Um ambiente seguro de *logs* como auxilio a computação forense.

Leandro Borges
Dalton Matsuo Tavares

ORGANIZAÇÃO DA APRESENTAÇÃO

1. Introdução.
2. Aspectos Legais.
3. Aspectos Técnicos.
4. Proposta do ambiente.
5. Conclusões.
6. Argüição.

INTRODUÇÃO

- Arquivos de log, muitas vezes não são vistos com bons olhos, e correm o risco de serem menosprezados pelos administradores de sistema que não sabem como e quão úteis estes arquivos podem ser.

- A análise de arquivos de log pode ser árdua e trabalhosa caso alguns cuidados não sejam tomados.

- Existem algumas considerações técnicas importantes que se deve levar em conta na hora de se construir uma infra-estrutura de log.

- Arquivos de log podem ser de grande valia em uma investigação criminal.

INTRODUÇÃO

Uma vez que estes arquivos podem ser usados, para nortear ou solucionar crimes cibernéticos, podemos acrescentar outros aspectos a introdução desta apresentação. Que trata-se da relevância do estudo de técnicas que possam ajudar a solucionar crimes virtuais.

- Crescimento assustador da abrangência da Internet, trouxe consigo um aumento considerável nas ameaças **financeiras**, de **negócio, entre outras**.
- Roubo de quantias monetárias utilizando-se a Internet como ferramenta. **(pessoas físicas ou jurídicas)**
- Ataques que prejudicam as operações de uma determinada empresa.**(ataques de negação de serviços em uma loja virtual)**
- Entre outros crimes como difamação; pornografia infantil; perseguição virtual; uso de identidade alheia, entre outros.

ASPECTOS LEGAIS

1. **A computação forense**
2. **Atual situação da legislação brasileira**
3. **A perícia judicial**
4. **Perito**
5. **Laudo pericial judicial**
6. **O caminho do delito ao julgamento**

A computação forense.

- Amplitude do estudo de técnicas forenses.
- Como resposta ao crescimento de crimes relacionados à informática, no final da década de 1980 e começo da década de 1990, as agências legais dos Estados Unidos começaram a trabalhar em conjunto de forma a proporcionar o treinamento de seus profissionais para lidar com este problema.
- A demanda por profissionais especializados capazes de solucionar crimes de informática cresceu juntamente com o crescimento dos crimes desse gênero. Este fato fez com que um termo antes utilizado em outras áreas da ciência fosse incorporado também à computação, dando origem ao termo computação forense.

A Atual Situação da Legislação Brasileira.

- Não existem leis que regulamentem o uso da Internet no Brasil.
- Todos os crimes praticados utilizando-se a Internet como ferramenta, atualmente, devem ser tipificados usando-se o código penal vigente.
- Existem muitos projetos de lei em tramite no Senado Federal que buscam a regulamentação da Internet no Brasil.
- Dentre eles o PL 5.403/01 merece destaque, pois este determina que os provedores terão que manter arquivados os históricos de acesso de seus usuários por um ano como forma de combater o uso indevido da rede.

A Perícia Judicial.

- No senso comum a perícia é uma "vistoria técnica", um "exame ou vistoria de caráter técnico e especializado", um tipo de "exame feito por perito", e que pode não ser necessariamente técnica, mas uma prática quando feita por pessoas com conhecimentos adquiridos por longos anos de trabalho em uma determinada área do conhecimento.

- Perícia Judicial

- Perícia Extrajudicial: vistoria de seguro, laudo de obras, inquéritos policiais.

O Perito.

- Em geral, perito é uma pessoa ou profissional que detém experiência e conhecimentos sobre determinada área ou campo do conhecimento; que realiza a perícia cujo parecer fundamentará resoluções, abrirá precedentes e fundamentará decisões pelo resultado do seu trabalho em um laudo pericial.

- Características de um bom perito: postura, capacidade intelectual e profissional, condições psicológicas para não se deixar envolver pelo resultado, dignidade e probidade profissional.

Laudo Pericial Judicial.

- E no laudo que o perito responderá às perguntas formuladas pelo juiz. Nele será feita a exposição da perícia realizada e seu resultado.

