Proposta de Ambiente Experimental para Avaliação de Sistemas de Detecção de Intrusão

Lana Letícia Schuster dos Santos, Renato Bobsin Machado, Gustavo dos Santos Vieira
Laboratório de Pesquisa em Segurança Computacional (LAPSEC)
Universidade Estadual do Oeste do Paraná (UNIOESTE)
Foz do Iguaçu, Brasil

***Abstract*—The increasing number of cyber security incidents over the years brings the urge for application of methodologies to prevent and detect malicious activity. LAPSEC has been studying several approaches on intrusion detection by applying artificial intelligence, and there is a need to evaluate the efficiency and effectiveness of these methodologies. This work proposes an experimental environment for the simulation of network traffic considering normal and malicious to analyze the behavior of intrusion detection approaches.**

Keywords—Detection of computational attacks; evaluation; computer attacks; network traffic simulation; artificial intelligence.

***Resumo*—Com o crescente número de incidentes de segurança computacional ao passar dos anos, métodos de prevenção e detecção de atividades maliciosas se fazem necessários. O LAPSEC vem estudando diversas abordagens de detecção de intrusão aplicando inteligência artificial, e com isso surge a necessidade de avaliar a eficiência e eficácia destas técnicas. Esse trabalho propõe um ambiente experimental para a simulação de ataques computacionais atuais, de modo que possa ser usado para a avaliação de métodos de detecção de intrusão.**

Palavras-chave—Detecção de ataques; avaliação; ataques computacionais; simulação de tráfego de rede; inteligência artificial.

I. Introdução

A segurança computacional se tornou indispensável no atual contexto tecnológico, onde existe uma alta taxa de compartilhamento de informações e tráfego de dados [1]. Observa-se ainda um crescente número de incidentes de segurança reportados no decorrer dos anos, como apresenta as estatísticas do CERT.br (Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil).

Tendo em vista esse cenário, o estudo de Sistemas de Detecção de Intrusão tem recebido atenção no campo da computação [2]. Tais mecanismos atuam no monitoramento de redes de computadores com a finalidade de identificar eventos de caráter malicioso [3].

Existem diversas abordagens de sistemas de detecção de intrusão em estudo. Para a avaliação dessas abordagens podem ser utilizadas bases de dados, porém, atualmente ainda são poucas bases de dados de eventos de rede, e que possivelmente estão desatualizadas [4].

Neste trabalho propõe-se a criação de um ambiente computacional específico para a simulação de ataques computacionais, permitindo assim que os eventos de redes gerados por tais ataques possam ser utilizados como grupo controle para a avaliação de métodos de detecção de intrusão.

II. Ataques computacionais

A. Classificação de Ataques

A tarefa de classificação de ataques computacionais se faz importante para o entendimento do problema, e a aplicação correta de medidas de prevenção e detecção desses incidentes, ainda que não exista um padrão aceito [5].

Em seu trabalho, Bishop [6] propôs uma taxonomia voltada para vulnerabilidades encontradas em sistemas Unix. Sua taxonomia apresenta seis eixos, onde cada vulnerabilidade é classificada em cada um deles. Tais eixos informam a natureza da vulnerabilidade, tempo em que foi introduzida ao sistema, quais os ganhos relacionados à sua exploração, o que afeta, componentes mínimos para que sua exploração seja possível, e a fonte de sua identificação [7].

Howard [8] construiu sua taxonomia voltada para incidentes computacionais, onde é apresentada como um fluxo de processo, que consiste em cinco estágios:

- Atacantes: Tipo de atacante, podendo ser *hacker*, espião, terrorista, concorrente de uma empresa, entre outros;
- Ferramentas: Meio de exploração de vulnerabilidades de dispositivos ou rede;
- Acesso: Etapa execução dos ataques, a fim de adquirir acesso não autorizado aos dados armazenados ou em transmissão;
- Resultados: Consequência resultante do ataque, como por exemplo, negação de serviço, descoberta de informações, entre outros;
- Objetivos: Motivo do ataque.

Outra abordagem de classificação foi proposta por Wood e Stankovic [9], a qual realiza uma categorização específica de ataques de Negação de Serviço, podendo assim auxiliar no melhor entendimento deste tipo de ataque [5].

