UNIVERSIDADE DE LISBOA
FACULDADE DE CIÊNCIAS
DEPARTAMENTO DE INFORMÁTICA

ANALISADOR COMPORTAMENTAL DE REDE

João Manuel Alexandre Cardana

MESTRE EM INFORMÁTICA

Novembro 2006

ANALISADOR COMPORTAMENTAL DE REDE

João Manuel Alexandre Cardana

Dissertação submetida para obtenção do grau de
MESTRE EM INFORMÁTICA

pela

Faculdade de Ciências de Lisboa

Departamento de Informática

Orientador:
Nuno Fuentecilla Maia Ferreira Neves

Júri:
Ana Paula Pereira Afonso
André Ventura da Cruz Marmoto Zúquete
Maria Dulce Pedroso Domingos

Novembro 2006

Resumo

A globalização das comunicações e a necessidade da partilha de informação, tem provocado um impacto inegável na segurança dos dados que transitam pelas redes de computadores. As vulnerabilidades que surgem constantemente, dia após dia, criaram a necessidade que novos dispositivos de segurança fossem desenvolvidos, com capacidades cada vez mais evoluídas. Por exemplo, equipamentos maioritariamente de prevenção de ataques, como as anteparas de segurança, deixaram de ser suficientes para fazerem face às ameaças, obrigando a que surgissem soluções para a descoberta de ataques/intrusões em tempo real.

Muitos dos sistemas de detecção de intrusões comercializados actualmente, são incapazes de localizar novos ataques, que não estejam previstos nas suas bases de dados. Estes equipamentos precisam assim de uma actualização periódica das assinaturas de ataques para que se mantenham eficazes. Neste trabalho propõe-se um sistema complementar, que se baseia numa análise comportamental do funcionamento da rede. Neste sistema existe uma fase inicial de aprendizagem, que resulta na definição de um comportamento padrão da rede. Depois, na fase de detecção, procuram-se anomalias com algum significado estatístico, correspondendo cada uma delas potencialmente a um ataque.

A solução proposta assenta em três processos distintos, que são executados com uma periodicidade reduzida. O processo de captura recolhe o tráfego existente na rede, retira alguns dados relevantes dos pacotes, e armazena-os numa estrutura hierárquica. No fim de cada período, o processo de análise aplica alguns métodos estatísticos para gerar um conjunto (caso exista) de excepções, que correspondem aos comportamentos anómalos que foram observados. Por último, o processo de decisão baseia-se nas excepções para, por exemplo, informar o administrador que um ataque está em curso, ou para interagir directamente com os outros equipamentos de rede de maneira a minorar (ou idealmente terminar) os efeitos do ataque.

A tese descreve uma concretização deste modelo, e faz uma avaliação do protótipo numa rede de computadores sujeita a vários tipos de ataques. Os resultados mostram que o modelo descrito é eficaz para detecção de diversos ataques de negação de serviço.

Palavras-Chave: Segurança informática, Detecção de intrusões, Análise de comportamentos anómalos na rede, Respostas a ataques, Agregação e tratamento de dados de rede.

Abstract

The globalization of the communications and the necessity of shared information infrastructures, have provoked an undeniable impact in the security of the data that transits through the networks. The vulnerabilities that appear constantly, day after day, have created a need for new security devices with more evolved capabilities. For example, equipments for attack prevention, like firewalls, are unable to cope with the current threats, and for this reason solutions have been developed for the discovery of attacks/intrusions in real time.

Most of the intrusion detection systems commercialized today are incapable of locating new attacks, which are not foreseen in their databases. These equipments need a periodic update of the attack signatures in order to continue to perform their activities in the expected way. In this thesis, we propose a complementary intrusion detection solution. This system has an initial learning phase, which results on a definition of the standard behavior of the network. Later, during the detection phase, it looks for anomalies with some statistical meaning, each one corresponding to a potential attack.

The proposed solution is based on three distinct processes that are executed with a small periodicity. The capture process collects the current traffic of the network, selects some data from the packets, and saves it in a hierarchical storage. In the end of each period, the analysis process applies some statistical methods to generate a set (in case they exists) of exceptions that correspond to the anomaly behavior that was observed. Finally, the decision process uses the exceptions, for example, to inform the administrator of an attack, or to interact with the other network equipment to reduce the effects of the attack.

The thesis also describes an implementation of this model, and makes an evaluation of the prototype on a network where several kinds of attacks exist. The results show that the described system is efficient for detention of a diverse set of denial of service attacks.

Keywords: Computer security, Intrusion Detection, Analysis of anomaly behaviors, Attack responses, Aggregation and data handling.

Agradecimentos

Desejo agradecer a todas as pessoas que, directa ou indirectamente, contribuíram para a realização desta Tese de Mestrado, especialmente ao meu orientador Professor Nuno Ferreira Neves.

A título mais pessoal, gostaria de agradecer à minha esposa Maria João todo o apoio e encorajamento que me deu durante os momentos de maior desânimo e na ajuda que me prestou nas correcções e nas constantes melhorias. Ao meu filhote Ricardo que tanto sofreu com o meu mau feitio e pela falta de tempo para as brincadeiras que ele tanto gosta. Ao meu pai, à minha mãe e à minha irmã. E aos meus amigos e familiares pelos fins-de-semana que se privaram e da tolerância demonstrada pelas minhas constantes faltas a compromissos marcados.

A todos o meu obrigado.

Índice

Lista de figuras

Lista de tabelas

Capítulo 1

Introdução

1.1 Enquadramento do trabalho

A evolução das redes ao longo da última década mudou radicalmente a nossa maneira de estar e comunicar. Os ambientes controlados em que predominavam as redes fechadas que recorriam a protocolos privados sem qualquer interligação com o exterior, foram na maioria dos casos abandonados. Hoje em dia, o "estar sempre ligado" é uma necessidade corrente que tem como consequência a utilização de meios de comunicação muito variados, assentando os mesmos em redes abertas. Esta necessidade introduz o conceito de meio partilhado a partir do qual se garante o acesso independentemente da localização do ponto de acesso e da infra-estrutura de transporte usada para transferência de informação.

Esta necessidade de interligação tem provocado um grande impacto ao nível da segurança da informação que transita nestes meios de comunicação, deixando assim de existir as redes simples, fechadas, sem interligação e partilha de informação, e transitando-se para as redes partilhadas. Estas redes encontram-se interligadas por meios distintos e heterogéneos como as Intranets, Extranets e a Internet, facilitando trocas mais rápidas de informação entre meios.

Com todas estas facilidades surgem uma série de questões. Genericamente o que se pretende é, "*Como posso usar um meio que é partilhado de modo a que a minha informação transite sem ser alterada, danificada ou observada por uma terceira parte que não pertence ao meu fluxo de informação? "*

Para se atingir este objectivo é preciso garantir a:

- *Confidencialidade dos dados*: A confidencialidade dos dados garante que a informação não é vista por utilizadores não autorizados.
- *Autenticidade dos dados*: A informação transferida deve identificar quem a transmite.
- *Não repudiação dos dados*: A informação deve possibilitar mais tarde provar quem a enviou.
- *Integridade dos dados*: A integridade dos dados previne a modificação não autorizada da informação, a verificação da identidade e autenticidade de um

utilizador ou agente externo de um sistema, a fim de assegurar a integridade de origem.

- *Disponibilidade*: A disponibilidade deve garantir um acesso contínuo aos meios de comunicação.

Claro que existem uma série de mecanismos disponíveis que permitem resolver as questões acima indicadas, no entanto estes mecanismos levam a um aumento da complexidade das redes, tais como:

- Cifra da informação de modo a garantir a confidencialidade dos dados.
- Autenticação prévia dos interlocutores de modo a garantir autenticidade dos dados.
- Assinaturas digitais de documentos de modo a garantir a não repudiação.

Com a possibilidade de existir toda esta troca de informação independentemente do meio de interligação, a exposição aumenta e a segurança dos sistemas/comunicações necessita de crescer para fazer face aos inúmeros ataques. Para garantir a protecção, aumentamos a complexidade dos sistemas e ficamos perante a situação em que *"quanto maior a segurança a dar a um sistema maior a sua complexidade"*.

Este tipo de sistemas/comunicações estão sujeitos a uma série de ameaças como por exemplo:

- *Interrupção*: permite interromper uma comunicação e proceder à modificação da informação associada a um tipo de transacção electrónica.
- *Usurpação*: aproveitamento da informação obtida associada a um tipo de transacção electrónica de forma a ser utilizada em proveito próprio.
- *Fraude*: a praticada contra elementos de informática, das quais são exemplos a sabotagem informática, o furto de dados e a espionagem informática.

Este tipo de ameaças pode ser classificadas como: passivas, activas, intencionais ou acidentais.

- As ameaças *passivas* são aquelas que não provocam alteração ou modificação da informação, enquanto as *activas* são as que provocam uma modificação da informação intervindo nos estados de um sistema.

- As ameaças *acidentais* são as que não estão associadas a intenções premeditadas. Alguns exemplos de ameaças acidentais são a falta de formação que pode provocar descuidos na gestão da rede. Nas ameaças *intencionais* existe uma intenção premeditada na execução, como por exemplo a observação de dados com ferramentas simples de monitorização de redes.

Estas ameaças aparecem às vezes sob a forma de um vírus ou um verme (do Inglês Worm), e tratando-se estes de produtos que visam atacar um qualquer computador que esteja isolado ou inserido numa rede de computadores. Um dos objectivos dos vírus digitais é o de invadir e provocar a destruição, tendo a capacidade de se multiplicar inúmeras vezes, causando desta forma o avanço da infecção.

As infecções deste tipo são cada vez mais fáceis de acontecer. Para se perceber um pouco como se deu esta evolução, pode-se recuar aos anos 80, altura em que apareceram os primeiros vírus activados na inicialização do computador (do Inglês Boot Process) e onde o processo de contaminação era muito lento, podendo levar semanas a acontecer. Já na década de 90, com o divulgar do computador como posto de trabalho e com o aparecimento de sistemas operativos mais simples de utilizar, surgem os vírus/vermes tal e qual como os conhecemos, em que o período de contaminação é reduzido de semanas para dias. Desta forma aparecem os vírus com base em macros que incidem sobre ferramentas de trabalho usadas no dia à dia, tais como os processadores de texto, clientes de mail e outros. A evolução destes processos de infecção tem nos nossos dias um grande impacto ao nível de ataques de negação de serviço (DoS, do Inglês Denial of Service), tendo como principal objectivo a degradação do desempenho das redes alvo, de modo a deteriorar um determinado serviço ou rede.

Actualmente os ataques são executados de forma distribuída, denominados DDoS (do Inglês Distributed DoS), deixando agora de estar confinados a uma infra-estrutura para passarem a ser distribuídos, podendo ser despoletados de um qualquer ponto de um meio partilhado. Esta forma de ataque DDoS tem como base a utilização de agentes de software que se encontram espalhados numa infra-estrutura de rede e segundo uma ordem central vão iniciar um ataque coordenado contra um alvo comum.

Hoje em dia, tornou-se relativamente simples a obtenção das ferramentas usadas neste tipo de ataques. Basta para tal o acesso aos sites que exploram este tipo de assuntos, e que as disponibilizam sem qualquer custo a quem as quiser usar. A complexidade de utilização destas ferramentas também é extremamente baixa, comparado com a complexidade da concepção das mesmas. Existem mesmo determinadas ferramentas que dispõem de menus muito simples para seleccionar o ataque que se pretende despoletar.

1.2 Soluções de mitigação

Actualmente existem uma série de soluções que permitem tratar este tipo de ataques, muitas delas são denominadas de sistemas de detecção de intrusões (IDS, do Inglês Intrusion Detection System) [1]. Em alguns casos este tipo de sistemas assenta na prévia catalogação dos ataques em assinaturas [2]. Noutros casos, existem mesmo sistemas que se baseiam na detecção de anomalias de rede, tendo como base o conhecimento do funcionamento da mesma [3]. Todo este conhecimento resulta de uma fase prévia de aprendizagem do comportamento normal da rede. Após esta fase, aplica-se este comportamento ao processo de análise da rede, determinando-se se algo está fora dos limites do comportamento padrão, o que indicaria um possível ataque.

Alguns destes sistemas são pró-activos relativamente à resolução de problemas, podendo ter associados uma série de acções para resolução das anomalias detectadas. Existem várias acções que podem ser despoletadas, tais como:

- *Bloqueio de sessões de forma automática ("TCP Reset"):* acção de bloqueio de uma sessão TCP/IP, em que se interage com a sessão terminando-a para que a transacção associada fique concluída, através da utilização da flag de *Reset* do campo de *Control* do protocolo TCP [4].
- *Desvio de tráfego para sistemas de limpeza de informação:* a este tipo de sistemas estão associados dois tipos de mecanismos [5]. O primeiro interpreta o que se passa na rede, analisando desvios ao comportamento padrão. O outro, ao receber uma instrução do primeiro, interage com a rede obrigando o tráfego anómalo a ter como destino ele próprio, fazendo deste modo uma separação/limpeza entre o tráfego anómalo e o normal.

- *Colocação de barreiras ao tráfego anómalo:* as barreiras são colocadas automaticamente quando é detectada uma anomalia na rede [6]. Este mecanismo automático tem como objectivo colocar determinados filtros ao tráfego anómalo mais próximo da origem do mesmo. Associado a este tipo de barreiras está a dificuldade de avaliar o tráfego anómalo. Outros sistemas apontam para a capacidade de se ter inteligência própria, de modo a que sejam tomadas decisões de bloqueio automático, recorrendo à capacidade deste tipo de equipamentos estarem colocados em série na rede.
- *Registo do tráfego anómalo:* os registos de tráfego anómalo, para que posteriormente através de mecanismos de correlação de eventos seja feita uma análise da rede, são processos que estão associados a ferramentas de auditoria [7]. É um tipo de solução que assenta num ponto central de recepção de eventos produzidos por diferentes equipamentos de rede, podendo despoletar uma série de recomendações de correcção das diferentes anomalias detectadas.
- *Fluxos de informação:* baseia-se na capacidade de os equipamentos de comunicação poderem registar fluxos de informação, sendo um fluxo de informação constituído por diferentes campos que o identificam: endereço origem/destino e tipo de protocolo utilizado. Centralizando todo este tipo de informação aumenta-se a capacidade de pro-actividade na resposta a anomalias detectadas na rede, facilitando deste modo o ajuste de determinadas configurações, tais como: ajuste de políticas de qualidade de serviço, capacidade de interpretar quais os protocolos existentes ou quais os que consomem mais recursos de rede [8].

1.3 Contribuição

Os mecanismos existentes, no entanto, não tratam bem uma série de excepções relativas à análise de tráfego gerado na rede. Estas excepções assentam essencialmente em determinados protocolos, tais como os seguintes exemplos o indicam:

- *Tipo e quantidade de informação*: que tipo de informação é tipicamente acedida, que quantidade de informação por protocolo fluí num determinado período de

tempo, quais os acessos mais comuns em termos aplicacionais, como por exemplo análise de acessos a servidores de transferência de ficheiros.

- *Objectos desconhecidos relativamente a determinados protocolos:* numa rede existe uma série de protocolos não catalogados que podem ter impacto no seu desempenho. A falta de controlo destes protocolos desconhecidos leva, grande parte das vezes, ao projecto de sucessivas evoluções dos equipamentos de rede de modo a que mais tráfego possa ser suportado, tendo por vezes consequências no dimensionamento da largura de banda usada na comunicação.
- *Comportamento da rede ao nível de protocolos não catalogados e que existem na rede:* perceber como as aplicações usam estes protocolos e que tipo de informação fluí na rede.
- *Transferências de informação:* detecção de tráfego anormal relativo a transferências de grandes quantidades de informação entre pontos da rede onde esse tipo de transferências não é usual ou permitido. Como exemplo: transferência de informação para um computador que se encontre localizado externamente relativamente à infra-estrutura.
- *Anomalias detectadas ao nível de protocolos:* pacotes que violem o comportamento padrão com dimensões que não são usuais.

Os exemplos anteriores normalmente não são tratados pelas ferramentas actuais, pois podem estar enquadrados no comportamento normal da rede. Nesta tese pretende-se construir um analisador comportamental para os diversos tipos de protocolos que flúem numa rede e garantir a sua interacção com os componentes activos de rede, tais como: encaminhadores (do Inglês router), comutadores (do Inglês switch) e anteparas de segurança (do Inglês firewall), de modo a que seja possível ajustarem a rede com base no seu comportamento.

Se um protocolo ao nível aplicacional fluí numa rede e consome em média uma determinada largura de banda, esta informação pode ser usada para ajustar a rede em termos de qualidade de serviço. Caso o impacto deste protocolo na rede tenha como efeito degradar o funcionamento da mesma, então como solução deve-se bloquear ou reduzir o fluxo deste tipo de tráfego de forma a garantir que os comportamentos anómalos possam ser corrigidos de maneira automática e ajustados de acordo com o comportamento padrão da rede. Pretende-se

que este ajuste seja feito de uma forma genérica, automatizada, e independentemente do equipamento de comunicações que se pretende configurar.

1.4 Estrutura da tese

A estrutura da tese assenta nos capítulos:

- O segundo capítulo destina-se a estudar o funcionamento dos sistemas de detecção de intrusões existentes, sendo explicado o seu funcionamento ao nível dos sistemas baseados em assinaturas e outros que se baseiam em detecção de anomalias de rede. Neste capítulo serão também abordados alguns mecanismos de correlação de informação existentes e como os mesmos podem interagir com uma infra-estrutura de rede, com o objectivo de potenciar a integração de todos os componentes da rede na prossecução de uma política de segurança comum.
- No terceiro capítulo explica-se em detalhe a componente da solução que tem como objectivo a correcção dos problemas acima referidos, reflectindo-se nesta parte todas as opções tomadas relativamente a alguns métodos existentes de tratamento de informação de registos de transferência de dados (do Inglês logging information), fluxos de informação que determinados equipamentos de rede conseguem capturar, de modo a poderem ser analisados por sistemas centralizados e dedicados. Pretende-se neste capítulo fazer uma descrição dos processos envolvidos nesta componente, tais como: recolha, análise, decisão e geração de mensagens genéricas.
- No quarto capítulo é feita uma descrição da concretização do componente e um conjunto de testes, tendo como objectivo a demonstração prática da solução proposta no capítulo anterior. Em particular deseja-se mostrar a pro-actividade do sistema relativamente à detecção de anomalias de rede e sua correcção em tempo real.

Capítulo 2

Trabalho Relacionado

Neste capítulo faz-se uma abordagem dos sistemas de detecção de intrusões relativamente ao modo como operam na rede, os métodos que utilizam para detectar intrusões e como interagem com os componentes activos de rede. Nesta abordagem apenas são considerados os IDS de rede [10], sendo esquecidos outros tipos de IDS, como os baseados na máquina (do Inglês Host IDS) [9], uma vez que estes são pouco relevantes para o trabalho da tese.

2.1 Detectores de intrusão

As ferramentas para segurança de computadores e redes existem para proporcionar transacções seguras. A grande parte das instituições concentra as suas defesas em ferramentas preventivas tais como anteparas, ignorando os sistemas de detecção de intrusões.

Os IDS são equipamentos passivos que tem como objectivo observar todo o tráfego ao longo de um caminho específico, tendo como principal acção o envio de eventos de aviso, sobre a descoberta de uma actividade suspeita, normalmente para uma consola de gestão. Uma grande parte dos IDS realiza as suas operações a partir da análise de padrões ao nível da infra-estrutura de rede [10].

- Tentativas de entrada em sistemas protegidos.
- Número de ligações detectadas.
- Volume de informação trocada na rede.

2.1.1 Localização dos IDS

Os ataques têm a sua origem em qualquer ponto da rede, quer se trate de redes locais ou outras. Muitas vezes, pode não ser suficiente a colocação dos equipamentos de monitorização apenas nos pontos de entrada na rede. Estes equipamentos de monitorização, também conhecidos por sensores ou detectores de intrusão, podem também estar localizados:

- Atrás de anteparas que permitam o acesso a zonas críticas.
- Em segmentos de rede associados a zonas desmilitarizadas (DMZ, do Inglês demilitarised zone) que contêm serviços públicos, do tipo: servidores de Web, transferência de ficheiros (FTP, do Inglês File Transfer Protocol), resolução de nomes

(DNS, do Inglês Domain Name System), ou servidores associados a comércio electrónico.

- Por detrás de concentradores de túneis [11], para observar tráfego decifrado.
- Em segmentos de rede que contêm servidores empresariais ou serviços de Intranet que são sensíveis de acordo com a política de segurança usada.
- Em segmentos utilizados por servidores de gestão.
- Na Intranet empresarial onde residam serviços críticos.
- Nos pontos de junção entre a Extranet, a rede interna e as redes remotas, bem como, nas junções da rede empresarial e das redes de parceiros de negócio.

Adicionalmente à colocação de equipamentos de monitorização, os gestores de redes recorrem a mecanismos de bloqueio de ataques tais como: filtros de controlo aplicados nas interfaces dos encaminhadores e nas anteparas internas de modo a prevenir os ataques ou o contágio dos recursos associados aos sistemas de informação.

2.1.2 Limitações à observação de tráfego

A grande maioria das redes tem vindo a migrar os concentradores (do Inglês Hub) para topologias de comutadores ao longo destes últimos cinco anos. Os concentradores funcionam por difusão do tráfego por todas as interfaces, facilitando a captura de informação em qualquer interface, permitindo desta forma que sensores de monitorização consigam automaticamente ver e capturar todo o tráfego que atravesse o concentrador.

Os comutadores enviam o tráfego apenas para a interface que tem o endereço MAC (Medium Access Control) do destino do pacote. Deste modo os detectores de intrusão não conseguem ver e capturar o tráfego que atravessa o comutador em circunstâncias normais. De modo a fazer face a esta limitação, as interfaces de monitorização associadas aos IDS devem ser ligadas a uma porta do comutador que permita a observação do tráfego de todas as interfaces ou de todas as redes virtuais (VLAN, do Inglês Virtual Local Area Network) associadas. Desta forma os comutadores devem suportar a funcionalidade de copiar tráfego de uma interface, ou conjunto de interfaces ou mesmo dum conjunto de redes virtuais, para uma

interface onde reside o equipamento de detecção de intrusões, recebendo tráfego de entrada ou saída.

2.2 Técnicas de detecção de intrusões

Um sistema de IDS é um processo ou conjunto de processos, cuja função é detectar actividades incorrectas, maliciosas ou anómalas. Pode ser definido como uma forma de monitorização e análise de eventos ocorridos num ambiente de sistemas de computadores, na procura de sinais que indiquem a existência de problemas de segurança. Apresenta-se como uma espécie de alarme anti-intrusão para computadores, podendo observar as actividades relativas a um computador ou a uma rede, recorrendo à geração de alarmes e podendo tomar acções reactivas quando uma intrusão ou abuso é detectado.

2.2.1 Terminologia

Quando se fala de sistemas de detecção de intrusões utilizam-se um conjunto de termos que importa clarificar, os principais termos são:

- *Política de segurança:* conjunto de normas internas definidas pela a empresa e que devem ser seguidas para que todas as ameaças sejam minimizadas e combatidas eficientemente.
- *Ataque:* qualquer tentativa de uma pessoa não autorizada em comprometer a funcionalidade de um sistema.
- *Vulnerabilidade:* problema associado a um sistema de informação que pode levar, quando explorado por um ataque, a uma quebra das regras definidas na política de segurança.
- *Intrusão:* violação da política de segurança definida para os sistemas de informação, invasão de um sistema para provocar o mau uso do mesmo.
- *Alarme:* Associado à detecção de violação de uma regra da política de segurança.

- *Falso Positivo:* utilizado para designar uma situação em que um dispositivo detectou uma actividade como sendo um ataque ou intrusão, quando na verdade essa actividade não era maliciosa.
- *Falso Negativo:* ocorre quando uma intrusão real acontece, mas o dispositivo de detecção considerou-a uma acção legítima.

2.2.2 Como classificar uma intrusão

De uma forma simples, podemos dizer que um intruso é alguém que tenta invadir um sistema ou fazer mau uso do mesmo, mas: O que é invadir um sistema? O que é fazer mau uso do sistema? Um utilizador que tenta aceder a um sistema e que erra três vezes a senha, pode ser classificado como um intruso?

Uma intrusão pode ser detectada de duas formas possíveis:

- *Intrusão devido à má utilização do sistema*: a monitorização incide sob uma análise das acções que ocorrem no sistema, e as intrusões correspondem a acções maliciosas previamente catalogadas como tal, por exemplo, num conjunto de assinaturas.
- *Intrusão devido a comportamento anómalo*: são detectadas com base na observação de alterações de comportamento relativamente ao comportamento padrão do sistema. Este método recorre usualmente a duas fases, uma fase denominada de aprendizagem onde se define o perfil do sistema, e de seguida segue-se o processo de monitorização no qual se avalia as divergências relativamente ao perfil definido na fase de aprendizagem.

2.2.3 Mecanismos associados à detecção de intrusões

Um IDS pode ser constituído utilizando um conjunto variado de mecansimos nomeadamente:

- Detecção com padrões conhecidos.
- Detecção com base em estados do comportamento padrão.
- Descodificação por protocolo.