- O Laudo Pericial Judicial deve apresentar os seguintes requisitos: o relatório, a parte expositiva, a parte conclusiva e a parte autenticativa.

- Falaremos do relatório quando falarmos sobre os aspectos técnicos.

ASPECTOS LEGAIS

O caminho do delito ao julgamento.

- A comissão do crime cibernético.
- A Denuncia.
- A abertura de um inquérito policial.
- A apuração e descoberta do infrator.
- Infrator responde a um processo judicial.

ASPECTOS TÉCNICOS

1. **A Elaboração de um relatório pericial bem estruturado.**

2. **As fases de um ataque.**

3. **Discussão sobre métodos de *logging* e seus problemas.**

4. **Problemas quanto a segurança do protocolo syslog.**

5. **Daemons de log alternativos ao syslog.**

6. **Como garantir a integridade e autenticidade dos arquivos de log gerados.**

ASPECTOS TÉCNICOS

A elaboração de um relatório pericial bem estruturado.

- A aquisição dos dados.
- Análise dos resultados.
- Esquematização e organização do relatório
- Escrevendo o relatório.
- Revisando o relatório.

As fases de um ataque.

- *Probe*
- *Penetrate*
- *Persist*
- *Propagate* ***(vírus, worms)***
- *Paralize*

Discussão sobre métodos de *logging* e seus problemas.

- Log Local
- Log Remoto (Centralizado e Descentralizado)

Problemas quanto a segurança do protocolo syslog.

- Comunicação utiliza se de UDP.
- Mensagens trafegam em formato texto
- Mensagens são armazenadas em formato texto
- Não oferece suporte a autenticação
- Erros programáticos, vulnerabilidades

Daemons de log alternativos ao syslog.

- Sylog-ng: TCP/IP, integração com Banco de dados, facilidade da organização das informações de eventos de sistema por ele gerados. **("priority/facility")**

- NSyslog: Utiliza TCP/IP e criptografia SSL. Não funciona muito bem em Linux, por sua incompatibilidade com o klog. Outos Unix-Like são amplamente suportados.

- Modular Syslog: Assinatura dos eventos com PEO-1 e L-PEO, suporta integração com banco de dados e a utilização de expressões regulares para filtrar os dados logados.

A PROPOSTA DO AMBIENTE

Softwares Utilizados.

- Syslog-ng
- Stunnel
- Scanlogd
- Nmap **(primeira fase do ataque)**

Ambiente de Testes.

- O ambiente de testes é um cenário simplificado onde foram estudados os comportamentos do ambiente proposto. Este ambiente é composto por três máquinas: alfa, beta e gama.

Ambiente de Testes.

- Máquina alpha: desempenha o papel de servidor de logs. Tem como objetivo o armazenamento dos arquivos de log gerado pelos dispositivos de rede, neste caso em específico, armazenar os logs de beta

