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

Forense digital é um conjunto de técnicas de coleta e análise de evidências geradas por computadores e humanos que tem por objetivos, entender a sequência de eventos que permitiu que um ataque fosse perpetrado, impedir que a vulnerabilidade que tornou possível um ataque seja utilizada novamente e apoiar um processo legal (SANG, 2013). A forense digital cresceu a partir de técnicas usadas na forense tradicional, começou de forma ad-hoc, passou por uma fase de adaptação aos requisitos legais até a era de ferramental avançado de coleta e análise (CHARTERS, 2009).

A utilização crescente de virtualização, ferramentas online e hospredagem em núvem, esta inviabilizando algumas práticas forenses (SHARMA; SABHARWAL, 2012). Especificamente a funcionalidade da elasticidade de carga ofertada pelos provedores de nuvem por meio da qual infraestrutura pode ser alocada e desalocada dinamicamente, trouxe o problema da volatilidade dos dados nas máquinas virtuais. Com algumas ameaças que não deixam evidências em disco (ALJAEDI et al., 2011), a memória de uma máquina despejada de um pool seria para sempre perdida, com ela evidências importantes. O ferramental forense disponível hoje esta pouco adaptado a desafios trazidos pela nuvem, focam em completude, resposta a incidente e raros geram evidências aceitaveis em um processo legal (REICHERT; RICHARDS; YOSHIGOE, 2015) (DYKSTRA; SHERMAN, 2012).

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

ALJAEDI, A. et al. Comparative Analysis of Volatile Memory Forensics. *IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT) and IEEE International Conference on Social Computing (SocialCom)*, p. 1253–1258, 2011.

CHARTERS, I. The Evolution of Digital Forensics. n. January, p. 1–39, 2009.

DYKSTRA, J.; SHERMAN, A. T. Acquiring forensic evidence from infrastructure-as-a-service cloud computing: Exploring and evaluating tools, trust, and techniques. *Digital Investigation*, Elsevier Ltd, v. 9, n. SUPPL., p. S90–S98, 2012. ISSN 17422876. Disponível em: <http://dx.doi.org/10.1016/j.diin.2012.05.001>.

REICHERT, Z.; RICHARDS, K.; YOSHIGOE, K. Automated forensic data acquisition in the cloud. *Proceedings - 11th IEEE International Conference on Mobile Ad Hoc and Sensor Systems, MASS 2014*, p. 725–730, 2015.

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.

SHARMA, H.; SABHARWAL, N. Investigating the Implications of Virtual Forensics. *Advances in Engineering, Science and Management (ICAESM), 2012 International Conference on*, p. 617–620, 2012.