- Assinaturas baseadas em heurística.
- Detectores de anomalias.

Nestes mecanismos aparece um novo termo denominado de assinatura, que se refere a um conjunto de condições que quando encontradas indicam que foi observado um tipo de evento normalmente associado a uma intrusão.

2.2.3.1 Detecção com padrões conhecidos

Assenta na procura de uma sequência fixa de bytes num pacote de dados. Na maioria dos casos o padrão é encontrado se o pacote suspeito estiver associado a um protocolo comum. Este tipo de aproximação ajuda a reduzir a inspecção feita em todos os pacotes, contudo pode ser difícil de aplicar quando se faz a análise de protocolos não associados a portos definidos. Por exemplo os cavalos de Tróia (do Inglês Trojan Horse) são programas que são instalados sem o consentimento do utilizador da máquina e que têm como objectivo actividades maliciosas na máquina onde passam residir [12].

A estrutura de uma assinatura é muitas vezes baseada num teste de padrões e numa acção a realizar caso o padrão se verificar:

- Se o pacote é do tipo IPv4.
- Se utiliza TCP como protocolo de nível 4 modelo OSI.
- Se tem como porto de destino o porto 222.
- Se os dados do pacote contêm a palavra “ataque”.
- Então deve ser disparado um alarme.

Este exemplo de teste de padrões é muito simples, sendo possível associar a estes testes uma série de alternativas, tais como:

- Incluir um ponto de início de busca do padrão.
- Incluir um ponto de fim de busca do padrão.
- Especificar quais os bits do campo de controlo do protocolo TCP que devem ser verificados e/ou usados.

As principais vantagens deste método de detecção são:

- É relativamente simples a detecção.
- Permite uma correlação directa, caso seja feita uma variação do padrão.
- Existe alguma segurança quanto à geração de alertas relativamente ao padrão especificado.
- Pode ser aplicado a todos os protocolos, definindo assim o seu funcionamento padrão e suas variantes.

As principais desvantagens deste método de detecção são:

- Pode levar ao aumento de alarmes falso positivos, se o padrão não for único, i.e., se corresponder a vários pacotes, incluindo alguns válidos.
- Qualquer modificação das características do ataque pode influenciar o número de eventos não detectados, aumentando deste modo o número de falso negativos.
- Requer múltiplas assinaturas de forma a ser possível tratar vulnerabilidades simples que podem ser exploradas de diferentes formas.
- É usualmente limitado à inspecção de pacotes individuais e não se aplica da melhor maneira a um conjunto de pacotes, como a natureza de tráfego associada ao HTTP.
- Requer uma actualização periódica da lista de assinaturas.

2.2.3.2 Detecção com estados do comportamento padrão

Este método é mais sofisticado e baseia-se na análise completa do estado de um conjunto de eventos. Este tipo de assinatura adiciona o conceito de procura de padrões não só nos pacotes individuais mas também ao estado dos pacotes associados a um contexto, que é constituído pelo conjunto de pacotes de um dado tipo de transacção. Significa assim que este tipo de sistemas considera na sua análise a ordem da chegada dos pacotes associada ao fluxo de informação relativa a protocolos do tipo TCP [13].

Como é que este cenário pode afectar a procura simples de padrões? Em vez da procura do padrão em todos os pacotes, o sistema tem de manter a informação de estado sobre os pacotes que foram observados anteriormente na transacção que está a ser monitorizada. Para se perceber a diferença, podemos recorrer ao seguinte cenário que se baseia no ataque apresentado anteriormente: Supondo que o ataque que estamos a analisar é executado

recorrendo a uma aplicação cliente/servidor, e está definido no IDS como método de padrão de ataque a detecção de uma palavra-chave. Se o ataque é executado então qualquer pacote TCP enviado para o destino no porto 2222 com a palavra “ataque” é detectado, sendo disparado um alarme. Mas, se o ataque for fragmentado em dois pacotes distintos, contendo o primeiro pacote a palavra “ata” e o segundo pacote a palavra “que”, o detector baseado em padrões não detecta o ataque e o alarme não é disparado. O método baseado em estados vai permitir deste modo, guardar o estado do primeiro pacote recebido com a palavra “ata”, completando a verificação quando receber o segundo pacote com a palavra “que”, sendo detectado e accionado o alarme.

As principais vantagens deste método de detecção são:

- Permite uma correlação directa entre a definição da vulnerabilidade e o padrão, sendo mais específico.
- Geração de alertas de acordo com o padrão especificado.
- Este método pode ser aplicado em qualquer protocolo.
- Torna a evasão à detecção mais difícil de acontecer.

As principais desvantagens deste método de detecção são:

- Requer um esforço maior na definição das assinaturas, apresentando um motor de validação baseado em estados, necessitando de maiores recursos ao nível do hardware necessário na concretização.
- Pode criar o aumento de alarmes falso positivos, se o padrão não for único tal como o gerador de assinaturas assumiu.
- Qualquer modificação nas características do ataque pode influenciar o número de eventos não detectados, aumentando deste modo o número dos falso negativos.
- Requer múltiplas assinaturas de maneira a ser possível tratar vulnerabilidades simples que podem ser exploradas sob diferentes formas.

2.2.3.3 Detecção por protocolo

O método de descodificação ou interpretação por protocolo é visto como uma extensão inteligente relativamente ao método detecção com estados do comportamento padrão. Esta classe de assinaturas é realizada recorrendo à descodificação de vários elementos dos dados de maneira semelhante ao usado pela aplicação cliente/servidor. Quando os elementos do protocolo são identificados, o IDS aplica as regras definidas para aquele protocolo, em particular verifica se está de acordo com a sua especificação (e.g., o seu RFC-Request for Comments), e depois avalia se está a acontecer alguma violação ao mesmo. Em alguns casos, estas violações são encontradas pela simples validação de um determinado campo associado ao protocolo, enquanto noutras situações recorre-se a técnicas mais avançadas tais como dimensões dos campos e número de argumentos.

A única possibilidade de validar incidentes que ocorram relativamente ao tipo de campos que é passado a um protocolo, seria o de identificar previamente o funcionamento do protocolo. Não perceber o protocolo por completo pode ter como consequência o aparecimento dos "falsos negativos", se o protocolo permite comportamentos a que os algoritmos de teste de padrões tenham dificuldade em tratar, como por exemplo: se o protocolo permitir num dos campos do cabeçalho o valor NULL, então qualquer algoritmo associado a teste de padrões vai falhar porque encontra algo como por exemplo **s**x00**t**x00**o**x00**p**x00 em vez de "stop". Se o motor de busca tiver como base a descodificação relativamente ao protocolo então, passa a ser possível o detectar dos NULLs e o retirar dos mesmos sendo disparado o alarme em que a palavra "stop" foi detectada associado ao protocolo [14].

As principais vantagens deste método de detecção são:

- Minimiza os alarmes falso positivos se o protocolo estiver bem definido.
- Permite por directa correlação detectar uma variação a um ataque.
- Detecta violações às regras de funcionamento de um protocolo.

As principais desvantagens deste método de detecção são:

- Conduz ao aparecimento de falso positivos se a especificação que define o protocolo permitir aos utilizadores diferentes tipos de interpretação, sendo criadas áreas cinzentas relativamente ao tratamento de informação.

- Necessita de desenvolvimento de um programa associado que valida as opções de utilização do protocolo definido no RFC.

2.2.3.4 Detecção com assinaturas baseadas em heurísticas

Os métodos baseados em heurísticas assentam essencialmente na necessidade de definição de um conjunto de regras e instruções simples, geralmente expressas numa linguagem de programação, que se destinam a encontrar soluções para problemas complexos ou mal definidos. Embora nem sempre a melhor solução seja encontrada, a programação heurística assegura, em geral, uma boa solução para os problemas.

Este tipo de assinaturas utiliza alguns tipos de algoritmos lógicos, baseados em avaliações estatísticas de tipos de tráfego. Um bom exemplo deste tipo de assinaturas é a detecção de varrimentos de portos. Este tipo de assinatura baseia-se na definição de um limite numérico de portos únicos que uma máquina pode usar, de acordo com o seu comportamento em rede. Esta assinatura restringe o tipo de pacotes denominados de interessantes para esse conjunto de portos, tais como: pacotes tipo “SYN” utilizados no estabelecimento de uma ligação TCP. Adicionalmente, pode existir mais uma regra que diz que todos os pacotes transmitidos tenham como origem essa mesma máquina. Este tipo de método requer a manipulação de limiares de modo a que seja ajustado de acordo com os padrões de funcionamento da rede que se pretende monitorar [15].

As principais vantagens deste método de detecção são:

- Detecção de alguns tipos de actividade suspeita ou maliciosa não são tratados correctamente pela maioria dos outros métodos.

As principais desvantagens deste método de detecção são:

- Necessita de grande afinação e customização de acordo com o funcionamento da rede, de modo a minimizar os alarmes falsos positivos.

2.2.3.5 Detectores de anomalias

Este tipo de método assenta tipicamente na análise de tráfego de rede que se desvia do tráfego dito normal. A maior dificuldade deste método é definir primeiro o que é normal, e neste caso podemos considerar este tipo de sistemas como heurísticos.

Alguns sistemas são construídos de forma a aprenderem o que é o comportamento normal, sendo o seu maior desafio eliminar a possibilidade de classificar o comportamento de anómalo quando na realidade se trata de um comportamento normal. Ao assumir que o comportamento relativo a determinado tráfego é dito de normal, o sistema deve permitir diferenciar entre o que são desvios permitidos e o que representa tráfego relacionado com um ataque.

Associado a este tipo de metodologia existe a definição de perfil de comportamento. Estes sistemas baseiam-se em alertas na mudança de como os utilizadores interagem com a rede. Existem uma série de limitações e problemas na detecção e análise na mudança de comportamento. Factos interessantes podem ser aprendidos com base na tendência de funcionamento da rede, associando algoritmos a estas tendências, mas devido à não especificidade requer uma investigação apurada de acordo com cada contexto.

Um dos métodos de detecção de anomalias é o que se baseia na descoberta de anomalias por protocolo. Este método é mais específico e encontra-se relacionado com a descodificação do protocolo. Porque as definições de um protocolo estão bem definidas, este tipo de anomalias não necessitam de uma fase de aprendizagem. Um exemplo de uma anomalia relativa a um protocolo pode ser a existência de um valor inesperado num campo de dados [16].

Outro tipo de anomalias podem ser identificadas usando-se métodos estatísticos que identificam o funcionamento da rede, recorrendo a fases de aprendizagem com o objectivo de extrair o seu comportamento. Esta detecção faz-se através de factos estatísticos para determinados tipos de tráfego, como por exemplo, sistemas que detectam o aumento de tráfego UDP, TCP ou ICMP. Estes algoritmos comparam as taxas de tráfego corrente com referências históricas, gerando alertas com base em desvios entre as duas. Os níveis limite de análise dos desvios podem ser configurados pelo o utilizador de acordo com o que foi observado anteriormente na rede.

As principais vantagens deste método de detecção são:

- Permite detectar ataques conhecidos e não conhecidos.

- Não necessita do desenvolvimento de novas assinaturas.

As principais desvantagens deste método de detecção são:

- De um modo geral estes sistemas não estão habilitados para fornecer dados quanto a intrusões com qualquer granularidade.
- Dependem do ambiente onde os sistemas fazem a sua aprendizagem (i.e., quão próximos do comportamento "Normal" eles funcionam).

2.2.3.6 Selecção das metodologias?

Uma questão se coloca é qual dos métodos é o melhor? Uma das aproximações possíveis é a utilização de detectores de intrusões de rede com funcionalidades acima descriminadas, mas aplicados de acordo com a seguinte ordem:

- Detecção com base em métodos heurísticos.
- Detecção com base em padrões.
- Descodificação por protocolo e métodos estatísticos associados a anomalias.

2.3 Técnicas associadas à configuração e ajuste

A configuração e ajuste dos IDS são factores críticos para o sucesso na concretização deste tipo de sistemas. Sem o necessário ajuste os IDS geram alertas em resposta a todo o tráfego que pertença a um determinado critério, o que leva a que o número de alarmes falsos possa exceder a capacidade de tratamento e análise, o que reduz o valor da informação produzida. Os IDS que não sejam ajustados ou afinados geram alarmes associados a ataques que não são importantes tratar de acordo com o contexto a proteger e deixam de ser efectivos pela quantidade de informação gerada.

Existe no entanto uma série de linhas de orientação relativamente ao ajuste [17,18]:

1) Identificar possíveis pontos de rede onde colocar os IDS de forma a garantir a máxima eficiência. Por exemplo a colocação de um sensor no segmento de rede que interliga o acesso à Internet, sem a utilização de filtros de tráfego, pode degradar o desempenho do sensor.

2) Aplicar uma primeira configuração associada a zonas, que consiga reflectir grupos de recursos de rede distintos, permitindo definir tipos de assinaturas activas para cada grupo a proteger. Desta forma os IDS passam a ser operados por grupos o que simplifica a sua gestão.

3) Monitorar o sensor enquanto se procede ao ajuste, retirando todos os alarmes que sejam causados pelo comportamento normal da rede.

4) Analisar os alarmes produzidos, validando se um alarme é ou não resultado de um falso positivo. Algumas sugestões são:

    - Verificar se o alarme gerado é uma actividade maliciosa ou um comportamento normal da rede.
    - Se o alarme resultar de uma actividade normal da rede, então deve ser avaliada a origem que fez despoletar o alarme.
    - Se a origem do alarme for um servidor, então deve ser avaliado qual o comportamento da aplicação que gerou o alarme, e identificar o tipo de actividade.
    - Se a origem for um equipamento de rede (encaminhador, comutador, etc.), deve ser consultada a equipa que faz a gestão da rede.
    - Desenvolver uma análise das ameaças a que o sistema está sujeito, de modo a determinar o impacto e que tipo de resposta o sistema de detecção deve dar.

    Quando um evento falso positivo é identificado, deve ser validado se a actividade que causou o alarme pode ser modificada para evitar a geração do alarme. Mas se o serviço ou aplicação gerador dos alarmes é necessário, e não pode ser desactivado, pode-se em alternativa configurar o sistema de detecção para ignorar o alarme, para aquele sistema em concreto.

    Uma das possibilidades de configuração destes sistemas é o agrupamento por perfil de assinaturas activas, de acordo com quatro categorias possíveis:

    - Assinaturas associadas a “exploits”: estas assinaturas estão associadas a um tipo de tráfego que visa comprometer serviços de rede através de um “buffer overflow”, ou por ataques contínuos a sistemas de autenticação associados a passwords de modo a conseguir entrar no sistema, ou outros.

- Assinaturas associadas a tentativas de reconhecimento: estas assinaturas estão associadas a tráfego que permite enumerar que sistemas existem e os serviços de rede que dispõem.
- Assinaturas associadas a detecção de palavras: estas assinaturas detectam violações com base na procura de palavras-chave no tráfego de rede. Por exemplo, um detector de intrusões pode enviar um alarme sempre que for detectada a palavra-chave “Confidencial” associada a tráfego de mail ou de transferência de ficheiros.
- Assinaturas associadas a ataques DoS: este tipo de ataques visam degradar o desempenho ou tornar indisponível um determinado serviço. Por exemplo, a geração de uma quantidade exagerada durante um período de tempo de pacotes de rede do tipo TCP com a flag de SYN activa, levando ao consumo de largura de banda ou ao consumo de recursos de uma máquina de forma a interromper o serviço normal.

5) Concretização de acções de resposta tais como: o envio de pacotes TCP com a flag Reset activa, a reconfiguração dos equipamentos de segurança efectuada em tempo real, ou apenas a contabilização do tráfego detectado para efeitos de monitorização.
6) Actualização de novas assinaturas pode ser feita de modo automático, mas deve-se ter em linha de conta o ajuste referido nos pontos anteriores. Um dos pontos a salientar na activação de novas assinaturas é o facto do tempo que se consome para monitorar e ajustar de modo a reduzir os alarmes falso positivos.

2.4 Reportar e classificar os ataques

Quando um ataque é detectado, o sensor procede à avaliação do valor que a ameaça representa para a rede de acordo com um critério estabelecido, que vai desde baixo impacto até ao valor de alto impacto na rede [19].

O incidente é reportado para uma consola de gestão, que funciona como um repositório central de eventos relacionados com a detecção de actividades maliciosas. Este ponto central de gestão permite guardar as actividades ou despoletar um alarme relacionado com o conjunto de

actividades detectadas, e nalguns casos possibilita a correlação de eventos provenientes de diferentes actividades (ver Figuras 2.1 e 2.2).

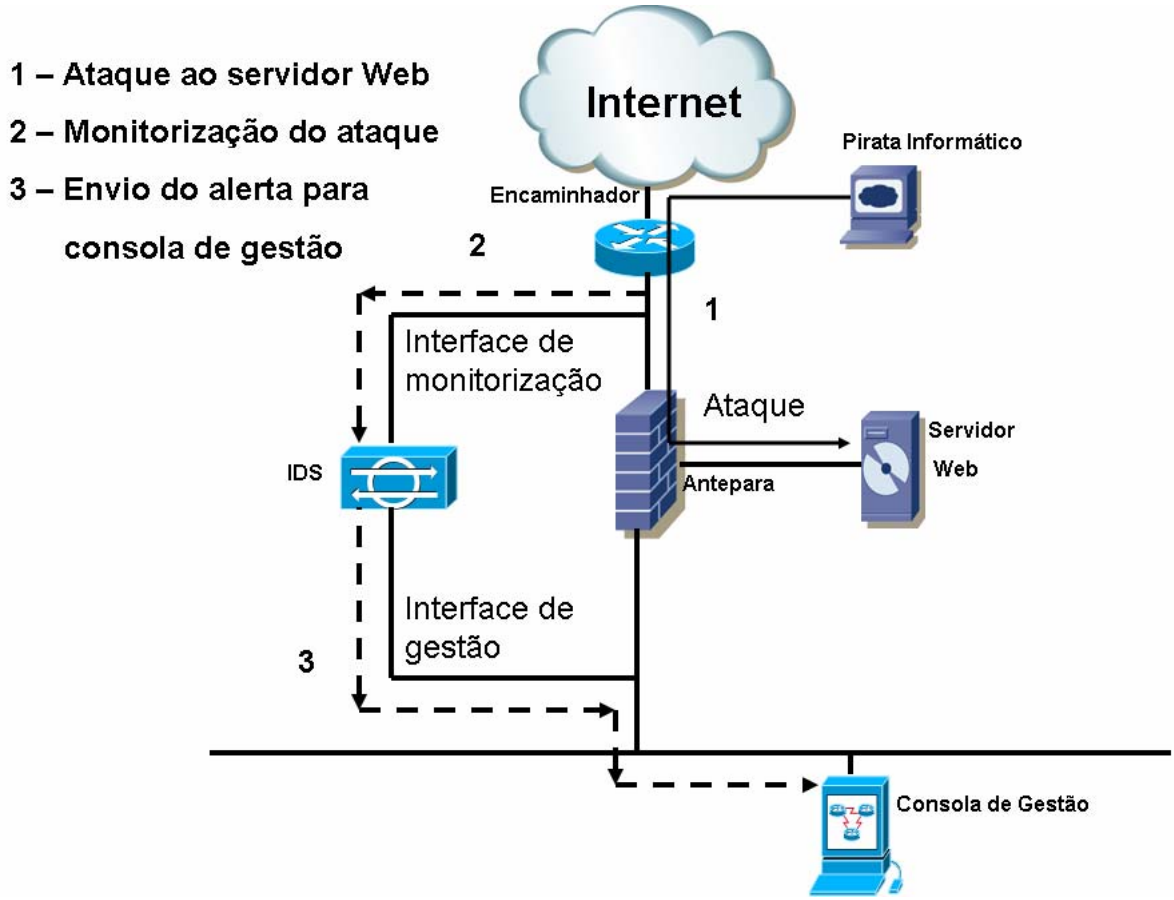


Figura 2.1 - Detecção de um ataque e envio de um alerta.

Uma consola de gestão pode coleccionar eventos de grupos de IDS (ver na Figura 2.2 o grupo de IDS A, B, C). Os eventos reportados por estes IDS podem estar a ser avaliados como tendo baixo impacto quando analisados em separado, mas quando correlacionados podem ter um impacto considerado como elevado. Deste modo a consola de gestão deve ter a funcionalidade de correlação de eventos e avaliação do impacto dos mesmos como se fosse um incidente.

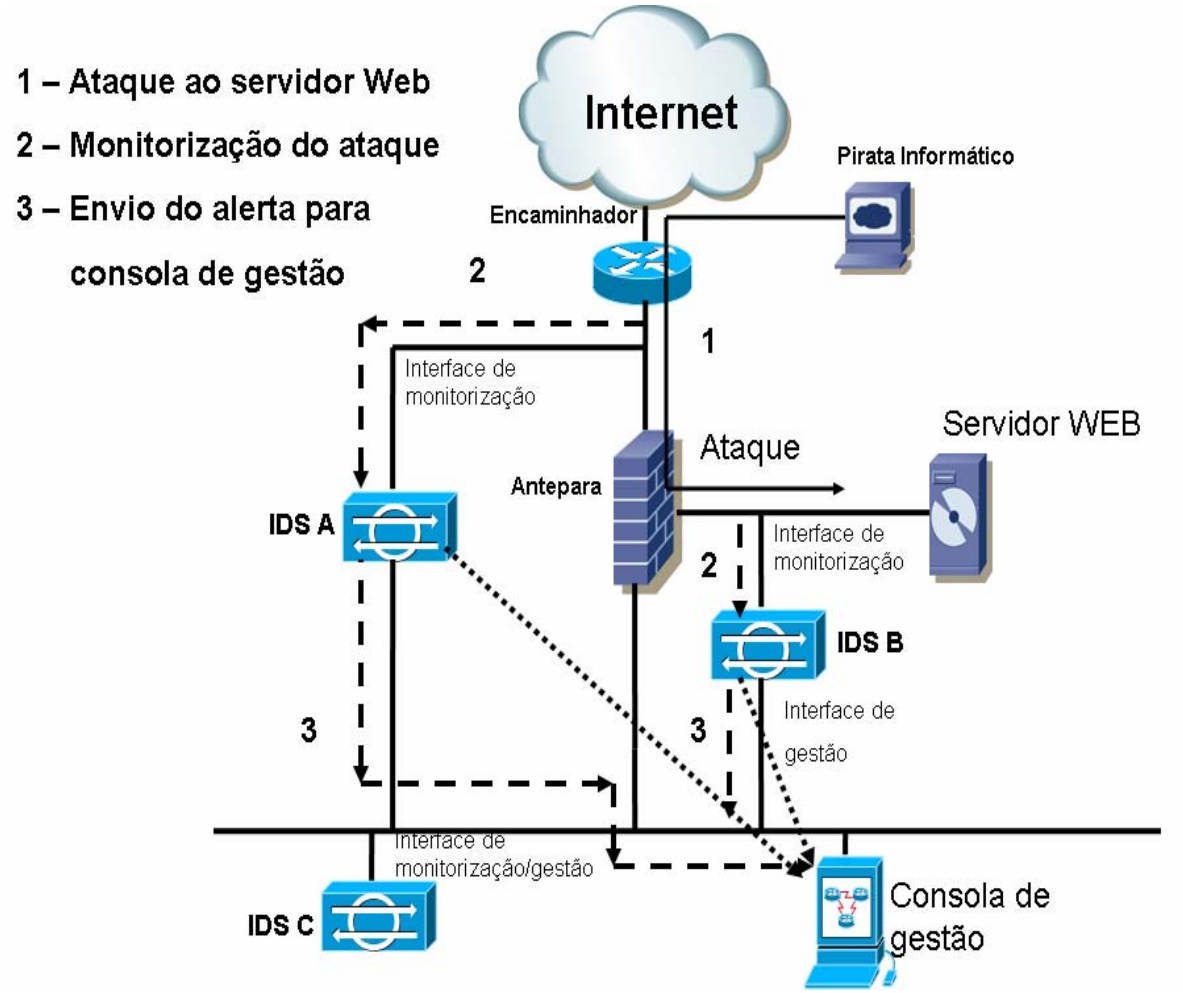


Figura 2.2 - Detecção de um ataque por um grupo de IDS e envio de alertas.

2.4.1 Acções correctivas associadas

Depois de um ataque ser detectado, um IDS pode responder de diversas maneiras. Segue-se alguns exemplos [20]:

- Geração de um alarme: Os alarmes gerados por um IDS são tipicamente encaminhados para uma plataforma de gestão ou consola, onde são registados, analisados ou nalguns casos correlacionados.
- Geração de sessões de captura de informação: Este tipo de sessões está associado à recolha de informação relacionada com uma sessão, sobre a utilização abusiva de um

recurso de rede. O registo desta informação é feito quando um determinado evento ou eventos acontecem, tais como a detecção da palavra “Confidencial” numa sessão. Quando uma condição deste tipo surge, o IDS regista num período de tempo todos os pacotes associados à transacção nos dois sentidos.

