

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMA DE INFORMAÇÃO**

**PROPOSTA DE IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE INTRUSÃO
NA REDE DE COMPUTADORES DA FARN**

**PROPOSTA DE IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO NA REDE DE COMPUTADORES DA FARN**

Monografia apresentada ao Curso de Graduação
em Sistema de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
para a obtenção do grau de Bacharelado em
Sistema de Informação

Ana Helena Horta Galvão

Orientador:

Ricardo Kleber Martins Galvão

**NATAL/RN
2005**

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO

ANA HELENA HORTA GALVÃO

BACHARELADO EM SISTEMA DE INFORMAÇÃO

PROPOSTA DE IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO NA REDE DE COMPUTADORES DA FARN

**PROPOSTA DE IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE INTRUSÃO
NA REDE DE COMPUTADORES DA FARN**

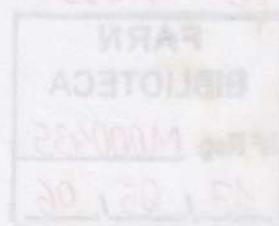
Monografia apresentada ao Curso de Graduação
em Sistema de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
para a obtenção do grau de Bacharelado em
Sistema de Informação.

Monografia apresentada ao Curso de Graduação
em Sistema de Informação da Faculdade Natalense
para o Desenvolvimento do Rio Grande do Norte
para a obtenção do grau de Bacharelado em
Sistema de Informação.

Orientador:

Ricardo Kleber Martins Galvão

NATAL/RN
2005



Catálogo na Publicação – Biblioteca da FARN
Setor de Processos Técnicos

Galvão, Ana Helena Horta

Proposta de implantação de um sistema de detecção de intrusão na rede de computadores da FARN / Ana Helena Horta Galvão. – Natal: FARN, 2005.
35 f.

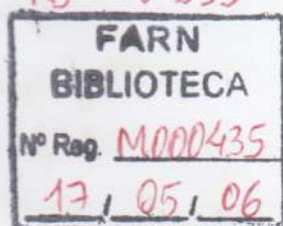
Orientador: Ricardo Kleber Martins Galvão

Monografia (Graduação em Sistemas de Informação) – Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte.

1. Segurança de Redes – Monografia. 2. Redes de Computadores – Monografia. 3. Sistema de Defesa – Monografia. I. Título.

RN/FARN/BC

CDU 004.7



M
004.7
G 171 p
2005

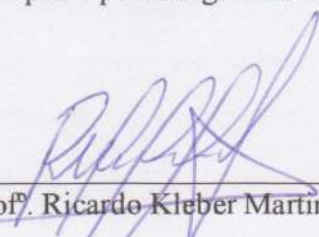
NATAL
2005

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO
DO RIO GRANDE DO NORTE
BACHARELADO EM SISTEMA DE INFORMAÇÃO**

**PROPOSTA DE IMPLANTAÇÃO DE UM SISTEMA DE DETECÇÃO DE
INTRUSÃO NA REDE DE COMPUTADORES DA FARN**

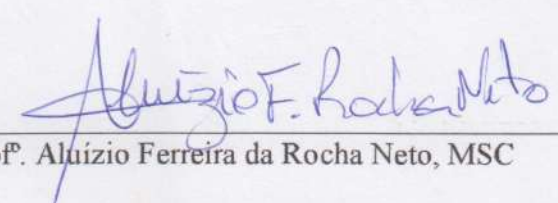
Ana Helena Horta Galvão

Monografia apresentada em 17 de DEZEMBRO de 2005 pela banca examinadora
composta pelos seguintes membros:



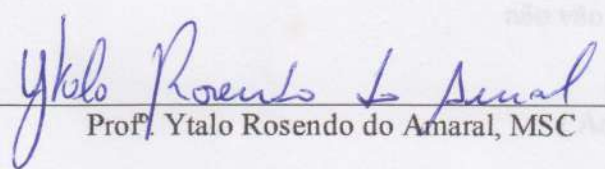
Prof.^o Ricardo Kleber Martins Galvão

Orientador



Prof.^o Aluizio Ferreira da Rocha Neto, MSC

Examinador



Prof.^o Ytalo Rosendo do Amaral, MSC

Examinador

Natal/RN, 17 de DEZEMBRO de 2005

AGRADECIMENTOS

A Deus pela oportunidade de vida e por todas as bênçãos que me concede e dá a ganhar.

Ao meu marido Nelson que foi meu principal incentivador na conclusão deste curso.

As minhas filhas Mariana, Juliana e Cristiane por terem sempre me incentivado a seguir firme nos meus ideais.

Aos professores que me deram a oportunidade de novos conhecimentos, em especial ao professor Ricardo Kleber, pela orientação fornecida durante o desenvolvimento deste trabalho igualmente contribuindo para minha formação acadêmica e profissional.

Aos meus amigos de turma com quem pude compartilhar estes quatro anos.

Enfim, a todos que direta ou indiretamente colaboraram para a concretização desse trabalho de graduação.

"Aqueles que passam por nós,
não vão sós, não nos deixam sós.
Deixam um pouco de si,
levam um pouco de nós."
(Antoine de Saint-Exupery)

AGRADECIMENTOS

A Deus pela oportunidade da vida, e por todas as bênçãos que me concede a cada amanhecer.

Ao meu marido Nelson que foi meu principal incentivador na conclusão deste curso.

As minhas filhas Mariana, Juliana e Cristiana por terem sempre me incentivado a seguir firme nos meus ideais.

Aos professores que me deram a oportunidade de novos conhecimentos, em especial ao professor Ricardo Kleber, pela orientação fornecida durante o desenvolvimento deste trabalho igualmente contribuindo para minha formação acadêmica e profissional.

Aos meus amigos de turma com quem pude compartilhar esses quatro anos.

Enfim, a todos que direta ou indiretamente colaboraram para a concretização desse trabalho de graduação.

ABSTRACT

RESUMO

Este trabalho apresenta uma proposta de implantação de um sistema de detecção de intrusões na rede da FARN, componente essencial em um ambiente cooperativo. Foi feito um estudo sobre o ambiente computacional da rede de computadores da FARN, com o objetivo de identificar a estrutura física e lógica de interconexão, além dos equipamentos de conectividade, roteamento e filtragem. A partir da constatação de ausência de mecanismos de detecção de tráfego de dados não convencionais caracterizados como tentativas de intrusão, propõe-se a instalação/configuração de um IDS para auxiliar na detecção de ataques e intrusões maliciosas que possam acontecer na rede da FARN, a fim de monitorar, capturar dados da rede e identificar ataques baseados em padrões (assinaturas). O modelo proposto baseia-se na ferramenta Snort, de uso gratuito e código fonte aberto.

Palavras-chave: segurança, redes de computadores, detecção de intrusões.

ABSTRACT

This work presents a proposal of implementation of a detection system of intrusions in the one of the net of FARN, essential component in a cooperative environment. A study on the computational environment of the computer network of the FARN was made with the objective to identify the physical and logical structure of interconnection, beyond the equipment of connectivity and filtering. Without mechanisms of detection of traffic not characterized conventional data as intrusion attempts, it is considered necessary to install and configure an IDS to assist the detection of attacks and malicious intrusions that can happen in the net of the FARN, in order to monitor, to capture and to identify attacks based on signatures. The considered model is based on Snort tools, free use and open code source.

Figura 3 - Tráfego das Sub-redes do FARN	27
Figura 10 - Exibição dos Detalhes dos Ataques Detectados ACID	31
Figura 11 - ACID exibindo o conteúdo do pacote suspeito	32

Key Words: security.computer network.detection of intrusions.