Em sua tese, Kendall [10] realizou um trabalho para a criação de uma base de dados a partir do tráfego de rede, onde haviam conexões oriundas tanto de ataques computacionais quanto tráfego considerado não malicioso. Para a identificação dos exemplos gerados, foi utilizado um *label* que poderia receber o valor "normal" ou o nome do ataque.

Cada um desses ataques utilizados como identificador se enquadram em uma das quatro grandes categorias utilizadas por Kendall, sendo elas: Probe, Remote to Local (R2L), User to Root (U2R) e Denial of Service (DoS).

Atualmente, a base de dados KDD CUP 99, e sua derivada, NSL-KDD são utilizadas na avaliação de sistemas detecção de intrusão, por serem uma das poucas bases públicas disponíveis [11]. Por essa razão, o seu modo de classificação de ataques será abordada com maiores detalhes nesse trabalho.

B. Probing

Ataques do tipo *probing*, ou no português sondagem, geralmente são efetuados antes de iniciar efetivamente um ataque. São ataques automatizáveis, com o objetivo de coletar informações sobre o alvo, a fim de identificar possíveis vulnerabilidades, o que auxilia na escolha de ferramentas e técnicas de exploração [12].

Pode ser efetuado sobre uma rede, onde é possível descobrir os dispositivos conectados à ela, ou diretamente à esses dispositivos, o que permite verificar informações como o sistema operacional do alvo, serviços ativos, assim como possivelmente suas versões, entre outras informações. Esse ataque consiste basicamente no envio de pacotes à essas portas, e verificar a resposta obtida [13].

C. Remote to Local

Quando um atacante realiza a exploração de vulnerabilidades, consegue acesso à rede ou à máquina da vítima, é um ataque chamado de Remote to Local [11].

De acordo com [10] e [14], existem diversas formas de se adquirir acesso ao alvo, como por exemplo a aplicação de técnicas de *bruteforce*, onde o atacante testa diferentes combinações de usuário e senha repetidas vezes, até que encontre uma combinação existente. Pode ser aplicado ainda engenharia social, na tentativa de enganar a vítima, podendo passar informações de login para o atacante [15].

D. User to Root

Após o *Remote to Local* ser efetuado, o atacante obtêm acesso como usuário desprivilegiado da máquina alvo. O próximo passo é efetuar a exploração de vulnerabilidades locais para obter controle total da vítima.

Existem diversas técnicas de escalação de privilégios. O invasor pode se aproveitar de credenciais fracas, interceptar tráfego de rede para identificar informações que possam conceder acesso, má configuração de serviços, exploração de vulnerabilidades do ambiente, entre outras abordagens [16].

E. Denial of Service

Está técnica consiste na realização de inúmeras requisições são a um recurso, de tal modo que o mesmo não é capaz de responder nem mesmo às requisições legítimas por estar totalmente ocupado [14]. Esse tipo de ataque pode ser destinado à um alvo específico ou à uma rede, com o objetivo de congestioná-la [17].

III. Sistemas de detecção de intrusão

Como apresentado em [4], sistemas de detecção de intrusão são projetados para capturar e analisar informações que trafegam na rede, a fim de identificar descumprimentos dos princípios da segurança. Esses incidentes possuem diversas causas, como por exemplo vírus de computador, atacantes tentando obter acesso à sistemas através da Internet, ou um usuário fazendo mal uso de seus privilégios [19].

Existem diversas abordagens de sistemas de detecção de intrusão já consolidadas no mercado tanto *open-source*, quanto ferramentas pagas. Como exemplo, pode-se citar os sistemas Snort (https://snort.org/), Bro (https://www.bro.org/), Suricata (https://suricata-ids.org/), OSSEC (https://www.ossec.net/), Tripwire (https://www.tripwire.com/), entre outros.

Na literatura estão presentes diversas abordagens de detecção de intrusão que empregam inteligência artificial, com o intuito de otimizar a eficiência e eficácia, assim como complexidade de espaço e tempo de detecção.