- Alguns detectores de intrusões têm a capacidade de ser pro-activos na resolução de problemas, através da execução acções correctivas em tempo real, tais como (ver Figura 2.3):
  - A introdução de filtros de tráfego nos encaminhadores para bloquear tráfego proveniente do endereço IP que está despoletar o ataque [21].
  - A capacidade de terminar sessões TCP entre o endereço de origem do ataque (IP origem+Porto origem) e o endereço de destino (IP destino+Porto destino) através da utilização de um pacote com a flag TCP Reset activa [22].
  - O bloqueio automático (do Inglês Shunning) do ataque, refere-se à capacidade do IDS para interagir automaticamente com os vários equipamentos de rede que concretizam a política de segurança, negando o acesso por utilizador ou rede. Para realizar esta funcionalidade, o IDS reconfigura toda a rede relativamente a filtros de tráfego, podendo assim ser reduzido o número de ataques logo ao nível periférico [23].

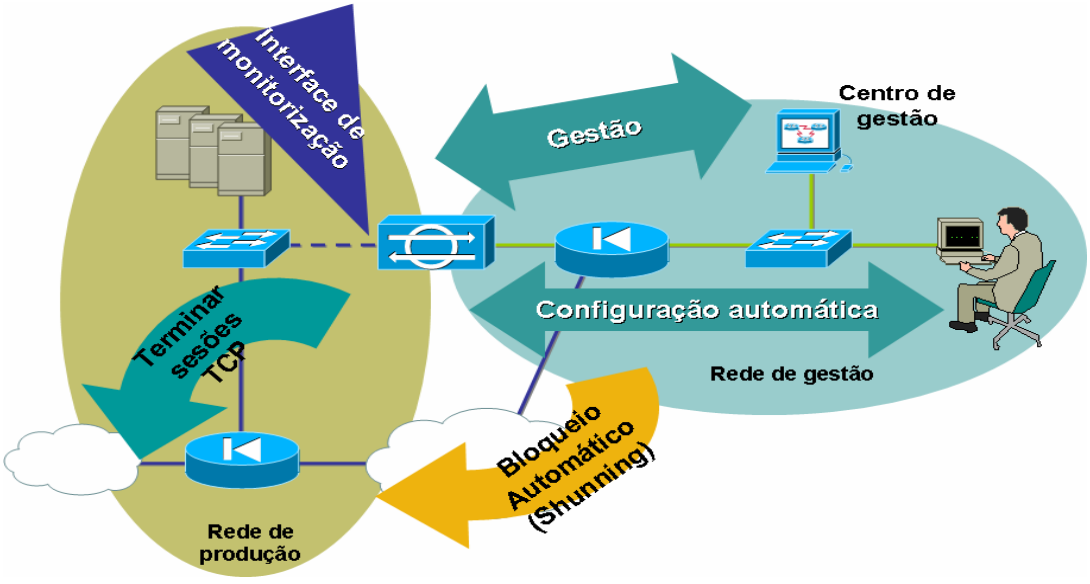


Figura 2.3 - Detecção e correcção automática do ataque.

2.4.2 Recursos humanos associados

Os sistemas de validação e resposta a ameaças têm vindo a evoluir, reduzindo o tempo de investigação relativo aos alarmes gerados pelos IDS. A automatização da análise permite a redução de alarmes falsos, com resultado de que os recursos humanos apenas analisam os alarmes válidos e que necessitam de investigação.

Existem no entanto concretizações de IDS ao nível do sistema operativo, denominados de HIDS (do Inglês Host IDS), que bloqueiam automaticamente actividades consideradas maliciosas. Adicionalmente, os IDS de rede permitem algum nível de automatização relativamente à recuperação, quando o ataque é detectado de acordo com um padrão de ataque já catalogado.

A concretização da detecção de intrusões e monitorização de mensagens associadas a eventos de rede necessita de recursos humanos disponíveis para a resposta a incidentes. Os recursos humanos associados a 24 horas são aproximadamente cinco, com três rotações de 8 horas cada, 7 dias por semana. O tempo dispendido na análise de alertas e mensagens depende do número de IDS de rede, os agentes IDS utilizados e da resposta que se deseja. A decisão deve ser tomada com base no valor dos recursos a proteger e o valor expectável de perda se os recursos de suporte ao negócio forem comprometidos, bem como a política de segurança associada.

2.5 A evolução da detecção para a protecção

Os IDS funcionam como equipamentos passivos que analisam o tráfego ao longo de determinados pontos da rede. Uma das acções resultantes é a geração de alertas ou avisos para uma consola de gestão sobre alguma actividade suspeita detectada, tendo sempre associado o instante em que a actividade ocorreu.

A evolução destes equipamentos tende para soluções que apresentam funcionalidades de protecção, sendo actualmente denominados de sistemas de protecção de intrusões (IPS, do inglês Intrusion Protection System). Estes sistemas, para além de detectarem intrusões em tempo real, também têm capacidades próprias para actuarem sobre as actividades suspeitas detectadas [24].

Os sistemas de IPS contrariamente aos sistemas de IDS, que estão localizadas em paralelo com a rede e se limitam a receber cópias do tráfego que fluí na rede, estão colocados em série na rede garantindo deste modo o bloqueio do tráfego em tempo real (ver Figura 2.4).

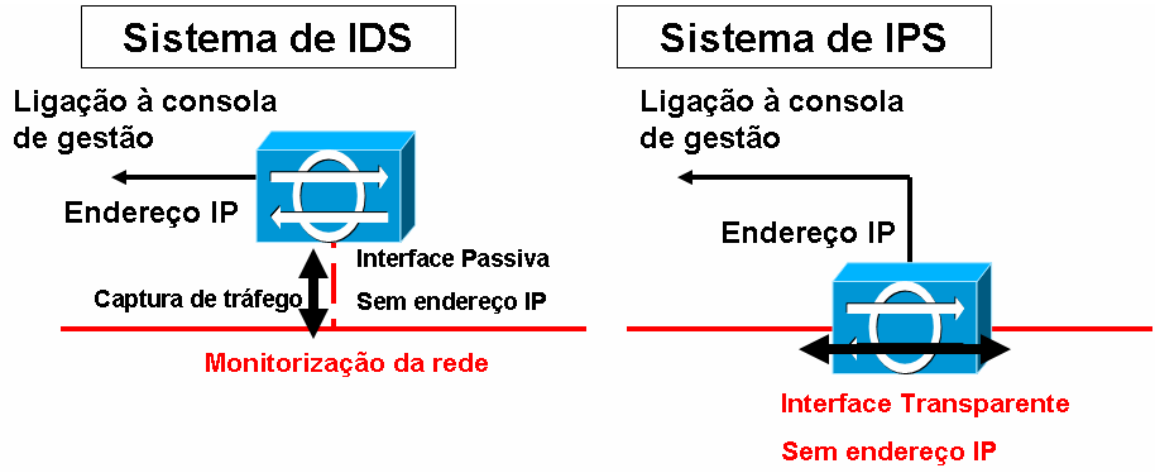


Figura 2.4 - Sistemas de IDS vs IPS.

Os sistemas de IPS têm a capacidade de identificar uma intrusão, bem como a sua relevância, o impacto, a direcção da mesma, permitindo assim uma análise do evento ou eventos. No entanto existem aplicações em que se torna necessário utilizar sistemas híbridos, que recorrem à utilização de ambos os sistemas com funcionalidades distintas (ver Figura 2.5).

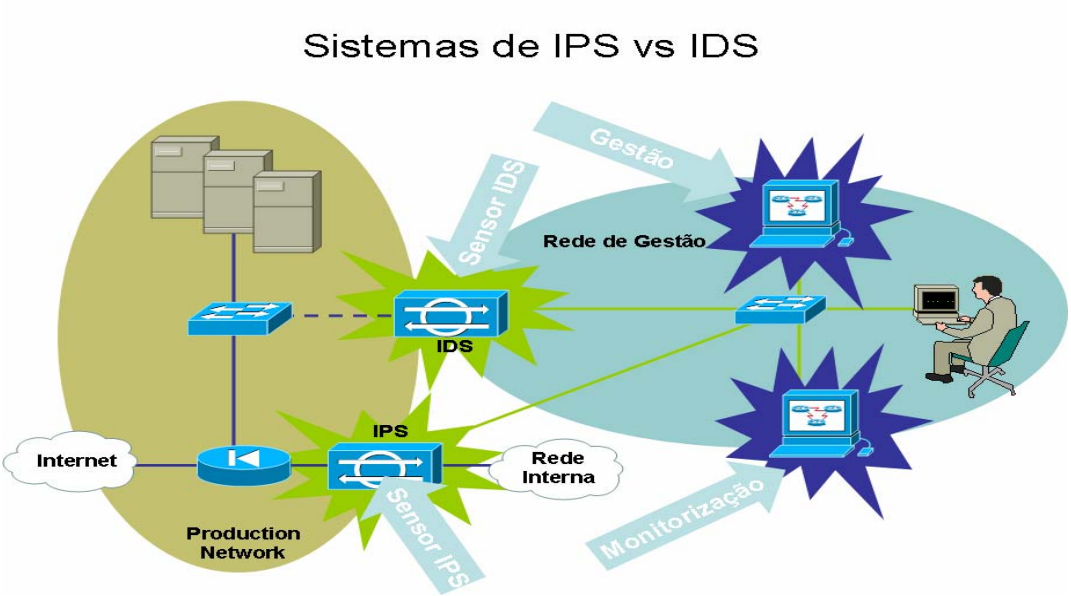


Figura 2.5 - Sistemas de IPS vs IDS colocados em rede.

A prevenção contra intrusões assenta fundamentalmente na utilização de mecanismos de correlação e análise de eventos, reduzindo desta forma o número de alarmes produzido, tendo como objectivo criar uma nova metodologia de análise de risco sob a forma de incidente que está associada a um conjunto de eventos (ver Figura 2.6).

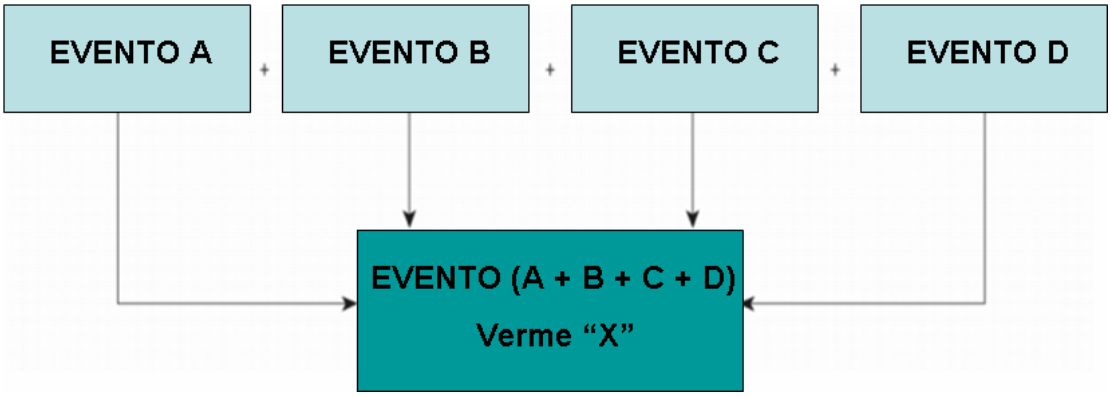


Figura 2.6 - Correlação de eventos ao nível do sistema de IPS.

Com a análise de risco [25] abandona-se os modelos simplistas que associam um valor de impacto a cada evento através da definição de um intervalo [1 (pouco crítico) – 5 (muito crítico)], deste modo passamos a ter uma análise associada à:

- Severidade do evento.

  Avaliação do evento segundo um intervalo de análise.

- Relevância do ataque.
- Valor dos sistemas a proteger.
- Valor das assinaturas.

O resultado é um valor numérico sob a forma de índice que automaticamente é correlacionado de modo a que o tráfego válido não sofra danos nem seja bloqueado. Os desafios associados aos sistemas de IPS são:

- No desenho da rede devem ser colocados em série vs paralelo.
- A colocação em série cria potencialmente pontos de congestionamento.

- São necessárias actualizações frequentes.
- Existe sempre a possibilidade de eventos falsos positivos.

Os IDS são mais fáceis de colocar numa rede, pois funcionam em paralelo com a rede, não provocando a interrupção das comunicações em caso de falha. A introdução dos IPS requer uma análise mais atenta na sua colocação, porque fazem parte do caminho que o tráfego segue na rede. Por outro lado permitem uma resposta automática a um ataque que ocorra na rede, reduzindo assim o tempo de respostas a uma sequência de eventos.

O congestionamento associado a tráfego de pico não deve causar problemas à rede, mantendo o mesmo estado de operacionalidade. O problema associado às frequentes actualizações e à existência de eventos falso positivos mantém-se de igual modo nos IPS tal como existia nos IDS. Mas os IPS apresentam a vantagem nesta área porque as decisões são tomadas com base na análise de conjuntos de dados de informação deixando deste modo a análise de eventos de forma isolada. Os eventos falso positivos são um grande problema pois levam ao armazenamento de grandes quantidades de informação e a uma análise e correlação em tempo real.

2.6 Conclusão

O objectivo deste capítulo foi o de apresentar sistemas de detecção de intrusões. Mostrar a sua interacção com os recursos que se pretende proteger, recorrendo a diferentes mecanismos para detecção de intrusões. Foram abordados os tipos de monitorização de rede, como se deve iniciar o processo de colocação de IDS na rede e sua afinação, de modo a não se causar nenhum impacto na infra-estrutura que se pretende observar. A evolução de sistemas tipo IDS para IPS também foi considerada, indicando-se quais as características bem como a capacidade de correlação de eventos, permitindo desta forma a redução de alarmes e eventos falsos positivos.

Capítulo 3

Analisador Comportamental de Rede

Neste capítulo define-se uma arquitectura que permita endereçar uma série de excepções quanto à análise de tráfego gerado na rede e que não são bem tratadas pelos mecanismos existentes de detecção de intrusões. A arquitectura sugerida propõe uma evolução dos sistemas de detecção e protecção contra intrusões. Esta evolução pressupõe a adição de um ou mais componentes de recolha e análise de informação dos dados que circulam na rede, para que posteriormente se tomem decisões ao nível dos recursos envolvidos na transmissão de dados, tais como: encaminhadores, comutadores, anteparam. Enquadramento do estudo relativamente ao modelo OSI [26], incide sob as componentes associadas às camadas 3 a 7 do modelo (ver Figura 3.1).

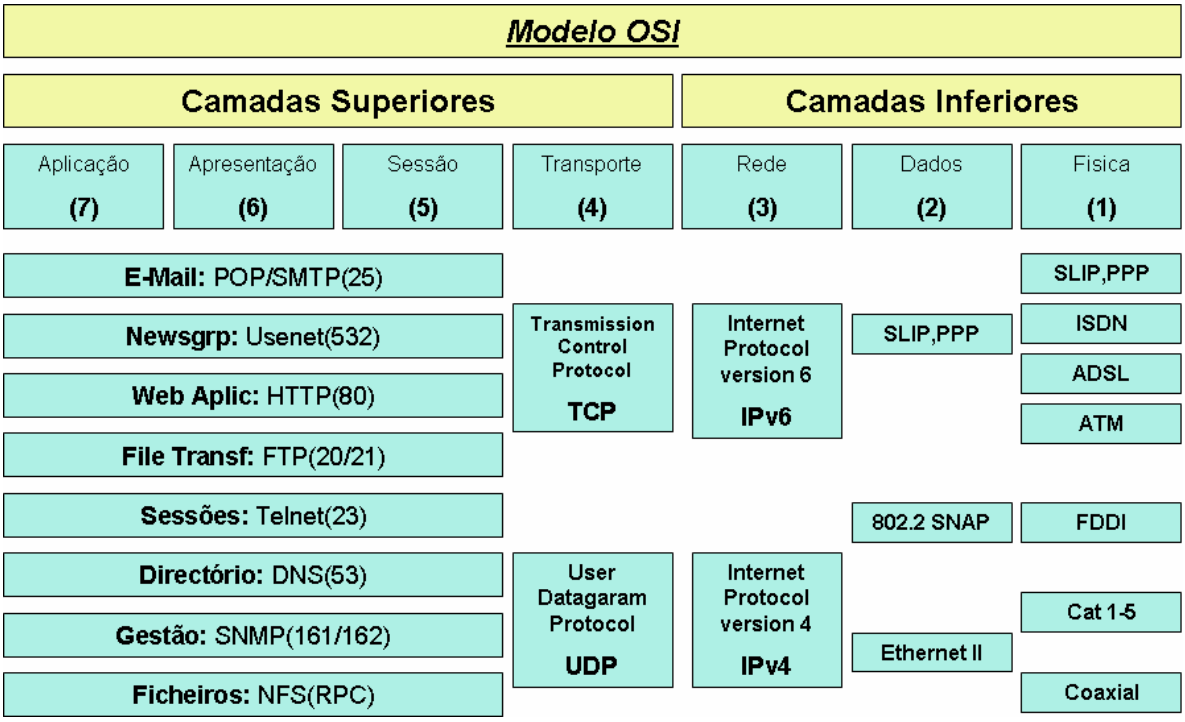


Figura 3.1 - Enquadramento com o modelo OSI.

3.1 Modelo do sistema

Os principais processos que são necessários tomar em consideração no sistema encontram-se divididos em (ver Figura 3.2):

- Processo de recolha de informação.
- Processo de análise de informação.
- Processo de decisão.

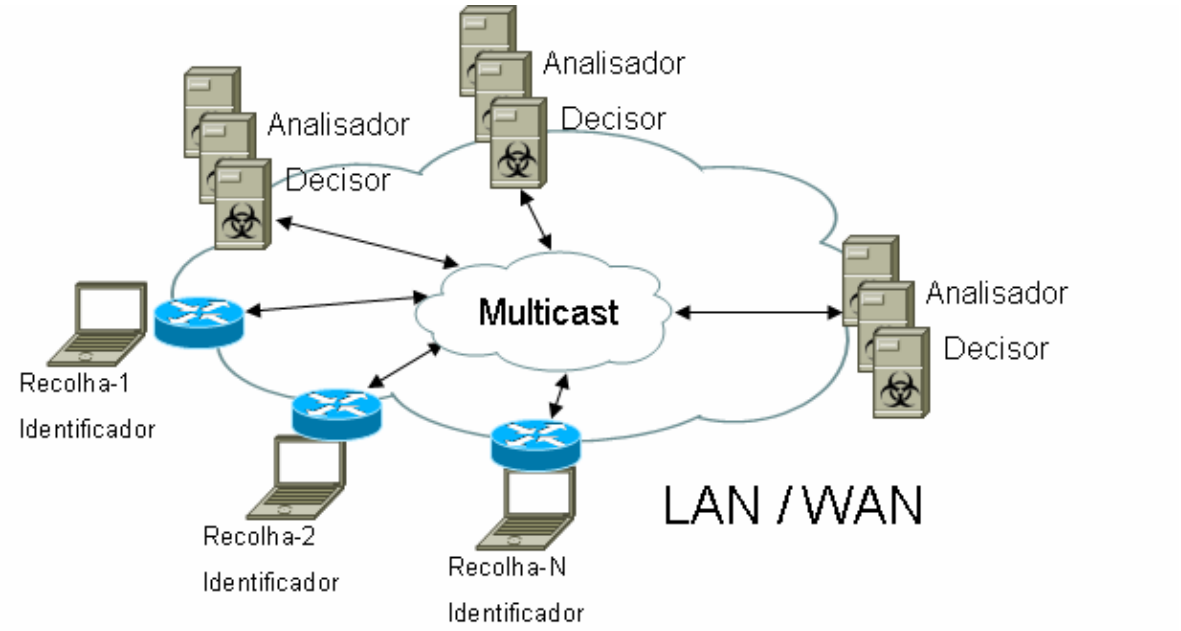


Figura 3.2 - Componentes principais da arquitectura do sistema.

O modelo assume que os processos de recolha de informação registam todos os dados relativos aos pacotes relevantes para a análise. Em seguida, procede-se a uma fase de análise da informação e sua correlação, tendo como objectivo final a geração de uma série de instruções a serem executadas nos componentes de rede. Estas instruções irão permitir que as anomalias sejam corrigidas de forma automática.

3.2 Descrição dos processos

Este modelo utiliza processos distintos que permitem separar as várias fases. Os processos estão relacionados de uma forma sequencial, em que o processo de recolha é responsável pela captura dos pacotes e pelo seu armazenamento, de modo a servir de base de informação ao processo de análise. A análise é apenas efectuada após aplicação de alguns métodos estatísticos que produzem uma série de instruções a serem enviadas ao processo de decisão.

Este por sua vez interage com os vários agentes existentes de acordo com a família de equipamentos (ver Figura 3.3) através de uma linguagem padrão XML (Extended Markup Language) [27].

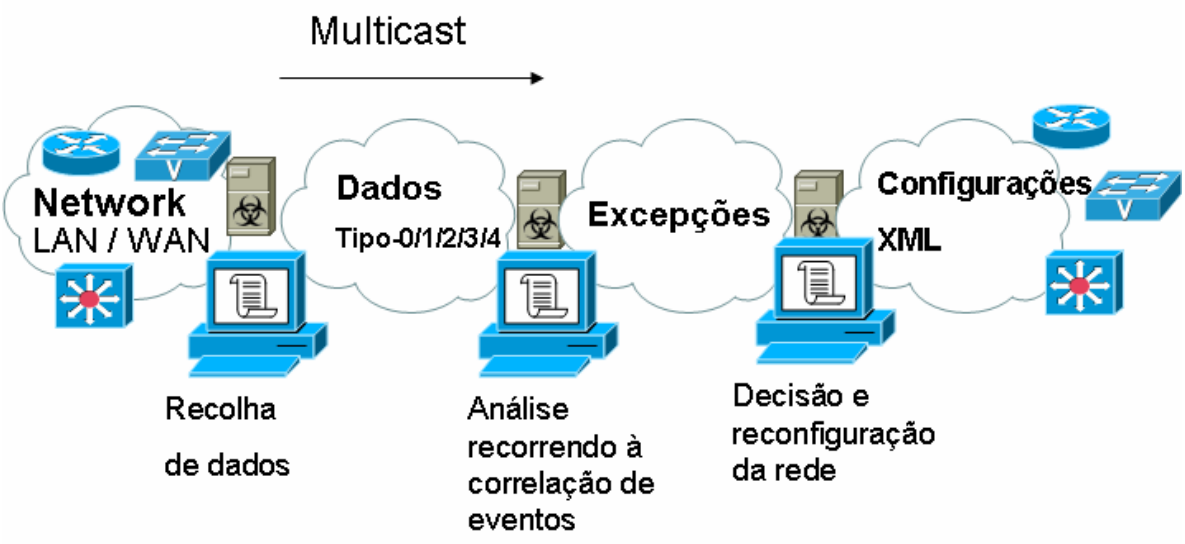


Figura 3.3 - Encadeamento dos processos.

3.2.1 Processo de recolha de informação

A fase de recolha pretende ser um processo que funcione em tempo real. A recolha de informação é efectuada ao nível da rede do modelo OSI, incidindo sobre o pacote IP (ver secção 3.2.1.1), de forma a capturar o cabeçalho e alguma informação relacionada com os dados transportados.

O processo de recolha está encarregue também do tratamento inicial dos pacotes recolhidos, permitindo gerar as seguintes fontes de informação em intervalos de 100 segundos (na concretização actual):

- Dados Tipo-0 correspondem à informação recolhida em bruto (ver Figura 3.4).
- Dados Tipo-1 têm toda a informação relativa aos protocolos que se encontram suportados em TCP e UDP (por exemplo DNS, HTTP).
- Dados Tipo-2 contém a informação acumulada sobre os protocolos que operam directamente sobre o IP, tais como TCP, UDP, ICMP, IGMP, etc.

- Dados Tipo-3 corresponde a informação acumulada relativa ao protocolo IP.
- Dados Tipo-4 é a informação sobre os fluxos detectados, sendo contabilizada de acordo com o tipo de protocolo.