LISTA DE ABREVIATURAS

LISTA DE FIGURAS

Figura 1 – Arquitetura da pilha de protocolos TCP/IP.....	15
Figura 2 – Caracterização de um Incidente de Segurança.....	17
Figura 3 – Caracterização de um IDS Snort.....	19
Figura 4 – Servidor 01 – Esquema de Rede.....	22
Figura 5 – Servidor Webserver – Esquema de Rede.....	24
Figura 6 – Servidor Acadêmico – Esquema de Rede.....	26
Figura 7 – Servidor Admin – Esquema de Rede.....	27
Figura 8 – Tráfego das Sub-redes da FARN.....	28
Figura 9 – Tela Inicial do ACID.....	30
Figura10 – Exibição dos Detalhes dos Ataques Detectados ACID.....	31
Figura 11– ACID exibindo o conteúdo do pacote suspeito.....	32

TCP Transmission Control Protocol

UDP User Datagram Protocol

SUMÁRIO

I INTRODUÇÃO	LISTA DE ABREVIATURAS	11
1 REFERENCIAL TEÓRICO		14
ACID	Analysis Console for Intrusion Databases	14
DNS	Domain Name Server	14
ED	Escola Doméstica de Natal	15
FARN	Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte	16
FTP	File Transfer Protocol	16
HTTP	Hypertext Terminal Protocol	18
IDS	Intrusion Detection System	18
IMAP	Internet Message Access Protocol	20
IP	Internet Protocol	20
MTA	Mail Transport Agent	20
SNMP	Simple Network Management Protocol	21
SMTP	Simple Mail Transfer Protocol	24
TCP	Transmission Control Protocol	25
UDP	User Datagram Protocol	26
3.3 Descrição Física de Conectividade		27
3.4 Software/Hardware do IDS		28
3.4.1 Software do IDS		28
3.4.2 Hardware do IDS		32
4 ANÁLISE DE RESULTADOS		33
5 CONCLUSÃO		34
REFERÊNCIAS		35

SUMÁRIO

1 INTRODUÇÃO.....	11
2 REFERENCIAL TEÓRICO	14
2.1 REDE DE COMPUTADORES.....	14
2.1.1 Camadas TCP/IP.....	14
2.2 Segurança da Informação.....	15
2.3 Sistemas de Detecção de Intrusão(IDS).....	16
2.3.1 Definições	16
2.3.2 Tipos de Sistemas de Detecção de Intrusão.....	18
2.3.3 O Snort IDS.....	18
3 METODOLOGIA.....	20
3.1 LEVANTAMENTO DO AMBIENTE COMPUTACIONAL DA FARN.....	20
3.1.1 Servidor 01 – Roteador/Firewall da Rede Interna.....	20
3.1.2 Servidor WEBSERVER - Servidor de E-Mail.....	21
3.1.3 Servidor ACADEMICO – Domínio Windows	24
3.1.4 Servidor ADMIN – Domínio Windows.....	25
3.2 Definição do Posicionamento do IDS.....	26
3.3 Descrição Física de Conectividade.....	27
3.4 Software/Hardware do IDS.....	28
3.4.1 Software do IDS.....	28
3.4.2 Hardware do IDS	32
4 ANÁLISE DE RESULTADOS.....	33
5 CONCLUSÃO	34
REFERÊNCIAS	35

1. INTRODUÇÃO

O advento da comunicação entre equipamentos computacionais interligados em rede, e, mais especificamente, a utilização da internet têm facilitado a comunicação, reduzindo distâncias e diminuindo o custo de comunicação.

As tecnologias ligadas a informação têm evoluído a uma velocidade espantosa. Computadores avançados com processadores de mais de 2 GHz de velocidade, redes com banda larga, *softwares* inteligentes que determinam seu comportamento de acordo com as condições do sistema, tudo para auxiliar nas mais diversas atividades. Por outro lado, existem algumas pessoas que preferem utilizar esses *softwares* e toda essa tecnologia para causar danos a outros. Surgem os famosos “*crackers*”, que ao contrário dos “*hackers*”, invadem sistemas e destroem ou roubam dados, suas ações são sempre maliciosas. A segurança na conexão à internet nunca é cem por cento garantida, analistas de segurança encontram aí sua maior fonte de problemas.

Atualmente a sociedade passa por uma revolução, onde a informação vale muito. Assim, perdê-la pode causar sérios danos ao funcionamento de uma empresa. Imagine uma base de dados por algum motivo danificada, temporariamente indisponível ou até destruída, os problemas seriam muito sérios. Desta maneira, técnicas de prevenção e contramedidas têm sido desenvolvidas a fim de dar maior segurança às informações armazenadas.

Há alguns anos, a única forma de controlar o acesso a uma rede era por meio de filtragem no próprio roteador (dispositivo que encaminha os pacotes de rede) ou por um dispositivo chamado *Firewall*, que bloqueia o tráfego para portas não desejadas. O problema é que o controle utilizando estes mecanismos é estático, isto é, se uma determinada porta é utilizada como entrada para ataques a uma rede corporativa, ela pode ser bloqueada no *firewall*, porém, a partir de então não poderá ser utilizada pra um tráfego normal da rede que necessite acessar esta porta bloqueada.

Nos dias atuais a segurança da informação tem se acentuado devido aos constantes ataques a sistemas, principalmente contra redes de computadores. Com isso têm surgido

novas ferramentas para tentar aumentar a segurança dessas redes e sistemas. Uma dessas novas ferramentas chama-se IDS (*Intrusion Detection System*). Sistemas que podem ser classificados de diversas formas, porém possuem um ponto em comum: detêm uma inteligência capaz de identificar se determinado tráfego é normal ou não. Eles não bloqueiam portas simplesmente, como fazem os *firewalls*.

A FARN, Faculdade Natalense para o Desenvolvimento do RN, tem uma estrutura de rede considerável, mantendo informações importantes armazenadas em máquinas ligadas nesta rede. Esta situação favorece a utilização de técnicas de *hacking* (ataques) contra estas máquinas em busca de uma possível obtenção de privilégios.

Em uma sondagem inicial à administração da instituição para fomentar a viabilidade do início deste projeto, constatou-se que, atualmente, a FARN tem implementado um *firewall* para filtragem de pacotes entre sua intranet e a Internet, mas, ainda não utiliza nenhum tipo de detector de intrusões (IDS).

Fatores como volume de dados de/para a rede corporativa da instituição, número de alunos utilizando ativamente esta rede e disponibilização de vários serviços ao público externo, ou seja, com acesso permitido a partir da Internet, ratificam a necessidade de um projeto para instalação imediata de um IDS na FARN.

Esta monografia tem por objetivo geral a proposta de implantação de uma solução de identificação de ataques contra a rede da FARN, utilizando, para isto um software/hardware de Detecção de Intrusões em Redes de Computadores.

Foi necessário estudar o ambiente computacional da FARN, identificar os pontos críticos da rede da FARN.

Em análise prévia do ambiente computacional da FARN, e mais especificamente, das soluções utilizadas atualmente com vistas a proteger as informações que trafegam entre sua rede corporativa e a internet, alguns pontos foram observados e servem de fundamentos, justificando a necessidade do estudo apresentado neste trabalho.

A administração da FARN não sabe atualmente se existem ataques internos, como também não sabe se a rede já foi atacada, nem o quanto está sendo atacada. As ferramentas utilizadas na rede de computadores da FARN não têm condições de identificar um ataque em andamento, nem tampouco estão preparadas para lidar com um ataque. A instituição não tem como levantar dados sobre ataques a seus servidores, sendo o *firewall* o único

sistema que bloqueia, mas não registra os ataques, apenas analisa os registros mas não sendo possível detectar ataques contra sua rede corporativa ou mesmo ataques internos.

2.1 - A análise dos registros (*logs*) do *firewall* em funcionamento na FARN não é suficiente para o fornecimento dos dados sobre os possíveis ataques que a instituição tem sofrido a partir da Internet contra a sua rede corporativa e principalmente, sobre os possíveis ataques internos, isto é, partindo da rede corporativa para a Internet ou mesmo de máquinas da rede corporativa contra máquinas da mesma rede.

A função de um IDS em uma rede de computadores é justamente complementar as atividades do *firewall* fornecendo informações sobre os tipos de ataque com detalhes sobre origem, destino e técnicas utilizadas.

A incorporação de um sistema de detecção de intrusões na rede corporativa da FARN é, portanto, mais que necessária.

O projeto utiliza pesquisa bibliográfica por trabalhar e pesquisar material já publicado sobre segurança de redes, sistemas de detecção de intrusão, utiliza artigos de revistas, periódicos e sites de Internet.

2.1.1 Pesquisa de laboratório envolvendo procedimentos de investigação sobre intrusão de redes de computadores e suas conseqüências.

Pesquisa descritiva, pois, descreve as características de um determinado software criado para a finalidade deste projeto.

Pesquisa exploratória onde se entende toda a situação a partir de estudos feitos por diferentes autores sobre o tema.

