Hamilton Fonte II

Modelo de plano de pesquisa - PCS5012 - 2016/1

São Paulo

2016

Resumo

O objetivo é coletar dados de memória de processos em máquinas em núvem de modo que os mesmos sejam aceitos em um processo legal. Através de um método que visa associar os dados relacionados a máquina de onde eles saíram, de modo a ajudar a diminuir a quantidade de dados a ser analisada propondo uma mudança no paradigma da coleta assim fechando uma rota de fuga para criminosos escaparem pela via legal.

Segundo a norma ABNT, o resumo deve ressaltar o objetivo, o método, os resultados e as conclusões do documento.

1 Descrição do problema de pesquisa

Utilização da nuvem para atos ilícitos. Com o crescimento da utilização da nuvem ilícitos tambem aumentam. Quando um ilícito acontece a forense tenta reconstruir a sequência de (RAHMAN; KHAN, 2015) eventos de modo a entender como ele ocorreu e mitigar as vulnerabilidades que permitiram a sua realização e a questão legal de apoio ao processo legal

Boa parte da forense digital herdou práticas da forense tradicional. Dificultades das práticas forenses existentes para coletar evidência da nuvem por causa do carater multi inquilinato e multi jurisdição e elasticidade aliado a dificuldade de se ter uma evidência válida em um processo alíado a ameaças que não deixam rastros em disco.

As soluções disponiveis até o momento estão focada mais no lado tecnológico do que no jurídico e a maioria focada na parte reativa da forense e poucas na parte preventiva. Muitas na completude da evidência do que. O volume de dados aumentando muito dificulta a analise cria um backlog imenso caráter volátil da nuvem leva a perda de informações importantes para o processo legal (SANG, 2013) e investigativo.

2 Objetivos

Criar um mecanismo de coleta dados de memória volátil de uma máquina em nuvem de modo a que sejam aceitos em um processo forense.
- Ser capa de reproduzir o processo independente da máquina existir ou não
- A taxa de erro do processo ser conhecida.
- Ser capaz de suportar a análise forense do incidente com no máximo 10% da informação comparada com processos de coleta utilizados hoje.
- Não violar a jurisdição de outros países - Não violar a privacidade de usuários da núvem não envolvidos na investigação.

3 Método

Através de conteinerização, janela de dados e coleta fora do sistema de nuvem. Apresentar a evidência para um devogado, sei lá

4 Revisão bibliográfica

automated data acquisition in the cloud
Digital forensics framework for a cloud environment
Evidence and cloud computing the virtua machine introspection approach
Design and implementation of FROST: FoRensic tools for Open STack
Automated Forensic Data Acquisition in the cloud
A log based approach to make digital forensics easier on cloud computing
Volatile memory acquisitio using backup for forensic investigation

5 Resultados esperados

Fechar uma das portas de fuga para criminosos na núvem hoje.Fornecer mais um mecanismo de coleta de dados para investigação. Propor uma mudança de paradigma da coleta de modo a
diminuir a quantidade de informação que precisa de análise.

Referências

RAHMAN, S.; KHAN, M. N. A. Review of live forensic analysis techniques. *International Journal of Hybrid Information Technology*, v. 8, n. 2, p. 379–388, 2015. Disponível em: <http://www.sersc.org/journals/IJHIT/>.

SANG, T. A log-based approach to make digital forensics easier on cloud computing. *Proceedings of the 2013 3rd International Conference on Intelligent System Design and Engineering Applications, ISDEA 2013*, p. 91–94, 2013.