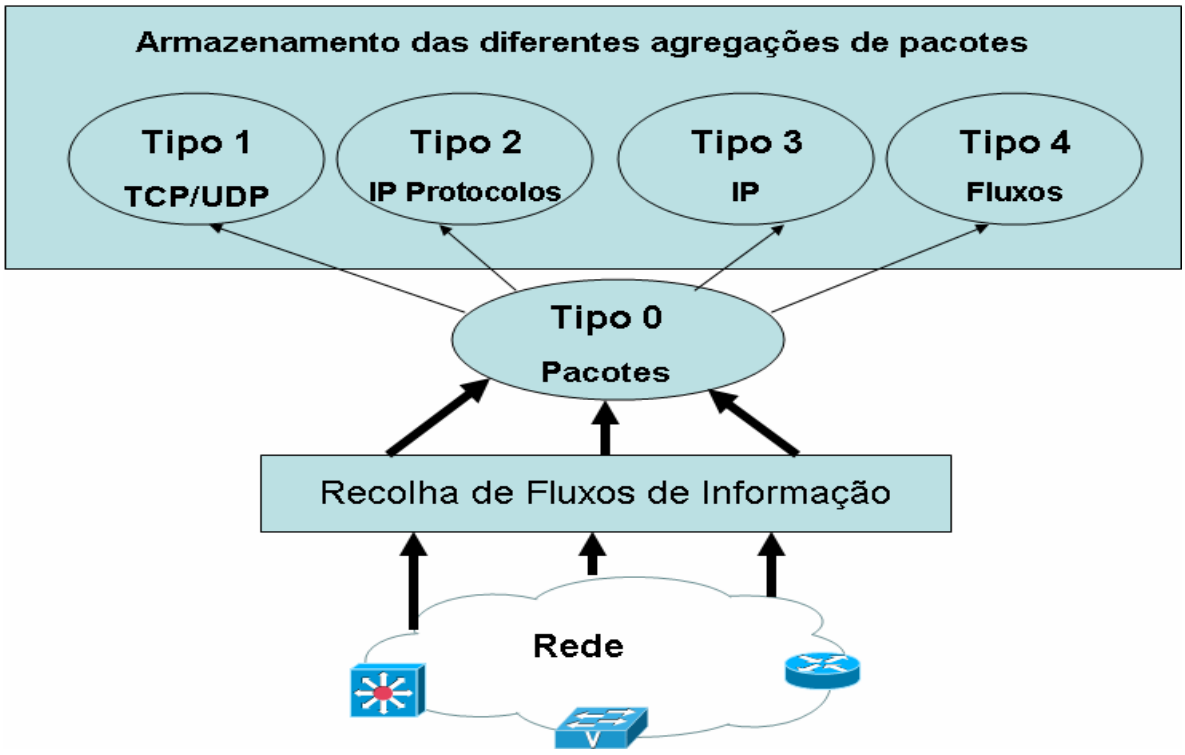


Figura 3.4 - Tipos de dados no processo de recolha.

3.2.1.1 Protocolos fundamentais

Todos os pacotes que são capturados têm como protocolo de rede o IP (ao nível 3 do modelo OSI). Para tornar mais fácil a compreensão da constituição dos cabeçalhos e funcionamento dos protocolos, seguem-se várias secções que descrevem sucintamente os protocolos.

Internet Protocol (IP)

Referenciado como protocolo de nível 3 do modelo OSI, contém informação sobre os endereços dos emissores e destinatários, e alguma informação de controlo que permite que os pacotes sejam encaminhados entre dois pontos de rede (ver Figura 3.5). Este protocolo está

documentado no RFC 791 [28]. A Tabela 3.1 apresenta os campos que constituem um pacote IP.

A uma comunicação que se baseia no protocolo IPv4 tem como principais características:

- Não existe validação de estabelecimento das ligações.
- Não garante a entrega de pacotes através da rede.
- Suporta a fragmentação de pacotes, como resultado do pacote atravessar determinadas ligações que requerem um número máximo de bytes inferior ao tamanho do pacote.
- Não oferece um controlo de fluxo ou congestão.

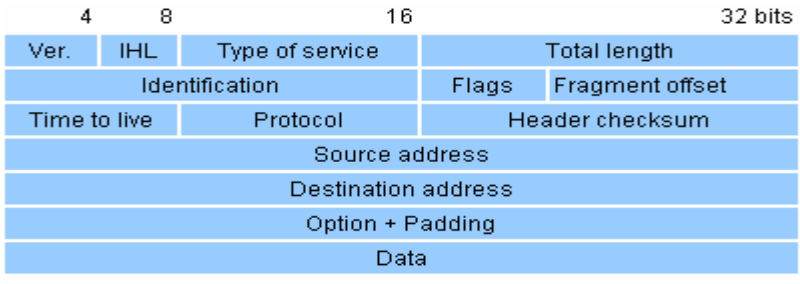


Figura 3.5 - Formato de um pacote IPv4 que é tratado no processo de recolha.

Version	Indica qual a versão usada (e.g., 4 para o IPv4)
IP Header Length	Indica a dimensão do cabeçalho em múltiplos de 32 bits
Type-of-Service	Define a importância dos dados que transporta
Total Length	Especifica a dimensão incluindo os dados+cabeçalho
Identification	Contém um número inteiro que identifica o pacote
Flags	Consiste em três bits: Bit Low pacote pode ser fragmentado, Bit Middle o pacote contém o ultimo fragmento de uma série de pacotes fragmentados, o Bit High não é usado
Fragment Offset	Indica a posição do fragmento dos dados relativamente ao pacote original
Time-to-Live	Contador que é decrementado por cada encaminhador por onde o pacote passa
Protocol	Indica qual o protocolo que vai tratar o pacote após o processamento IP estar completo, e que está um nível acima no modelo OSI: (1): ICMP, (6): TCP, (17): UDP
Header Checksum	Código para detecção de erros
S*ource Address*	Endereço IP que especifica a origem dos pacotes
Destination Address	Endereço IP que especifica o destino dos pacotes
Options	Permite o suporte de várias opções, tais como segurança
Data	Dados transaccionados

Tabela 3.1 - Explicação dos campos de um pacote IP.

Internet Control Message Protocol (ICMP)

O Internet Control Message Protocol (ICMP) é um protocolo da camada de rede do modelo OSI que possibilita a troca de mensagens de erros, e que normalmente são devolvidos ao emissor de um determinado pedido. As mensagens de erro podem ser de diferentes classes, e incluem informação relacionada com problemas do tipo: Echo Request and Reply, Destination Unreachable, Redirect, Time Exceeded, Router Advertisement. Este protocolo está documentado no RFC 792 [29].

Para evitar sobrecarregar a rede com este tipo de mensagens, se uma mensagem ICMP não é entregue com sucesso, então não é gerada uma segunda mensagem.

Transmission Control Protocol (TCP)

O protocolo Transmission Control Protocol (TCP) permite a transmissão de mensagens do tipo orientado à ligação, com fiabilidade. Suporta um conjunto de mecanismos associados à recuperação de faltas, garantindo assim a entrega com sucesso de pacotes de um determinado protocolo de alto nível. O TCP definido no RFC793 [30], e o seu cabeçalho contém um conjunto de informação (ver Figura 3.6), parte dela encontra-se explicada na Tabela 3.2. Na tabela são apenas apresentados os campos que vão ser alvo de tratamento por parte do IDS.

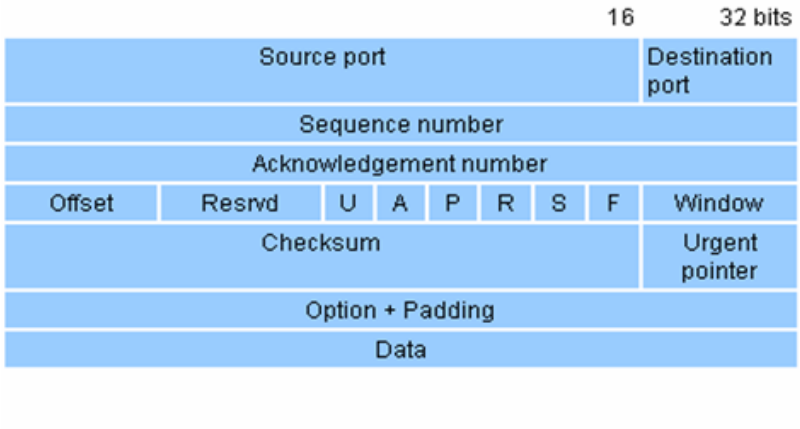


Figura 3.6 - Cabeçalho de um pacote TCP.

Source Port:	Campo que define qual é o porto de origem utilizado (16 bits)
Destination Port:	Campo que define qual é o porto de destino utilizado (16 bits)
Control Bits: 6 bits	Campo codificado a 6 bits da esquerda para a direita URG: ponteiro de urgência ACK: bit de confirmação RST: abortar a ligação SYN: inicio de ligação FIN: terminar a ligação
Data	Dados a serem passados ao protocolo de nível superior

Tabela 3.2 - Explicação dos campos de um pacote TCP.

Aproximadamente 90% das redes recorrem ao protocolo TCP para o transporte de tráfego, sendo usado por aplicações do tipo FTP, HTTP.

User Datagram Protocol (UDP)

O protocolo User Datagram Protocol possibilita a transmissão de mensagens sem controlo do estado da ligação e sem a garantia de sucesso na entrega. Cada pacote UDP, à semelhança do TCP, tem associado um porto de origem e de destino, permitindo assim múltiplas transacções provenientes da mesma máquina. O UDP encontra-se definido no RFC 768 [31], e o seu cabeçalho pode ser observado na Figura 3.7.

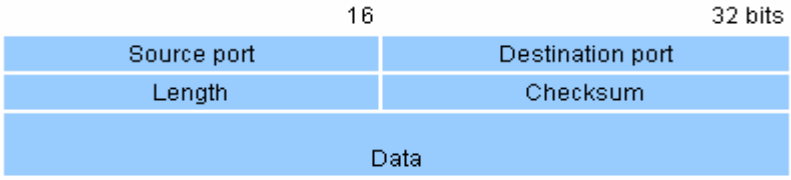


Figura 3.7 - Cabeçalho de um pacote UDP.

Como se trata de um protocolo em que não é controlado o estado da ligação, é muitas vezes usado em transacções mais simples. Por exemplo é utilizado pelo SNMP uma vez que este

protocolo não necessita de garantir a entrega dos pacotes (SNMP-Simple Network Management Protocol) [32].

3.2.1.2 Definição de um fluxo de informação

A definição de fluxos de informação tem como objectivo guardar os dados relativos a transacções por tipo de protocolo, para que seja possível identificar determinados desvios ao funcionamento normal da rede. Infelizmente cada protocolo tem uma definição diferente relativamente ao que pode ser contabilizado ou guardado como sendo um fluxo, por exemplo:

- Fluxo TCP: tem uma duração associada, e devido às características deste protocolo consegue-se sempre identificar o início e o fim de uma transacção através das flags associadas:
  - Estabelecimento da ligação (Flags SYN e SYN-ACK).
  - Troca de dados e confirmação da recepção dos dados (Flag ACK).
  - Fim da transacção (Flag FIN).
- Fluxo UDP: não tem uma duração associada; é um tipo de protocolo em que não existe as fases acima descritas sendo muito complexo ter uma definição de transacção e perceber qual é o serviço específico a que se está a aceder.
- Fluxo ICMP: identificado pelo tipo de mensagens trocadas, sendo possível definir diferentes transições de estados.

Como resultado da análise dos protocolos atrás mencionados optou-se por recolher a informação da Tabela 3.3 que descreve os campos capturados pelo processo de Recolha.

Nestes mecanismos aparece um novo termo denominado de assinatura, que se refere a um conjunto de condições que quando encontradas indicam que foi observado um tipo de evento normalmente associado a uma intrusão.

Tipos de campos	Descrição
IP-Origem	Quem inicia o pedido
IP-Destino	Destino do pedido
Protocolo	Protocolo utilizado (TCP, UDP, ICMP, IGMP, etc)
Porto-Origem	Porto de origem (caso do TCP/UDP)
Porto-Destino	Porto de destino (caso do TCP/UDP) →Protocolo utilizado (HTTP, FTP, SNMP, etc)
Total de Bytes	Total de bytes transmitidos durante os 100 segundos na captura de tráfego
Total de Pacotes	Total de pacotes transmitidos durante os 100 segundos de captura de tráfego
Instante de Inicio da transacção	Instante em que a transacção foi iniciada Fluxo TCP iniciado com a flag de SYN activa; outros fluxos quando é detectado um início de transacção, caso não exista nenhuma transacção em curso
Instante de Fim da transacção	Instante em que o fluxo foi terminado Fluxo TCP terminado quando é detectado a flag de RESET ou FIN; outros fluxos quando é detectada a finalização de uma transacção, ou seja quando não houver mais dados transmitidos durante um intervalo de tempo
Flags-TCP	Definição das flags utilizadas, só com significado quando se trata de um fluxo TCP: SYN, SYN-ACK, RST, FIN
Tipos de mensagens ICMP	Echo, Echo-Reply, Unreach, Time Exceed, Redirect

Tabela 3.3 - Lista de campos capturados para a definição dos fluxos.

3.2.1.3 Armazenamento de informação

O armazenamento da informação relativa ao estado de uma rede pode ser de difícil concretização. Colocam-se tipos de questões como: Devem-se armazenar os eventos completos ou só uma parte deles? Como configurar um equipamento que permita armazenar este tipo de eventos? Estas questões acabam por ter impacto no dimensionamento do equipamento em várias vertentes tais como: capacidade de disco, desempenho, escalabilidade, definição hierárquica da estrutura de armazenamento, mecanismos de sincronização de informação, correlação de eventos e acesso a dados históricos.

Estrutura de armazenamento

A estrutura de armazenamento usa uma arquitectura que é suportada num sistema de informação associado ao tempo em que foi capturada a informação. O sistema de informação utilizado na captura baseia-se numa estrutura de dados que assenta em 4 ficheiros:

- Ficheiro de dados Tipo-0, com toda a informação em bruto dos dados recolhidos, com o seguinte formato:
  - IP Origem e IP Destino.
  - Porto Origem e Porto Destino.
  - Flags (Protocolo TCP) ou Tipos de mensagens ICMP.
  - Pacotes e bytes transaccionados.
  - Instante da ocorrência da transacção.
- Ficheiro de dados Tipo-1, com toda a informação acumulada relativa aos protocolos suportados em TCP e UDP, ex: HTTP, FTP, SNMP, com o seguinte formato:
  - Pacotes e bytes transaccionados que foram acumulados.
  - Flags (ex: HTTP, FTP, etc) ou tipos mensagens ICMP.
  - Instante de ocorrência da última transacção.

- Ficheiro de dados Tipo-2, com toda a informação acumulada relativa aos protocolos IP, tais como TCP, UDP, ICMP, IGMP, etc, com o seguinte formato:
  - Pacotes e bytes transaccionados que foram acumulados.
  - Flags (Protocolo TCP) ou tipos mensagens ICMP.
  - Instante da ocorrência da última transacção.
- Ficheiro de dados Tipo-3, com toda a informação acumulada relativa ao protocolo IP, com o seguinte formato:
  - Pacotes e bytes transaccionados que forram acumulados.
  - Tempo de ocorrência da última transacção.
- Ficheiro de fluxos de informação Tipo-4, sendo contabilizado de acordo com o tipo de protocolo, tais como:
  - Protocolo TCP: Fluxo de informação associado aos campos:
    - IPOrigem, PortoOrigem, IPDestino, PortoDestino.
    - Flags associadas (SYN+ACK+RST+FIN).
    - Bytes, Pacotes.
  - Protocolo UDP: Fluxo de informação associado aos campos:
    - IPOrigem, PortoOrigem, IPDestino, PortoDestino.
    - Bytes, Pacotes.
  - Protocolo ICMP: Fluxo de informação associado aos campos:
    - IPOrigem, IPDestino.
    - Tipos de mensagens ICMP.
    - Bytes, Pacotes.
  - Protocolo Outros: Fluxo de informação associado aos campos:
    - IPOrigem, IPDestino.
    - Bytes, Pacotes.

3.2.2 Processo de análise de informação

O processo de análise de informação incide sobre os dados produzidos pelo processo de recolha, e pretende-se nesta fase fazer uma aprendizagem do comportamento relativo aos protocolos detectados na fase de recolha.

Na fase de aprendizagem é possível definir o funcionamento padrão relativamente aos diferentes protocolos que flúem na rede durante um determinado período de tempo. Esta fase encontra-se descrita na Figura 3.8, onde se encontra definida a ordem do processamento pelos diversos módulos.

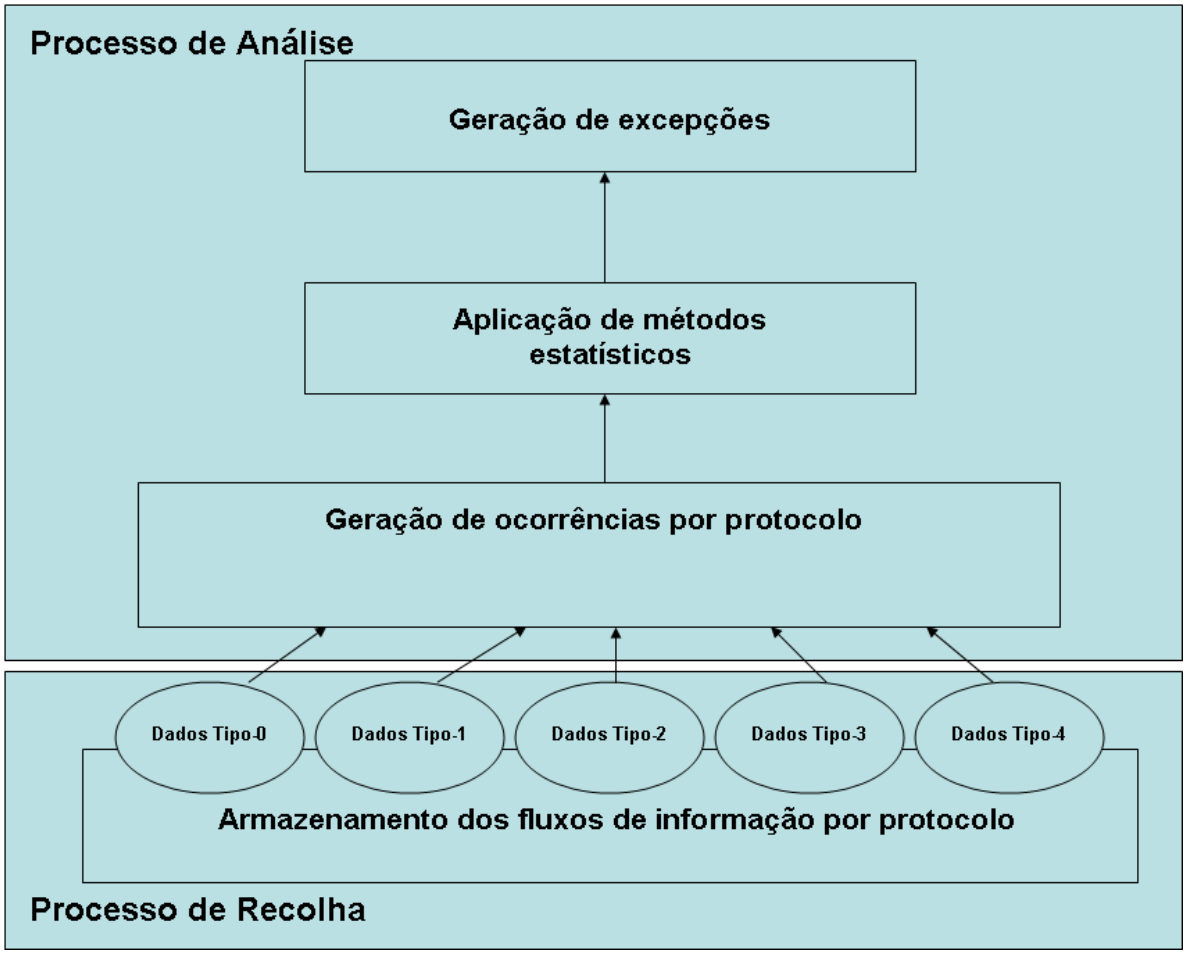


Figura 3.8 - Processo de análise de informação.

3.2.2.1 Módulo de gestão de ocorrências por protocolo

O processo de Análise utiliza como fonte de informação os dados gerados pelo processo de Recolha, através da utilização dos ficheiros com os dados Tipo 0 a 4. Estes dados são tratados como ocorrências por protocolo, dando origem à contabilização de ocorrências por intervalo de tempo, que para o caso em análise é de 100 segundos. As ocorrências detectadas serão a base do processo de aprendizagem. Para compreendermos melhor o processo de agregação, podemos utilizar o seguinte exemplo:

- Dados Tipo-0 com 4 pacotes capturados:
  - Protocolo=TCP

    IP Origem=a.a.a.a Porto Origem=aaaa

    IP Destino=b.b.b.b Porto Destino=bbbb

    Pacote(1) Origem→Destino, Bytes Transmitidos=40

    Pacote(2) Origem←Destino, Bytes Transmitidos=40
  - Protocolo=TCP

    IP Origem=d.d.d.d Porto Origem=dddd

    IP Destino=e.e.e.e Porto Destino=eeee

    Pacote(1) Origem→Destino, Bytes Transmitidos=30

    Pacote(2) Origem←Destino , Bytes Transmitidos=30
- Dados Tipo-1 com os dados acumulados gerados:
  - Protocolo TCP porto destino=bbbb, terá a seguinte informação:
    - Quantidade de bytes transmitidos = 80 bytes
    - Quantidade de pacotes transmitidos = 2
  - Protocolo TCP porto destino=eeee, terá a seguinte informação:
    - Quantidade de bytes transmitidos = 60 bytes
    - Quantidade de pacotes transmitidos = 2

- Dados Tipo-2 com os dados acumulados gerados:
    - Protocolo TCP, terá a seguinte informação:
        - Quantidade de bytes transmitidos =140 bytes
        - Quantidade de pacotes transmitidos = 4
- Dados Tipo-3 com os dados acumulados gerados:
    - Protocolo IP, terá a seguinte informação:
        - Quantidade de bytes transmitidos =140 + (20*4)=220 bytes
        - Quantidade de pacotes transmitidos = 4

Os dados produzidos pelo processo de recolha, guardados nos ficheiros acima referidos, são contabilizados como ocorrências de acordo com os Tipos registados no processo de recolha, dando origem aos seguintes ficheiros:

Acumulados Tipo-1 : Protocolos TCP + Port (bbbb), TCP + Port (eeee).

Acumulados Tipo-2 : Protocolos TCP, UDP, ICMP, IGMP, etc.

Acumulados Tipo-3 : Protocolo IP.

3.2.2.2 Módulo de aplicação dos métodos estatísticos

Este módulo recorre a métodos estatísticos para a análise, e como resultado da combinação dos mesmos define o comportamento da rede que é usado no processo de aprendizagem e no processo de detecção de anomalias. A análise pode ser feita por intervalo de tempo:

- De x em x segundos interpretar o comportamento.
- De x em x minutos interpretar o comportamento.
- De x em x horas interpretar o comportamento.
- De x em x dias interpretar o comportamento.

A opção sobre o intervalo de tempo recaiu sobre a utilização de um intervalo de 100 segundos, valor esse que permite detectar grande parte dos ataques não causando grande impacto ao nível de espaço requerido para armazenamento de informação.

Exemplos de métodos estatísticos que podem ser utilizados

- *Média:* A média [33] é utilizada para cálculo dos valores médios encontrados para o tráfego que se pretende catalogar. Deste modo obtém-se o valor médio de tráfego durante um período de tempo que define o comportamento.

$$\overline{x} = \frac{x_1 + x_2 + \ldots + x_n}{n} = \frac{\sum_{i=1}^{n} x_i}{n},$$

- *Moda*: A moda [34] permite obter o valor central mais utilizado durante um intervalo de tempo especificado para análise. Este valor central de tráfego mais comum permite avaliar o factor de pico de rede, e que deve estar correlacionado com a média para o mesmo período de tempo.

- *Mediana:* A mediana [35] permite obter o valor central obtido depois de ordenados todos os dados de um modo crescente ou decrescente. Permite deste modo obter qual foi o consumo mais ou menos padrão, durante um intervalo de tempo.

- *Variância:* A variância [36] é a medida que se obtém somando os quadrados dos desvios das observações da amostra, relativamente à sua média, e dividindo pelo número de observações da amostra menos um:

$$s^2 = \frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{n-1} = \frac{\sum_{i=1}^{n} (x_i^2) - n\overline{x}^2}{(n-1)}.$$

- *Desvio Padrão:* Uma vez que a variância envolve a soma de quadrados, a unidade em que se exprime não é a mesma que a dos dados. Assim, para se obter uma medida da variabilidade ou dispersão com as mesmas unidades que os dados, toma-se a raiz quadrada da variância e obtemos o desvio padrão [37]. Deste modo obtém-se quais os desvios

assinalados relativamente a determinados comportamentos ditos de padrão anteriormente colectados.

$$s = \sqrt{\frac{\sum_{i=1}^{n} (x_i - \overline{x})^2}{(n - 1)}}$$

O desvio padrão é uma medida que só pode assumir valores não negativos e quanto maior for, maior será a dispersão dos dados. Algumas propriedades do desvio padrão, que resultam imediatamente da definição, são:

- o desvio padrão é sempre não negativo e será tanto maior, quanta mais variabilidade houver entre os dados.
- se s = 0, então não existe variabilidade, isto é, os dados são todos iguais.

Qual o método estatístico que melhor se adapta?

Os métodos estatísticos acima referidos no entanto apresentam desvantagens na sua utilização. Por exemplo fazendo uma análise relativamente à média, pode-se concluir que é uma medida pouco resistente, pois é influenciada por valores ou muito grandes ou muito pequenos. O mesmo tipo de problema se coloca relativamente ao desvio padrão, o que seria de esperar já que na sua definição entra a média que é não resistente. Assim, se a distribuição dos dados for bastante enviesada, não é conveniente utilizar a média como medida de localização, nem o desvio padrão como medida de variabilidade. Estas medidas só dão informação útil, respectivamente sobre a localização do centro da distribuição dos dados e sobre a variabilidade, se as distribuições dos dados forem aproximadamente simétricas.

