Fundação Educacional do Município de Assis
Instituto Municípal de Ensino Superior de Assis - IMESA

RAÍSSA HELENA BEGOSSO

# COMPUTAÇÃO FORENSE

ASSIS
2010

RAÍSSA HELENA BEGOSSO

# COMPUTAÇÃO FORENSE

Projeto de pesquisa apresentado ao Curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.
**Orientanda:** Raíssa Helena Begosso
**Orientador:** Luiz Carlos Begosso

Assis
2010

FICHA CATALOGRÁFICA

BEGOSSO, Raíssa Helena

Computação Forense / Raíssa Helena Begosso. Fundação Educacional do Município de Assis – FEMA – Assis, 2010.

42p.

Orientador (a): Luiz Carlos Begosso.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Computação Forense. 2. Segurança.

CDD: 001.6
Biblioteca da FEMA

# COMPUTAÇÃO FORENSE

**RAÍSSA HELENA BEGOSSO**

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Bacharelado em Ciência da Computação, analisado pela seguinte comissão examinadora:

Orientador: _____

Analisador: _____

Assis
2010

# DEDICATÓRIA

Dedico este trabalho aos meus pais Luiz Ricardo e Denise Begosso, que me deram a oportunidade mais preciosa: a de obter conhecimento através dos estudos. Amo vocês!

# AGRADECIMENTOS

Primeiramente, agradeço a Deus, por me guiar e iluminar minha jornada diariamente.

À minha família, pelo apoio constante e por não me permitirem desistir nos momentos difíceis.

Ao meu querido orientador, Luiz Carlos Begosso, pela paciência e seus ensinamentos valiosíssimos.

Aos meus colegas e amigos, pelo companheirismo e constantes motivações.

A todas as pessoas que, direta ou indiretamente, contribuíram para a realização deste trabalho.

# RESUMO

O desenvolvimento tecnológico proporciona à sociedade mundial cada vez mais comodidades e vantagens em todos os aspectos da vida moderna. Os acessos à Internet aumentam a cada dia, provenientes de organizações, governamentais ou não, ou simplesmente de usuários comuns, tendo em vista o nível cada vez maior de usabilidade de recursos computacionais.

Entretanto, conforme cresce a facilidade de uso de tais recursos, também aumentam os números de incidentes de quebras de segurança de redes e sistemas. É com o objetivo de prevenir e solucionar tais eventos, que surge a computação forense.

**Palavras - chave**: computação forense; segurança.

# ABSTRACT

The technological development provides the world society with comfort and advantages in every aspect of modern life. Each day, more and more organizations and common users access the Internet, considering the ever increasing level of usability of computer resources.

However, as the simplicity in using such resources increases, so do the numbers of incidents of security breaches of networks and systems. Computer forensics comes to avoid and solve such problems.



**Keywords**: computer forensics; security.

# LISTA DE ILUSTRAÇÕES

Figura 1 – Relação Ciência da Computação, Criminalística e Computação Forense.....14

Figura 2 – *Modus operandi* de um invasor.....21

Figura 3 – Ações após a intrusão do sistema.....22

Figura 4 – Cenário ideal de segurança de redes.....34

**SUMÁRIO**


| | |
|---|---|
| **1 – Introdução** …….. | 11 |
| 1.1 – Motivação ……. | 11 |
| 1.2 – Perspectiva de contribuição ……. | 12 |
| 1.3 – Metodologia de trabalho ……. | 12 |
| 1.4 – Estrutura do trabalho ……. | 13 |
| **2 – Sobre a computação forense** ……. | 14 |
| **3 – Perícia de crimes eletrônicos** ……. | 20 |
| 3.1 – Considerações iniciais sobre a perícia de crimes eletrônicos …….. | 20 |
| 3.2 – Atuação dos invasores ……. | 20 |
| 3.3 – Metodologias de resposta a incidentes de segurança …… | 24 |
| 3.4 – Coleta de evidências ……. | 25 |
| 3.4.1 – *Live Analysis* ……. | 26 |
| 3.4.2 – *Network Analysis* ……. | 29 |
| 3.4.3 – *Post Mortem Analysis* ……. | 30 |
| **4 – Cenário Ideal** ……. | 34 |
| **5 – Conclusão** ……. | 39 |
| **Bibliografia** ……. | 41 |

# 1 - Introdução

Os meios eletrônicos, tais como computadores e celulares, conectados ou não à rede mundial de computadores, vêm nos proporcionando cada vez mais informações e soluções.

Através da tecnologia computacional, em constante aperfeiçoamento, pessoas do mundo todo podem se comunicar e interagir, com finalidades sociais, comerciais ou educacionais.

Todavia, na medida em que a tecnologia se desenvolve, os casos de crimes digitais também crescem continuamente, muitas vezes causando problemas graves, com difíceis soluções.

A computação forense, disciplina cada vez mais estudada pelos profissionais de informática, bem como da esfera jurídica, tem a finalidade de auxiliar na resolução de tais problemas.

O presente trabalho tem por objeto uma breve apresentação de conceitos e aspectos gerais da computação forense e a discussão de técnicas utilizadas na perícia de crimes eletrônicos.

Para ilustrar tal questão, esta pesquisa apresenta também um estudo de caso, sobre uma ferramenta inteligente de investigação de delitos digitais.

## 1.1. Motivação

A constante presença do Direito e da Informática na vida moderna demanda estudos e normatizações. Sabe-se que o ordenamento jurídico brasileiro ainda carece de regulamentação específica sobre a Informática, principalmente sobre a computação forense.

Existe, consequentemente, a necessidade de se estabelecer diretrizes, a fim de se produzir reflexões que possam esclarecer a prática da computação forense, para que seja possível legitimá-la.[1]

Importante notar também que, durante o levantamento bibliográfico para a elaboração deste trabalho, foi possível observar a carência de literatura abrangendo os dois assuntos. A maioria das informações existentes se encontra registrada em língua inglesa, restando necessário disponibilizar algum material em língua portuguesa.

### 1.2. Perspectiva de contribuição

Com a elaboração deste trabalho, pretende-se produzir uma reflexão sobre o assunto ao leitor, porém, sem esgotá-lo. A pesquisa realizada deve contribuir para o aprimoramento e informação de outros pesquisadores.

Por conter traduções em português de alguns textos técnicos em inglês, também pretende promover uma melhor compreensão por leitores interessados no tema.

Após da conclusão deste trabalho, planeja-se divulgar o tema por meio de artigos, participações em congressos e envolvimento em outros projetos de pesquisa.

### 1.3. Metodologia de trabalho

Para a realização deste trabalho, foi utilizada principalmente pesquisa bibliográfica em fontes diversas, como por exemplo, artigos, teses, livros e outras informações retiradas da internet de sites de órgãos idôneos.

---

[1] PINTO, Marcio Morena. O Direito da internet: o nascimento de um novo ramo jurídico . **Jus Navigandi**. Disponível em: <http://jus2.uol.com.br/doutrina/texto.asp?id=2245>. Acesso em: 21 abr. 2010

Além disso, será apresentado, ao final, um estudo de caso, em que se apresenta um cenário ideal de segurança de redes. A partir de tais fontes, foi possível obter as informações necessárias para o desenvolvimento do presente trabalho.