2. REFERENCIAL TEÓRICO

2.1 - REDE DE COMPUTADORES

Os computadores interligados em redes estão em constante comunicação. Para que a comunicação seja completa existe um longo processo. Este processo obedece uma arquitetura de camadas de redes chamadas de TCP/IP.

De acordo com Mancin (2002):

TCP/IP (Transmission Control Protocol/Internet Protocol) é um protocolo para comunicação de computadores, ou melhor, é uma pilha de protocolos. Um protocolo é um conjunto de regras que governa uma conversação entre computadores distantes geograficamente, permitindo a troca de mensagens entre eles, para transmissão de dados.

2.1.1 – Camadas TCP/IP

A comunicação entre dois hosts começa quando o usuário faz um download de uma página da web num programa chamado browser, antes de requisitar a página o computador deve empacotar suas requisições e envia-las através de vários processos e camadas do protocolo (Figura 1). Cada camada representa uma porção na longa caminhada que será efetuada entre o computador de origem e de destino. O computador de destino recebe toda esta informação, as desempacota e entrega a camada correspondente de sua implementação.

Esta arquitetura é constituída de 4 camadas:

- Camada de aplicação: camada localizada no topo da pilha na hierarquia. É responsável pela disponibilidade de comunicação entre os hosts interessados e avalia se existem recursos disponíveis para a comunicação ocorrer. Ex: Telnet, FTP (File Transfer Protocol). Processos que utilizam a rede.
- Camada de transporte: abaixo da camada de aplicação está a camada de transporte que agrega vários aspectos de como os dois hosts irão se comunicar e é responsável pelo aspecto de confiabilidade que irá ocorrer na comunicação. Possui dois

protocolos: TCP (Transmission Control Protocol), o qual é referenciado por sua confiabilidade, orientado a conexão, permite a entrega sem erros de um fluxo de bytes e controla também o fluxo para que um transmissor mais rápido não sobrecarregue um receptor mais lento; e o UDP (User Datagram Protocol), que não possui compromisso no quesito confiabilidade, e não é orientado a conexão,

- Camada de rede: camada responsável pela movimentação de dados entre o computador de origem e destino, nesta camada funcionam os protocolos de endereçamento como o IP (Internet Protocol)
- Camada de enlace: camada responsável pela comunicação entre os hosts, levando em conta os diferentes meios onde os dados estarão envolvidos, como por exemplo, a transmissão de redes diferentes.

Cada camada representa uma porção na caminhada entre o computador de origem e o de destino. O de destino recebe toda a informação, desempacota e entrega a camada correspondente a sua implementação.

Telnet	FTP	SMTP	NSF	SNMP	TFTP	Nível de Aplicacoes
Fluxo Confiavel(TCP)			Datagrama de Usuario (UDP)			Nível de Transporte
Internet Protocol						Nível da Rede
Interface Fisica						Nível de Enlace e Fisico

Figura 1. Arquitetura da pilha de protocolos TCP/IP (Esmilda, 2005)

2.2 – Segurança da Informação

Segundo Soares (1995), “pode-se definir segurança como sendo a tentativa de minimizar a vulnerabilidade de bens e recursos, sendo vulnerabilidade qualquer fraqueza que possa ser explorada para atacar um sistema.”

2.3 – Sistemas de Detecção de Intrusão (IDS)

Os mecanismos atuais mais utilizados de detecção de intrusão procuram por assinaturas de ataque, que nada mais são do que padrões que indicam usualmente intenções maliciosas ou suspeitas. Essas atividades suspeitas podem variar de acordo com a política de segurança adotada pela empresa que utiliza o IDS, isto é, o nível desejado de informação sobre o tráfego de rede que o IDS fornece é determinado por esta política preestabelecida. No sistema computacional precisa-se determinar se deseja-se monitorar fluxos de rede, processos internos de uma estação ou servidor, ou ainda um sistema de arquivos. Deve-se deixar claro para quem enviar os alarmes ou relatórios e como estes devem ser enviados, tendo como alternativas o email, Pager ou ainda um pacote SNMP.

2.3.1 – Definições

Para Melo (1994):

O termo intrusão pode ser caracterizado como uma violação da política de segurança de um sistema. A detecção de intrusão monitora e analisa os eventos de uma rede de computadores, visando encontrar qualquer atividade que comprometa a confidencialidade, integralidade e disponibilidade de recursos computacionais ou de rede.

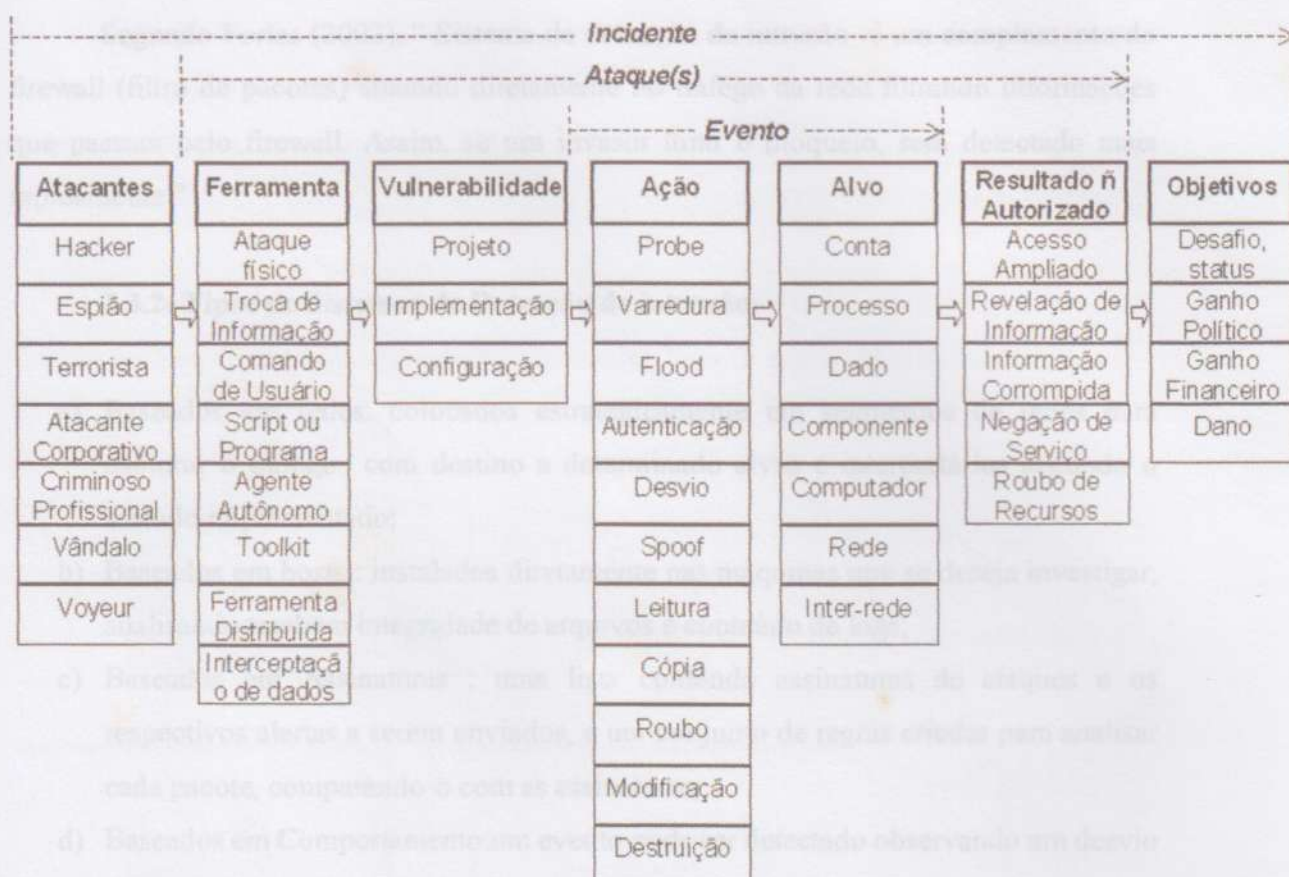


Figura 2. Caracterização de um Incidente de Segurança (Howard, 1998)

Amoroso (1999) define detecção de intrusão como sendo o processo de identificar e responder a atividades maliciosas dirigidas a computadores e recursos de rede.