Como medida de localização, a mediana é mais robusta do que a média, pois não é tão sensível aos dados. Quando a distribuição é simétrica, a média e a mediana coincidem. A mediana não é tão sensível, como a média, às observações que são muito maiores ou muito menores do que as restantes. Por outro lado a média, tem a vantagem de reflectir o valor de todas as observações.

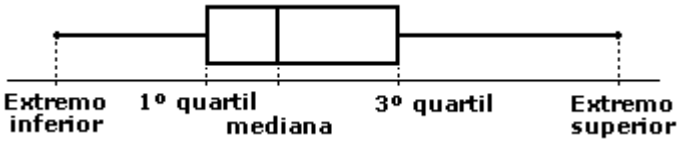
Como neste caso os dados a tratar podem ter qualquer tipo de distribuição simétrica ou não, optou-se por assentar o processo de aprendizagem sobre um método estatístico que não fosse

sensível ao tipo de distribuição. De forma a resolver este problema optou-se pela não utilização dos métodos estatísticos Média e Desvio Padrão, incidindo a escolha pela utilização da Mediana como método estatístico.

A utilização da Mediana por si só não nos permite definir o comportamento padrão, mas se recorrermos aos Diagramas de Extremos ou Caixa dos Bigodes, que recorre à mediana para definir o ponto central da amostra, conseguimos desta forma definir diferentes intervalos de análise.

O que é um diagrama de extremos?

É um tipo de representação gráfica em que se realçam algumas características da amostra [38]. O conjunto dos valores da amostra compreendidos entre o 1º e o 3º quartis, que vamos representar por Q1 e Q3, é representado por um rectângulo (caixa) com a Mediana indicada por uma barra. A largura do rectângulo não dá qualquer informação, pelo que pode ser qualquer. Consideram-se seguidamente duas linhas que unem os meios dos lados do rectângulo com os extremos da amostra. Para obter esta representação, começa por se recolher da amostra, informação sobre 5 números, que são: os 2 extremos, a mediana, e o 1º e 3º quartis. A representação do diagrama de extremos e quartis tem o seguinte aspecto:



O extremo inferior é o mínimo da amostra, enquanto que o extremo superior é o máximo da amostra.

Variações: Algumas vezes as rectas externas (chamados de bigodes) têm diferentes métodos de construção, mas os 25º, 50º e 75º percentis são sempre calculados.

Interpretação do diagrama de extremos:

- a caixa central inclui os 50% dos dados centrais.
- os bigodes mostram a amplitude dos dados, isto é a diferença entre o maior e o menor valores.
- a simetria é indicada pela caixa e bigodes e pela localização da mediana.

Usando os cinco números para reconhecer simetria nos dados:

- a distância de Q1 à mediana é igual à distância da mediana até Q3.
- a distância do valor mínimo até Q1 é igual à distância do valor máximo até Q3.
- a mediana é igual à média.

Usando os cinco números para reconhecer assimetria nos dados:

- para conjuntos assimétricos à direita, a distância de Q3 ao valor máximo excede em muito a distância do valor mínimo até Q1. A mediana é maior que a moda.
- para conjuntos assimétricos à esquerda, a distância do valor mínimo até Q1 excede em muito a distância de Q3 ao valor máximo. A mediana é menor que a moda.

Definição do funcionamento padrão no período de aprendizagem

A definição do funcionamento padrão utiliza os ficheiros de ocorrências sobre os quais incidirá o processamento relativo à construção dos diagramas de extremos. Os desvios são verificados com base na definição de uma hierarquia de agregações de ocorrências de 3 níveis diferentes (ver Figura 3.9), tais como:

- Hierarquia 1, protocolos TCP/UDP.
    - HTTP, FTP, SNMP, DNS, etc.
- Hierarquia 2, protocolos ICMP/TCP/UDP/etc.
- Hierarquia 3, protocolo IP.

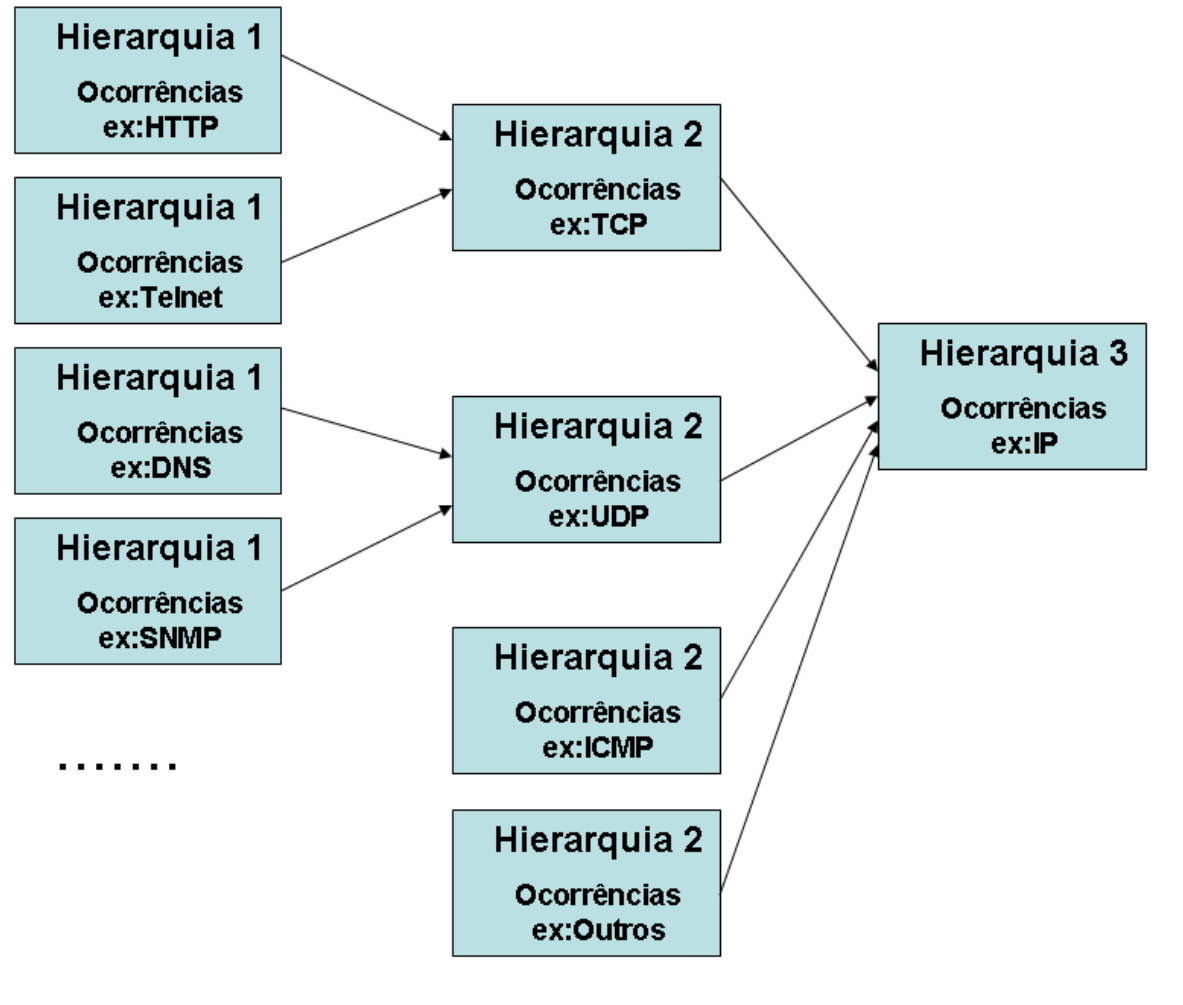


Figura 3.9 - Diagrama de hierarquias.

Funcionamento padrão para protocolos TCP da hierarquia 1

Definição do tipo de dados associado à hierarquia 1, ver Figura 3.10:

- Tipos de flags mais comuns e o seu estado e consequentes desvios, permite detectar ataques DoS.
- Análise de desvios relativamente aos vários protocolos utilizados ao nível do TCP, discriminando os mesmos ao nível dos portos de destino utilizados, permite fazer uma análise de variações relativamente:
    - Largura de banda utilizada e consequentes desvios.

- Número de pacotes transmitidos e consequentes desvios.

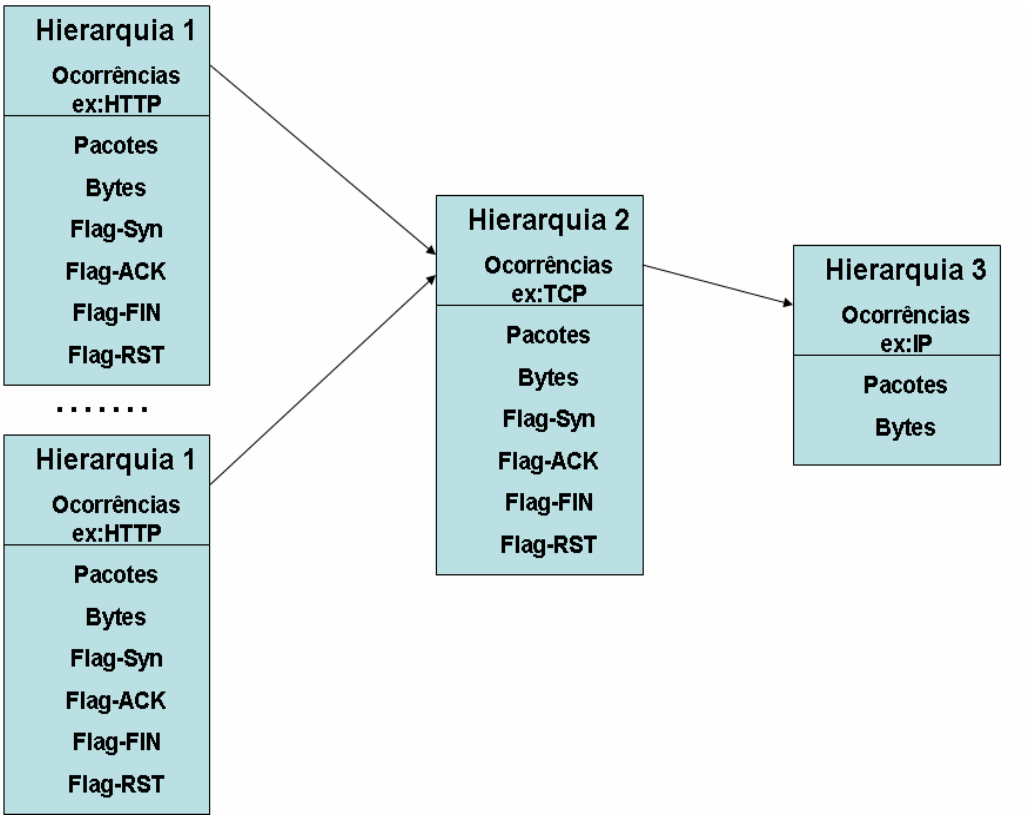


Figura 3.10 - Diagrama de hierarquias para protocolos TCP.

Funcionamento padrão para protocolos UDP da hierarquia 1

Estabelecendo um funcionamento padrão permite-nos perceber o comportamento da rede relativamente a (ver figura 3.11):

- Análise de desvios relativamente aos vários protocolos utilizados ao nível do UDP, discriminando o mesmo ao nível dos portos de destino utilizados, permitindo fazer uma análise de variações relativamente:
  - Largura de banda utilizada e consequentes desvios.
  - Número de pacotes transmitidos e consequentes desvios.

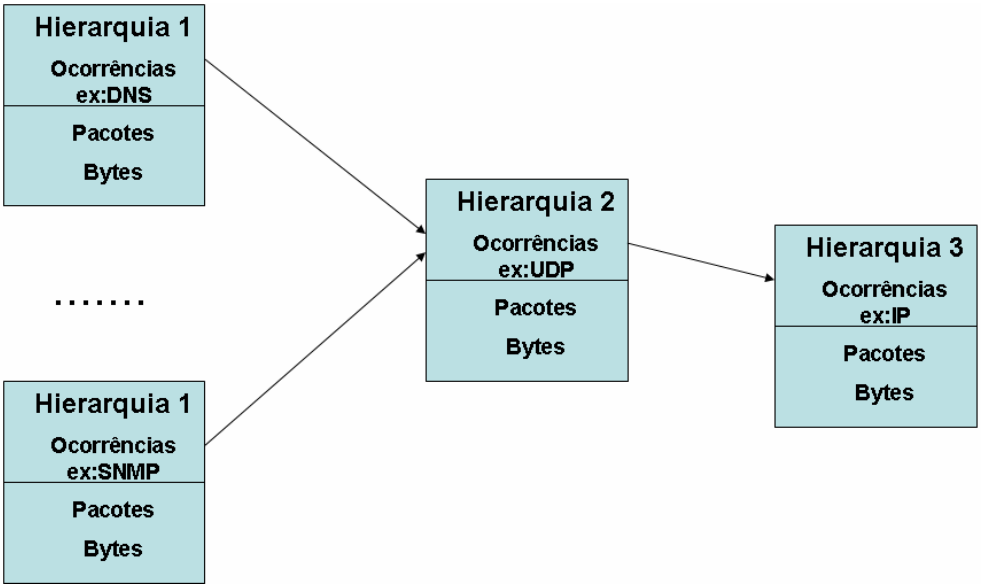


Figura 3.11 - Diagrama de hierarquias para protocolos UDP.

Funcionamento padrão protocolo ICMP da hierarquia 2

Estabelecendo um funcionamento padrão permite-nos perceber o comportamento da rede relativamente a (ver Figura 3.12):

- Tipos de erros mais comuns e consequentes desvios, possibilitando a detecção de ataques DoS.
- Largura de banda utilizada e consequentes desvios.
- Número de pacotes transmitidos e consequentes desvios.

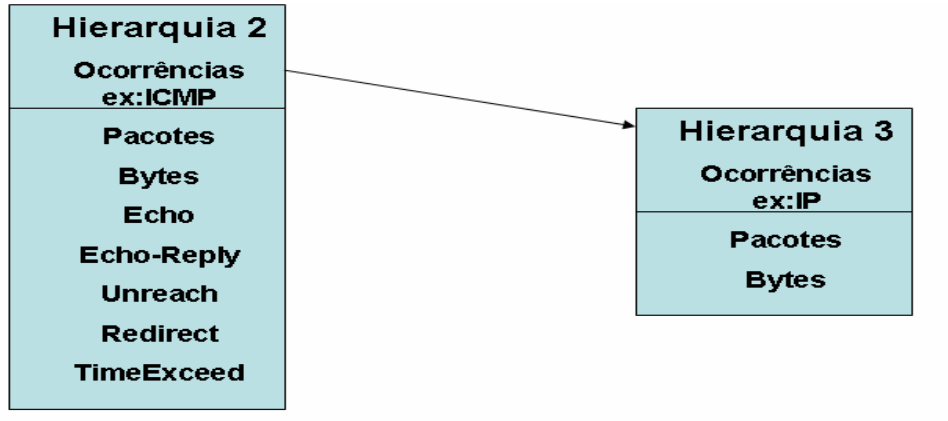


Figura 3.12 - Diagrama de hierarquias de ocorrências protocolos ICMP.

Funcionamento padrão protocolos da hierarquia 2

A hierarquia 2 integra os protocolos referidos anteriormente e outros, de uma forma agregada, permitindo a detecção de anomalias que possam ter escapado na análise de dados da hierarquia 1. Isto pode suceder devido à análise ser feita de modo isolado ao nível dos portos utilizados pelas aplicações, podendo desta forma ser só detectado relativamente a uma análise de forma agregada dos vários portos, ou outros protocolos que não estejam associados à hierarquia 1. Estabelecendo um funcionamento padrão permite-nos perceber o comportamento da rede relativamente (ver Figura 3.13):

- Largura de banda utilizada e consequentes desvios.
- Número de pacotes transmitidos e consequentes desvios.

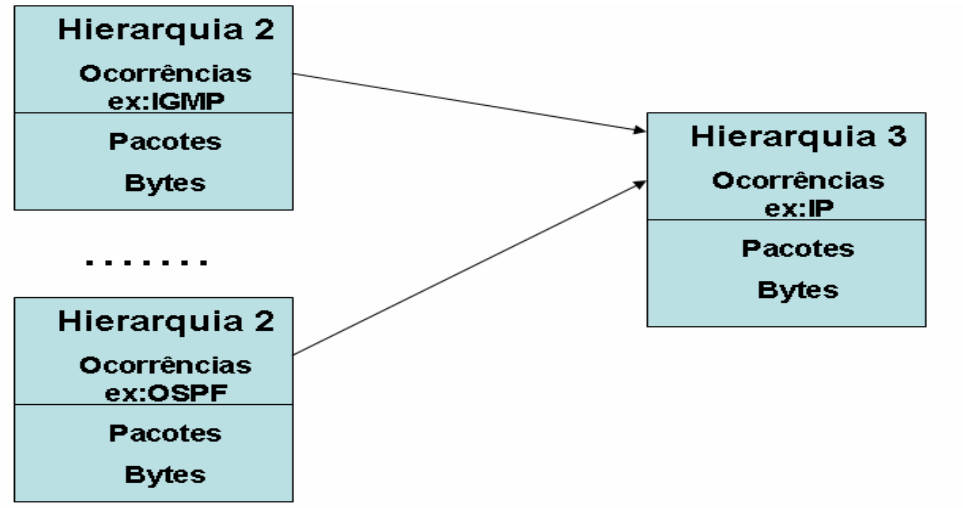


Figura 3.13 - Diagrama de hierarquias para outros protocolos.

Funcionamento padrão para protocolos da hierarquia 3

Tal como a hierarquia 2, a hierarquia 3 pretende complementar as análises efectuadas de maneira a que uma anomalia que não tenha sido detectada ao nível das agregações feitas nas hierarquias 1 e 2, possa ser detectada relativamente ao nível desta hierarquia. Estabelecendo um funcionamento padrão permite-nos perceber o comportamento da rede relativamente:

- Largura de banda utilizada e consequentes desvios.

- Número de pacotes transmitidos e consequentes desvios.

3.2.2.3 Módulo de geração de excepções

Depois de se completar a análise estatística (i.e., aplicar os diagramas de extremos e achar as medianas, etc) sobre as hierarquias anteriormente descritas, procede-se à análise dos desvios dos dados ou pacotes que estão a ser recebidos pelo processo de Recolha. Os desvios detectados dependem do nível hierárquico a que os dados estão associados:

- Hierarquia 1 e 2:
    - Os desvios no caso dos protocolos tipo TCP estão relacionados com:
        - Pacotes
        - Bytes
        - Flags (SYN, ACK, FIN, RST)
    - Os desvios no caso dos protocolos tipo UDP estão relacionados com:
        - Pacotes
        - Bytes
    - Os desvios no caso dos protocolo tipo ICMP estão relacionados com:
        - Pacotes
        - Bytes
        - Tipo mensagens (Echo, EchoReply, Unreach, Redirect, TimeExceed)
- Hierarquia 3:
    - Os desvios, estão relacionados com:
        - Pacotes
        - Bytes

3.2.3 Processo de decisão

O objectivo desta fase é tomar decisões com base nas excepções que foram geradas pelo processo de análise de informação. Todas estas decisões podem provocar alterações de configuração dos equipamentos de rede intervenientes no processo. Na Figura 3.14 encontram-se representadas as interacções entre os processos anteriormente descritos com o processo de decisão.

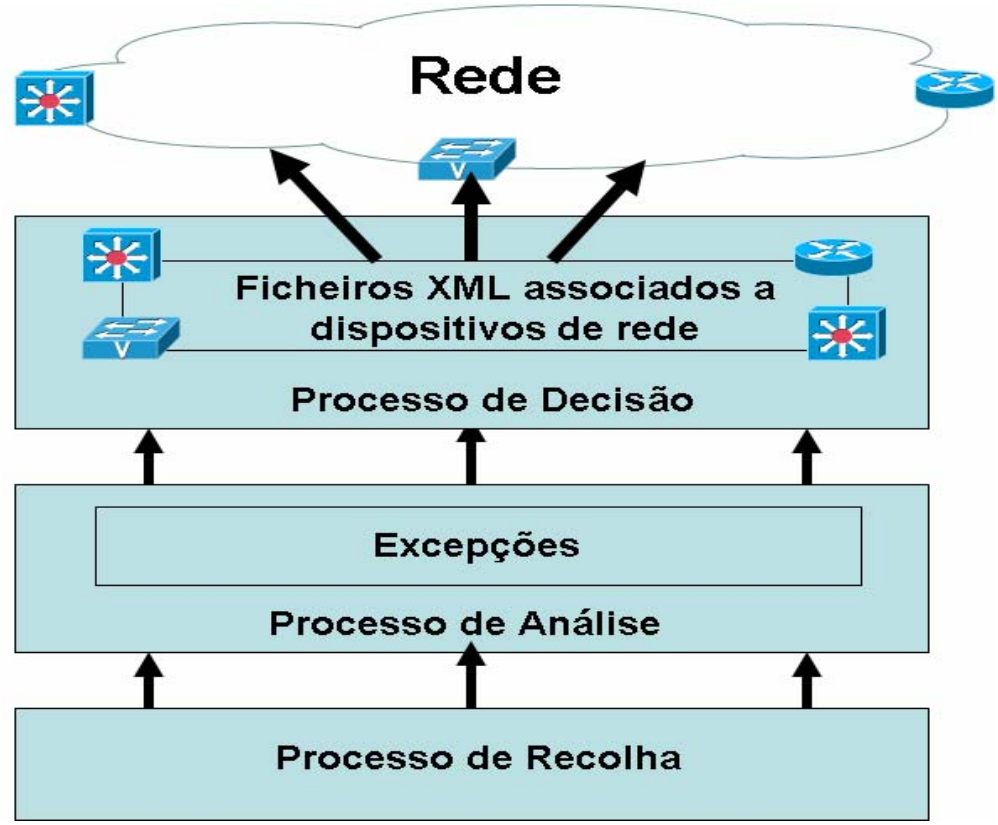


Figura 3.14 - Processo de decisão.

3.2.3.1 Funcionamento do processo de decisão

O processo de decisão visa tratar as excepções geradas para gerar recomendações sob a forma de ficheiros XML. O tratamento da informação produzida pelos processos de Recolha e Análise vai permitir a geração de eventos do tipo (ver figura 3.15):

- *Geração de gráficos*: baseados em filtros de pesquisa à base de dados de conhecimento que foi armazenada.
- *Eventos de gestão de largura de banda:* associados à reconfiguração de equipamentos durante o período de funcionamento da rede.
- *Geração de alarmes:* para uma consola de gestão ou plataforma de gestão recorrendo a protocolos do tipo SNMP ou a geração de informação de logging.
- *Eventos de filtro:* associados ao bloqueio de tráfego como resultado de anomalias detectadas pelo processo de decisão relativamente aos desvios em relação ao comportamento padrão do protocolo em análise.

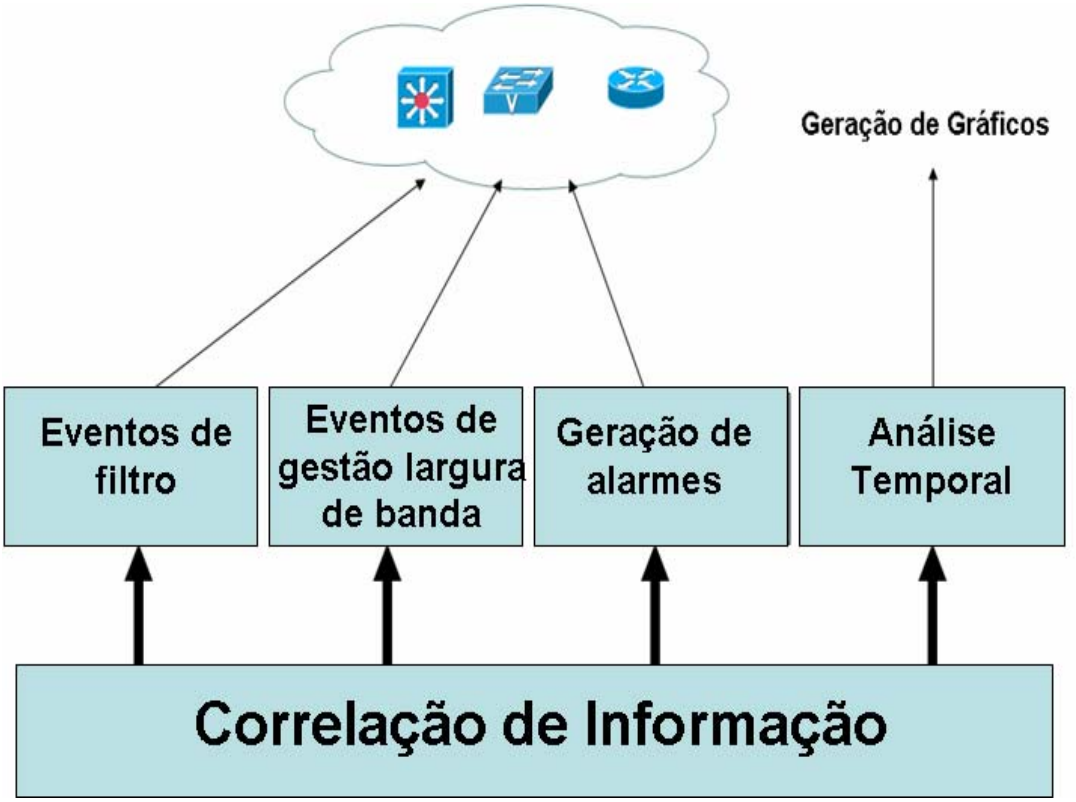


Figura 3.15 - Arquitectura do processo de decisão.