## 1.4. Estrutura do trabalho

O presente trabalho é dividido em 5 capítulos, da forma como segue:

Capítulo 1: Introdução

Na introdução é feita uma breve descrição das questões que se pretende abordar e discutir ao longo do trabalho.

Capítulo 2: Sobre a Computação Forense

Este capítulo traz uma investigação aprofundada dos conceitos e definições sobre computação forense. Além disso, também discute algumas das mais comuns ameaças digitais e seus impactos.

Capítulo 3: Perícia de Crimes Eletrônicos

Sendo o capítulo mais extenso do trabalho, aqui se discute sobre técnicas de perícia digital, atuação e perfil dos invasores, geração de evidências, além dos tipos de análises *Live*, *Network* e *Post Mortem*.

Capítulo 4: Cenário Ideal

Neste capítulo será discutido um cenário que utiliza ferramentas de segurança em diferentes camadas da rede.

Capítulo 5: Conclusão

Aqui são apresentadas as conclusões do trabalho, na forma de elucidar as questões levantadas.

## 2 – Sobre a Computação Forense

A cada dia, pesquisadores dos diversos ramos da ciência apresentam ao mundo novas tecnologias, cujo intuito é auxiliar-nos na busca pelas soluções para vários de nossos problemas.

O advento da internet foi um dos avanços que mais nos beneficiou, e isso ainda vem ocorrendo, devido às suas constantes evoluções, pois, irrefutavelmente, o acesso à informação é o primeiro passo para encontrarmos a solução procurada.

Atualmente, através de meios eletrônicos, é possível disponibilizar e consultar todo tipo de informação sempre que desejarmos e em qualquer lugar, pois dispomos de meios velozes e de fácil uso e acesso.

Contamos também com o crescimento constantes dos serviços disponíveis pela internet, além da ampliação e otimização de sua infra-estrutura. No entanto, com isso temos cada vez mais softwares com finalidades ilícitas, que podem ser utilizados e acessados facilmente, trazendo o significativo crescimento de invasões de computadores. (MELO, 2009, p. 2)

E é exatamente por este motivo, que a internet pode ser utilizada universalmente, por pessoas com objetivos variados, do aprendizado ao entretenimento, inclusive para a prática de crimes.

Não podemos negar que o uso de meios eletrônicos para o cometimento de crimes e consequente obtenção de provas dos mesmos, são fatores muito recentes, que ainda carecem de estudo, técnicas aperfeiçoadas e regulamentação legal. Com o objetivo de auxiliar e esclarecer tais investigações, é que surgiu a disciplina da computação forense.

Para melhor elucidar o tema, vejamos a seguir algumas definições feitas por profissionais da área tecnológica e jurídica.

O professor Sandro Melo (2009, p. 13) faz uma definição ramificada de computação forense, conforme segue:

> A Computação Forense pode ser definida como uma área da Ciência da Computação que se desenvolve gradualmente para atender à demanda oriunda da Criminalística, e também como uma parte da Criminalística que se apropria de fundamentos da Ciência da Computação.

Para ilustrar esta definição, a Figura 1 nos mostra a relação entre Ciência da Computação, Criminalística e a área de conhecimento comum entre elas, denominada Computação Forense.

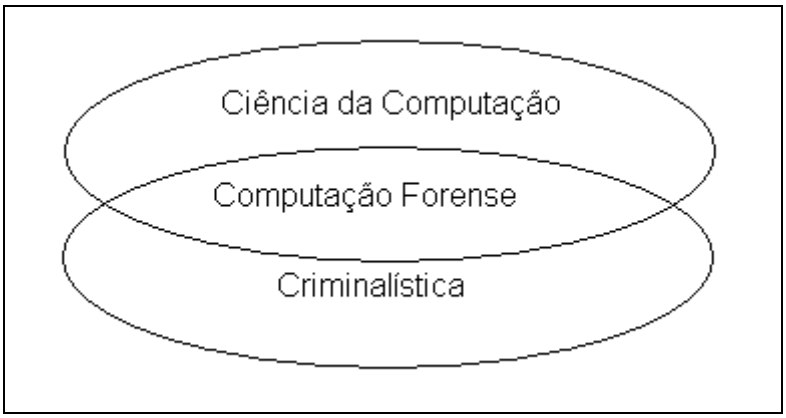


Figura 1: Relação Ciência da Computação, Criminalística e Computação Forense (In: MELO, 2009, p. 2)

Apesar de não reconhecer a computação forense como uma disciplina científica formal, a organização governamental norte americana US-CERT a define, de um ponto de vista técnico, como:

> A disciplina que combina elementos de direito e ciência da computação para coletar e analisar dados de sistemas computacionais, redes, comunicações sem fio e dispositivos de armazenamento, de forma se preserve a integridade da evidência coletada, para que esta possa ser utilizada efetivamente em juízo.

Já a analista forense, Erin Kenneally, na publicação *;login:*, explica que o termo se refere às "ferramentas e técnicas para recuperar, preservar e examinar dados armazenados ou transmitidos em forma binária".

O delegado de polícia, José Mariano de Araujo, através seu site[2], define computação forense como a área que estuda a extração ou supressa de arquivos e informações a partir dos discos rígidos de um computador.

Basicamente, esta nova disciplina consiste em investigar e reconstituir fatos ilícitos através da identificação, coleta e análise de evidências ou informações magneticamente armazenadas ou codificadas. (MERCURI, 2005)

Para a US-CERT, a prática da computação forense auxilia na garantia da integridade e sobrevivência de uma infraestrutura de rede. Entender aspectos legais e técnicos dessa área é fundamental para que informações vitais sejam obtidas, caso uma rede seja comprometida.

A computação forense tem como objeto os crimes eletrônicos. Em uma definição ampla, crimes eletrônicos são aqueles que envolvem quebra de segurança digital, uso de computadores no cometimento de atos ilícitos, prática de atividades ilícitas cujo alvo é um computador, ou coleta e armazenamento de informações referentes a outro crime. (MERCURI, 2005)

É importante lembrar que grande parte dos negócios tem conquistado espaço na Internet, ambiente no qual o dinheiro também é digital. Isso constitui um grande atrativo para que criminosos passem a atuar em tal esfera.

Podemos encontrar, por exemplo, entre outros tipos de agentes criminosos, indivíduos, ou até mesmo quadrilhas organizadas, que fazem uso de falsificação de web sites de bancos, com o intuito de obter credenciais e

---

[2] http://mariano.delegadodepolicia.com/tecnicas-de-investigacao-de-cibercrimes-–-parte-23/

manipular contas correntes de clientes da instituição financeira. (MELO, 2009, p. 2)

Mas à computação forense também competem, por exemplo, casos de validação de provas em ações trabalhistas ou cíveis ou em crimes de calúnia, injúria, difamação e pedofilia.

De acordo com Araujo (2010), elementos obtidos por profissionais da área de computação forense podem ser usados em várias circunstâncias diferentes. Além de evidências criminais, alguns exemplos são a comprovação de fraude, casos de assédio e discriminação no trabalho, e até mesmo a prova de adultério para fins de divórcio.