Proctor (2001) descreve, dentre outras definições, que detecção de intrusão é a tarefa de coletar informações de uma variedade de fontes - sistemas ou redes - e então analisá-las buscando sinais de intrusão e de mau-uso. Vale considerar alguns detalhes em ambas as definições. No primeiro caso, o termo detecção de intrusão é usado tanto no sentido de detecção propriamente dito como na reação a essa atividade. Isso amplia a funcionalidade dos IDSs, impondo a eles a difícil tarefa de reagir aos ataques detectados. Proctor (2001), por sua vez, cria uma distinção entre os termos intrusão e mau-uso, sendo o primeiro compreendido por ataques originados externamente, e o segundo, ataques originados de dentro da organização.

Segundo Fortes (2002), “ Sistema de detecção de intrusão é um complemento do firewall (filtro de pacotes) atuando diretamente no tráfego da rede filtrando informações que passam pelo firewall. Assim, se um invasor furar o bloqueio, será detectado mais rapidamente.”

2.3.2- Tipos de Sistemas de Detecção de intrusão:

- a) Baseados em redes: colocados estrategicamente em segmentos de redes para capturar o tráfego com destino a determinado alvos e interpretá-los segundo o método implementado;
- b) Baseados em hosts : instalados diretamente nas máquinas que se deseja investigar, analisando também integridade de arquivos e conteúdo de logs;
- c) Baseados em Assinaturas : uma lista contendo assinaturas de ataques e os respectivos alertas a serem enviados, e um conjunto de regras criadas para analisar cada pacote, comparando-o com as assinaturas;
- d) Baseados em Comportamento: um evento pode ser detectado observando um desvio de comportamento esperado tanto dos sistemas como dos usuários.

2.3.3- O Snort IDS

Um IDS bastante utilizado é o Snort. Este sistema foi desenvolvido por Martin Roesch, é gratuito, e tem seu código aberto para que terceiros possam analisar e até mesmo acrescentar novas funcionalidades.

Outros softwares livres foram desenvolvidos para auxiliar na tarefa de análise de tráfego e detecção de intrusões numa rede. Um exemplo é o ACID (Analysis Console for Intrusion Detection) que mostra de forma mais inteligível os logs do Snort armazenados em um banco de dados.

O Snort é capaz de fazer análise de tráfego em tempo real, faz análise de protocolos, examina os pacotes recolhidos na rede e procura por palavras chaves. A principal função é detectar ações maliciosas na rede através da análise de tráfego. Seu código fonte foi desenvolvido na linguagem de programação C.

Para uma solução mais robusta, com dados sumarizados e interface amigável, é necessário que se instalem softwares auxiliares, como um banco de dados, um servidor web e o ACID para mostrar os resultados.

O Snort IDS é baseado em assinaturas e apresenta uma estrutura como a apresentada na Figura 3..

O sistema operacional proposto é o Linux, embora todos os softwares possuam versões para outros sistemas (FreeBSD, OpenBSD, Solaris, e em algum deles, Windows).

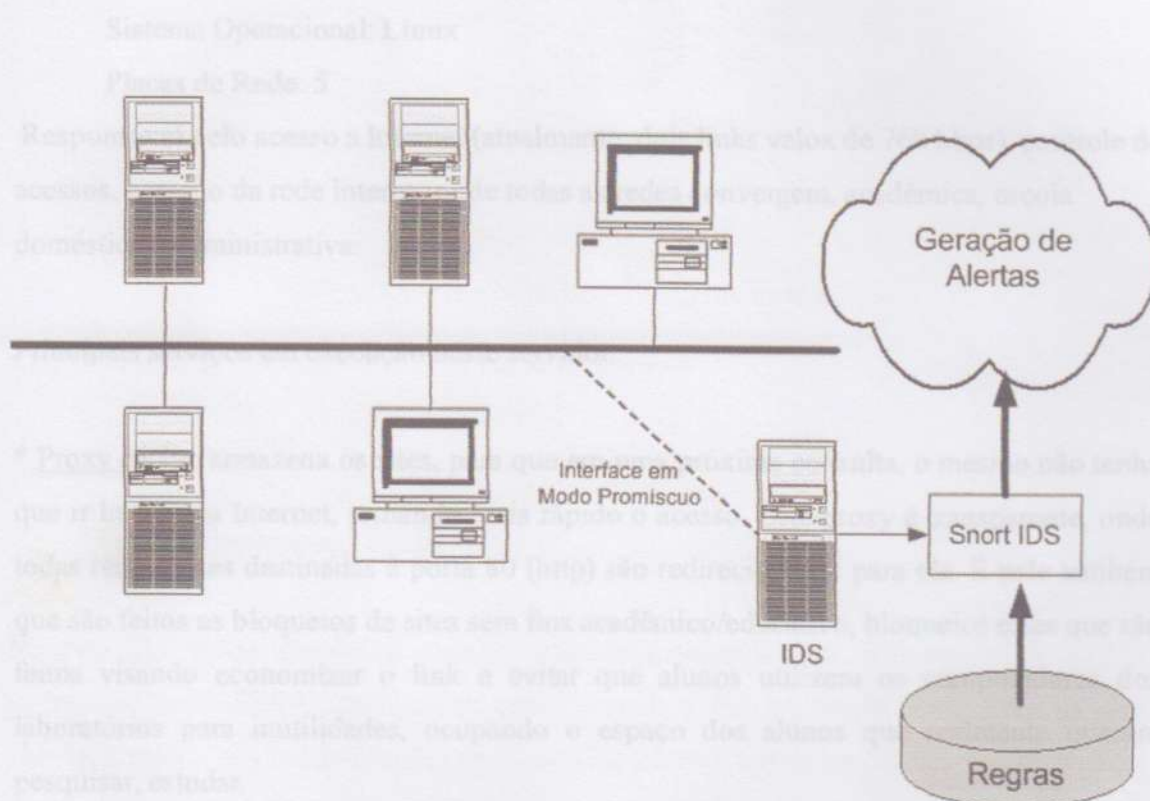


Figura 3. Caracterização de um IDS Snort

3. METODOLOGIA

3.1 LEVANTAMENTO DO AMBIENTE COMPUTACIONAL DA FARN

3.1.1 Servidor 01 – Roteador/Firewall da rede interna

Configuração:

Sistema Operacional: Linux

Placas de Rede: 5

Responsável pelo acesso a Internet (atualmente, dois links veloz de 768 kbps), controle de acessos, coração da rede interna, onde todas as redes convergem, acadêmica, escola doméstica e administrativa.

Figura 4 – Servidor 01 – Esquema da rede

Principais serviços em execução neste servidor:

* Proxy cache: armazena os sites, para que em uma próxima consulta, o mesmo não tenha que ir buscar na Internet, tornando mais rápido o acesso. Este proxy é transparente, onde todas requisições destinadas à porta 80 (http) são redirecionadas para ele. É nele também que são feitos os bloqueios de sites sem fins acadêmico/educativo, bloqueios estes que são feitos visando economizar o link e evitar que alunos utilizem os computadores dos laboratórios para inutilidades, ocupando o espaço dos alunos que realmente querem pesquisar, estudar.

* Firewall: Responsável pelos bloqueios (ex: MSN Messenger), quais redes terão acesso entre si (ex: a rede adm acessa todas as outras redes e a rede acadêmica enxerga somente a rede acadêmica), quais computadores terão acesso a Internet, redirecionamentos, etc.

