificar os dados capturados. Em seguida, os pacotes são enviados para o mecanismo de detecção, no qual serão comparados com um conjunto de regras que contêm informações sobre ataques conhecidos, como por exemplo, cavalos de troia.

Se um pacote corresponder às informações de alguma regra, ele será enviado para o gerador de alertas. Esses alertas podem ser registrados em um arquivo de log ou armazenados em um banco de dados. A partir dos alertas gerados, pode-se executar ações específicas com base no ataque identificado. O **Quadro 1** mostra alguns comandos básicos do Snort.

Comando	Função
snort –v	Imprime os cabeçalhos dos pacotes TCP/IP na tela.
snort –vd	Mostra também os dados contidos no pacote.
snort –vde	Mostra também os cabeçalhos de enlace.
snort -vde -l log.txt	Gera os alertas em um arquivo de nome log.txt.
snort -vde -l log -h 192.168.0.2	Realiza a detecção de intrusão nos pacotes destinados ao IP 192.168.0.2

Quadro 1 - Lista com comandos básicos do Snort

Vídeo 04 - Snorby na Prática

Auditoria

Auditoria está intimamente ligada à segurança computacional e, nessa área, tem como papel verificar se os requisitos de segurança da informação da empresa estão sendo implementados adequadamente.

O auditor é a pessoa que realiza o procedimento de auditoria. Tal procedimento envolve verificar se a política de segurança da empresa está realmente implementada no sistema computacional. Para tanto, primeiramente, são descritas as atividades que exigem segurança. Em seguida, é verificado se todas essas atividades estão realmente implementadas. Por fim, apontam-se os problemas encontrados.

Parece simples? Mas, não é! Avaliar toda a segurança do sistema envolve muita coisa!

Portanto, o auditor deve ser um profissional muito bem preparado e possuir um vasto conhecimento em:

- sistemas operacionais, banco de dados, processamento distribuído;
- sistemas de controle de acesso;
- firewalls, criptografia;
- softwares usados na empresa;
- planejamento e avaliação de gestão da informação;
- ética, bom relacionamento, comunicação oral e escrita, senso crítico etc.

Resumindo, podemos dizer que a segurança e a auditoria são interdependentes, ou seja, uma depende da outra para produzirem os efeitos desejáveis à alta administração. A segurança tem a função de garantir a integridade, confidencialidade e disponibilidade dos sistemas e dos dados da empresa. A auditoria, por sua vez, serve para verificar se a segurança está sendo implementada de forma correta e se os dados e sistemas estão realmente protegidos.

Segundo [NCSC 87], o mecanismo de auditoria tem importantes objetivos:

- permitir a revisão de padrões de acesso, o histórico dos acessos (log) a processos e o uso dos mecanismos de proteção e quão eficazes eles são;
- permitir a descoberta de tentativas dos usuários e de pessoas externas de burlar os mecanismos de proteção;
- permitir a descoberta de qualquer uso de privilégios não autorizados;
- fornecer uma maneira do usuário saber que as tentativas de burlar os mecanismos de proteção são registradas e descobertas.

Em suma, auditoria é uma maneira importante de se verificar se a rede realmente está segura, e deve ser um mecanismo adotado por todas as organizações para garantir a segurança da sua rede.

Resumo

Nesta aula, você estudou que um IDS tem como finalidade detectar se houve uma tentativa de invasão à rede e se houve comprometimento de algum elemento. Em caso positivo, o IDS deve alertar o administrador dessa rede. Você também conheceu três tipos de IDS e seus problemas. Aprendeu que os *honeypots* não resolvem um problema de segurança específico, mas são ferramentas que contribuem para a segurança da rede. Além disso, conheceu um pouco sobre o Snort. Também aprendeu que a auditoria é essencial para verificar se os procedimentos de segurança estão sendo usados corretamente em uma empresa.

Autoavaliação

1. Dê exemplos de informações que são analisadas por HIDS.
2. Por que os *honeypots* devem ser instalados fora da rede?
3. Por que um dos componentes do Snort é um sniffer?
4. Marque V ou F, V para verdadeiro e F para falso:

   ( ) Todo *honeypot* é um IDS.
   ( ) A auditoria corrige as falhas de segurança de uma empresa.
   ( ) Apenas um NIDS pode detectar problemas de segurança direcionados a toda uma rede.
   ( ) O falso positivo acontece quand os IDS não identificam ataques reais.

Referências

BARBOSA, André S. **Sistemas de detecção de intrusão Seminários Ravel:** CPS760. UFRJ. Disponível em: <http://www.lockabit.coppe.ufrj.br/downloads/academicos/IDS.pdf>. Acesso em: 20 jul. 2012.

BORGES, P. C.; COUTINHO, R. T. **Análise de sistema de detecção de intrusos em redes de computadores.** 2007. 133f. Monografia (Trabalho de Conclusão de Curso) – Universidade de Franca, Franca, 2007. Disponível em: <http://snort.org.br/arquivos/Monografia-pedro.pdf>. Acesso em:30 ago. 2009.

CASWELL, Brian et al. **Snort 2: sistema de detecção de intrusão.** Rio de Janeiro: Alta Books, 2003.

NAKAMURA, E.; GEUS, P. L. **Segurança em Redes em Ambientes Cooperativos.** Futura, 2002.

NATIONAL COMPUTER SECURITY CENTER - NCSC. **A guide to understanding audit in trusted systems.** 1987. Disponível em: <http://niatec.info/pdf.aspx?id=78>. Acesso em: 30 ago. 2012.

SNORT: the easy tutorial: introduction. Disponível em: <http://openmaniak.com/snort.php>. Acesso em: 30 ago. 2012.

VIVA O LINUX. gerenciamento de redes. Disponível em: <http://www.vivaolinux.com.br/artigo/Snort-Gerenciamento-de-redes?pagina=4>. Acesso em: 30 ago. 2012.