Tais delitos, quando praticados, deixam pistas, que devem ser investigadas pela autoridade policial competente. Entretanto, um investigador não é capaz de analisar cada informação contida em um computador para identificar quais são relevantes para a elucidação do fato e quais devem ser ignoradas.

Cabe mencionar também quais os tipos mais usuais de ameaças digitais e explicar sobre seus impactos nas redes de computadores. De acordo com Sandro Melo (2009, p. 10):

> *Malware* pode ser definido como *Malicious Software*, ou software malicioso, ou seja é um termo genérico que engloba todos os tipos de programas especificamente desenvolvidos para executar ações maliciosas em um computador. O *malware* contém ameaças reais de vários tipos e propósitos.

Dessa forma, o autor cita e explica alguns exemplos de malware, como: vírus, *worm*, *bots* e *botnet*, *backdoors*, *trojan*, *keyloggers* e outros programas *spyware*, e *rootkits*.

Os vírus podem alocar-se em programas executáveis, infectando-os, mas dependem da execução dos hospedeiros para sua propagação. Neste sentido, o sistema operacional Linux apresenta a vantagem de impedir que um binário

possa ser executado automaticamente, contexto esse que dificulta a ação e a propagação dos vírus.

*Worms* são softwares com capacidade de auto propagação, enviando cópias de si mesmos para computadores com qualquer tipo de sistema operacional. Os *bots* são semelhantes aos *worms*, mas possuem capacidade de comunicação com o invasor, o que possibilita que seja controlado remotamente. Por conta de tal fato, *crackers* conseguem infectar inúmeros computadores, criando as chamadas *botnets*.

Comumente, as *backdoors* são utilizadas por invasores para assegurar o seu retorno ao sistema comprometido. São mecanismos utilizados de forma furtiva, alterando recursos do sistema para impedir sua identificação.

Para o roubo de informações, os invasores se utilizam de *trojans* e *keyloggers*. Dentre estes, o primeiro possibilita até mesmo o controle da máquina infectada. Já o segundo, possui o objetivo de capturar para o invasor tudo o que é digitado naquela máquina.

Por fim, os *rootkits*, após sua instalação automática, utilizam técnicas para esconder processos e dados inerentes ao mecanismo, dificultando sua identificação. Eles instalam binários, módulos e bibliotecas que possuem recursos de backdoors, keyloggers, entre outros.

Considerando a quantidade de dados que uma máquina moderna é capaz de armazenar, uma pessoa não conseguiria realizar essa análise dentro de um período conveniente.

É fato notório que faltam profissionais capacitados para atuar nesta área, bem como falta literatura sobre o assunto, não apenas em língua portuguesa, como nas demais. No Brasil, a competência para investigação de crimes digitais é da Polícia Federal. Porém, sabemos que os fatos ilícitos ocorridos especificamente dentro da competência territorial do Estado de São Paulo, são investigados pela Polícia Civil.

Também é evidente a ausência de legislação específica sobre crimes eletrônicos, sua investigação e consequente apuração e levantamento de provas relevantes. Existem hoje apenas projetos de lei, mas tais projetos são insuficientes para a regulamentação desta situação.

Ao mesmo tempo em que a tecnologia computacional evolui e cada vez mais computadores se conectam, os crimes eletrônicos também se tornam mais sofisticados e coordenados.[3] Assim, é possível que vários terminais sejam utilizados na execução de um ilícito, fazendo com que seja ainda mais difícil que um examinador humano consiga concluir a investigação de forma eficiente dentro do prazo legal.

Portanto, além das técnicas de investigação digital, precisa-se do amparo de ferramentas inteligentes, que possam realizar o trabalho de investigação de maneira ágil e precisa.

Esclarecida essa importância, estudaremos a seguir algumas técnicas de investigação digital.

[3] http://www.forensics.nl/

# 3 – Perícia de Crimes Eletrônicos

## 3.1. Considerações iniciais sobre a investigação forense computacional

Antes de iniciarmos o estudo sobre perícias digitais propriamente ditas, é relevante fazer algumas observações sobre o tema da investigação forense computacional, do ponto de vista jurídico.

Araujo (2010), esclarece que as provas colhidas durante um inquérito devem ser preservadas, visando o seu aproveitamento no processo judicial. Isso significa que, durante uma investigação forense computacional, algumas regras devem ser observadas.

Primeiramente, o sistema investigado deve ser protegido de qualquer tipo de manipulação durante a operação. Se possível, recomenda-se possuir uma cópia do disco rígido, bem como realizar a identificação e recuperação de todos os arquivos e aplicativos instalados, inclusive aqueles que haviam sido excluídos.

É necessário que se faça uma avaliação do sistema como um todo, incluindo sua estrutura. Deve-se identificar os acessos ou cópias ocultas ou protegidas, e arquivos temporários. O monitoramento de fatores gerais relativos à atividade dos usuários também é importante.

Por fim, recomenda-se que seja feito um relatório detalhado, além de se manter um registro completo de todas as atividades realizadas no decurso do inquérito policial.

## 3.2. Atuação dos invasores

Quando se conhece as técnicas e ferramentas utilizadas por um invasor, é mais simples desenvolver formas para reagir aos ataques de forma efetiva.

Portanto, para que o tema das perícias digitais seja melhor compreendido, é importante introduzi-lo com um breve estudo sobre a atuação e perfil dos invasores.

Uma vez conhecidas as técnicas utilizadas por esses agentes, é possível obtermos uma visão dos principais pontos do processo de invasão a um sistema e, dessa forma, antecipar onde, potencialmente, serão gerados dados para uma perícia forense computacional.

O delegado de polícia José Mariano de Araujo, em seu site, explica que os casos mais comuns de crimes digitais são a divulgação não autorizada de informações corporativas, furto de dados de clientes, espionagem industrial, danos maliciosos, além de crimes contra a honra e ameaças.

Sendo o objetivo da perícia forense computacional reconstruir os passos dos invasores, é importante obter informações dos ativos de rede, como, por exemplo, IDS[4], firewalls e servidores de registro.

Em regra, uma invasão ocorre conforme ilustra a Figura 2. Primeiramente, de acordo com Sandro Melo (2009, p. 22), é necessário que o invasor possa identificar, pelo menos, uma vulnerabilidade, para conseguir ter acesso ao sistema que pretende invadir. Esta vulnerabilidade pode ser uma falha em uma aplicação, ou na configuração de um ativo de rede.

[4] Em inglês, Intrusion Detection System, que se traduz como Sistema de Detecção de Intrusos.

