Evento	Salão UFRGS 2016: SIC - XXVIII SALÃO DE INICIAÇÃO CIENTÍFICA DA UFRGS
Ano	2016
Local	Campus do Vale - UFRGS
Título	Mitigação e Detecção de Ataques em Redes SDN utilizando NFV
Autor	PEDRO HENRIQUE ARRUDA FAUSTINI
Orientador	ALBERTO EGON SCHAEFFER FILHO

Mitigação e Detecção de Ataques em Redes SDN utilizando NFV

Autor: Pedro Henrique Arruda Faustini | **Orientador**: Dr. Alberto Egon Schaeffer Filho
Instituição: Universidade Federal do Rio Grande do Sul (UFRGS)

Redes de computadores são formadas a partir da conexão de hosts. Tal conexão ocorre por meio de troca de pacotes, conduzida por switches e roteadores. Tradicionalmente, para se alterar o comportamento desses dispositivos é necessário modificá-los um a um - o que pode ser custoso. Em uma rede definida for software (*software defined network,* ou SDN), por outro lado, a maneira com que esse encaminhamento é feito é definida por um software controlador, que tem visão global da rede. Ele confere programabilidade aos administradores e torna o gerenciamento do fluxo de pacotes mais simples, pois fica desacoplado do hardware. Apesar dessa flexibilidade, redes SDN estão sujeitas a diversas ameaças, o que torna necessária a investigação de mecanismos de detecção e mitigação de ataques.

É importante para a rede manter níveis aceitáveis de operação frente a eventos como ataques ou sobrecarga operacional. Uma forma de atingir isso é monitorá-la, por exemplo, verificando quais portas de cada host estão abertas, o que pode indicar uma brecha para ataques. Tipicamente, módulos que realizam funções de monitoramento são implementados sobre hardware dedicado, otimizado para a execução de tarefas específicas. Tais módulos são chamados de *middleboxes*. Contudo, recentemente tem se tornado popular a noção de virtualização de rede (*Network Function Virtualization*, ou NFV), cujo objetivo é substituir tais middleboxes por software executado em hardware de propósito geral.

Neste contexto, o presente trabalho investiga mecanismos para detectar ataques e reagir da forma mais apropriada para mitigá-los. Vislumbra-se que tais mecanismos possam ser providos na forma de NFVs dispostas em diferentes pontos na rede. Até o momento, foi desenvolvido um módulo que varre as *flow-tables* dos switches presentes na rede e armazena em um banco de dados quais endereços IP estão a eles conectados. Posteriormente, um host na rede acessa essas informações e invoca outro módulo que realiza um *port scan* (verifica quais portas estão abertas em cada host) nele e nos demais encontrados. Esse escaneamento informa quais portas e serviços estão ativos em cada máquina, o que norteia a busca por pontos na rede que possam ser alvo de ataques. Este módulo foi desenvolvido na linguagem Python e utiliza a ferramenta Nmap para executar o escaneamento de maneira concorrente, armazenando as informações coletadas em um banco de dados.

Verificou-se que o tempo de escaneamento aumenta linearmente de acordo com o número de hosts na rede. Também observou-se que leva-se mais tempo para escanear um host que tenha todas as portas fechadas em comparação a outro com alguma aberta (possivelmente em função da espera por timeout na ferramenta de escaneamento).

Os próximos passos incluem a conversão do módulo que realiza *port scan* para uma NFV usando o framework *Escape*. Estamos investigando a aplicação de técnicas baseadas em *reinforcement learning* para decidir qual NFV seria invocada para tratar um evento maligno. Dessa forma, tem-se como objetivo definir a tomada de ações de mitigação com base em uma recompensa, onde deve-se utilizar o algoritmo para descobrir quais ações conferem as maiores recompensas. Uma recompensa aqui poderia ser, por exemplo, o tempo levado para mitigar um ataque. Para ataques idênticos, distintas recompensas seriam obtidas iniciando a mitigação por diferentes NFVs, devido à colocação dessas na topologia da rede.

Espera-se com este trabalho contribuir para tornar redes SDN mais seguras contra ataques, mesclando características de programabilidade de SDN com a maleabilidade de NFV. Futuramente, há a possibilidade de se explorar um espectro mais amplo de detecção e mitigação que não se restrinja somente a *port scanning*.