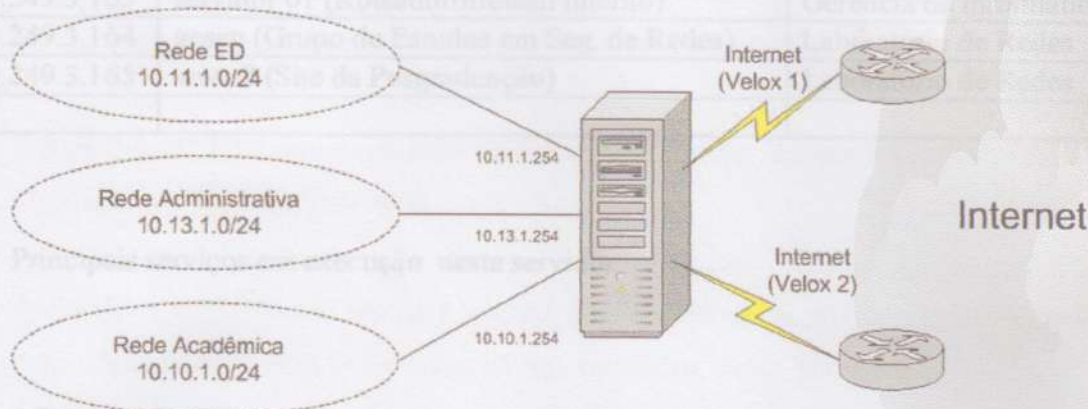


Figura 4 – Servidor 01 – Esquema da rede

3.1.2 Servidor WEBSERVER – Servidor de E-Mail

Configuração:

Sistema Operacional: Linux

Placas de rede: 2

Responsável pelos domínios: farn.br, escoladomestica.com.br, uninatal.br, hc.g12.br registrados na FAPESP, responsável pelos e-mails @farn.br, usado como DNS na rede interna, hospeda os sites da Escola Doméstica, Henrique Castriçano, Ensino a Distância e o Webmail da FARN. Possui um pequeno banco de dados para consultas realizadas pelos sites. Possui acesso a Internet através de um link dedicado pela Diginet, que fornece a FARN uma pequena faixa de IP, 200.249.3.160/29:

* Mail Scanner: faz a checagem dos e-mails utilizando o Anti-Spam e o Anti-Vírus.

IP	Dominio	Local
200.249.3.161	Roteador cisco	Gerência de Informática
200.249.3.162	webserver (servidor web/email)	Gerência de Informática
200.249.3.163	servidor 01 (Roteador/firewall interno)	Gerência de Informática
200.249.3.164	geseg (Grupo de Estudos em Seg. de Redes)	Laboratório de Redes
200.249.3.165	www2 (Site da Posgraduação)	Laboratório de Redes

Principais serviços em execução neste servidor:

- * Servidor SMTP: mais conhecido como MTA (Mail Transport Agent), recebe e envia os emails.
- * Servidor POP3: servidor para que os usuários tenham acesso por clientes de email, como Outlook Express, mozilla thunderbird, etc.
- * Servidor IMAP: IMAP significa Internet Message Access Protocol, possibilita o manuseio de forma otimizada dos e-mails, necessário para o funcionamento do webmail.
- * Anti Vírus: identifica vírus e scripts maliciosos, bloqueando e-mails e removendo anexos de acordo com as regras determinadas.
- * Anti Spam: tenta identificar Spams (mensagens indesejáveis) e bloqueá-los. As mensagens são examinadas e pontuadas (seguindo regras) de acordo com o conteúdo, por exemplo uma mensagem com anexos, palavras chaves (comuns em spams), fotos, com html terá uma pontuação muito maior do que uma mensagem apenas com texto puro. Mensagens com pontuação até 6, considerá-se limpa, não spam, mensagens com a pontuação entre 6 e 14 são marcadas com a tag "{Spam?}" para verificar se realmente é spam e para que possam ser filtradas por clientes de e-mail e no webmail, as mensagens com pontuação acima de 14 pontos serão bloqueadas e armazenadas por um tempo limite.
- * Mail Scanner: faz a checagem dos e-mails utilizando o Anti-Spam e o Anti-Vírus.

3.1.3 Servidor ACADEMICO – Domínio Windows

* **Servidor DNS:** responsável pelos domínios: farn.br, escoladomestica.com.br, uninatal.br, hc.g12.br e usado para resolução de nomes na rede interna (DNS primário ou secundário). É nele onde configurá-se os subdomínios dos domínios citados.

Sistema Operacional: Windows 2000 Server

* **Servidor HTTP:** hospeda os sites da Escola Doméstica, Henrique Castriciano, Ensino a Distância e o Webmail da FARN.

Configura o domínio de utilização de rede Windows, ACADEMICO, ligado à rede

* **Servidor SFTP:** utilizado por alguns professores para enviar arquivos para seus respectivos sites (áreas), como material para os alunos, notas, etc.

também é planejado para a rede ED

Principais serviços em execução neste servidor

3.1.4 Servidor WEBSERVER – Domínio Windows

* **Servidor DHCP:** envia dinamicamente endereços IP para as estações da rede acadêmica e ED.

* Servidor DNS, servidor de conversão de

* **Active Directory:** Banco de dados com de usuários da instituição, para a segurança, diretivas de segurança (Group Policy).



Figura 5 – Servidor WEBSERVER – esquema de rede

3.1.3 Servidor ACADEMICO – Domínio Windows

Configuração:

Sistema Operacional: Windows 2000 Server

Placas de rede: 2

Configura o domínio de utilização de rede Windows, ACADEMICO, ligado à rede acadêmica e ED. Neste domínio estão as contas de usuário de alunos, serviços administrativos da instituição e administradores das redes acadêmica e ED. O domínio também é oferecido para a rede ED.

Figura 6 – Servidor ACADEMICO – configuração de rede

Principais serviços em execução neste servidor:

3.1.4 Servidor ADMIN – Domínio Windows

* Servidor DHCP: envia dinamicamente endereços IP para as estações das redes acadêmica e ED.

* Servidor DNS: servidor de conversão de 'nomes totalmente qualificados'/'endereços IP' para as redes acadêmica e ED.

* Active Directory: Banco de dados com as contas de usuários do domínio, grupos de segurança, diretivas de segurança (Group Policies).

Principais serviços em execução neste servidor:

Servidor DHCP: envia dinamicamente endereços IP para as estações da rede adm.

Servidor DNS: servidor de conversão de 'nomes totalmente qualificados'/'endereços IP' para a rede adm.

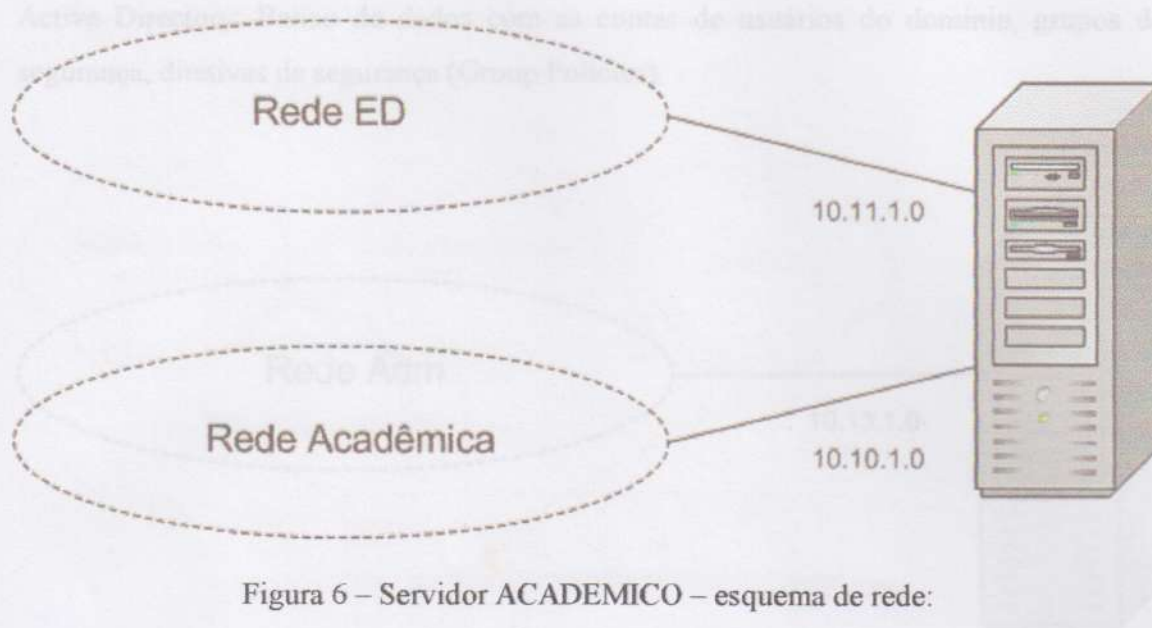


Figura 6 – Servidor ACADEMICO – esquema de rede:

Figura 7 – Servidor ADMIN – esquema de rede:

3.1.4. Servidor ADMIN – Domínio Windows

Configuração:

Sistema Operacional: Windows 2000 Server

Placas de rede: 1

Configura o domínio de utilização de rede Windows, ADMIN, ligado à rede adm. Neste domínio estão as contas do corpo administrativo da instituição, serviços administrativos da instituição e administradores das redes adm, acadêmica e ED.

