Seminário de Iniciação Científica
Universidade do Estado de Santa Catarina
27º SIC UDESC

# Análise de varreduras de portas contra tagged virtual LAN em nuvens computacionais OpenStack com honeypots de baixa interatividade

Nicolas Peter Lane[1], Charles Christian Miers[2]

[1]Acadêmico do Curso de Ciência da Computação DCC/CCT – PROBIC/UDESC 2016/1 – nicolas@colmeia.udesc.br
[2]Orientador, Departamento de Ciência da Computação DCC/CCT – charles.miers@udesc.br

Palavras-chave: Segurança. VLAN tagging. Nuvens computacionais.

A computação em nuvem traz uma nova tendência para o seu futuro com diversas aplicações em linhas de pesquisa e de mercado. No entanto, tal mudança de paradigma causa grande preocupação com segurança, uma vez que é de conhecimento científico a escalabilidade com que vulnerabilidades são exploradas em sistemas computacionais. Assim, como os consideráveis impactos sobre os serviços relativos às organizações envolvidas em tais incidentes. 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. Nesse contexto, não foi possível identificar a existência de referências relativas a redes segmentadas *VLAN tagging* (VLANT) em nuvens computacionais abertas do tipo *Infrastructure-as-a-Service* (IaaS) usando OpenStack voltadas à segurança, a fim de verificar se os princípios básicos da *Information Security* (IS) são satisfeitos nos serviços oferecidos pela mesma. Deste modo, esta pesquisa identifica ameaças factuais na infraestrutura interna de uma nuvem computacional e a sua mitigação por meio da análise de um vetor de vulnerabilidades contra VLANT que reside na infraestrutura de uma nuvem computacional, a fim de identificar quais destas apresentam-se como ameaças capazes de sobrepujar os mecanismos de segurança de nuvens computacionais baseadas no OpenStack utilizando-se de *honeypots* de baixa interatividade. A *Fig.* 1 ilustra um cenário de experimentação.

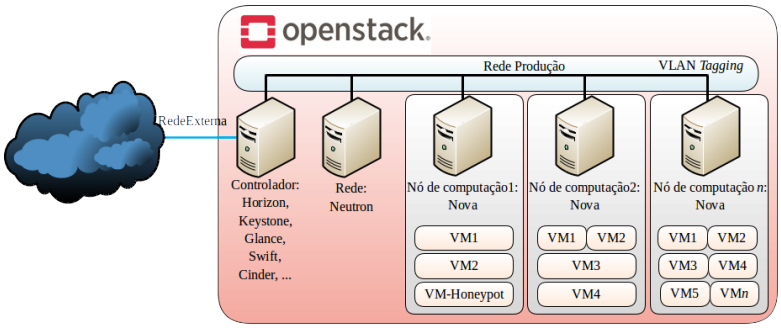


**Fig. 1:** *Cenário de experimentação*

Com este fim, vide *Fig. 1,* é proposta realizar a implantação de *honeypots* em duas redes internas à nuvem computacional. Uma rede de testes isolada e composta de três nós (*i.e., honeypot*, atacante, e armazenamento de *logs*) e outra na rede de produção, ambas internas à infraestrutura da nuvem computacional do LabP2D. Na rede de testes o *honeypot* dispõe de serviços que possuam as vulnerabilidades vide o vetor, como apresentado na *Tab. 1.*

| Ataque | CAM Table | protocolo ARP | Trunking | VPQ | CDP | Switch | BPDU |
|---|---|---|---|---|---|---|---|
| CAM Table Overflow | X | | | | | | |
| ARP Attack | | X | | | | | |
| Switch Spoofing | | | X | | | | |
| Double Tagging Attack | | | X | | | | |
| VPQ Attack | | | | X | | | |
| CPD Attack | | | | | X | | |
| Multicast Brute-Force Attack | | | | | | X | |
| Random Frame-Stress Attack | | | | | | X | |
| STP Attack | | | | | | | X |
| Frequência | 1 | 1 | 2 | 1 | 1 | 2 | 1 |

**Tab 1:** *Vetor de vulnerabilidades exploradas em VLANs*

De modo, que a sua exploração ofereça risco factual à infraestrutura da organização. Tais serviços quando explorados pelo atacante resultam em uma catalogação de dados (*logging*) respectiva às condições do ataque (*e.g.*, data, horário, endereço IP do host usado pelo atacante, *etc.*). Este *logging* por sua vez será enviado ao *host* de armazenamento, que uma vez processado, resulta em gráficos que permitam a análise da presente situação da rede de testes. Vide tal análise, na rede de produção os *honeypots* dispõem apenas das vulnerabilidades que mostrarem-se críticas vide o ambiente de testes. Deste modo, na rede de produção não haverá qualquer modificação na configuração já existente na rede. Sendo assim, o ambiente de produção é capaz de obter resultados reais do uso de *honeypots* de baixa interatividade, provendo a organização meios efetivos de realizar análises referentes ao tráfego que interage com sua infraestrutura de rede e deste modo fornecendo parâmetros aos administradores da mesma para corrigir tais vulnerabilidades.

Com o propósito de tornar tal fim possível, uma pesquisa aprofundada em *honeypots* foi desenvolvida que resultou em uma taxonomia flexível e concisa submetida na PST2017 e em um artigo de segurança voltado a ambientes computacionais de alto desempenho publicado e apresentado no ERAD2017. Atualmente o projeto visa concluir os testes com *honeypots* e realizar uma nova publicação na CLOSER2018.

Referências:


Gonzales, D., 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, no. 99 (2015): 1–1. doi:10.1109/TCC.2015.2415794.

Malyuk, A., and N. Miloslavskaya. “Information Security Theory for the Future Internet.” In *2015 3rd International Conference on Future Internet of Things and Cloud (FiCloud)*, 150–57. ROME: IEEE, 2015. doi:10.1109/FiCloud.2015.12.