No trabalho de Souza [20], é apresentada uma abordagem de detecção de intrusão híbrida, composta por uma rede neural artificial (RNA) *feedforward* do tipo *Multilayer Perceptron*, e a aplicação do algoritmo K-Nearest Neighbors (KNN). Seu trabalho tem como objetivo unir as vantagens dos dois métodos, ou seja, a rápida detecção da RNA juntamente com a alta taxa de acerto do KNN.

A instância a ser classificada passa primeiramente pelo modelo RNA, gerando uma saída entre -1 (comportamento não intrusivo) e 1 (comportamento intrusivo). Aquelas instâncias com valores intermediários são submetidos ao algoritmo KNN [20].

IV. MATERIAIS E MÉTODOS

O propósito deste trabalho consiste na construção de um ambiente experimental para a simulação de ataques computacionais atuais, com o intuito de construir um uma base de eventos atualizada, que poderá ser utilizada para a avaliação de métodos de detecção de intrusão.

Tal ambiente computacional poderá ser utilizado também para a geração e atualização de bases de eventos de redes a partir de ataques computacionais, assim como de tráfego de rede normal.

Para a construção do ambiente experimental foi utilizada a virtualização Oracle VM Virtualbox, onde cada uma das quatro máquinas virtuais configuradas possui o sistema operacional Debian 9 “Stretch”.

A máquina hospedeira do ambiente virtual possui as seguintes especificações:

- Sistema Operacional Windows 10, 64 bits;
- Processador Intel i5-7200U 2.50 GHz 2.71 GHz;
- RAM 8 GB.

Como ilustrado na Figura 1, o ambiente contará com uma máquina destinada a simular o tráfego de rede, que será composto por eventos normais e de caráter malicioso.

As classes de ataque que serão executadas seguirá a classificação como em [10], ou seja, ataques do tipo *Probing*, *Remote to Local*, *User to Root* e *Denial of Service*.

Dentre os ataques *Probing* que serão executados estão: SYN Scan, ACK Scan, FIN Scan, XMAS Scan, UDP Scan, ICMP Scan, e IGMP Scan. Esses ataques consistem basicamente no envio pacotes às portas do alvo, e aguardam a resposta desta.

Os ataques do tipo *Denial of Service* selecionados foram: UDP Flood, SYN Flood, ICMP Flood, ACK Flood, FIN Flood.

Sobre as demais classes de ataque serão realizados ainda ataques do tipo *Bruteforce*: isso será realizado por meio de uma *wordlist*, onde serão realizadas repetidas tentativas de obter possíveis credenciais do sistema; e *Buffer Overflow*, ou no português, transbordamento de dados, ou seja, um programa ultrapassa o tamanho do *buffer* ao escrever dados, o que permite a inserção de código malicioso na máquina da vítima.

As ferramentas utilizadas para a aplicação desses ataques serão: Nmap, Hping3, Metasploit, THC Hydra, e alguns scripts que exploram determinadas vulnerabilidades disponíveis no site Exploit DB (https://www.exploit-db.com/).

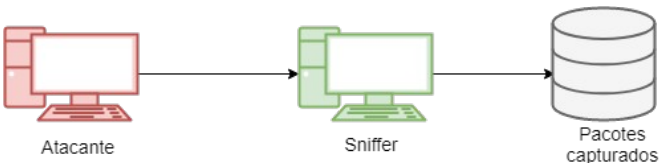

Fig. 1. Geração de tráfego de rede.

O tráfego gerado será capturado por uma máquina contendo um *sniffer*, Wireshark 2.6.3, que armazenará os pacotes no formato “.pcap”. Após essa etapa de geração de tráfego, esses pacotes serão submetidos aos métodos selecionados para avaliação de [20] e um sistema de detecção de intrusão consolidado no mercado, o Snort 2.9.11.1, como apresentado na Figura 2.

Os pacotes submetidos ao Snort estarão no formato PCAP, porém, para as abordagens de [20], os pacotes deverão passar por uma extração de atributos para que o formato seja compatível com a entrada aceita desses algoritmos.

V. RESULTADOS PARCIAIS E CONCLUSÃO

Os resultados parciais incluem o estudo dos elementos tecnológicos, a definição do método experimental, e a realização de simulações da captura de pacotes a partir da submissão de ataques *Probing* e *Denial of Service*.