Principais serviços em execução neste servidor:

Servidor DHCP: envia dinamicamente endereços IP para as estações da rede adm.

Servidor DNS: servidor de conversão de 'nomes totalmente qualificados'/'endereços IP' para a rede adm.

Active Directory: Banco de dados com as contas de usuários do domínio, grupos de segurança, diretivas de segurança (Group Policies).

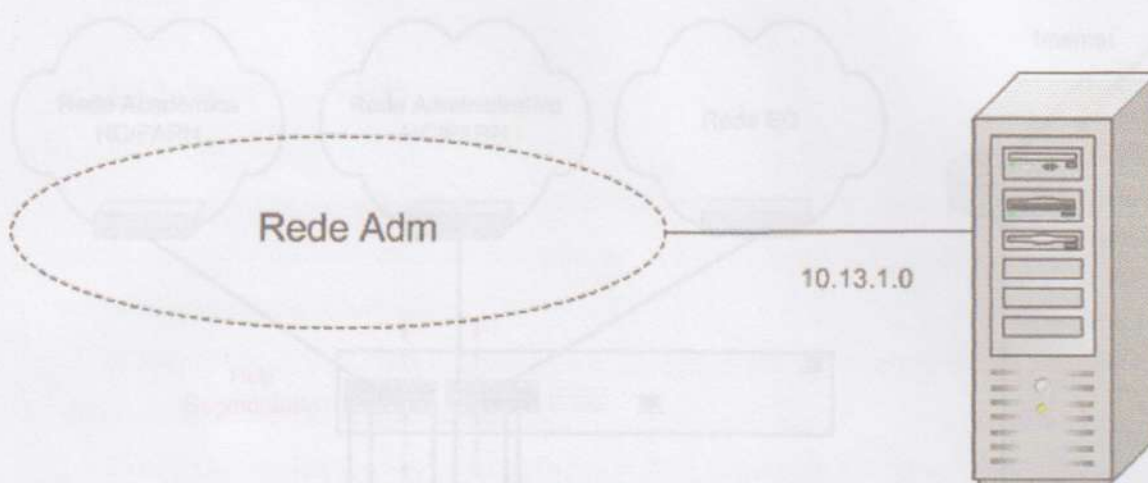


Figura 7 – Servidor ADMIN – esquema de rede

OBS: Os servidores ADMIN e ACADEMICO representam os pontos centrais das três intranets do complexo ED-HC-FARN, e não possuem acesso externo. São mantidos sob diretivas de segurança locais, protegendo seus próprios serviços dos usuários das redes internas. Possuem estratégias de segurança contra falhas de hardware e software. Externamente, eles recebem os serviços e são protegidos pelos servidores de frente (que utilizam sistema operacional linux) e roteador.

3.2- DEFINIÇÃO DO POSICIONAMENTO DO IDS

A escolha do segmento de rede para a instalação do IDS levou em conta a disposição física e lógica dos principais servidores da instituição, bem como das sub-redes da Internet.

Assim, como a rede da FARN tem 03 (três) sub-redes distintas, optou-se pela configuração de um IDS com 03 (três) placas de rede, sendo cada uma delas conectada a uma sub-rede específica (administrativa, acadêmica e ED)

3.4- SOFTWARE/HARDWARE DO IDS

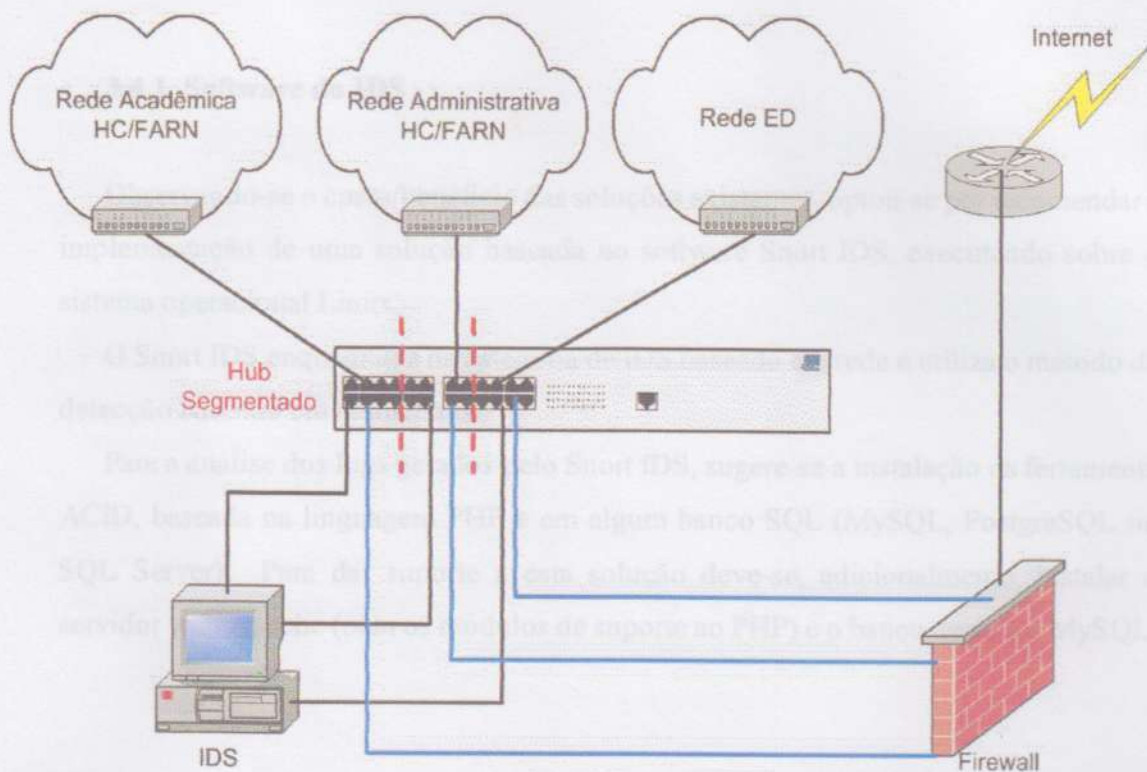


Figura 8. Tráfego das sub-redes da Farn

3.3- DESCRIÇÃO FÍSICA DE CONECTIVIDADE

Para que o IDS capture dados em tráfego pela rede sem ser ele um roteador, deve-se, além de habilitar o modo promiscuo em suas interfaces, utilizar como elemento de conectividade um hub ou um switch com porta de monitoramento.

Com base nos ativos disponíveis na FARN, optou-se por utilizar um hub com suporte a segmentação, segmentando-o em 03 (três) sub-redes, sendo que, em cada uma destas, são conectadas:

- uma interface do Firewall
- uma interface do IDS
- o switch principal de cada sub-rede

Assim, garante-se a análise pelo IDS de todo o tráfego nas 03 (três) sub-redes da Instituição, conforme figura 04.

3.4— SOFTWARE/HARDWARE DO IDS.

3.4.1. Software do IDS

Observando-se o custo/benefício das soluções existentes, optou-se por recomendar a implementação de uma solução baseada no software Snort IDS, executando sobre o sistema operacional Linux.

O Snort IDS enquadra-se na categoria de IDS baseado em rede e utiliza o método de detecção baseado em assinaturas.

Para a análise dos logs gerados pelo Snort IDS, sugere-se a instalação da ferramenta ACID, baseada na linguagem PHP e em algum banco SQL (MySQL, PostgreSQL ou SQL Server). Para dar suporte a esta solução deve-se, adicionalmente, instalar o servidor web Apache (com os módulos de suporte ao PHP) e o banco de dados MySQL.