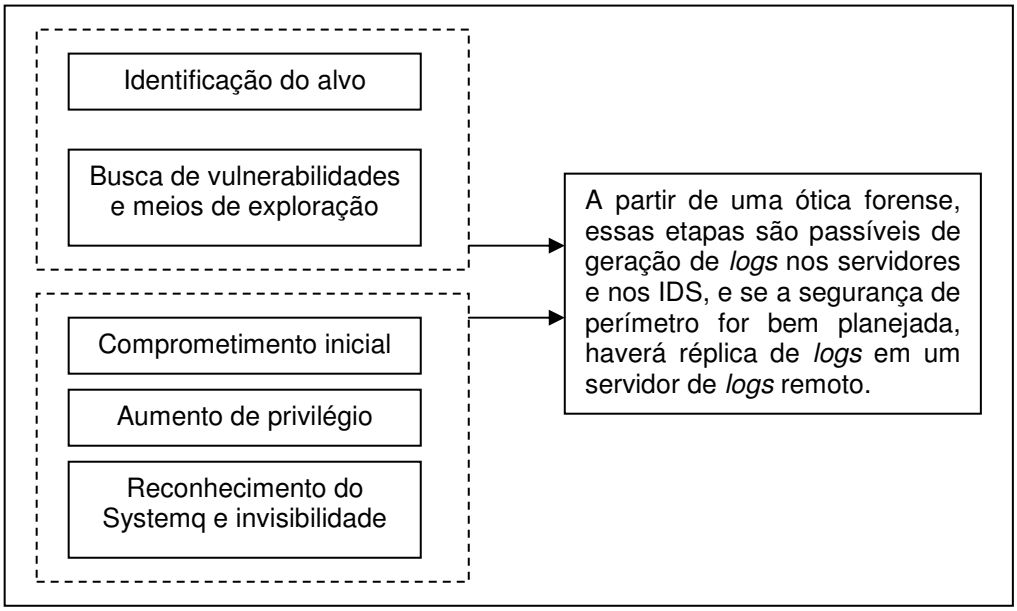


Figura 2: *Modus operandi* de um invasor. (In: MELO, 2009, p. 21)

Uma invasão pode ocorrer de forma clássica, começando por um levantamento de informações básicas, técnica denominada *footprinting*. Através dessa técnica, o invasor busca informações de contato e DNS disponíveis em registros do protocolo WHOIS, capturando pacotes montados pela pilha TCP/IP e analisando-os, por meio de *scanners* de *fingerprint*.

Em seguida, o invasor utiliza *port scanners* para testar portas lógicas e identificar as que estão abertas. Caso existam meios de detecção de varreduras, isso pode disparar alertas em IDS ou no servidor alvo.

Entretanto, ainda de acordo com Sandro Melo, pode ser quase impossível realizar tal detecção, se o invasor, em cada ação, evitar as técnicas de varredura que possam chamar atenção.

Se, por exemplo, a invasão ocorrer somente na porta 80 de um servidor, uma única vez, torna-se improvável identificá-la, caso a comunicação seja cancelada; salvo se a porta não estiver ativa no servidor e exista um sistema de detecção de intrusos que registre a solicitação da conexão indevida.

O autor Sandro Melo explica que, após a invasão do sistema, alguns infratores instalam na máquina alvo ferramentas que auxiliam no controle do sistema, ocultam as atividades ilícitas e ainda apagam seus rastros (e.g. registros de *logs*). Este fenômeno pode ser melhor observado na Figura 3.

Apesar do uso de tais técnicas, ainda é possível identificar uma invasão, tendo em vista que o próprio ato de manipular arquivos de um sistema já caracteriza a sua ocorrência.

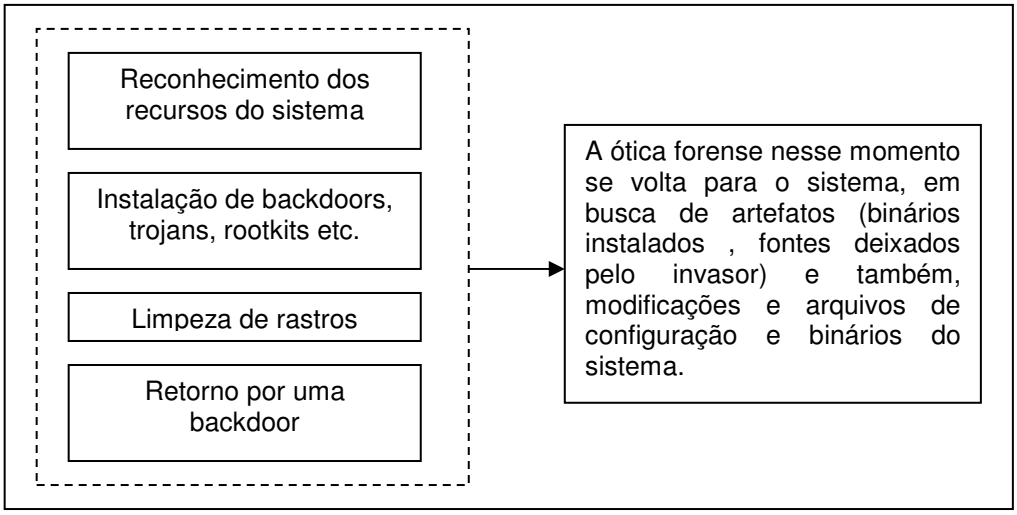


Figura 3: Ações após a intrusão do sistema. (In: MELO, 2009, p. 24)

Logo, é importante que o alvo da invasão não possibilite o levantamento de mais informações, tendo em vista que o invasor pode aproveitar tais aberturas e vulnerabilidades para causar danos.

Também vale mencionar que a evolução tecnológica proporciona ferramentas cada vez mais acessíveis, e não apenas financeiramente. Qualquer usuário mal intencionado e com conhecimentos básicos de computação pode causar um incidente de segurança, devido à crescente usabilidade de ferramentas com finalidades ilícitas, disponíveis na própria internet.

Percebe-se que o nível de conhecimento que uma pessoa deve ter para realizar uma invasão tem caído constantemente, enquanto a sofisticação dos seus ataques vem aumentando.

Dessa forma, podemos concluir que, mesmo tomando todas as precauções necessárias, o risco ainda existe. Por isso, as organizações que possuem servidores conectados à Internet, devem adotar políticas de gestão de segurança, para que as reações aos ataques sejam efetivadas de forma ágil.

### 3.3. Metodologias de resposta a incidentes de segurança

Para que uma rede consiga reagir a incidentes de segurança, deve ser capaz de obter informações sobre potenciais eventos, que possam gerar evidências importantes para a Perícia Forense Computacional.

De acordo com Sandro Melo (2009, p. 30), um profissional de segurança deve ser capaz de identificar alguns elementos, para que consiga reagir de forma eficiente a um ataque.

Dentre esses fatores, podemos citar como exemplos:

a) a origem do incidente: se foi interna ou externa à rede;
b) a motivação e o objetivo do atacante: por exemplo, se o ataque visa violar a integridade de certas informações, e se provoca danos a hardware ou software;
c) a tecnologia utilizada: como vimos anteriormente, que tipo de malware foi executado no sistema invadido;
d) os danos causados e sua extensão: serviços que ficaram temporariamente inativos.

Melo (2009) também explica que, para impedir a paralisação de algum ativo de rede importante para a organização vítima do ataque, é necessário que a equipe de segurança efetive sua reação com agilidade.

