Análise de varreduras de portas contra *Virtual LAN tagging* em nuvems computacionais baseadas em OpenStack com honeypots de baixa interatividade

Nicolas Peter Lane, Charles Christian Miers

[1] Departamento de Ciência da Computação (DCC)
Centro de Ciências Tecnológicas (CCT) – Universidade do Estado de Santa Catarina (UDESC)

nicolas@colmeia.udesc.br, charles.miers@udesc.br

Resumo. *O artigo propõe a análise de ameaças e mecanismos de segurança utilizando Low Interaction Honeypots (LIH) por meio de uma perspectiva de segurança voltada às redes segmentadas VLAN tagging em nuvens computacionais baseadas no OpenStack. Deste modo, permitindo a elaboração de uma proposta de estratégia para detecção de ameaças em serviços oferecidos por nuvens computacionais baseadas em OpenStack.*

1. Introdução

A computação em nuvem traz uma nova tendência para o futuro da computação com diversas aplicações em campos de estudo e de mercado. No entanto, tal mudança de paradigma causa preocupação com segurança, uma vez que é de conhecimento comum a escalabilidade com que vulnerabilidades são exploradas em sistemas computacionais. Assim, como os consideráveis impactos sobre o desempenho e os serviços às organizações envolvidas em tais incidentes.

Desse modo, a existência da necessidade de concessão de privilégios individuais (*e.g.,* privacidade, segurança, *etc.*), na qual, o cliente precise abdicá-los em conjunto com seus dados à integridade e a disponibilidade dos servidores do provedor responsável pelo serviço contratado (*e.g.,*, política de privacidade, posicionamento da empresa, comprometimento com segurança, *etc.*), torna esta questão de relevante importância [4]. Embora existam pesquisas no âmbito de segurança em diversas áreas de nuvens computacionais com *Low Interaction Honeypots (LIH)*, tais pesquisas utilizam-se de plataformas proprietárias e fechadas, o que compromete a sua reprodutibilidade [3]. Nesse contexto, não foi possível identificar a existência de referências, relativas a redes segmentadas *VLAN tagging* em nuvens computacionais abertas do tipo *Internet-as-a-Service (IaaS)* usando OpenStack com o foco em segurança, de modo a verificar se os princípios básicos da *Information Security (IS)* estão sendo satisfeitos nos serviços oferecidos pela mesma. Portanto, com esse propósito, o presente artigo consiste na proposta de uso do LIH em redes segmentadas *VLAN tagging* em nuvens computacionais de código aberto, a fim de mitigar ameaças por meio do tratamento de vulnerabilidades resultantes da análise dos dados obtidos por tais honeypots nesses ambientes.

2. Definições

2.1. Nuvens computacionais abertas IaaS

As nuvens computacionais em redes de produção são tipicamente ambientes computacionais virtualizados que empregam hipervisores do Tipo 1 (*Bare-metal*). Cada respectiva

camada da nuvem computacional corresponde aos recursos, controle das instâncias virtualizadas e a administração/controle dos recursos de hardware disponíveis fisicamente para os diversos clientes da nuvem computacional (*e.g., Internet-as-a-Service (IaaS)*, *Platform-as-a-Service (PaaS)*, *etc.*) [2]. Estas nuvens podem ter sua implantação (*i.e.,* pública, privada, híbrida e comunitária) e política de desenvolvimento de software do controlador aberto *e.g.,* OpenStack, *etc.*) ou proprietário (*e.g.,* Amazon AWS, *etc.*) [2]. Nesse sentido, serviços providos por nuvens computacionais abertas de alto desempenho do tipo IaaS com OpenStack possuem demanda de diversas organizações. Esta demanda pode depender do nível de *Quality of Service (QoS) / Service Level Agreement (SLA)* oferecido e prestado pela nuvem computacional, satisfazendo os princípios básicos de IS (*e.g.*, integridade, disponibilidade e confidencialidade).