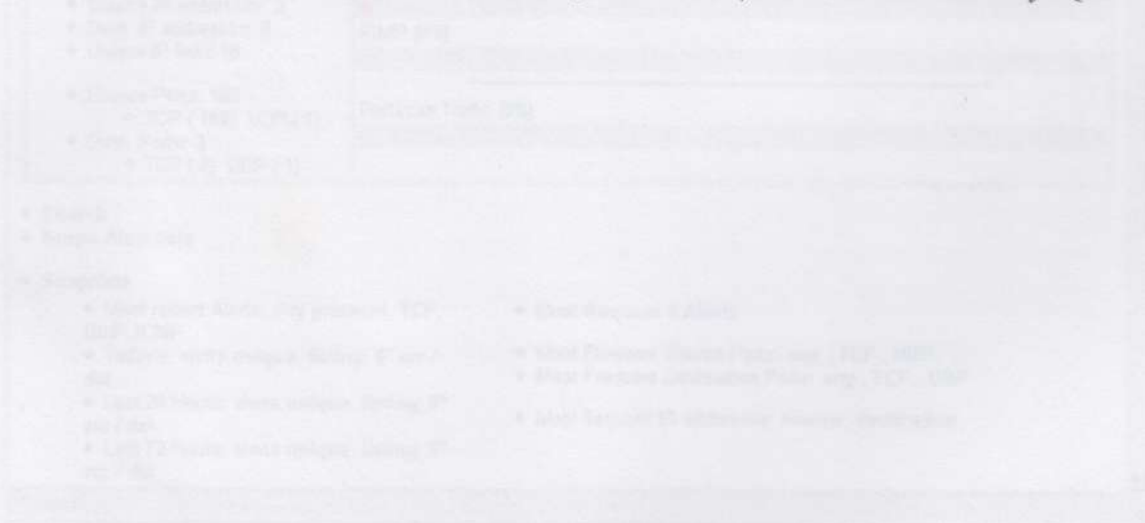


Figura 9. Tela Inicial da ACID

A tela principal do ACID, conforme Figura 9, apresenta um sumário dos dados armazenados na base de dados do aplicativo, como total de alertas, percentual de ataques por protocolo, dentre outros.

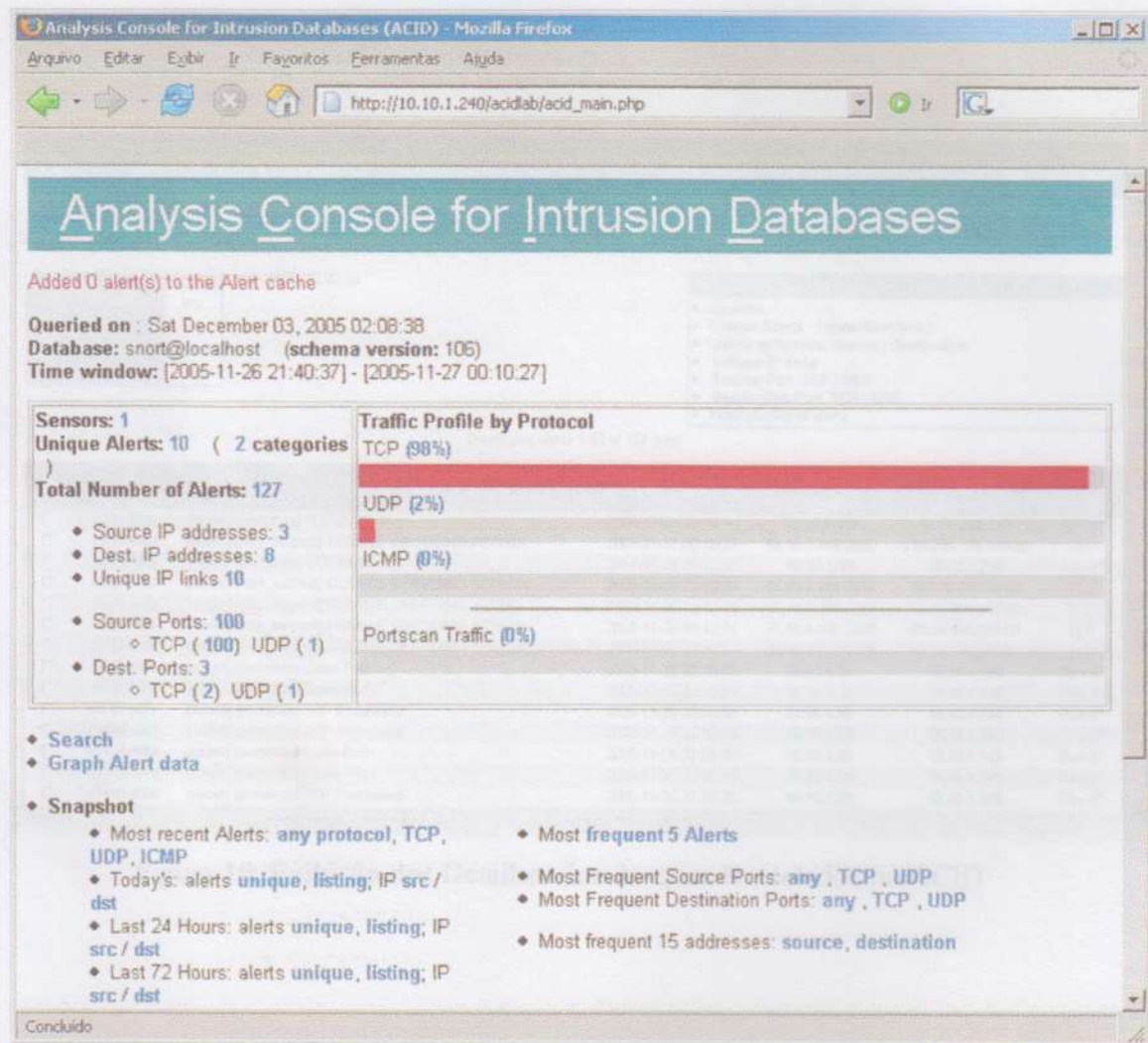


Figura 9. Tela Inicial do ACID

A figura 10 apresenta uma exibição detalhada de todos os ataques que foram detectados pelo ACID onde se tem detalhes das assinaturas, dos endereços de origem e endereços de destino dos ataques, bem como dia e horário dos ataques.

The screenshot shows the ACID Query Results page in a Mozilla Firefox browser. The page title is "Query Results". It includes a search bar and a "Back" link. A message states "Added 0 alert(s) to the Alert cache". The "Queried DB on" is "Sat December 03, 2005 02:20:09". A table shows the criteria used for the query: Meta Criteria (any), IP Criteria (any), Layer 4 Criteria (none), and Payload Criteria (any). A "Summary Statistics" box lists: Sensors, Unique Alerts (classifications), Unique addresses: source | destination, Unique IP links, Source Port: TCP | UDP, Destination Port: TCP | UDP, and Time profile of alerts. Below this, it says "Displaying alerts 1-50 of 127 total". A table lists the detected attacks with columns: ID, Signature, Timestamp, Source Address, Dest. Address, and Layer 4 Proto.

ID	Signature	Timestamp	Source Address	Dest. Address	Layer 4 Proto
#0 (1.415)	[snort] (portscan) TCP Portsweep	2005-11-26 23:30:16	10.10.1.148	82.94.245.158	Raw IP
#1 (1.416)	[snort] (http_inspect) DOUBLE DECODING ATTACK	2005-11-27 00:10:27	10.10.1.148.2082	216.250.141.190.80	TCP
#2 (1.410)	[snort] (portscan) TCP Portsweep	2005-11-26 23:12:15	10.10.1.39	10.10.1.240	Raw IP
#3 (1.414)	[snort] (http_inspect) DOUBLE DECODING ATTACK	2005-11-26 23:12:25	10.10.1.148.3614	207.46.216.60.80	TCP
#4 (1.413)	[snort] (http_inspect) DOUBLE DECODING ATTACK	2005-11-26 23:12:24	10.10.1.148.2082	65.54.194.118.80	TCP
#5 (1.412)	[snort] (http_inspect) DOUBLE DECODING ATTACK	2005-11-26 23:12:24	10.10.1.148.2489	65.54.168.250.80	TCP
#6 (1.411)	[snort] (http_inspect) DOUBLE DECODING ATTACK	2005-11-26 23:12:24	10.10.1.148.2079	65.54.194.118.80	TCP
#7 (1.409)	[snort] (portscan) Open Port	2005-11-26 23:10:59	10.10.1.39	10.10.1.145	Raw IP
#8 (1.408)	[snort] (portscan) Open Port	2005-11-26 23:10:59	10.10.1.39	10.10.1.145	Raw IP
#9 (1.407)	[snort] (portscan) TCP Portsweep	2005-11-26 23:10:36	10.10.1.39	10.10.1.240	Raw IP
#10 (1.406)	[snort] (portscan) TCP Portsweep	2005-11-26 22:57:06	10.10.1.39	10.10.1.145	Raw IP
#11 (1.405)	[snort] (portscan) Open Port	2005-11-26 22:55:55	10.10.1.39	10.10.1.145	Raw IP
#12 (1.404)	[snort] (portscan) Open Port	2005-11-26 22:55:55	10.10.1.39	10.10.1.145	Raw IP
#13 (1.403)	[snort] (portscan) TCP Portsweep	2005-11-26 22:55:25	10.10.1.39	10.10.1.145	Raw IP

Figura 10. Exibição dos Detalhes dos Ataques Detectados no ACID

3.4.2 Hardware do IDS

O conteúdo do pacote suspeito será exibido conforme a Figura 11 detalhando porta de origem e porta de destino do ataque e outras características do pacote.