Em outras palavras, o profissional de segurança deve ser bem qualificado e estar apto a dedicar-se à qualidade, de forma que deve dominar, em todos os casos, a tecnologia adotada pela empresa.

Além disso, a norma NBR ISSO/IEC 17799:2005 estabelece que deve haver na instituição uma política de segurança, contendo um plano de ação estruturado, em que a equipe consiga reportar e documentar os fatos, para o caso de ataques digitais.

Segundo as recomendações da referida norma, é muito importante que a equipe de segurança também seja capaz de trocar informações por meio de canais seguros, tanto interna, quanto externamente, a fim de evitar incidentes recorrentes.

Finalmente, vale ressaltar também que todas as ações tomadas pelos profissionais da segurança, ainda que não sejam relacionadas a um incidente, devem ser devidamente documentadas, para referência futura.

### 3.4. Coleta de evidências

No início de uma perícia em um sistema violado, o profissional de segurança procura identificar como ocorreu e qual a extensão do prejuízo causado, ou seja, quais informações e aspectos do sistema operacional foram afetados.

Após essa fase de reconhecimento inicial, o perito deve proceder à coleta e análise de evidências, visando obter o máximo possível de dados periciais digitais. As informações são obtidas nas áreas de atuação dos usuários e também no kernel do sistema operacional, e deve-se fazer uma busca detalhada nos dados do sistema.

Consoante Sandro Melo (2009), evidências digitais possuem determinadas características específicas, como, por exemplo: podem ser duplicadas com precisão, preservando-se o original durante a perícia; é possível verificar caso tenham sido alteradas; são passíveis de modificação durante a análise, devido à sua volatilidade.

Esta fase de busca de evidências pode ser dividida em três etapas: as análises *Live*, *Network* e *Post Mortem*. A seguir, discutiremos brevemente sobre cada uma delas.

### 3.4.1. *Live Analysis*

Antes de iniciarmos o estudo da *Live Analysis* propriamente dita, é relevante uma discussão sobre a volatilidade e o tempo de vida de um dado pericial digital. Segundo Melo (2009, p. 34), “o tempo de vida de uma evidência digital pode variar de acordo com o local em que ela está armazenada.”

Isso significa que quanto mais volátil for um dado, mais difícil é a sua extração e menos tempo há para obtê-lo. No entanto, algumas informações acabam sendo consideradas irrelevantes para a perícia, tamanha a sua volatilidade. É o caso dos dispositivos de armazenagem na CPU, como *caches* e registradores, tendo em vista que seu estado é alterado no momento da captura.

Apesar do alto nível de volatilidade de determinadas informações, como o estado do sistema operacional e o conteúdo da memória principal, elas podem ser importantes na identificação de ataques em curso.

Melo (2009) enumera algumas informações que podem ser obtidas durante a *Live Analysis*, como, por exemplo: dispositivos de armazenagem da CPU; memória de periféricos; memória principal do sistema; tráfego de rede; estado do sistema operacional; dispositivos de armazenagem secundária; arquivos de registros; análises de *malwares* identificados.

De acordo com ele, esses dados serão posteriormente utilizados, durante a fase de *Post Mortem Analysis*. A primeira etapa, *Live Analysis*, termina no momento em que o sistema é desligado, após todas as informações serem coletadas do disco rígido. É, então, realizada uma cópia bit a bit do mesmo, a qual será utilizada na procura de possíveis evidências para a perícia forense.

O autor ainda aponta que pode haver dificuldades na geração da imagem do disco rígido, como nos casos em que o desligamento da máquina influencia o funcionamento da organização, ou quando o disco possui volume muito grande de dados. Embora existam riscos, a tomada dessas medidas é necessária.

Vale lembrar também que, quando se trata de dispositivos periféricos, é importante que a coleta de evidências seja feita durante a *Live Analysis*, tendo em vista que, após o desligamento do sistema, certas informações podem não ser mais encontradas.

Para a busca de dados periciais na memória principal do sistema, investigadores comumente utilizam *dumps* de memória através da geração de *core files* ou *crash dumps*, pois nela se encontram informações voláteis, como processos em execução, dados manipulados, entre outras informações ainda não salvas em disco.

Ao ser executado, o processo do *dump* é alocado na memória, alterando parte das informações obtidas. Mas isso não impede a verificação dos processos que se encontravam ativos na memória no momento da coleta.

Os *crash dumps* são fontes úteis de dados, pois possuem “uma imagem da memória do sistema no momento em que uma falha inesperada acontece, funcionando como uma espécie de caixa preta do sistema” (MELO, 2009, p. 39). Isso significa que, no momento da falha, os *crash dumps* realizam a gravação de todas as informações que se encontravam na memória, permitindo sua análise posterior.

Sandro Melo (2009) expõe a importância da análise do tráfego de rede. Esta atividade pode ser realizada através de *sniffers*, programas que capturam datagramas na rede e fazem sua decodificação. Através dessa atividade são obtidos vários tipos de informação, como, por exemplo: portas e endereços IP duvidosos; tráfego incompatível com o padrão do protocolo; requisições HTTP suspeitas etc.

Dentro da análise do tráfego de rede, existem outras que, segundo Melo (2009), são de grande relevância e também devem ser realizadas. Entre elas, podemos citar: atividades de redes de roteamento; atividades de aplicações que utilizam *Raw Socket*; e processos inerentes aos serviços de redes.

O autor discorre também sobre a importância das seguintes análises: estado do sistema operacional; módulos de *kernel*; informações de *logs*; informações de horário do sistema; informações do disco rígido; e a duplicação do disco. A seguir, passaremos a discutir cada uma delas.

Ao analisar o sistema operacional, o perito se depara com informações valiosas referentes à origem e tipo do ataque realizado. Dados como os de processos ativos em memória podem ser perdidos com o desligamento da máquina, e são necessários para identificar instalações de *malwares* ou conexões suspeitas ou não autorizadas.

Os módulos de *kernel* possuem diversas funções em um sistema; entre elas, a de interceptar e reescrever as chamadas do sistema operacional. Além disso, um *malware* pode assumir a forma um módulo de *kernel*, comprometendo o desempenho do sistema. Consequentemente, a busca por dados nos módulos em memória é de extrema importância.

Outra questão importante, é a coleta de informações dos registros do sistema, também conhecidos por *logs*. A partir dessa análise, pode-se verificar a ocorrência de fatos, como, por exemplo, atividades de usuários e processos, e conexões e outras atividades da rede. No entanto, a investigação pode ser prejudicada, caso a estrutura de registro seja alterada pelo invasor com o propósito de eliminar vestígios (MELO, 2009).

A averiguação do horário do sistema é importante para que o investigador registre suas atividades. Assim, suas ações não se confundem com as do próprio invasor. Além disso, é importante que se faça uma coleta de informações do disco, bem como uma imagem *bit* a *bit* do mesmo, a fim de se obter uma garantia dos dados mais voláteis.

Enfim, se essas análises forem feitas de forma adequada, é possível reconstruir a comunicação entre o invasor e o sistema atacado, fundando-se uma sequência de eventos que pode ser comparada com demais informações obtidas no sistema.