3.2.3.2 Correlação de informação no processo de decisão

Quando se fala de correlação de informação, uma questão sobressai de imediato, é que informação deve ser cruzada e o efeito que se pretende obter? A informação produzida por

equipamentos de comunicações é muito vasta. Podemos assim ter mecanismos de armazenamento de informação que não são mais que repositórios sem qualquer interligação ou mesmo tratamento. Estes tipos de sistemas assentam essencialmente em acções reactivas, relativamente ao acontecimento de eventos.

Nos dias de hoje, não se pretende só guardar informação sobre os eventos, mas também sim tratar essa informação em tempo real. A evolução vai no sentido de abandonar os sistemas reactivos passando deste modo para sistemas pro-activos.

Tendo como base o parágrafo anterior, advém do mesmo um grande desafio. Como explorar esta situação de modo a sermos o mais objectivo possível no tratamento e análise de informação. Na correlação de informação pretende-se uma análise em torno dos seguintes itens:

- Interpretação ao nível das hierarquias definidas anteriormente:
    - Hierarquia 1 vs Hierarquia 2.
    - Hierarquia 2 vs Hierarquia 3.
    - Host/Servers recebedores dos fluxos, IP Destino.
    - Protocolos mais usados e largura de banda usada.
    - Estados de pico.
    - Protocolo TCP, o estudo das flags (SYN, ACK, RESET, FIN).
        - Interpretação de pacotes SYN.
        - Análise de flags de RESET e FIN.

Os itens acima mencionados podem ser correlacionados como um todo, permitindo deste modo uma geração de alarmes aquando da detecção de um comportamento anómalo.

Uma maneira de se fazer a correlação baseia-se na análise temporal. A análise temporal recorre à utilização da informação armazenada pelos processos de Recolha e Análise, no momento da definição de funcionamento padrão, com o objectivo de comparar o tráfego actual com o que foi observado durante a aprendizagem. Com base nos diagramas de extremos calculados, pode-se obter informação em tempo real do tráfego e definir os valores: Baixo,

Médio, Alto de tráfego em número de bytes/pacotes ou flags ou mensagens detectadas durante o período de análise.

Esta análise tem sempre associado um valor temporal relacionado com a ocorrência de cada registo, permitindo desta maneira ter uma associação entre o valor obtido e o intervalo de tempo em que ocorreu esse mesmo valor.

3.2.3.3 Geração de gráficos da informação recolhida

A geração de gráficos visa dotar o sistema de uma representação gráfica dos fluxos de informação detectados que podem definir o funcionamento padrão. De modo a ser possível definir o estado da rede de comunicações durante a colecta de informação que deu origem ao funcionamento padrão, comparando com o histórico dos comportamentos anteriormente registados.

A geração gráfica é composta por uma série de critérios de pesquisa que podem ser definidos de acordo com o funcionamento padrão criado. Como critérios a serem usados, que servem de base para a definição do funcionamento temos:

- Protocolos detectados durante o tempo de colecta.
- Quais os IP's Destino com mais consumo de largura de banda.
- Qual o consumo de largura de banda.
- Distribuição de ocupação de largura de banda por redes.
- Desvios ao nível das Flags protocolo TCP.
- Desvios ao nível das mensagens protocolo ICMP.

3.2.3.4 Geração de eventos/alarmes

O processo associado à geração de eventos/alarmes deve informar os equipamentos e gestores da rede dos resultados da análise.

Formato das mensagens produzidas

O formato das mensagens produzidas deve fornecer ao equipamento de comunicações uma sequência de instruções genéricas a serem traduzidas para uma linguagem de comandos que o

equipamento de comunicações perceba. De modo a dotar este modelo de uma interface padrão, a opção do formato na geração de instruções genéricas incidiu sobre XML (Extended Markup Language), permitindo assim uma integração com qualquer agente que realize a interface entre o XML produzido e o conjunto de instruções a serem dadas nos diferentes tipos de equipamentos de comunicações.

Tipo de mensagens produzidas

- Alarmes
    - Consumo de largura de banda excedido.
    - Detecção de uma nova aplicação na rede.
    - Comportamento anómalo detectado.
- Eventos de filtro
    - Bloquear determinado tráfego com base na origem/destino.
    - Desbloquear determinado tráfego.
- Eventos de gestão de largura de banda
    - Gestão de largura de banda à entrada das interfaces.
    - Definição de valores de limite de tráfego associados a todos os protocolos à excepção do protocolo TCP.
    - Definição de valores de limite de tráfego associados a protocolos do tipo TCP.

3.3 Conclusão

Este capítulo apresentou em detalhe a solução para detectar comportamentos anómalos com base em desvios relativamente ao comportamento padrão, tendo como base a utilização de métodos estatísticos para definir o mesmo. A análise dos comportamentos anómalos assentou sobre protocolos de qualquer tipo, analisando os seus desvios relativamente ao comportamento padrão, definido na fase de aprendizagem no processo de Análise. Os desvios detectados relativamente ao comportamento padrão deram origem a excepções que por sua vez são convertidas em XML, para serem enviadas como correcções para os equipamentos de

comunicações intervenientes no trajecto dos pacotes de rede. Deste modo possibilita-se o acerto do comportamento previamente registado em relação ao funcionamento padrão.

Capítulo 4

Concretização e Avaliação do Analisador

Este capítulo descreve a concretização do Analisador Comportamental de Rede (ACR), que é uma concretização da arquitectura proposta no Capítulo 3. O ACR tem por objectivo validar as opções e funcionalidades propostas pela arquitectura, proporcionando a execução de testes e a obtenção de resultados práticos.

O ACR foi desenvolvido para monitorar zonas de rede, identificando se o comportamento associado a determinados protocolos se desvia do funcionamento padrão definido na fase de aprendizagem. Como resultado final obtém-se uma série de acções de correcção a serem executadas nos equipamentos por onde os fluxos de dados transitam, de forma a acertar o comportamento, aproximando-o do comportamento padrão.

4.1 Arquitectura e concretização do ACR

O sistema baseia-se nos processos anteriormente descritos, dos quais se passa a referir como constituintes do modelo de sistema:

- Processo de recolha de informação.
- Processo de análise de informação.
- Processo de decisão.

4.1.1 Processo de recolha de informação

Os sniffers [39] são aplicações usadas em redes de computadores, pelos administradores para monitorar, interpretar e validar tipos de tráfego. Em algumas situações são também usados para detectar e corrigir problemas que eventualmente sejam descobertos. Basicamente permitem a captura de pacotes nos vários níveis do modelo OSI e a sua observação por parte do administrador. Este tipo de programas pode ajudar a perceber rapidamente os problemas associados a congestionamento de tráfego e filtros de acesso mal definidos.

Nesta secção vai-se mostrar como se pode conceber um processo de recolha graças à utilização de um sniffer. Para tal torna-se necessário explicar como o mesmo pode ser definido relativamente às diferentes camadas do modelo OSI.

4.1.1.1 Funções básicas de um sniffer

Um sniffer interage na grande maioria das vezes com a placa de rede, configurando-a para que opere em modo caracter (ou em SOCK_RAW). Para proceder à captura de pacotes torna-se também necessário configurar a placa de rede em modo promíscuo, o que significa que se vai escutar todo o tráfego que fluí na interface (quer este tráfego tenha como destino o endereço físico da máquina ou não). O modo promíscuo é muito usado para se coleccionar informação a partir de um concentrador ou da porta de um comutador com capacidades de redireccionamento de tráfego que não tenha só como destino o Mac-Address associado a essa porta.

A colocação de uma interface em modo promíscuo é feita, no caso sistema operativo Linux, executando o seguinte comando (com privilégios de root) na interface ethernet0 onde o sniffer está a ser utilizado:

 # ifconfig eth0 promisc

4.1.1.2 Biblioteca pcap para captura de pacotes

A biblioteca pcap [40] é usada para a captura de pacotes, possibilitando a utilização de filtros ao nível 3 e 4 do modelo OSI. A biblioteca tanto pode funcionar com a placa em modo promíscuo como não-promíscuo. A pcap oferece algumas funções para recepção e processamento de cada pacote. O controle de processamento de pacotes pode ser ajustado para um limite ou configurado para processar indefinidamente.

No caso do processo de recolha optou-se pela utilização da função pcap_open_live(), que serve para se obter o descritor da captura de pacotes, e para se indicar a interface de captura, o limite de bytes a capturar, e o tempo limite de armazenamento associado à captura. Em conjunto com a função pcap_loop(), permite que a recepção e o processamento de cada pacote seja associado a uma função, que para o caso se chama ProcessaPacotes(). Esta função tem a responsabilidade de tratar todos os pacotes que são lidos.

Segue-se um exemplo de utilização da função pcap_open_live() e pcap_loop():

```
char dev[20]="eth0";                    //nome da interface de rede
char errbuf[PCAP_ERRBUF_SIZE];    //registo e erros
pcap_t *handler;                        //apontador para a captura
//Acesso à placa de rede em modo promíscuo
handler = pcap_open_live(dev, BUFSIZ, TRUE, 1, errbuf);
if (handler==NULL) {
 fprintf( stderr, "%s\n", errbuf );
 exit( 1 );
}
//Inicia a captura de pacotes, utilização da função ProcessaPacotes()
pcap_loop(handler, -1, &ProcessaPacotes, NULL);
pcap_close(handler);
```

4.1.1.3 Captura de informação

O processo de recolha armazena os pacotes em bruto numa estrutura de dados em memória denominada Dados Tipo-0 (ver Tabela 4.1). A escrita em memória dos dados deve-se ao facto de não ser possível dimensionar uma fila de espera no processo de captura, provocado pela espera gerada nos acessos de escrita ao disco. De modo a resolver este problema, optou-se por associar uma zona de memória partilhada onde a função ProcessaPacotes() guarda os dados, e um processo concorrente de escrita acede aos dados acumulados para os transferir para disco. A transferência dos dados de memória para disco faz-se em intervalos de 100 em 100 segundos, quer isto dizer que de 100 em 100 segundos são criados ficheiros de Dados Tipo-0 com a informação em bruto da captura.

Após se concluir essa transferência existe um outro processo encarregue de gerar os diferentes acumuladores, também denominados de ficheiros de Dados Recolha tipo-1,2,3, associados aos

diferentes tipos de protocolo (ver Tabela 4.1). Um outro ficheiro de Dados Recolha tipo-4 é gerado, este orientado a fluxos de informação detectados durante os 100 segundos, e que tem como objectivo agregar fluxos de informação associados a qualquer protocolo.

typedef struct { unsigned int protocolo; char ip_origem[16]; char ip_destino[16]; unsigned int porto_origem; unsigned int porto_destino; unsigned long bytes; unsigned int flag1; unsigned int flag2; unsigned int flag3; unsigned int flag4; unsigned int flag5; long timestamp; unsigned char ocupado; **}DadosPacote;**	**typedef struct {** unsigned long bytes; unsigned long pacotes; unsigned int flag1; unsigned int flag2; unsigned int flag3; unsigned int flag4; unsigned int flag5; long timestamp; **}DadosPacoteResumo;**	**typedef struct {** unsigned int protocolo; char ip_origem[16]; char ip_destino[16]; unsigned int porto_origem; unsigned int porto_destino; unsigned long bytes; unsigned long pacotes; unsigned int flag1; unsigned int flag2; unsigned int flag3; unsigned int flag4; unsigned int flag5; long tempo_ini; long tempo_fim; **}FlowPacote;**
Formato de ficheiros de Dados Tipo-0	**Formato de ficheiros de DadosTipo-1,2,3**	**Formato de ficheiros de Dados Tipo-4**

Tabela 4.1 - Diferentes formatos produzidos pelo processo de recolha.

As várias interligações entre os processos de captura de informação e os processos acumuladores e de escrita em disco, encontram-se representados na Figura 4.1.

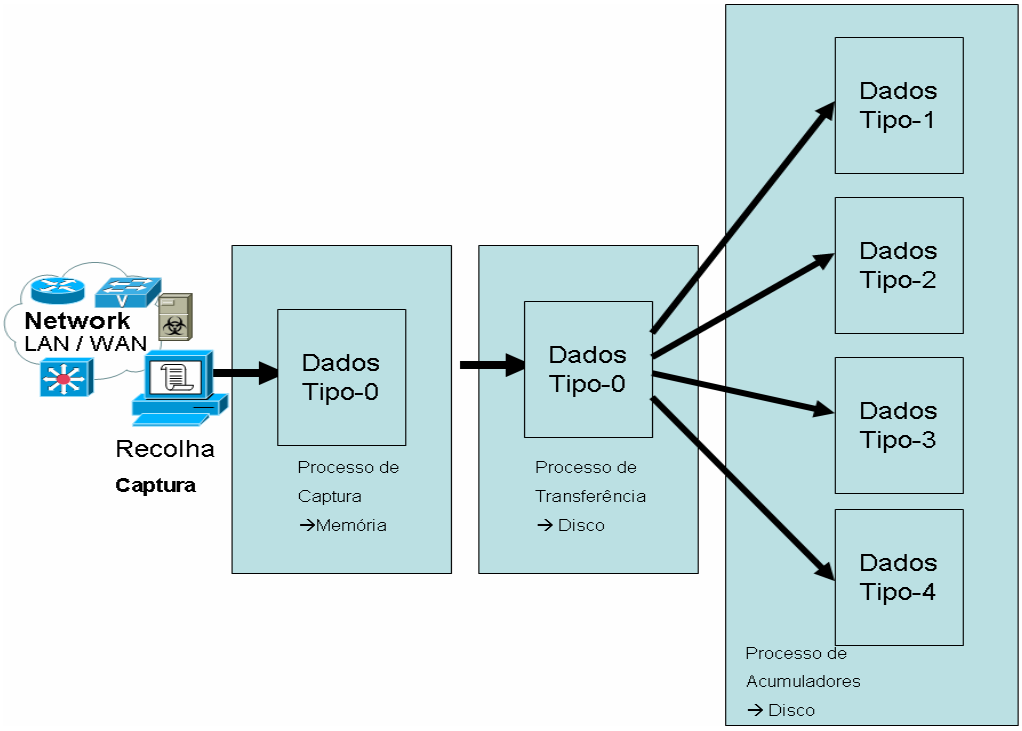


Figura 4.1 - Interligações entre processos no processo de recolha.

4.1.2 Processo de análise de informação

O processo de análise de informação recebe os dados produzidos pelo processo de Recolha. É neste processo que vão ser feitos os cálculos estatísticos, que como foi referido no capítulo anterior, se baseia no método do Diagrama de Extremos. Este método recorre à mediana para encontrar o ponto central da amostra e permite definir intervalos de funcionamento.

4.1.2.1 Intervalos de funcionamento

A definição dos intervalos é feita para os vários tipos de dados, de modo a que sempre que é tratado um ficheiro de Dados, seja do tipo 1,2,3, é gerada uma ocorrência. As ocorrências são guardadas em ficheiros de agregações, em que cada registo acumula uma ocorrência num intervalo de utilização de +/- 10% relativamente:

- Bytes transmitidos.
- Pacotes transmitidos.
- Flags detectadas (SYN, ACK, RST, FIN).

- Tipos de mensagens (Echo, Echo-Reply, Unreach, TimeExceed, Redirect, etc).

Os formatos usados para armazenar as ocorrências obedecem a 3 tipos, como se encontra indicado Tabela 4.2.

typedef struct { unsigned long valor; unsigned long ocorrencias; unsigned long timestamp; }AnalisaDados;	typedef struct { unsigned long valor; unsigned long ocorrencias; unsigned long timestamp; }AnalisaDados;	typedef struct { unsigned long valor; unsigned long ocorrencias; unsigned long timestamp; }AnalisaDados;
Formato de ficheiros de Agregações Tipo-1 **Exemplo:** **A-TP1-xxxxx-yyyy.txt** **xxxx=TCP/UDP** **yyyy=Port**	**Formato de ficheiros de Agregações Tipo-2** **Exemplo:** **A-TP2-xxxxx.txt** **xxxx=Protocolo**	**Formato de ficheiros de Agregações Tipo-3** **Exemplo:** **A-TP3.txt**

Tabela 4.2 - Diferentes formatos de agregações produzidos pelo processo de análise.

Por exemplo, se fizermos uma análise relativamente aos bytes transmitidos:

- Se ficheiros de dados Tipo-1, gerados pela Recolha em diferentes intervalos de tempo, apresentarem a seguinte informação:
  - Tipo-1(t1=0s) → R-TCP-HTTP : Bytes transmitidos=100
  - Tipo-1(t2=t1+100s) → R-TCP-HTTP : Bytes transmitidos=105
  - Tipo-1(t3=t2+100s) → R-TCP-HTTP : Bytes transmitidos=200
  - Tipo-1(t4=t5+100s) → R-TCP-HTTP : Bytes transmitidos=107
  - Tipo-1(t6=t5+100s) → R-TCP-HTTP : Bytes transmitidos=300
  - Tipo-1(t7=t6+100s) → R-TCP-HTTP : Bytes transmitidos=304
- O resultado no ficheiro de registos de ocorrências Tipo-1 são 3 registos com intervalos de +/- 10% de variação:
  - Registo-1: Bytes transmitidos=300, 2 ocorrências

- Registo-2: Bytes transmitidos=200, 1 ocorrência
- Registo-3: Bytes transmitidos=100, 3 ocorrências

4.1.2.2 Aplicação dos diagramas de extremos

Ao recorrermos ao método estatístico do Diagrama de Extremos necessitamos de encontrar a mediana da amostra. Como a mediana é o valor central depois de ordenados todos os dados, torna-se necessário garantir que o ficheiro sobre o qual incide o cálculo se encontra ordenado de um modo crescente ou decrescente. De forma a resolver esta questão optou-se pela utilização do comando Sort, disponível no Linux para ordenar os ficheiros de texto. Este comando pode ser chamado com a seguinte sintaxe:

sort <nome_do_ficheiro_a_ordenar> > <resultado_ficheiro_ordenado>

Exemplo: sort A-TP1-xxxxx-yyyyy.txt > A-TP1-xxxxx-yyyyy.txt#

A aplicação do Diagrama de Extremos pode então ser efectuada, de acordo com as seguintes fases. Veja-se o seguinte exemplo de um ficheiro de ocorrências:

- Registo-1: Bytes transmitidos=100, 2 ocorrências
- Registo-2: Bytes transmitidos=200, 1 ocorrência
- Registo-3: Bytes transmitidos=100, 3 ocorrências

Fase 1: Contabilizar o número total de ocorrências, que é igual a 6.

Fase 2: Detectar o ponto central da amostra, que neste caso está entre o valor 200 e 300:

(100)*2 (200)*1 (300)*3

ou

100 100 200 300 300 300

Fase 3: Ficamos com uma distribuição de 3 elementos para um lado e outros 3 elementos para o outro.

Fase 4: Detectar o ponto central nas duas sub-amostras:

Sub-amostra 1: 100 100 200

Sub-amostra 2: 300 300 300

Obtém-se: Ponto central Sub-amostra 1=100

Ponto central Sub-amostra 2=300

Fase 5: Determinar os valores para os diferentes quartis:

Quartil_25= 100

Quartil_75= 300

Fase 6: Colocar o resultado no primeiro registo do ficheiro agregações associado às ocorrências. O resultado obtido para o registo zero:

<Reg-Zero> <Quartil_25> <Quartil_75>

0000000000 0000000100 0000000300

4.1.2.3 Detecção dos desvios e geração de excepções

Com base nos resultados conseguidos com o diagrama de extremos, pode-se agora avaliar qualquer desvio relativamente aos valores obtidos, comparando os quartis com os dados a tratar. Desta forma, qualquer valor, como Bytes, Pacotes, Flags ou mensagens (ICMP), é validado em relação ao intervalo de quartis, e caso não esteja é então gerada uma excepção.

A excepção gerada é identificada em termos de ficheiro, como EXP-xxxxxx.txt, em que xxxxxx define o instante em que ocorreu a excepção, em intervalos de 100 segundos. O ficheiro gerado tem o seguinte formato, em termos de campos que constituem cada registo.

Campo 1: Nome do ficheiro de captura onde foi detectada a excepção:

`R-TP1-00006-00080-0011545200.txt`

`R-TP2-00006-0011545200.txt`

`R-TP3-0011545200.txt`

Campo 2: Tipo de anomalia detectada:

Caso seja TCP: pode tomar os seguintes valores:

F1: Flag SYN

F2: Flag ACK

F3: N/A

F4: Flag FIN

F5: Flag RST

Caso seja ICMP: pode tomar os seguintes valores:

I1: Echo

I2: Echo-Reply

I3: Unreach

I4: Time Exceed

I5: Router Advertisement

Outros valores: Bytes ou Pacotes

B: Bytes

P: Pacotes

Campo 3: Valor total de bytes detectados

Campo 4: Valor total de pacotes detectados

Campo 5, 6, 7, 8, 9: Totais de flags TCP ou mensagens ICMP detectadas

Campo 10: Quartil inferior

Campo 11: Quartil superior

Campo 12: Instante em que ocorreu a anomalia

4.1.3 Processo decisão

O processo de decisão tem como objectivo a tomada de decisões com base no tratamento das excepções que foram geradas pelo processo de análise de informação. O tratamento destas excepções usa uma linguagem padrão, que neste caso se optou por utilizar XML, de modo a simplificar a codificação e interpretação dos comandos a serem executados pelos agentes de software associados ao tipo de equipamento de rede. Ao executarem estes comandos, espera-se que a anomalia observada seja corrigida.

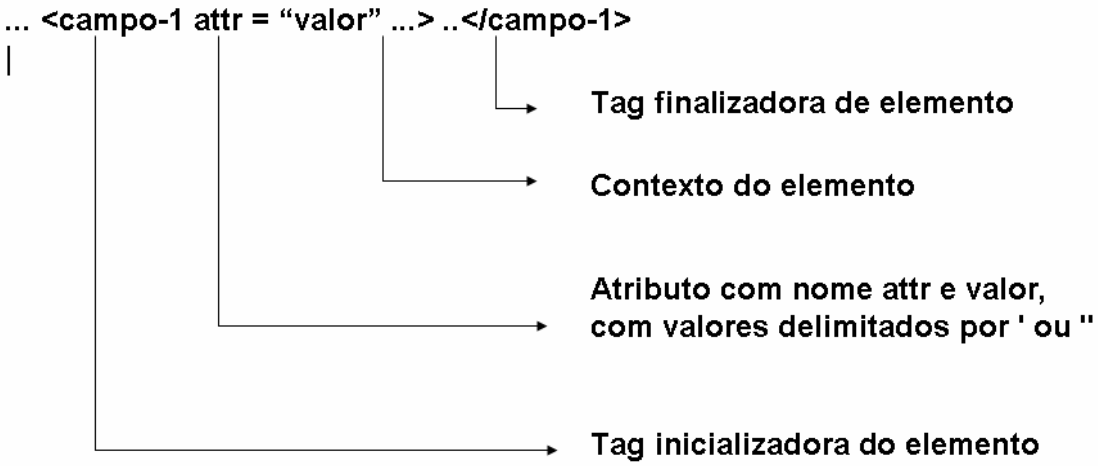
4.1.3.1 A utilização da linguagem padrão XML

O XML é uma especificação técnica desenvolvida pela W3C (World Wide Web Consortium - entidade responsável pela definição da área gráfica da internet) para superar as limitações do HTML, que é o padrão das páginas da Web. A linguagem XML é definida como o formato universal para dados estruturados na Web. Esses dados consistem em tabelas, desenhos, parâmetros de configuração, etc. A linguagem trata então de definir regras que permitem escrever esses documentos de forma que sejam adequadamente visíveis ao computador. Entre as funções principais do XML, tem-se:

- Descrever dados.
- Apresentar dados em algum formato, como HTML.
- Transportar dados.
- Trocar dados de forma transparente entre plataformas diferentes.

Como se trata de um formato texto-puro, o XML pode ser criado e editado em qualquer editor de texto moderno, suportando ainda a maioria das codificações de caracteres tais como ISO-8859-1 e UTF-8.

Um documento em XML é um texto em formato Unicode com tags de marcação (do Inglês markup tags) que denotam a seguinte estrutura:



Consideremos um exemplo em que foram detectadas algumas excepções (ver Tabela 4.3), encontrando-se armazenadas no ficheiro EXP-11545200.txt, em que o valor 11545200 representa o instante associado à recolha de informação durante um intervalo de 100 segundos.