2.2. Honeypot

Honeypots são ferramentas incisivas, caracterizadas como um software de segurança cujo seu valor à organização reside em ser escaneado, atacado ou comprometido por um atacante [6]. Nesse contexto, LIH são honeypots de baixa complexidade, e que são simples de serem instalados, configurados e mantidos por uma organização. Portanto, estas ferramentas são facilmente implantáveis em ambientes virtualizados (*e.g.*, contêineres, nuvens computacionais, máquinas virtuais, ambientes virtualizados de alto desempenho, *etc.*) e ambientes não virtualizados (*e.g.,* máquinas computacionais, máquinas computacionais de alto desempenho, *etc.*) [5]. Geralmente, tais soluções têm seu serviço limitado a emulação. Portanto, o principal valor que LIH oferece a infraestrutura de rede de uma organização é a detecção, uma vez que o atacante tem a sua iteração limitada (*e.g.,* Telnet, varredura de portas, *bruteforce* de login, *etc.*) por meio de serviços predefinidos fixos ou programáveis (*e.g.,* perl, shellscript, python, *etc.*). Desta forma, LIH oferecem baixo risco à infraestrutura de rede da organização, limitando o honeypot a coletar dados que dizem respeito às condições do ataque e não ao ataque em si (*e.g.,* data do ataque, horário do ataque, endereço IP da fonte do ataque, *etc.*). Tal fato, permite a utilização de LIH em nuvens computacionais abertas do tipo IaaS baseadas em OpenStack a fim de mitigar possíveis vulnerabilidades no ambiente virtualizado.

3. Identificação de vulnerabilidades e plano de testes

Diversas vulnerabilidades são exploradas por agentes maliciosos anualmente com os mais diversos propósitos (*e.g.,* individual, grupos, organizações, *etc.*) [5]. Diversos fatores caracterizam um ataque (*e.g.*, psicologia, métodos, ferramentas, conhecimento, *etc.*). Nesse sentido, há diversas técnicas que podem ser usadas para realizar uma intrusão a fim de comprometer um sistema computacional. De tal modo, que uma vulnerabilidade torna-se um potencial risco à infraestrutura de rede de uma organização, a medida que esta torna-se um vetor de vulnerabilidades exploráveis por terceiros [4]. Uma lista dos ataques mais recorrentes no ano de 2016 é apresentada na Tabela 1.

Tabela 1. Vetor de vulnerabilidades exploradas por ataques em 2016 [1]

Vulnerabilidade	Descrição	Porcentagem
Navegadores	É um ataque de exploração de vulnerabilidades em navegadores *web*. Que permite a execução de *malwares* por meio da esteganografia concedendo acesso privilegiado ao atacante.	36%
Bruteforce	É um ataque que testa todas as possibilidades de senhas contra um sistema computacional a fim de conceder acesso ao atacante.	19%
DDoS	Consiste de ataques sobre uma infraestrutura de rede. Com o propósito de indisponibilizar o serviço da organização a terceiros.	16%
SSL	É um ataque *man-in-the-middle* sobre uma conexão criptografada. Que permite acesso a informação em texto aberto durante a sua transmissão.	11%
Scam	É uma varredura na Internet em busca de computadores com portas abertas de modo a permitir acesso ao mesmo. Caracterizando-se por permitir o reconhecimento de alvos em potencial.	3%
DNS	Consiste de ataques realizados usando-se DNS (*e.g.*, *spoofing*, *hijacking*, *etc.*). Permitindo ao atacante acesso a informações privilegiadas de alvos em potencial que acessem tais domínios.	3%
Backdoors	É uma vulnerabilidade na implementação de um software, que visa permitir o acesso remoto de um atacante no mesmo.	3%
Outras	Compreende ataques realizados contra vulnerabilidades já conhecidas.	9%

As vulnerabilidades listadas na Tabela 1 servem como lista base dos ataques a serem monitorados na nuvem OpenStack de experimentação, com o intuito de verificar a existência de vulnerabilidades nas quais os mecanismos de segurança da nuvem mostrem-se incapazes de identificar em *VLAN tagging* entre os seus providos serviços. São implantados, usando a solução de código aberto *Honeyd*, LIH dentro destas nuvens para então verificar-se a existência de potenciais vulnerabilidades e quais as melhores práticas para sua detecção e medidas corretivas/preventivas. Um diagrama do LIH dentro da nuvem computacional OpenStack é apresentado na Figura 1.