### 3.4.2. *Network Analysis*

Também conhecida como Forense de Rede, a *Network Analysis* é a técnica de obtenção de "dados dos demais ativos de rede envolvidos em um incidente de segurança" (MELO, 2009). Esses dados são posteriormente confrontados com aqueles coletados durante a *Live Analysis*, e, dessa forma, auxiliam nas conclusões dos peritos sobre a invasão.

O uso da criptografia combinada com outros recursos, como *backdoors*, em uma invasão dificulta o trabalho do perito forense computacional, pois o *malware* pode até mesmo passar despercebido por um IDS. Ainda assim, ele deve coletar informações de ativos como, por exemplo: IDS, IPS[5], servidores de *logs* e conexões capturadas por *sniffers*.

Durante a *Network Analysis*, alguns fatores devem ser observados. Dentre eles, Sandro Melo (2009), cita: técnicas de levantamento de dados, como *footprint*, *fingerprint* e *port scanner*; confirmação de invasão ou *malware* automatizado; serviço utilizado para realizar a invasão; vulnerabilidades exploradas; origem da ameaça; tipo de usuário que realizou o ataque; possíveis falhas de segurança; instalação de *backdoors* ou *rootkits*; e tentativas de eliminação de rastros (*cleanlogs*).

Esses pontos acima mencionados são, comumente, seguidos em forma de questões, para que o perito forense computacional possa tentar respondê-las ao entrar em ação na busca por evidências. Conforme o contexto do incidente,

[5] Em inglês, Intrusion Protection System, que se traduz como Sistema de Proteção contra Intrusos.

as questões podem variar, proporcionando ao investigador diferentes resultados.

Melo (2009) aponta que a *Network Analysis* ocorre em dois momentos diferentes. O primeiro acontece com a busca por informações de comunicação de redes do servidor periciado, enquanto o segundo se dá quando o investigador adquire dados sobre demais ativos de rede, como servidores de *logs*, roteadores, IDS ou *firewalls*.

A primeira questão a ser verificada durante uma *Network Analysis* é o horário dos registros de logs e sua concomitância. Em seguida, o perito deve observar os arquivos do tipo PCAP[6], identificando o momento de início da atividade. Segundo Melo (2009), recomenda-se que os arquivos de *log* sejam separados de acordo com determinados intervalos de tempo, devido ao seu tamanho, possibilitando uma análise pormenorizada e precisa.

Cabe lembrar que também relevante é analisar conexões obtidas através de ferramentas de detecção de intrusos, bem como a reprodução das sessões ocorridas à época do ataque.

Além disso, realizar análises estatísticas é uma forma de identificar atividades suspeitas ou incomuns no sistema, pois elas se distinguem facilmente daquelas realizadas com habitualidade, atraindo a atenção do investigador forense.

### *3.4.3. Post Mortem Analysis*

A última etapa de análise da perícia forense computacional é também a mais longa, pois nela deve ser realizado um confronto entre as informações obtidas nas duas primeiras etapas. Por outro lado, sua complexidade proporciona evidências com ricas em detalhes, principalmente durante a análise da imagem do disco rígido.

[6] Packet Capture são aplicações de captura de tráfego de rede.

De acordo com Sandro Melo (2009), a primeira atividade a ser executada pelo perito, é a extração de todas as cadeias de caracteres dos arquivos inerentes ao ataque. Assim, será possível elencar nomes de arquivos e diretórios, resíduos de textos não sobrescritos nos *slackspaces* e de arquivos alojados em áreas não alocadas.

Em seguida, esclarece o autor que a imagem do disco rígido deve ser dividida em 5 camadas, sendo elas: física, de dados, de sistema de arquivos, de metadados, e de arquivos.

A camada física contém informações básicas do disco, bem como de dispositivos de armazenamento de dados, como, por exemplo, o próprio disco rígido e outras mídias. Ao serem criadas, as imagens devem passar por exame de integridade.

Na camada de dados, o perito adquire informações a respeito do particionamento, bem como do *boot*. Essa fase de análise se dá a partir da coleta *bit* a *bit* de mecanismos de armazenamento. Nela, o perito deve verificar características básicas de uma imagem, como tamanho e estrutura, além de montar imagens com múltiplas partições.

Já durante a análise da camada de sistema de arquivos, é necessário que o investigador busque informações inerentes à própria estrutura de arquivos do sistema. Para isso, deve executar sua pesquisa através de informações estatísticas sobre a organização da partição, bem como sobre a estrutura de *journaling*.

Metadados é a camada que fornece informações sobre elementos manipulados ou inseridos em áreas relacionadas ao incidente. Devem-se utilizar ferramentas capazes de mostrar informações estruturais, bem como de criar *timelines*.

Por fim, a análise da camada de arquivos é considerada a mais demorada. Durante a execução dessa atividade, é importante que se obtenha informações

sobre blocos de dados, áreas alocadas, não alocadas e *slackspace*. Também se devem examinar dados de arquivos e diretórios em imagens, ordená-los conforme o formato, buscar *malwares*, e recuperar arquivos a partir de assinaturas e imagens.

Durante a *Post Mortem Analysis*, o disco rígido deve ser minuciosamente examinado, tendo em vista que cada uma de suas partições contém informações relevantes para a perícia forense. Para isso, o investigador deve conhecer a "geometria do disco, ou seja, o número de cilindros, cabeças e setores para documentação" (MELO, 2009, p. 58), além dos espaços entre as partições e da enumeração de setores, cujo intuito é a autenticação do disco original. Deste modo, o perito poderá identificar com maior facilidade dados ocultos pelo invasor, ou mesmo indícios de informações que foram apagadas.

Quando o perito conhece, detalhadamente, cada um desses aspectos do disco rígido, ele é capaz de recuperar arquivos apagados ou que foram sobrescritos de forma parcial.

O exame de sistemas de arquivos é indispensável para a *Post Mortem Analysis*, porquanto permite a reconstrução de eventos inerentes a um ataque. Essa reconstrução se dá com a utilização de *mactimes*, isto é, marcas de tempo de arquivos. Assim, é possível obter indícios de que dados foram acessados ou modificados, além de programas que foram executados pelo atacante no sistema invadido.

Caso seja necessário, o perito também deve buscar identificar informações que foram escondidas pelo atacante. De acordo com Sandro Melo (2009), isso é possível através de combinações de nomes de diretórios com caracteres da tabela ASCII, ou, em outros casos, por meio de inserção de dados em arquivos *core*.

Além disso, o autor fala sobre a importância de arquivos temporários e excluídos para a *Post Mortem Analysis*. Os arquivos temporários funcionam

como um esboço para os arquivos finais com os controles da aplicação, sendo fontes valiosas de informação.

Identificar e recuperar arquivos excluídos é uma atividade de alta relevância para a perícia forense computacional. E é possível realizá-la, visto que, através de comandos de exclusão, um arquivo não é efetivamente extinto, conservando-se em uma área específica até que outra informação seja gravada naquele mesmo espaço. Áreas não alocadas, conhecidas como *slackspace*, também são fontes de informações significantes.