Fonte da Anomalia	Anomalia	Bytes	Pacotes	Flag/Msg	Flag/Msg	Flag/Msg	Flag/Msg	Flag/Msg	Quartil_25	Quartil_75	Tempo_Rec
R-TP1-00006-00080-0011545200.txt	F1	3400	84	52	42	0	0	29	6	41	1154520024
R-TP1-00006-00080-0011545200.txt	F5	3400	84	52	42	0	0	29	6	15	1154520024
R-TP2-00006-0011545200.txt	B	12034	84	52	42	0	0	29	6667	9174	1154520024
R-TP3-0011545200.txt	B	22345	84	52	42	0	0	29	3502	15345	1154520024

Tabela 4.3 - Exemplo de anomalias detectadas.

Analisando o resultado podemos concluir que para este caso foram detectadas as seguintes anomalias:

- *Anomalia F1 Tipo1:* no protocolo TCP/HTTP foram detectados cerca de 52 pacotes com a flag de SYN activa neste intervalo de tempo, que não se enquadram no intervalo de funcionamento definido (que tinha como valor mínimo 6 e valor máximo 41).
- *Anomalia F5 Tipo:* no protocolo TCP/HTTP foram detectados cerca de 29 pacotes com a flag de RST activa neste intervalo de tempo, que não se enquadram no intervalo de funcionamento definido (que tinha como valor mínimo 6 e valor máximo 15).
- *Anomalia Tipo2:* no protocolo TCP foram detectados cerca de 12074 bytes que não se enquadram no intervalo de funcionamento definido (que tinha como valor mínimo 6667 e valor máximo 9174).
- *Anomalia Tipo3:* no protocolo IP foram detectados cerca de 22345 bytes que não se enquadram no intervalo de funcionamento definido (que tinha como valor mínimo 3502 e valor máximo 15345).

4.1.3.2 Conversão gerada para XML

A conversão gerada para XML obedece às regras definidas para utilização do XML, de definição de "tags" e atribuição de valores. As tags que são usadas são as seguintes:

- Qualquer ficheiro XML, deve ter definido um cabeçalho que especifica a versão e a codificação utilizada:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
```

- Definição do "subject" associado à transacção, que tem por objectivo indicar o tipo de anomalia detectada e que pode ser de vários tipos:

```
<subject>Anomalias TCP flags</subject>
<subject>Anomalias desvio de bytes</subject>
<subject>Anomalias desvio de pacotes</subject>
<subject>Anomalias ICMP types</subject>
```

- A identificação do tipo de protocolo que foi identificado como anómalo:

```
<identificao>IP-X1-X2</identificacao>
   IP-Protocolo IP
   X1-Identifica se o protocolo é TCP=6 ou UDP=17
   X2-Identifica que tipo de protocolo TCP/UDP,
      ex:HTTP(80), Telnet(23), SMTP(25), FTP(21/22).
<identificao>IP-X1</identificacao>
   IP-Protocolo IP
   X1-Identifica qual o protocolo, TCP/UDP/ICMP/OSPF, etc
<identificao>IP</identificacao>
   IP-Protocolo IP
```

- Referência à fonte de informação onde a anomalia foi detectada:

```
<referencia>NomeDoFicheiro</referencia>
   NomeDoFicheiro=R-TP1-X1-X2-timestamp.txt
   NomeDoFicheiro=R-TP2-X1-timestamp.txt
   NomeDoFicheiro=R-TP3-timestamp.txt
```

- Intervalos associados aos quartis identificados aquando da ocorrência da anomalia:

```
<val-minimo>Quartil_25</val-minimo>
   Quartil_25=Valor numérico que identifica o limite inferior do
   diagrama de extremos à anómalia detectada.
<val-maximo>Quartil_75</val-maximo>
   Quartil_75=Valor numérico que identifica o limite superior do
   diagrama de extremos à anómalia detectada.
```

- Qual o tipo de anomalia relativamente à identificação feita no “subject”, e qual o valor identificado:
  - Anomalias relativas ao protocolo TCP:

    ```
    <val-SYN>Valor</val-SYN>
    <val-ACK>Valor</val-ACK>
    <val-FIN>Valor</val-FIN>
    <val-RST>Valor</val-RST>
    ```

  - Anomalias relativas ao protocolo ICMP:

    ```
    <val-ECHO>Valor</val-ECHO>
    <val-ECHO-REPLY>Valor</val-ECHO-REPLY>
    <val-UNREACH>Valor</val-UNREACH>
    <val-REDIRECT>Valor</val-REDIRECT>
    <val-TIME_EXCEED>Valor</val-TIME_EXCEED>
    ```

  - Anomalias relativas a desvios de quantidades de bytes transmitidos:

    ```
    <val-bytes>Valor</val-bytes>
    ```

  - Anomalias relativas a desvios de quantidades de pacotes transmitidos:

    ```
    <val-pacotes>Valor</val-pacotes>
    ```

Voltando ao exemplo anterior (ver Tabela 4.3), o resultado da conversão para XML:

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<subject>Anomalias TCP flags</subject>
<identificao>IP-6-80</identificacao>
<referencia>R-TP1-00006</referencia>
<val-minimo>6</val-minimo>
<val-maximo>41</val-maximo>
<val-SYN>52</val-SYN>
<timestamp>1154520024</timestamp>

<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<subject>Anomalias TCP flags</subject>
<identificao>IP-6-80</identificacao>
<referencia>R-TP1-00006</referencia>
<val-minimo>6</val-minimo>
<val-maximo>15</val-maximo>
<val-RST>29</val-RST>
<timestamp>1154520024</timestamp>

<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<subject>Anomalias desvio de bytes</subject>
<identificao>IP-6</identificacao>
```

```
<referencia>R-TP2-00006</referencia>
<val-minimo>6667</val-minimo>
<val-maximo>9174</val-maximo>
<val-bytes>12074</val-bytes>
<timestamp>1154520024</timestamp>
```

```
<?xml version="1.0" encoding="ISO-8859-1" standalone="yes"?>
<subject>Anomalias desvio de bytes</subject>
<identificao>IP</identificacao>
<referencia>R-TP3-0011545200.txt</referencia>
<val-minimo>3502</val-minimo>
<val-maximo>15345</val-maximo>
<val-bytes>22345</val-bytes>
<timestamp>1154520024</timestamp>
```

4.1.3.3 Agentes de conversão do XML para linguagem de comandos

Não faz parte deste trabalho a construção de vários agentes que interpretem o XML gerado pelo processo de Decisão, e que o convertem em comandos a serem enviados e executados nos equipamentos onde se pretende actuar, para controlar o comportamento anómalo detectado.

As acções a serem tomadas podem ser de diferentes tipos e são despoletadas de acordo com as funcionalidades dos equipamentos onde as mesmas serão executadas. As acções mais comuns são do seguinte tipo:

- Largura de banda
    - Limitar a velocidade de transmissão [41]: limitar a utilização de largura de banda a um intervalo de acordo com os dados definidos pela excepção produzida. Este tipo de acção pode ser aplicada sem problemas a protocolos que não sejam do tipo TCP, que não tenham associada uma janela de transmissão. Pois o facto de não existirem filas de espera associadas à transmissão pode provocar degradação na transmissão e recepção de dados.
    - Limitar a velocidade de transmissão para protocolos TCP [42]: com esta acção, como com a anterior, deseja-se limitar a utilização de largura de banda. Tem associada um mecanismo de filas de espera que entra em acção quando se excedeu o limite máximo de transmissão, permitindo guardar os dados até haver a possibilidade de se transmitir.
    - Filtros de bloqueio: recorrendo a este tipo de filtros podemos bloquear:

- Tráfego com destino a redes não conhecidas.
- Evitar o spoofing de endereços de origem não válidos.
- Controlar o estado das flags, permitindo só o estabelecimento de sessões para determinados IPs que tenham a flag de SYN activa.

- Interacção com sistemas de IDS: sendo possível definir uma assinatura em tempo real para gerar determinadas acções ao nível da detecção de intrusões.

Os ficheiros XML gerados são utilizados como dados de entrada para os agentes que vão interagir com os diferentes equipamentos de rede, através da conversão do XML em comandos a serem enviados aos equipamentos.

Seguem-se alguns exemplos de possíveis conversões efectuadas para equipamentos Cisco:

- Exemplo anomalia de desvio de bytes para o protocolo TCP, valor mínimo de funcionamento igual a 5557 bytes e valor máximo igual 9174 em 100 segundos. O valor do limite máximo excedido valor detectado igual a 12074.

  Limite mínimo em bits/s = (5557 *8)/100 = 444,56 bits/s

  Limite máximo em bits/s = (9174*8)/100 = 733,96 bits/s

  ! Definição do filtro de tráfego para interceptar tráfego TCP

  access-list 101 permit tcp any any

  ! Aplicar a limitação de largura banda na interface eth0 do encaminhador

  interface Ethernet0

  traffic-shape group 101 750 ! arredondamento do limite máximo

- Exemplo anomalia de desvio de bytes para o protocolo IP, valor mínimo de funcionamento igual a 3502 bytes e valor máximo igual 15345 em 100 segundos. O valor do limite máximo excedido valor detectado igual a 225345.

  Limite mínimo em bits/s = (3502 *8)/100 = 280,16 bits/s

  Limite máximo em bits/s = (15345*8)/100 = 1227,6 bits/s

  ! Definição do filtro de tráfego para interceptar tráfego IP

access-list 101 permit ip any any

! Aplicar a limitação de largura banda na interface eth0 do encaminhador

interface Ethernet0

traffic-shape group 101 1250 ! arredondamento do limite máximo

4.2 Testes

De modo a avaliar o protótipo construído, foram definidos uma série de testes com tráfego malicioso de modo a demonstrar as várias funcionalidades do ACR.

4.2.1 Ambiente de testes

O ambiente de testes utilizado assentou sobre uma rede com vários serviços (ver Figura 4.3), comuns, tais como: TCP/UDP, FTP, HTTP, ICMP, DNS, etc.

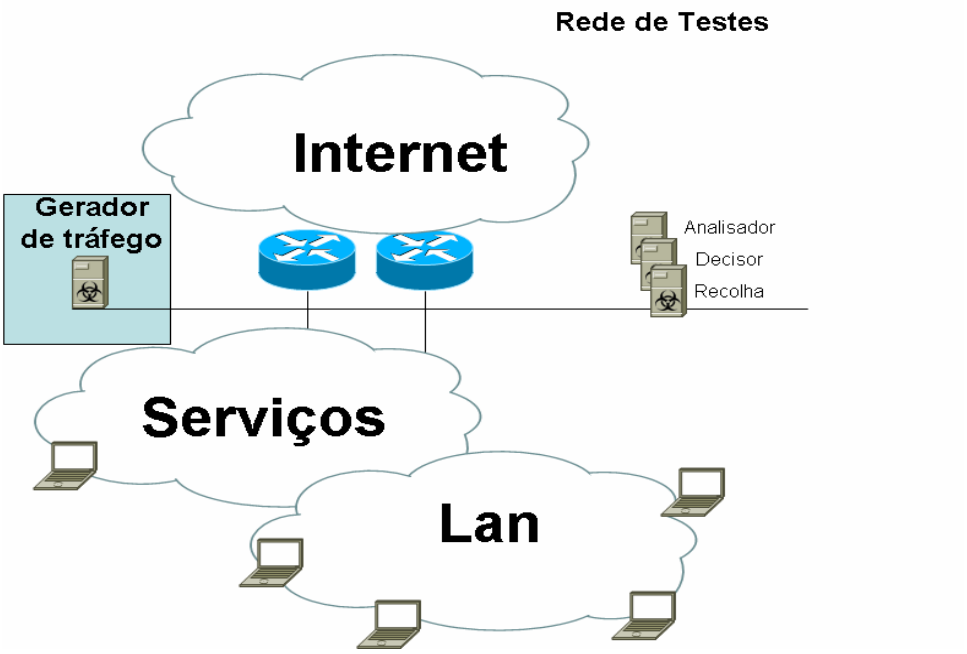


Figura 4.2 - Ambiente de testes.

4.2.2 Comportamento padrão

Primeiro analisou-se o comportamento da rede antes de se proceder á geração de tráfego anómalo. O comportamento padrão detectado durante uma semana, que equivale a cerca de 604800 segundos, deu origem a 6048 amostras, e teve como resultado a geração das seguintes fontes de informação associadas ao processo de recolha:

- R-TP0-<intervalo de tempo múltiplo de 100 segundos>.
- R-TP1-Associado a protocolos TCP e UDP que para o caso foram protocolos tipo HTTP,FTP, Telnet, DNS,.....
- R-TP2-Associado à agregação dos protocolos tipo 1(TCP/UDP) mas também a todos os outros, tais como: TCP, UDP, ICMP, IGMP, OSPF,.....
- R-TP3-Associado à agregação de todos os protocolos IP.
- R-TP4-Associado ao resultado da contabilização de todos os fluxos de informação detectados.

Aplicando o processo de análise ao resultado das diferentes fontes de informação produzidas no processo de recolha, obtivemos os vários tipos de agregação e consequentes diagramas de extremos:

- Comportamento padrão, agregação tipo-1
  - Diagrama de extremos protocolo HTTP, associado ao TCP:

Tipo-1-TCP-HTTP(80)			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP1-B-00006-00080.txt	176	173985
Pacotes	A-TP1-P-00006-00080.txt	4	436
Flag1=SYN	A-TP1-F1-00006-00080.txt	2	41
Flag2=ACK	A-TP1-F2-00006-00080.txt	2	401
Flag4=FIN	A-TP1-F4-00006-00080.txt	1	18
Flag5=RST	A-TP1-F5-00006-00080.txt	1	15

- Diagrama de caixa, protocolo Telnet, associado ao TCP:

Tipo-1-TCP-Telnet(23)			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP1-B-00006-00023.txt	100	3502
Pacotes	A-TP1-P-00006-00023.txt	1	80
Flag1=SYN	A-TP1-F1-00006-00023.txt	1	2
Flag2=ACK	A-TP1-F2-00006-00023.txt	1	79
Flag4=FIN	A-TP1-F4-00006-00023.txt	1	1
Flag5=RST	A-TP1-F5-00006-00023.txt	1	1

- Diagrama de caixa, protocolo FTP (Dados), associado ao TCP:

Tipo-1-TCP-FTP(20)			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP1-B-00006-00020.txt	100	14853849
Pacotes	A-TP1-P-00006-00020.txt	1	21573
Flag1=SYN	A-TP1-F1-00006-00020.txt	1	8
Flag2=ACK	A-TP1-F2-00006-00020.txt	1	21569
Flag4=FIN	A-TP1-F4-00006-00020.txt	1	6
Flag5=RST	A-TP1-F5-00006-00020.txt	1	1

- Diagrama de caixa, protocolo FTP (Controlo), associado ao TCP:

Tipo-1-TCP-FTP(21)			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP1-B-00006-00021.txt	100	2595
Pacotes	A-TP1-P-00006-00021.txt	1	44
Flag1=SYN	A-TP1-F1-00006-00021.txt	1	2
Flag2=ACK	A-TP1-F2-00006-00021.txt	1	43
Flag4=FIN	A-TP1-F4-00006-00021.txt	1	3
Flag5=RST	A-TP1-F5-00006-00021.txt	1	1

- Diagrama de caixa, protocolo DNS, associado ao UDP:

Tipo-1-UDP-DNS(53)			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP1-B-00006-00053.txt	852	1156
Pacotes	A-TP1-P-00006-00053.txt	6	8

- Comportamento padrão, agregação tipo-2
  - Diagrama de caixa, protocolo TCP:

Tipo-2-TCP			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP2-B-00006.txt	9495	173985
Pacotes	A-TP2-P-00006.txt	80	436
Flag1=SYN	A-TP2-F1-00006.txt	6	12
Flag2=ACK	A-TP2-F2-00006.txt	79	401
Flag4=FIN	A-TP2-F4-00006.txt	10	18
Flag5=RST	A-TP2-F5-00006.txt	1	15

  - Diagrama de caixa, protocolo ICMP:

Tipo-2-ICMP			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP2-B-00001.txt	100	960
Pacotes	A-TP2-P-00001.txt	1	16
Tipo=Echo	A-TP2-I1-00001.txt	1	8
Tipo=Echo Reply	A-TP2-I2-00001.txt	1	8
Tipo=Unreach	A-TP2-I3-00001.txt	1	1
Tipo=Time Exceed	A-TP2-I4-00001.txt	1	1
Tipo=Router Advertise	A-TP2-I5-00001.txt	1	1

  - Diagrama de caixa, protocolo UDP:

Tipo-2-UDP			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP2-B-00017.txt	852	1156
Pacotes	A-TP2-P-00017.txt	6	8

- Comportamento padrão, agregação tipo-3
  - Diagrama de caixa, protocolo IP:

Tipo-3			
Tipo de agregação	**Ficheiros de Agregação**	**Limite inferior**	**Limite Superior**
Bytes	A-TP3.txt	3502	174837
Pacotes	A-TP3.txt	35	444

4.2.3 Geração de tráfego anómalo

Os testes foram realizados sem se parar a análise do comportamento padrão, pelo contrário continuou-se a analisar a rede em termos de comportamento, enriquecendo o mesmo com mais dados a juntar ao histórico que tínhamos com uma semana de tratamento.

De modo a provocar anomalias ao comportamento padrão, optou-se pela geração de tráfego anormal numa rede, que explora uma série de vulnerabilidades existentes ao nível dos protocolos. Para se gerar o tráfego anómalo utilizaram-se algumas ferramentas disponíveis para Linux, nomeadamente uns poucos scripts em Perl.

4.2.3.1 Tipificação das anomalias

Anomalia 1 - Spoofed TCP SYN

Descrição: o computador que origina o ataque gera uma série de pacotes com emissor aleatório e envia para o computador a que se destina o ataque. O computador alvo do ataque envia pacotes SYN&ACK como resposta aos pacotes SYN, mas com destino o endereço aleatório (ver Figura 4.3) e adiciona uma entrada na fila de sessões activas. Como os pacotes SYN&ACK são enviados para destinos incorrectos ou inexistentes, a última parte do protocolo TCP nunca será completada e a entrada fica na fila de sessões até expirar (tipicamente um minuto) ou receber da parte do endereço aleatório um pacote com a flag RST activa. Com a geração de centenas de pacotes com origem aleatória é possível esgotar a fila de espera de sessões do computador de destino, iniciando um processo de rejeição de estabelecimento de serviços legítimos (e-mail, ftp ou WWW).

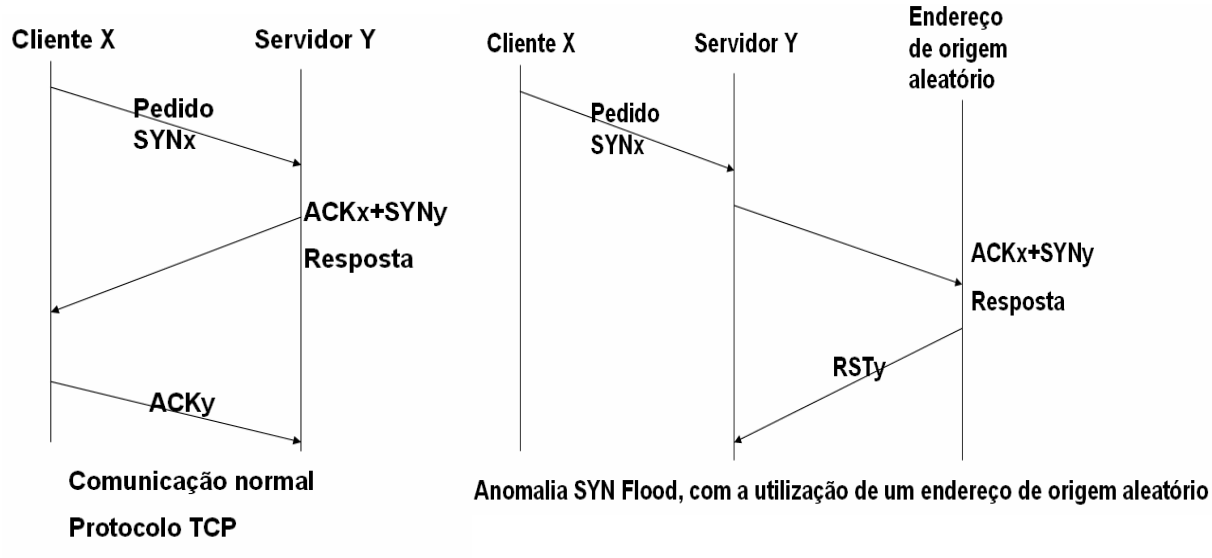


Figura 4.3 - Diferenças entre a comunicação normal e uma anomalia.

Detecção: excesso de flags SYN &ACK e um aumento de flags RST como resposta dos endereços aleatórios (ver Tabela 4.4 que descreve o comportamento desta anomalia).

Anomalia 1->Comportamento detectado ao nível do protocolo TCP---Porto 80(HTTP)							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
3400	84	52	42	0	0	29	1154520024

Tabela 4.4 - Comportamento da anomalia 1 - Spoofed TCP SYN.

Anomalia 2 - Spoofed UDP

Descrição: o computador que começa o ataque gera uma série de pacotes com origem aleatória e envia-os para o computador a que se destina o ataque. Com a geração de centenas de pacotes com origem aleatória é possível esgotar a capacidade de processamento do destinatário, iniciando um processo de rejeição de serviços legítimos.

Detecção: limite excedido relativamente ao número de pacotes detectado para este protocolo (ver Tabela 4.5 que descreve o comportamento).

Anomalia 2->Comportamento detectado ao nível do protocolo UDP---Porto 80(HTTP)							
Bytes	Pacotes	Flag-NA	Flag-NA	Flag-NA	Flag-NA	Flag-NA	Timestamp
2900	100	0	0	0	0	0	1154520121

Tabela 4.5 - Comportamento da anomalia 2 - Spoofed UDP.

Anomalia 3 - Spoofed ICMP/PING

Descrição: Ataque que utiliza pacotes do tipo "Echo" e "Echo-Reply" do protocolo ICMP, durante um intervalo de tempo em que as respostas do computador a que se destina os pacotes tipo "Echo", responde com pacotes do tipo "Echo-Reply" para destinos aleatórios, provocando um aumento de consumo de cpu.

Detecção: limite excedido relativamente ao número de mensagens ICMP do tipo EchoReq e EchoReply (ver tabela 4.6 que descreve o comportamento).

Anomalia 3->Comportamento detectado ao nível do protocolo ICMP							
Bytes	Pacotes	EchoReq	EchoReply	Unreach	Redirect	TimeExc	Timestamp
9200	100	50	50	0	0	0	1154520216

Tabela 4.6 - Comportamento da anomalia 3 - Spoofed ICMP/PING

Anomalia 4 - Spoofed TCP/SYNACK

Descrição: tipo de ataque em que o computador iniciador do ataque, gera pacotes com as flags SYN & ACK activas, com o objectivo de confundir o computador que está a ser alvo. Este ataque viola o funcionamento do protocolo TCP pois estes pacotes só devem ser recebidos após ter inicio uma ligação. O destinatário do ataque detecta o problema porque a ligação não consta da sua tabela de sessões activas. No entanto, o ataque acaba por provocar o consumo de CPU (e rede) ao se processar estes erros e gerar os pacotes que assinalam o problema para os destinatários.

Detecção: excesso de flags SYN & ACK sem ter sido iniciada qualquer ligação, e sem o fluxo ter dado entrada na hierarquia 4 (ver Tabela 4.7 que descreve o comportamento desta anomalia).

Anomalia 4->Comportamento detectado ao nível do protocolo TCP-Vários							
Anomalia 4.1->Comportamento detectado ao nível do protocolo TCP-Porto 80(HTTP)							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
144	2	1	1	0	0	0	1154520413
Anomalia 4.2->Comportamento detectado ao nível do protocolo TCP-Porto 443(HTTPS)							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
144	3	3	0	0	0	0	1154520415
Anomalia 4.3->Comportamento detectado ao nível do protocolo TCP-Porto 2077							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
48	1	1	0	0	0	0	1154520414
Anomalia 4.4->Comportamento detectado ao nível do protocolo TCP-Porto 4080							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
48	1	1	0	0	0	0	1154520416
Anomalia 4.5->Comportamento detectado ao nível do protocolo TCP-Porto 4100							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
48	1	1	0	0	0	0	1154520417
. . . . .							
Anomalia 4.Resumo-TCP->Comportamento detectado ao nível do protocolo TCP							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
3968	96	56	40	0	0	0	1154520426

Tabela 4.7 - Comportamento da anomalia 4 - Spoofed TCP/SYNACK.

Anomalia 5 - Spoofed TCP/FIN

Descrição: tipo de ataque em que o computador que começa o ataque gera pacotes com a flag FIN activa, informando o destino que pretende fechar uma sessão TCP que não tinha sido previamente aberta. Como no ataque anterior teremos o mesmo tipo de comportamento por parte do alvo.

Detecção: excesso de flags FIN & RST sem ter sido iniciada qualquer ligação, e sem o fluxo ter dado entrada na hierarquia 4 (ver Tabela 4.8 que descreve o comportamento desta anomalia).