The screenshot shows the ACID: Alert interface in a Mozilla Firefox browser. The address bar displays a URL: `http://10.10.1.240/acidlab/acid_gry_alert.php?submit=%233-%261-399%29&sort_order=`. The interface is divided into several sections:

- Options:** A dropdown menu showing "none".
- TCP Summary Table:**

source port	dest port	R	R	U	A	P	R	S	F	seq #	ack	offset	res	window	urp	chksum
4757	80			X	X					746638496	1679742992	8	0	1460	0	10717
- TCP Options:**

	code	length	data
#1	NOP	0	
#2	NOP	0	
#3	TS	8	002184C70085939F
- Payload:**

length = 271

Offset	Hex	ASCII
000	: 47 45 54 20 2F 2E 2E 2F 73 73 64 2E 69 6E 69 20	GET ../ssd.ini
010	: 48 54 54 50 2F 31 2E 31 0D 0A 43 6F 6E 6E 65 63	HTTP/1.1..Connection: Keep-Alive
020	: 74 69 6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65	..Host: 10.10.1.
030	: 0D 0A 48 6F 73 74 3A 20 31 30 2E 31 30 2E 31 2E	152..Pragma: no-cache..User-Agent: Mozilla/4.75
040	: 31 35 32 0D 0A 50 72 61 67 6D 61 3A 20 6E 6F 2D	[en] (X11, U; NetScape/4.75)
050	: 63 61 63 68 65 0D 0A 55 73 65 72 2D 41 67 65 6E	ssus)..Accept: image/gif, image/x-bitmap, image/jpeg, image/png, *
060	: 74 3A 20 4D 6F 7A 69 6C 6C 61 2F 34 2E 37 35 20	/*..Accept-Language: en..Accept-Charset: iso-8859-1,*;utf-8....
070	: 5B 65 6E 5D 20 28 58 31 31 2C 20 55 3B 20 4E 65	
080	: 73 73 75 73 29 0D 0A 41 63 63 65 70 74 3A 20 69	
090	: 6D 61 67 65 2F 67 69 66 2C 20 69 6D 61 67 65 2F	
0A0	: 78 2D 78 62 69 74 6D 61 70 2C 20 69 6D 61 67 65	
0B0	: 2F 6A 70 65 67 2C 20 69 6D 61 67 65 2F 70 6A 70	
0C0	: 65 67 2C 20 69 6D 61 67 65 2F 70 6E 67 2C 20 2A	
0D0	: 2F 2A 0D 0A 41 63 63 65 70 74 2D 4C 61 6E 67 75	
0E0	: 61 67 65 3A 20 65 6E 0D 0A 41 63 63 65 70 74 2D	
0F0	: 43 68 61 72 73 65 74 3A 20 69 73 6F 2D 38 38 35	
100	: 39 2D 31 2C 2A 2C 75 74 66 2D 38 0D 0A 0D 0A	

The status bar at the bottom indicates "Concluído".

Figura 11. ACID exibindo o conteúdo (payload) do pacote suspeito

3.4.2 Hardware do IDS

Para a implementação da solução proposta, o hardware deve ter memória e processador compatíveis com as necessidades de análise do tráfego nas três sub-redes da FARN. Assim, recomenda-se que disponha de, pelo menos, 512Mb de memória RAM e processador de, pelo menos, 1Ghz.

Atenção especial deve ser dada às placas de rede, já que estas são diretamente responsáveis pela captura dos dados nos segmentos. Pela robustez e qualidade reconhecidamente satisfatórias para este tipo de atividade, sugere-se placas 3Com ou Intel, com velocidade recomendável de 100Mbps (Fast Ethernet) e sugerida de 1Gbps (Gigabit Ethernet).

Se o computador não for adquirido já com a configuração final, recomenda-se observar se existem slots disponíveis para a instalação das 4 placas de rede.

4. ANÁLISE DE RESULTADOS

A análise dos registros (*logs*) do *firewall* em funcionamento na FARN não é suficiente para o fornecimento dos dados sobre os possíveis ataques que a instituição tem sofrido a partir da Internet contra a sua rede corporativa e principalmente, sobre os possíveis ataques internos, isto é, partindo da rede corporativa para a Internet ou mesmo de máquinas da rede corporativa contra máquinas da mesma rede.

A função de um IDS em uma rede de computadores é justamente complementar as atividades do *firewall* fornecendo informações sobre os tipos de ataque com detalhes sobre origem, destino e técnicas utilizadas.

A sugestão de utilização de software livre, barateia a implementação da solução, viabilizando financeiramente a solução como um todo.

A instalação dos softwares sugeridos em ambiente de testes (laboratório) demonstram a sua eficácia na identificação de ataques contra máquinas nos perímetros monitorados.

6. REFERÊNCIAS BIBLIOGRÁFICAS

5. CONCLUSÃO

ALLEN, M. *Intrusion Detection: An Introduction to Intrudet*. Sparta, New Jersey: Net Books, 1992.

FORTES, A. A instalação de uma solução IDS na rede da FARN, proposta neste trabalho, pode vir a representar um mecanismo extremamente importante à segurança da rede de computadores desta instituição.

A quantidade de informações adicionais advindas desta implantação poderão vir a ratificar a relevância deste trabalho, avaliadas as carências administrativas constatadas na fase de levantamento do ambiente computacional da FARN.

A implementação de um sistema de detecção de intrusão é imprescindível para se ter a noção real dos ataques e tentativas de ataques e também auxiliar na resposta a estes ataques em andamento.

NEHAQ, Teresa Cristina. *Arquitetura de redes de computadores OSI e TCP/IP*. São Paulo: Makron Books, 1994.

PROCTOR, Paul. *Practical Intrusion Detection Handbook*. New Jersey: Prentice Hall, 2001.

SGARES, Luis P.G. *Redes de Computadores: das LANs, MANs e WANs as redes ATM*. Rio de Janeiro: Campus, 1993.

TANENBAUM, Andrew. *Redes de Computadores*, tradução Vanderberg D. de Souza. Rio de Janeiro: Elsevier, 2003.

TORRES, Gabriel. *Redes de Computadores: Curso Completo*. Rio de Janeiro: Arca, 2001.

6. REFERÊNCIAS BIBLIOGRÁFICAS

- AMOROSO, Edward. **Intrusion Detection: An Introduction to Internet**. Sparta, New Jersey: Net Books, 1999.
- FORTES, Débora. **Segurança**. Sua empresa está vulnerável?.Info Exame.São Paulo.v.XVIII, n.195, junho.2002.
- GALVÃO, Ricardo. **Sistema de detecção de intrusão**. Disponível em: <http://www.ricardokleber.cjb.net> . Acesso em 15/04/2005.
- HOWARD, John D.;LONG STAFF, Thomas A. **A common language for computer security incidents**. Livermore, CA: Sandia National Laboratories, 1998.
- LARI, Paulo Augusto; AMARAL, Dino. **Snort, mysql, apache e acid.: guia pratico**. Rio de Janeiro: Brasport, 2004.
- MANCIN, Francisco. **Redes de Computadores**. São Paulo, 2002.
- MELO, Tereza Cristina. **Arquitetura de redes de computadores OSI e TCP/IP**. São Paulo:Makron Books. 1994.
- PROCTOR, Paul. **Practical Intrusion Detection Handbook**. New Jersey: Prentice Hall, 2001.
- SOARES, Luiz F.G.. **Redes de Computadores:das LANs,MANs e WANs as redes ATM**,Rio de Janeiro:Campus, 1995.
- TANENBAUM, Andrew. **Redes de Computadores**; tradução Vandenberg D. de Souza. Rio de Janeiro: Elsevier, 2003.
- TORRES, Gabriel. **Redes de Computadores: Curso Completo**.Rio de Janeiro:Axcel, 2001.