Para concluir a *Post Mortem Analysis*, o investigador deve identificar arquivos manipulados ou corrompidos, além da presença de arquivos maliciosos deixados pelo atacante no sistema invadido. Para isso, são utilizadas ferramentas como: rastreadores de funções, emuladores de máquinas, analisadores lógicos, ou até mesmo programas de monitoramento de tráfego de rede.

Enfim, se for realizada uma análise dinâmica, em tempo real, o perito pode obter resultados mais rápidos e precisos, sendo possível até mesmo observar o funcionamento completo do *malware* em questão, com base no estudo das mudanças provocadas no sistema.

Esclarecidos os detalhes e a importância da perícia forense computacional, passemos agora a estudar um cenário de segurança que contribui para o trabalho dos peritos.

## 4 – Cenário Ideal

A seguir, por ser pertinente ao tema do trabalho, apresentaremos um cenário de segurança proposto pelo especialista em segurança da informação, da empresa Triforsec, Rodrigo Ramos, para a publicação Evidência Digital (RAMOS, 2004).

O contexto da Figura 4 é o de uma rede composta por vários dispositivos de segurança, entre eles: filtros do roteador, *firewalls* e IDS. O autor utilizou, em seu exemplo, apenas ferramentas de *software* livre.

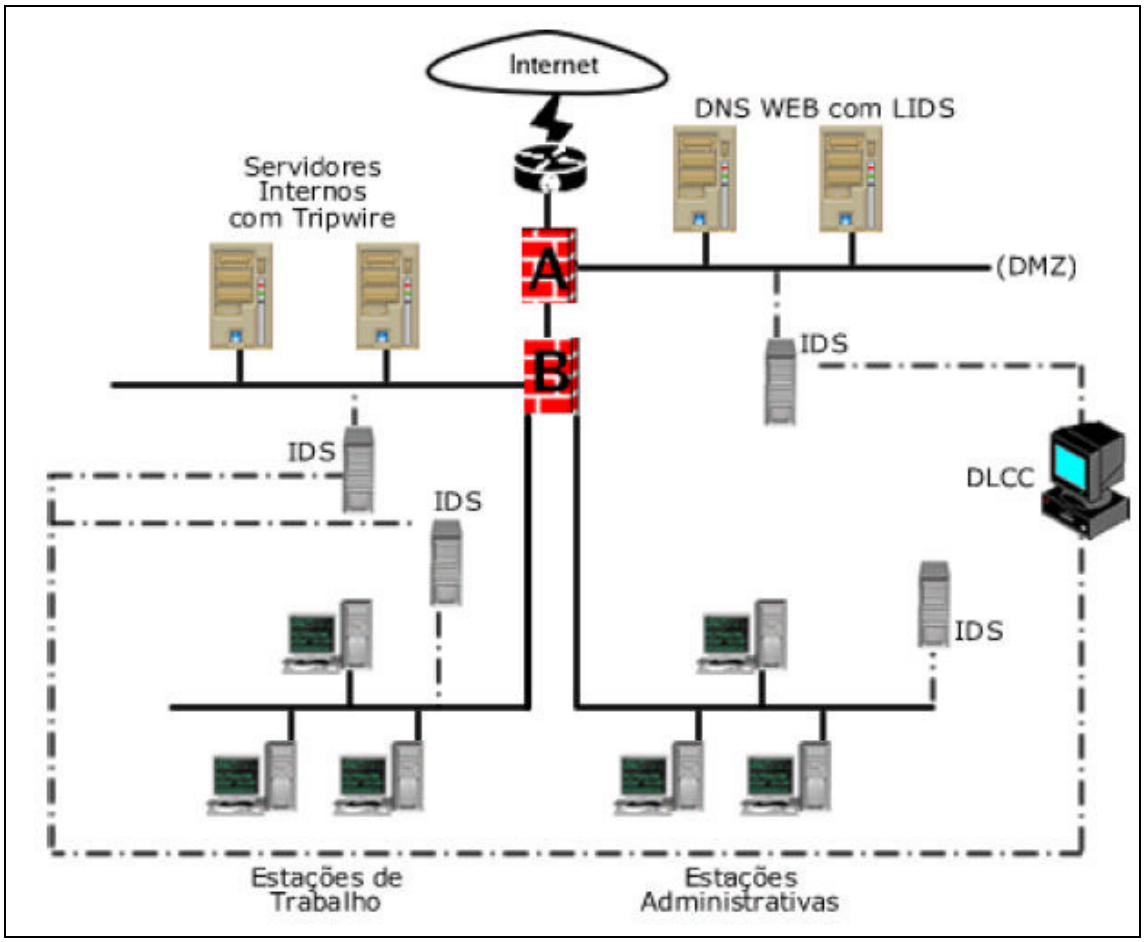


Figura 4: Cenário ideal de segurança de redes. (In: Ramos, 2004)

Vindo pela internet, um pacote, quer tenha sido requisitado ou não, tem o primeiro acesso a uma rede por meio do roteador. Este dispositivo deve possuir

filtros configurados, que são a primeira camada de segurança da rede em questão (RAMOS, 2004).

A configuração de tais filtros estabelece a permissão de entrada apenas para certos tipos de dados. Desse modo, quando um pacote chega a uma rede e, obrigatoriamente, passa pela filtragem, se não tiver aprovação expressa pela configuração do roteador, deverá ser recusado.

Ramos (2004) explica que existem dois tipos de filtragem: *ingress* e *egress filtering*. A primeira filtragem é aquela pela qual passam os pacotes que chegam da internet para a rede. Já o segundo tipo de filtragem estabelece permissões para a saída de pacotes da rede interna. Caso os pacotes tenham endereços IP com origens diferentes, sua saída deve ser proibida. Assim, o tráfego de pacotes com IP falsificado se reduz. Portanto, para uma boa conexão, é essencial que se configure o roteador.

Na situação proposta pelo autor, após sua passagem pelo roteador, os pacotes atingem a segunda camada de segurança da rede. Esta parte é composta por uma máquina, que contém um *firewall* (identificado pela letra “A” na Figura 4) e um sistema de detecção de intrusos (IDS). Caso o pacote tenha sido requisitado por uma máquina interna da rede, ele poderá ser direcionado para a zona desmilitarizada (DMZ, na sigla em inglês); caso contrário, ele poderá ser barrado.

Para melhor esclarecer o termo, Sandro Melo (2009, p. 109) define zonas desmilitarizadas como:

> Subredes com regras próprias de segurança, contendo servidores de acesso público a partir de uma rede maior insegura, normalmente a internet, forçando uma camada extra de segurança contra invasões a outros segmentos de rede existentes, como a intranet, que ficam em segmentos próprios.

O *firewall* realiza o controle e o acompanhamento dos pacotes que passam por ele, através de sua tabela de estados. Isso possibilita a identificação e

diferenciação entre pacotes que não foram solicitados e aqueles cuja requisição acabou de sair da rede.

Além disso, é importante que se configure o IDS para o monitoramento adequado do ambiente. Este dispositivo, de acordo com Ramos (2004, p. 50), "implementa uma outra camada de segurança, checando o cabeçalho e o *payload* do pacote procurando por um conteúdo anormal," que pode ser um código malicioso ou até mesmo algum tipo de comando para uma aplicação.