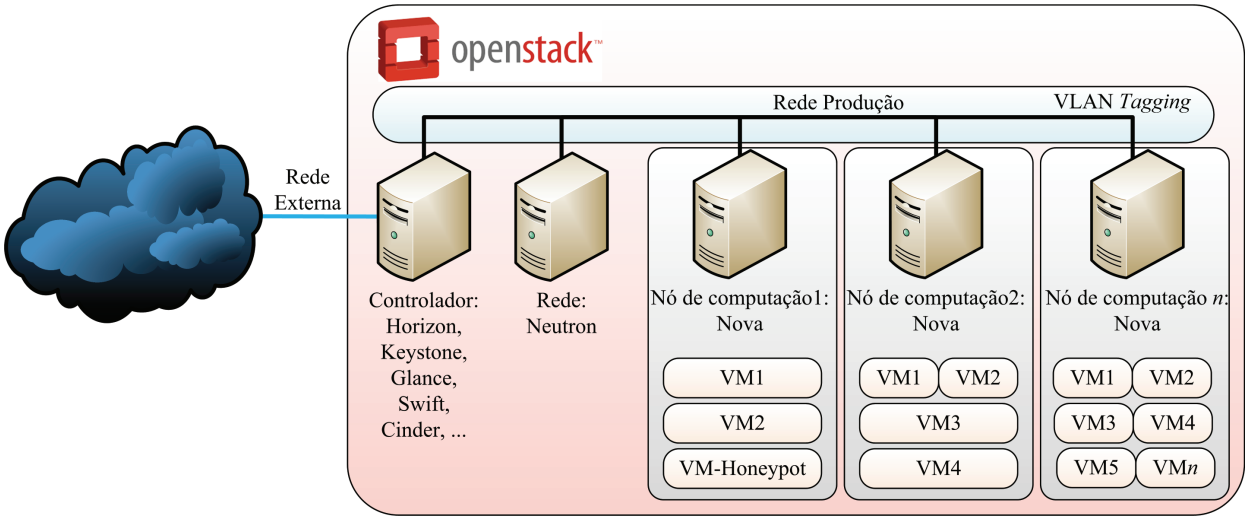

Figura 1. LIH dentro do OpenStack

Portanto, com base na Figura 1 e nos dados apresentados, é realizada a implantação de um ou mais LIH nas VLANs entre as instâncias de serviços oferecidos pela nuvem computacional com OpenStack no Laboratório de Processamento Paralelo e Distribuído (LabP2D) do CCT/UDESC. Tais instâncias são inicializadas em função dos serviços e do código fonte do LIH providos pelos servidores. Na nuvem do LabP2D, uma rede de testes é definida com LIH e o vetor de vulnerabilidades é testado contra os serviços da nuvem, posteriormente são desenvolvidos ataques contra as vulnerabilidades existentes entre os serviços ou específicos a determinados serviços providos pela nuvem. Está previsto também a realização dos experimentos em uma rede de produção existente

na nuvem do LabP2D com LIH, com o intuito de verificar a existência de vulnerabilidades nos serviços e se estas são capazes de corromper os mecanismos padrões de segurança providos pelo OpenStack. Os dados provenientes do honeypot são catalogados e analisados a fim de verificar se essas ameaças podem comprometer os requisitos de QoS/SLA de um serviço hospedado na nuvem computacional do LabP2D.

4. Resultados obtidos e considerações finais

Com base na análise realizada no artigo e nos dados obtidos por meio da implantação do LIH, é proposto desenvolver uma proposta de estratégia para a detecção de ameaças na nuvem computacional de alto desempenho OpenStack presente no LabP2D. Adicionalmente, tem-se a intenção de aplicar os LIH em outras nuvens computacionais OpenStack (*e.g., Yellow Circle*) para obter-se dados adicionais.

5. Agradecimentos

Os autores agradecem o apoio do Laboratório de Processamento Paralelo e Distribuído (LabP2D) no CCT da Universidade do Estado de Santa Catarina (UDESC).

Referências

[1] Calyptix. Top 7 Network Attack Types in 2016, June 2016.

[2] P De Hert, V Papakonstantinou, and I Kamara. The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection. page 26, 2014.

[3] D. Gonzales, J. Kaplan, E. Saltzman, Z. Winkelman, and D. Woods. Cloud-Trust - a Security Assessment Model for Infrastructure as a Service (IaaS) Clouds. *IEEE Transactions on Cloud Computing*, PP(99):1–1, 2015.

[4] A. Malyuk and N. Miloslavskaya. Information Security Theory for the Future Internet. In *2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud)*, pages 150–157, ROME, 2015. IEEE.

[5] Mohssen Mohammed and Habib-ur Rehman. *Honeypots and Routers: Collecting Internet Attacks*. CRC Press, 1st edition, 2015.

[6] L Spitzner. *Honeypots: tracking hackers*. Addison-Wesley, Boston, 1st edition, 2003.