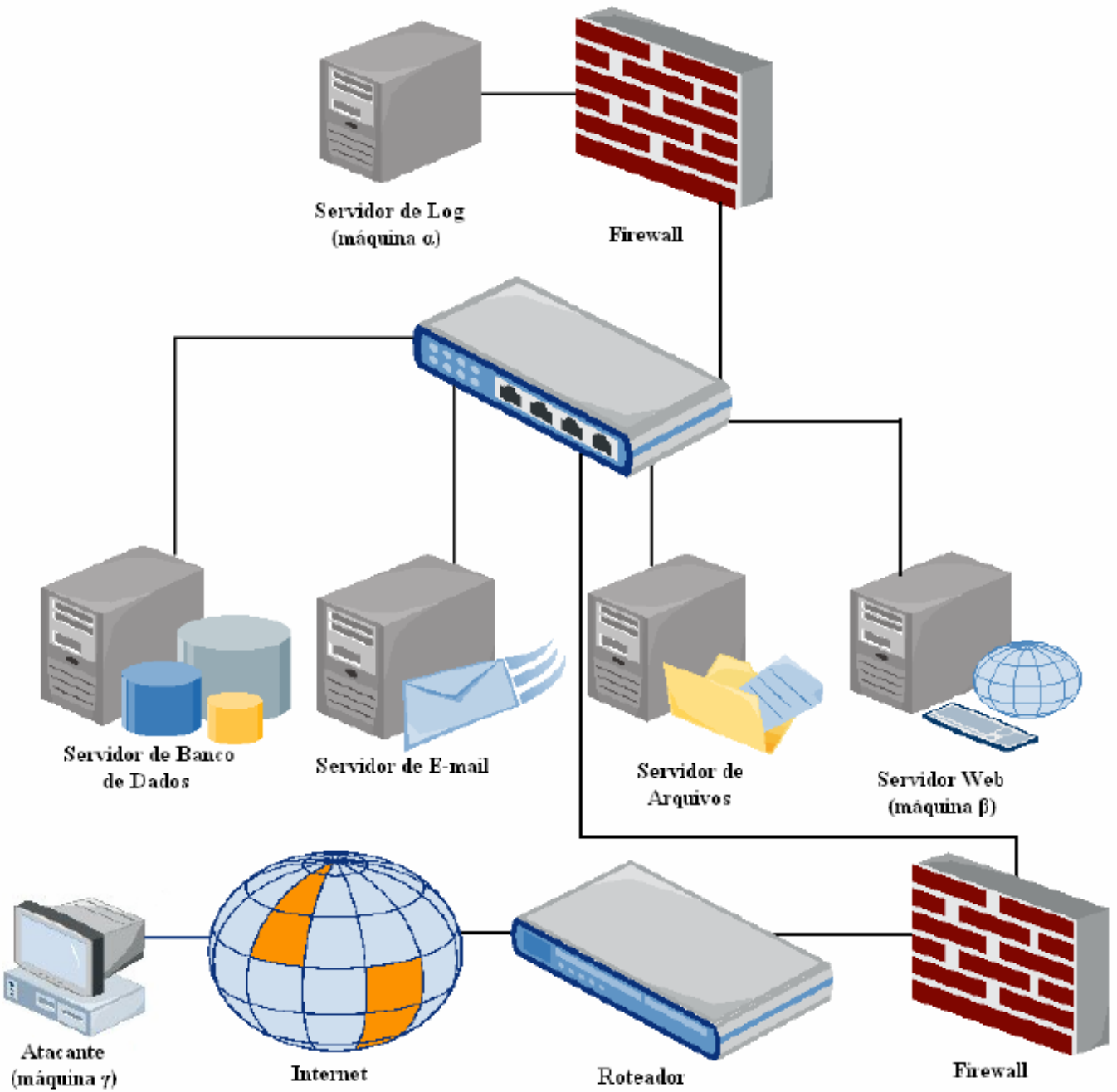
A PROPOSTA DO AMBIENTE

Ambiente de Testes.

- Maquina beta: esta máquina executa o papel de um servidor *web*, porém na pratica ela poderia ser qualquer outro servidor ou dispositivo conectado a rede. Tem o objetivo de servir como máquina alvo, que recebe os ataques de gama e envia seus eventos de *log* a alfa possibilitando desta forma o arquivamento seguro desses arquivos para as análises pertinentes.

Ambiente de Testes.

- Máquina gama: esta máquina tem o objetivo de executar as tarefas de varredura remota.


Servidor de Log
(máquina α)
Firewall
Servidor de Banco
de Dados
Servidor de E-mail
Servidor de
Arquivos
Servidor Web
(máquina β)
Atacante
(máquina γ)
Internet
Roteador
Firewall

Resultados dos Testes.

Foi possível no ambiente de desenvolvimento:

- Garantir a integridade e autenticidade dos arquivos de *log* gerados durante a primeira fase do ataque.

- Identificar as tentativas de varreduras remotas, mesmo com a utilização de *stealth scans.*

Resultados dos Testes.

Com o levantamento bibliográfico foi possível.

- Compreender a importância do trabalho de um perito, para a validação da prova virtual, transformando-a em um laudo.

- Compreender que a falta de tipificação para crimes cibernéticos no Brasil, pode dificultar, mas não compromete a incriminação do infrator.

Conclusão

Existe uma real potencialidade na utilização de arquivos de log para a computação forense. A utilização desse recurso juntamente com os artifícios legais apropriados, podem constituir uma ferramenta útil para coibir eventuais práticas criminosas a partir da detecção de ataques por meio de arquivos de log, usando os como uma forma uma prova efetiva.