Essa atividade se dá através da análise do protocolo, sendo possível reconhecer anormalidades de comportamento e regularizar a comunicação. Deste modo, o sistema de detecção de intrusos impede que pacotes enviados com intenções maliciosas consigam passar pela segurança.

Rodrigo Ramos (2004, p. 50) discorre ainda sobre a importância dos pré-processadores, que "evitam que o engenho de detecção desperdice processamento checando um pacote que já está incorreto por natureza."

O *Defense Layer Central Console* (DLCC) é uma ferramenta que permite controlar e monitorar remotamente vários sistemas de detecção e prevenção de intrusos. Ele possui um pacote responsável por integrar o IDS com o *firewall*, possibilitando até mesmo reconfigurações dinâmicas do *firewall* de acordo com eventos detectados.

Seu uso permite, conforme configuração prévia, a identificação de diversos elementos, entre eles: *malwares*; acessos não autorizados a aplicações em um servidor; *port scans*; requisições anormais; e outros problemas.

Entretanto, o autor atenta para o fato de que, quanto mais tipos de detecções diferentes, maior o processamento consumido, além da geração de relatórios e outras consequências desnecessárias para a segurança da rede.

Nas máquinas em que se encontram os *firewalls*, é de grande importância que existam também ferramentas que fornecem dados sobre o link. Ramos (2004)

aponta dispositivos que realizam o monitoramento do tráfego no link da rede, além de gerar relatórios em tempo real.

O autor coloca, por motivos de segurança, a zona desmilitarizada como um segmento que “separa recursos que precisam ser acessados constantemente a partir da internet, dos recursos da rede interna” (RAMOS, 2004, p. 50). Esse fator, integrado ao LIDS (*Linux Intrusion Detection System*), possibilita ocultar processos do sistema, detectar *port scans*, bem como evitar outros tipos de subversões. Além disso, Ramos (2004) ainda explica que a instalação de antivírus pode ser interessante para o monitoramento de arquivos dos servidores.

O segundo *firewall* (identificado pela letra “B” na Figura 4), “é responsável por implementar a política de acesso aos segmentos da rede e fazer o roteamento entre as máquinas” (RAMOS, 2004, p. 50). Em outras palavras, este dispositivo é que autoriza o acesso a um dos servidores internos, a partir das estações de trabalho, por exemplo, o que diminui riscos de infecção, visto que uma máquina infectada não consegue ter acesso a outras.

Também vale mencionar a relevância da segmentação da rede, conforme as funções e objetivos de seus usuários, pois, para uma maior segurança, os recursos devem ser restritos apenas àqueles grupos que os utilizam efetivamente.

Espalhados pela rede, existem alguns sensores IDS que não interagem com os *firewalls*. Pelo contrário, eles são acompanhados remotamente pelo DLCC, e são capazes de identificar ações ilícitas através de comparações feitas em suas bases de assinaturas e pré-processadores.

O DLCC permite, além disso, que todos os sensores IDS sejam monitorados de forma individual ou simultânea, conforme as necessidades de correlação de fatos. Assim, é possível diferenciar eventos isolados daqueles que fazem parte de ações coordenadas. Também é possível obter informações sobre potenciais

invasões através de relatórios e históricos da rede, pois o DLCC possui um banco de *logs* de seus agentes.

Finalmente, o Ramos (2004) explica a utilização da ferramenta Tripwire, presente nos servidores internos, que funciona como uma espécie de caixa preta do sistema, registrando todos os arquivos e, consequentemente, possíveis alterações nos mesmos. Os relatórios gerados por essa ferramenta auxiliam o investigador na análise do sistema invadido, durante a perícia forense computacional.

## 5 – Conclusão

Diante do exposto neste trabalho, foi possível perceber crescente a importância da computação forense para a segurança da informação. Atualmente, qualquer pessoa ou organização pode ser alvo de ataques e invasões digitais. Criminosos realizam esse tipo de atividade, seja para obter vantagens, seja para o furto de informações, ou, em alguns casos, pela simples intenção de prejudicar terceiros.

Vimos que, através da perícia forense computacional, é possível obter todo tipo de informações sobre os recursos utilizados, a forma como se deu, o horário e, até mesmo, a origem da invasão. Isso possibilita às vítimas decidirem ou não dar seguimento judicial ao caso, ou, no mínimo, procurarem adquirir formas atualizadas de segurança.

Pôde-se perceber também que a análise forense computacional, apesar de ser eficiente para a maioria dos casos em que é utilizada, também é muito complexa e trabalhosa. Em determinadas situações, todo o esforço não é recompensado pelos resultados, considerando que as informações tratadas podem ser extremamente voláteis.

Assim, é importante que seja realizada a segurança de todos os sistemas e redes utilizados por uma organização, ou mesmo por um usuário comum. Essa segurança deve ser planejada e executada de forma concisa e eficiente, tendo em vista que uma simples ferramenta de detecção de invasões instalada em uma máquina, não é suficiente para impedir a realização de danos.

Entretanto, percebemos que, mesmo com o auxílio dos dispositivos mais modernos disponíveis no mercado, sejam *softwares* livres ou proprietários, criminosos ainda conseguem driblar a segurança e invadir sistemas, praticando fraudes, ameaças, roubo de senhas e outras informações restritas, espionagem industrial, crimes contra a honra, entre outros ilícitos.

Isso se dá, como visto anteriormente, devido ao desenvolvimento tecnológico, que torna cada vez mais fácil o acesso e a utilização de computadores, aplicações e, até mesmo, linguagens de programação.

Em outras palavras, conforme as tecnologias de segurança e investigação aumentam, também cresce o número de ataques e outras atividades ilícitas, realizadas por criminosos cada vez mais atualizados.

Portanto, podemos concluir que, mesmo que a computação forense não seja a forma mais eficaz de prevenção a incidentes de segurança, ela ainda é indispensável para o bom funcionamento das organizações modernas.

Finalmente, tendo em vista a novidade do tema em questão, também é muito escassa literatura sobre o mesmo. Dessa forma, seria interessante a continuidade do presente trabalho, de modo a aprofundar o estudo das técnicas de investigação da computação forense.

**Bibliografia**

ARAUJO, José Mariano de. **Cyber Crimes – Delegado Mariano. Weblog sobre crimes eletrônicos no mundo**. <http://mariano.delegadodepolicia.com/>. Acesso em: 8 de junho de 2010.

KENNEALLY, Erin. **Computer Forensics – Beyond the Buzzword**. ;login:, v. 27, n. 4, agosto, 2002. p. 8-11.

MELO, Sandro. Computação Forense com Software Livre. Rio de Janeiro: Alta Books, 2009. 1ª edição.

MERCURI, Rebecca T. **Challenges in Forensic Computing.** Communications of the ACM. ACM, 2005.

RAMOS, Rodrigo. **Cenário Proposto I**. Evidência Digital, v. 3, julho, agosto e setembro, 2004. p. 49-51.

US-CERT. **Computer Forensics.** Disponível em: <http://www.us-cert.gov/>. 2008.