Anomalia 5->Comportamento detectado ao nível do protocolo TCP---Porto 80(HTTP)							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
4000	100	0	50	0	50	50	1154520517

Tabela 4.8 - Comportamento da anomalia 5 - Spoofed TCP/FIN.

Anomalia 6 - Large ICMP packets-IP/ICMP fragments

Descrição: geração de ataques com pacotes ICMP de dimensão superior à permitida pelo meio de transmissão, o que provoca a fragmentação destes pacotes e consequente aumento de processamento pela máquina a quem se destinam esses pacotes.

Detecção: a detecção deste tipo de anomalia pode ser feita recorrendo análise da variação do total de bytes trocados (conforme se pode verificar na Tabela 4.9), ou então verificar se o número de pacotes vs o número de tipos de pacotes ICMP detectados apresentam grandes diferenças. Neste caso foram detectados 6 pacotes associados a mensagens ICMP, sendo 3 pacotes "Echo_Request" e 3 pacotes "Echo_Reply" vs os 24 pacotes detectados.

Anomalia 6->Comportamento detectado ao nível do protocolo ICMP							
Bytes	Pacotes	EchoReq	EchoReply	Unreach	Redirect	TimeExc	Timestamp
30528	24	3	3	0	0	0	1154521530

Tabela 4.9 - Comportamento da anomalia 6 - Large ICMP packets-IP/ICMP fragments

Anomalia 7 - TCP half connections

Descrição: Durante uma ligação normal usando o protocolo TCP, a origem inicia uma sessão enviando um pacote com a flag SYN activa para o sistema de destino. Se o serviço associado ao pedido no sistema de destino está em modo de recepção de ligações, responde com um pacote com a flag ACK+SYN activa. Se o destino não tem o modo de recepção de ligações para aquele serviço activo, então responde um pacote com a flag RST activa. Olhando-se para estes dois tipos de respostas é possível determinar os serviços que se encontram activos, facilitando mais tarde os ataques por parte dos adversários.

Detecção: Este comportamento anómalo é detectado relativamente a uma comunicação entre uma máquina que fez o pedido de ligação e outra que respondeu a esse pedido, com a flag de ACK+RST activas como que informando que para aquele pedido esse serviço não se encontra activo. De notar que este comportamento provocou um desvio em relação às flags SYN+ACK+RST associadas à comunicação entre duas máquinas (ver Tabela 4.10 que descreve o comportamento).

Anomalia 7->Comportamento detectado ao nível do protocolo TCP---Porto 80(HTTP)							
Bytes	Pacotes	Flag-SYN	Flag-ACK	Flag-NA	Flag-FIN	Flag-RST	Timestamp
6667	104	55	62	0	0	25	1154521039

Tabela 4.10 - Comportamento da anomalia 7 – TCP half connections

Conclusão da análise das anomalias

Estas anomalias são em grande parte detectadas pelos actuais IDS/IPS. O objectivo destes testes foi o de demonstrar que é possível detectar estes comportamentos por desvios ao comportamento padrão de uma rede, sendo feita uma análise em termos hierárquicos. Este tipo de análise hierárquica facilita a detecção de anomalias que passem despercebidas na comunicação máquina-máquina mas que são detectados ao nível dos protocolos agregados. Uma vantagem deste tipo de análise, é que deixa de ser preciso definir no tempo diferentes intervalos de análise associados à fase de aprendizagem permitindo deste modo que ambas as fases funcionem em simultâneo.

4.2.3.2 Excepções geradas

Conforme as anomalias observadas, as excepções geradas tiveram como termo de comparação os desvios entre o comportamento padrão e o comportamento da anomalia. Uma anomalia é considerada como tal quando apresenta um desvio relativamente aos diagramas de extremos e só quando o enquadramento relativo ao comportamento padrão não está contido no intervalo definido entre o quartil_25 e o quartil_75.

Os desvios considerados resultaram de uma análise relativamente aos seguintes itens:

- Bytes
- Pacotes
- Flags (SYN, ACK, RST, FIN)
- Mensagens ICMP (EchoRequest, EchoReply, TimeExc, UnReach, Redirect)

Qualquer excepção que seja detectada tem sempre por base um comportamento anómalo, que ao ser detectado é corrigido evitando assim que esse comportamento fique associado a um comportamento padrão. De qualquer modo a passagem de um comportamento anómalo como

fazendo parte do histórico de análise para comportamento padrão ocorre sempre por defeito, caso não haja nenhuma acção de correcção associada à anomalia detectada.

4.3 Conclusão

Este capítulo apresentou a concretização do Analisador Comportamental de Rede (ACR). Pretendeu-se mostrar a sua aplicabilidade recorrendo a um conjunto de testes, que passaram pela definição do comportamento dito de padrão de uma rede e da aplicação de um conjunto de anomalias de modo a validar as características e funcionalidades propostas no ACR, visando deste modo a obtenção de resultados práticos aqui definidos por Excepções ao funcionamento da rede.

Capítulo 5

Conclusão e Trabalho futuro

A maioria dos sistemas de detecção de intrusões actuais funciona à base de padrões de ataques previamente catalogados e inseridos numa base de dados (ou noutro meio equivalente de armazenamento). A detecção de um potencial ataque faz-se através da comparação do tráfego observado (em cada instante) com as assinaturas catalogadas, sendo disparado um alarme ou a execução de uma acção correctiva, quando existe uma equivalência entre os dois. No entanto, as aplicações que utilizam uma infra-estrutura de rede têm um determinado comportamento. Faz então todo o sentido que o detector de intrusões tire partido desta informação para encontrar comportamentos anómalos, normalmente indicadores de ataques em progresso ou já consumados (através de uma intrusão).

O trabalho desenvolvido nesta dissertação propõe um analisador comportamental da rede, que pretende complementar as soluções existentes. Este detector usa como base do seu funcionamento um comportamento padrão da rede, que é definido num período inicial de configuração. A principal dificuldade é saber-se qual é a melhor altura para se efectuar esta aprendizagem, pois se a mesma ocorrer em períodos com pouco tráfego, esta não tipifica o funcionamento da rede. Como consequência podemos ter no processo de análise a ocorrência de eventos falso positivos. De modo a fazer face a esta situação optou-se por fazer uma avaliação constante do comportamento da rede, ou seja quanto mais tempo passar, mais o histórico de agregações caracteriza uma determinada rede.

Na solução proposta, aproveitou-se os mecanismos de captura de pacotes existentes, e que operam de maneira semelhante aos sniffers, e utilizaram-se estruturas armazenamento hierárquico e métodos estatísticos de agregação de resultados. O processo de análise pode residir no IDS com mais recursos, colocado num ponto central da rede, que receberá as agregações efectuadas pelos IDS periféricos. A partir desta informação, poderá realizar as operações de análise e correlação relativamente aos desvios do comportamento padrão. Esta funcionalidade permite dotar o IDS central duma visão global dos comportamentos detectados na rede, em tempo real, e fazer uma possível integração com os actuais equipamentos de rede (anteparas, encaminhadores, etc) sob a forma de instruções XML, recorrendo a agentes dedicados para o efeito.

Relativamente a trabalho futuro, o ambiente de testes onde os mesmos decorreram permitiu verificar que se podia evoluir para análises de tráfego relativamente a comunicações máquina a máquina e para avaliações dos conteúdos dos pacotes trocados. Desta forma as anomalias seriam detectadas a níveis superiores do modelo OSI, permitindo assim que se explorasse melhor as potencialidades dos equipamentos de rede (anteparas, encaminhadores) relativamente a correcções no tráfego que fluí na rede.

No Capítulo 4 foi feita uma primeira análise das capacidades e virtualidades do mecanismo de detecção comportamental proposto na tese.

Como trabalho futuro, haveria toda a utilidade em se alargar as experiências efectuas em várias direcções, nomeadamente: o teste e análise dum maior número de tipos de ataque diferentes; a comparação da solução descrita com os sistemas de detecção de intrusões existentes e que se encontram comercializados para empresas.

Bibliografia

[1] A. Whitaker, D. Newman, “Penetration Testing and Network Defense”, CiscoPress.com, 2005.

[2] Cisco.com, “What is Intrusion Detection?”, 2004 http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/networking_solutions_audience_business_benefits_list.html

[3] S. McClure, J. Scambray and G. Kurtz, “Hacking Exposed”, McGraw Hill, 2005

[4] C. Paquet, W. Saxe, “Business Case for Network Security”, CiscoPress.com, 2004

[5] Cisco.com, “Defeating DDoS Attacks”, 2006 http://www.cisco.com/en/US/products/ps5887/products_white_paper0900aecd8011e927.shtml

[6] A. Soule, K. Salamatian, N. Taft, “Combining Filtering and Statistical Methods for Anomaly Detection”, 2005 http://www.usenix.org/events/imc05/tech/full_papers/soule/soule.pdf

[7] Cisco.com, “Cisco Security Monitoring Analysis and Response System”, 2005 http://www.cisco.com/application/pdf/en/us/guest/products/ps6241/c1031/cdccont_0900aecd802bdc4f.pdf

[8] Cisco.com, “Netflow Services and Applications” http://www.cisco.com/en/US/products/ps6601/products_ios_protocol_group_home.html

[9] D. Rainkow, “IDS bolster network defense, know your options: HIDS & NIDS”, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2819361-2,00.html

[10] F. Ned, “Ferramentas de IDS”, 2004

http://www.rnp.br/newsgen/9909/ids.html

[11] Cisco Training, “Implementing Cisco Intrusion Prevention System (IPS) v5.0”, 2006.

[12] Cisco.com, “Pattern Matching”, 2004 http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_command_reference_chapter09186a008019d6ce.html

[13] Informit.com, “Intrusion Detection Overview”, 2004 http://www.informit.com/articles/article.asp?p=174342&rl=1

[14] Cisco.com, “Network Based Application Recognition Performance Analysis”, 2004, http://www.cisco.com/en/US/products/ps6616/products_white_paper0900aecd8031b712.shtml

[15] R. Maxion, K. Tan, “Benchmarking Anomaly-Based Detection Systems”, 1st International Conference on Dependable Systems & Networks, 2000 http://www.cs.cmu.edu/afs/cs.cmu.edu/user/maxion/www/pubs/maxiontan00.pdf

[16] G. Maselli, L. Deri, S. Suin, “Design and Implementation of an Anomaly Detection System”, 2004, http://luca.ntop.org/ADS.pdf

[17] Cisco.com, “SAFE: IDS Deployment, Tuning, and Logging in Depth”, 2005 http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_package.html

[18] N. Desai, “Optimizing NIDS Performance”, 2004 http://www.securityfocus.com/infocus/1589

[19] Cisco.com, “Cisco IPS risk rating explained”, 2004, http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_white_paper0900aecd80191021.shtml

[20] M. Ashley, “Fine-tune your IDS/IPS”, 2006 http://www.comnews.com/stories/articles/0706/0706fine_tune.htm

[21] Cisco.com, “Defining Filters on a sensor”, 2004

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d974.html#754746

[22] J. Larsen, “Understanding IDS Active Response Mechanisms”, 2002

http://www.securityfocus.com/infocus/1540

[23] A. Cuff, “Intrusion Detection Terminology”, 2003

http://www.securityfocus.com/infocus/1733

[24] S. Taylor, J. Wexler, “IDS vs IPS is one strategy better”, 2003

http://www.networkworld.com/newsletters/frame/2003/1013wan2.html

[25] Cisco.com, “Risk Analysis”, 2006

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_data_sheet0900aecd801eeea5.html

[26] A. S. Tanenbaum, “Redes de computadores”, 1997

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/osi_prot.htm

http://www.comlab.hut.fi/studies/ 1130/L1_Overview/01_OSI%20model.doc

[27] H. Kenedy, “Extended Markup Language”, RFC 3252, 2002

ftp://ftp.isi.edu/in-notes/rfc3252.txt

[28] Information Science Institue, “Internet Protocol“,RFC 791, 1981

ftp://ftp.rfc-editor.org/in-notes/rfc791.txt

[29] J. Postel, “Internet Control Message Protocol”, RFC 792,1981

ftp://ftp.rfc-editor.org/in-notes/rfc792.txt

[30] Information Science Institue, “Transmission Control Protocol“, RFC 793

ftp://ftp.rfc-editor.org/in-notes/rfc793.txt

[31] J. Postel, “User Datagram Protocol”, RFC 768, 1980

ftp://ftp.rfc-editor.org/in-notes/rfc768.txt

[32] J. Case, “Simple Network Management Protocol”, RFC 1157, 1990 ftp://ftp.rfc-editor.org/in-notes/rfc1157.txt

[33] Média, http://alea-estp.ine.pt/html/nocoes/html/cap4_2_1.html

[34] Moda, http://alea-estp.ine.pt/html/nocoes/html/cap4_3_1.html

[35] Mediana, http://alea-estp.ine.pt/html/nocoes/html/cap4_4_1.html

[36] Variância, http://alea-estp.ine.pt/html/nocoes/html/cap5_2_1.html

[37] Desvio Padrão, http://alea-estp.ine.pt/html/nocoes/html/cap5_3_1.html

[38] Diagrama de Extremos, http://alea-estp.ine.pt/html/nocoes/html/cap3_2_35.html

[39] Ethereal.com, “Sniffer Ethereal”, http://www.ethereal.com/

[40] V. Jacobson, C. Leres e S. McCanne, “PCAP Library”, 2002 http://www.tcpdump.org/pcap.htm,

[41] Cisco.com, “Rate-Limiting”, 2006 http://www.cisco.com/en/US/tech/tk543/tk545/tk764/tsd_technology_support_sub-protocol_home.html

[42] Cisco.com, “Traffic Shapping”, 2006 http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_configuration_guide_chapter09186a00800bd8ef.html

Glossário

- **Antepara de Segurança (do Inglês Firewall):** nome dado ao dispositivo que tem por função regular o tráfego de rede entre redes distintas e impedir a transmissão de dados nocivos ou não autorizados de uma rede para outra. Dentro deste conceito incluem-se, geralmente, os filtros de pacotes e proxy de protocolos. É utilizado para evitar que o tráfego não autorizado possa fluir de um domínio de rede para o outro. Apesar de se tratar de um conceito geralmente relacionado com a protecção contra invasões, a antepara não possui capacidade de analisar toda a extensão do protocolo, ficando geralmente restrito ao nível 4 da camada OSI. Existe na forma de software e hardware, ou na combinação de ambos. A instalação depende do tamanho da rede, da complexidade das regras que autorizam o fluxo de entrada e saída de informações e do grau de segurança desejado.
- **Acerto de largura de banda (do Inglês Traffic Shapping):** é o condicionamento do débito de redes, com a finalidade de prioritizar o tráfego e gerir a largura de banda disponível.
- **Ataque por esgotamento de tampão (do Inglês Buffer overflow):** o esgotamento de um tampão de dados acontece quando o tamanho de uma escrita em memória ultrapassa a sua capacidade máxima de armazenamento do tampão.
- **Boot:** em computação, boot é o termo em inglês para o processo de iniciação do computador que carrega o sistema operativo quando a máquina é ligada.
- **Cavalo de Troía (do Inglês Trojan horse):** é um programa que age como a lenda do cavalo de Tróia, entrando no computador, e facilitando uma porta para um possível invasor. O conceito nasceu de simples programas que se faziam passar por esquemas de autenticação, em que o utilizador era obrigado a inserir as senhas, pensando que estas operações eram legítimas. Por exemplo, na autenticação de uma shell o trojan iria guardar a password e mascarar a conta (que seria do dono do trojan) para que parecesse legítima (a conta da vítima).
- **Comutador (do Inglês Switch):** é um dispositivo utilizado em redes de computadores para reenviar tramas entre os diversos nós. Possuem diversas portas, assim como os

concentradores, e operam na camada 2 do modelo OSI. A diferença entre o comutador e o concentrador é que o comutador segmenta a rede internamente, sendo que a cada porta corresponde um segmento diferente, o que significa que não haverá colisões entre pacotes de segmentos diferentes — ao contrário dos concentradores cujas portas partilham o mesmo domínio de colisão.

- **Concentrador (do Inglês Hub):** é um aparelho que interliga diversas máquinas (computadores) em LANs. O concentrador é indicado para situações com poucos terminais de rede, pois o mesmo não comporta um grande volume de tráfego passando por ele ao mesmo tempo. Esta limitação prende-se com o facto de funcionar internamente por difusão enviando a mesma informação de uma rede para todas as máquinas interligadas.
- **DDoS (Distributed Denial of Service):** correspondem a ataques distribuídos de negação de serviços. O DDoS é um ataque *DoS* ampliado, ou seja, usa a instalação de vários agentes maliciosos remotos em muitos computadores localizados em várias partes da Internet. O invasor consegue coordenar esses agentes *em massa* para amplificar o volume do ataque, podendo utilizar até milhares de computadores para atacar uma determinada máquina ou rede.
- **DMZ (do Inglês DeMilitarized Zone):** também conhecida como rede de perímetro, a DMZ é uma pequena rede situada entre uma rede confiável e uma não confiável, geralmente entre a rede local e a Internet. A função de uma DMZ é manter todos os serviços que possuem acesso externo (HTTP, FTP, etc) separados da rede local, limitando o dano em caso de comprometimento de algum serviço nela presente por algum invasor. Para atingir este objectivo os computadores presentes numa DMZ não devem conter nenhuma rota de acesso à rede local.
- **DNS (Domain Name Service):** é um sistema de gestão de nomes hierárquico e distribuído. O servidor DNS traduz nomes para os endereços IP e endereços IP para nomes respectivos, permitindo a localização de máquinas num determinado domínio.
- **Encaminhador (do Inglês Router):** é um equipamento usado para fazer a comunicação entre diferentes redes de computadores. Este equipamento possibilita a comunicação entre computadores distantes entre si e até mesmo com protocolos de comunicação diferentes. São dispositivos que operam na camada 3 do modelo OSI. A principal função destes

equipamentos é seleccionar a porta mais apropriada para comutar os pacotes recebidos. Ou seja, encaminhar os pacotes para o melhor caminho disponível para um determinado destino.

- **Estampilha temporal (do Inglês Timestamp):** tempo obtido associado a uma acção ou transacção.
- **Explorar vulnerabilidade (do Inglês Exploit):** é um programa de computador que permite tirar partido de vulnerabilidades de outros programas - como o próprio sistema operativo ou serviços de interacção de protocolos (ex: servidores Web). Geralmente elaborados por piratas informáticos como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por agentes maliciosos a fim de ganhar acesso não autorizado a sistemas.
- **Extranet:** a extranet de uma empresa é a porção de sua rede de computadores que faz uso da Internet para partilhar com segurança parte do seu sistema de informação. Tomado o termo em seu sentido mais amplo, o conceito confunde-se com Intranet. Uma Extranet também pode ser vista como uma parte da empresa que é estendida a utilizadores externos ("rede extra-empresa"), tais como representantes e clientes. Outro uso comum do termo Extranet corresponde a parte privada de um site, onde somente utilizadores registados e autenticados podem navegar.
- **Falso positivo:** utilizado para designar uma situação em que um dispositivo detectou uma actividade como sendo um ataque ou intrusão, quando na verdade essa actividade não era maliciosa.
- **Falso negativo:** ocorre quando uma intrusão real acontece, mas o dispositivo de detecção considerou-a uma acção legítima.
- **Flags TCP:** o campo de controlo do pacote TCP é constituído por 6 flags (SYN, ACK, RST, PSH, FIN) que permitem controlar as diferentes fases da comunicação.
- **FTP (File Transfer Protocol):** é um protocolo que define uma forma bastante rápida e versátil de transferir arquivos (também conhecidos como ficheiros), sendo um dos mais usados na internet.

- **HIDS (Host Intrusion Detection System):** sistema de detecção de intrusões ao nível de uma máquina.
- **HTTP (HyperText Transfer Protocol):** é um protocolo da camada de Aplicação do modelo OSI, utilizado para transferência de dados na World Wide Web.
- **ICMP (Internet Control Message Protocol):** protocolo integrante do Protocolo IP, definido pelo RFC 792, e utilizado para fornecer relatórios de erros à fonte original.
- **IDS (Intrusion Detection System):** permite detectar intrusões, ou tentativas de ataque, a redes ou sistemas através da análise de tráfego ou da análise do perfil de um utilizador. Todos os alertas gerados por um IDS são guardados num registo de ocorrências, que posteriormente pode ser utilizado para identificar os atacantes.
- **Internet:** é um conglomerado de redes em escala mundial que interliga milhões de computadores, e que permite o acesso a informações e todo tipo de transferência de dados.
- **Intranet:** é uma rede de computadores privada que utiliza as mesmas tecnologias que são utilizadas na Internet. O protocolo de transmissão de dados de uma intranet é o TCP/IP e sobre ele podemos encontrar vários tipos de serviços de rede comuns na Internet, como por exemplo o e-mail, chat, grupo de notícias, HTTP, FTP entre outros.
- **IPS (Intrusion Protection System):** denominados de sistemas de protecção ou prevenção contra de intrusões, que para além de detectarem intrusões em tempo real também têm a capacidade de actuarem sobre as actividades suspeitas.
- **Logs:** o log de dados é o termo utilizado para descrever o processo de registo de eventos relevantes num sistema computacional. Esse registo pode ser utilizado para restabelecer o estado original de um sistema ou para que um administrador conheça o seu comportamento no passado. Um arquivo de log pode ser utilizado para auditoria e diagnóstico de problemas em sistemas computacionais. Muitos sistemas operativos e uma infinidade de programas de computador incluem alguma forma de log de dados. Alguns sistemas operacionais disponibilizam um serviço de log de dados chamado Syslog (descrito na RFC 3164), que filtra e registra as mensagens destinada ao log, livrando as aplicações do ônus de manter o seu sistema de log próprio sem interligação.

- **MAC (Media Access Control):** é o endereço físico da estação, ou melhor, da interface de rede. É um endereço de 48 bits, representado em hexadecimal. O protocolo é responsável pelo controle de acesso de cada estação à rede Ethernet. Este endereço é o utilizado na camada 2 do Modelo OSI.

  Exemplo: 00:00:5E:00:01:03

  Os três primeiros octetos são destinados à identificação do fabricante, os 3 posteriores são fornecidos pelo fabricante. É um endereço universal, não existem, em todo o mundo, duas placas com o mesmo endereço.

- **Modelo OSI (Open Systems Interconnection):** é um conjunto de padrões ISO relativo à comunicação de dados. Um sistema aberto é um sistema que não depende de uma arquitectura específica. Este modelo é dividido em camadas hierárquicas, ou seja, cada camada usa as funções da própria camada ou da camada anterior, para esconder a complexidade.

- **Network IDS:** ver IDS ou IPS.

- **RFC (Request for Comments):** é um acrónimo para o documento que descreve um protocolo da Internet previamente antes de ser considerado um standard.

- **SNMP (Simple Network Management Protocol):** é um protocolo de gestão de rede da camada de aplicação que facilita o intercâmbio de informação entre os dispositivos de rede. O SNMP possibilita aos administradores de rede gerir o desempenho da rede, encontrar e resolver problemas, e planear o crescimento desta.

- **TCP (Transmission Control Protocol):** é um dos protocolos sob os quais assenta o núcleo da Internet nos dias de hoje. A versatilidade e robustez deste protocolo tornou-o adequado para redes globais, já que este verifica se os dados são enviados de forma correcta, na sequência apropriada e sem erros, pela rede.

- **UDP (User Datagram Protocolo):** dá às aplicações acesso directo ao serviço de entrega de datagramas, como o serviço de entrega que é dado pelo IP. O UDP não garante a fiabilidade de entrega, sendo um protocolo não orientado para a conexão.

- **URL (Universal Resource Locator):** é o endereço de um recurso (um ficheiro, uma impressora etc.) disponível numa rede; seja a Internet, ou uma rede empresarial Um URL tem a seguinte estrutura: `protocolo://máquina:porto/caminho/recurso`
- **Verme:** é um programa auto-replicante, semelhante a um vírus. O vírus infecta um programa e necessita deste programa hospedeiro para se propagar. O verme é um programa completo e não precisa de outro programa para se propagar. Além da replicação, um verme pode ser projectado para fazer outras coisas, como danificar arquivos num sistema ou enviar documentos por email. O verme pode trazer embutido programas que geram algum tipo de problema ou que tornam o computador infectado vulnerável a outros ataques. Um verme pode provocar danos apenas com o tráfego de rede gerado pela sua reprodução.
- **Vírus:** é um programa malicioso desenvolvido por programadores que, como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores utilizando diversos meios. A maioria das contaminações ocorre pela execução de um ficheiro em anexo de um e-mail. A segunda causa de contaminação é pela a utilização de um sistema operativo desactualizado, sem a aplicação de correcções que bloqueiam chamadas maliciosas aos recursos disponíveis.
- **VLAN:** uma rede local virtual, normalmente denominada de **VLAN**, é uma rede logicamente independente. Várias VLANs podem coexistir num mesmo comutador.
- **XML (Extended Markup Language):** é uma recomendação da W3C para gerar linguagens de marcação para necessidades especiais. XML é um subtipo de SGML (Standard Generalized Markup Language) capaz de descrever diversos tipos de dados, com o propósito principal a facilidade de partilha de informações através da Internet.