Nas próximas etapas devem ser realizados os demais ataques computacionais definidos, assim como a captura dos respectivos pacotes. Posteriormente será realizada uma avaliação comparativa em relação a eficácia de dos métodos de detecção de intrusão selecionados.

Espera-se, por meio da realização deste trabalho, a construção de um ambiente computacional capaz de auxiliar na construção de bases de eventos computacionais, a partir da simulação de ataques atuais, podendo servir como grupo controle para distintos métodos de detecção de intrusão.

Após a conclusão da etapa de geração de tráfego de rede e submissão desses pacotes aos métodos de detecção de intrusão selecionados, será realizada uma comparação entre os resultados obtidos de [10] com os resultados deste trabalho, onde foram simulados ataques atuais, já que a base NSL-KDD, utilizada na geração e avaliação do modelo de [10], está potencialmente desatualizada em relação às abordagens de ataques computacionais existentes atualmente.

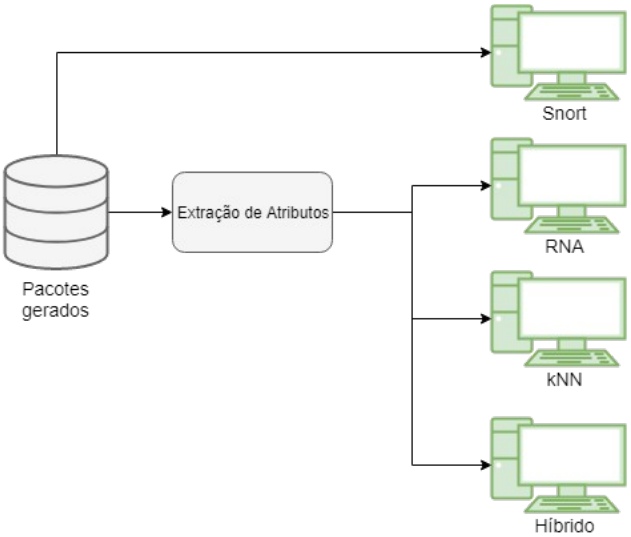

Fig. 2. Submissão dos pacotes capturados.

REFERENCES

[1] ÖZGÜR, A.; ERDEM, H. A review of kdd99 dataset usage in intrusion detection and machine learning between 2010 and 2015. PeerJ PrePrints, PeerJ Inc., 2016.

[2] CROSBIE, M.; SPAFFORD, G. Defending a computer system using autonomous agents,West Lafayetee: Dept. of Computer Sciences pp. 12–16, 1995.

[3] LIAO, H.-J. et al. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications, v. 36, n. 1, p. 16 – 24, 2013. ISSN 1084-8045.

[4] EL-HAJJ, W.; AL-TAMIMI, M.; ALOUL, F. Real traffic logs creation for testing intrusion detection systems. WIRELESS COMMUNICATIONS AND MOBILE COMPUTING, 2014.

[5] ONIK, M. H. et al. A novel approach for network attack classification based on sequential questions. Annals of Emerging Technologies in Computing, 2018.

[6] BISHOP, B. A.; taxonomy of UNIX system and network vulnerabilities, 1995.

[7] HANSMAN, S. A. taxonomy of network and computer attack methodologies, 2003.

[8] HOWARD, J. D. An Analysis Of Security Incidents On The Internet 1989-1995.,1997.

[9] WOOD, A. D.; STANKOVIC, J. A. A taxonomy for denial-of-service attacks in wireless sensor networks. 2004.

[10] KENDALL, K. A database of computer attacks for the evaluation of intrusion detection systems. In: DARPA OFF-LINE INTRUSION DETECTION EVALUATION, PROCEEDINGS DARPA INFORMATION SURVIVABILITY CONFERENCE AND EXPOSITION (DISCEX), VOL. [S.l.: s.n.], 1999.

[11] TAVALLAEE, M. et al. A detailed analysis of the kdd cup 99 data set. In: IEEE. Computational Intel ligence for Security and Defense Applications, 2009. CISDA 2009. IEEE Symposium on. [S.l.], 2009. p. 1–6.

[12] ALLODI, L.; MASSACCI, F. Security events and vulnerability data for cybersecurity risk estimation. Risk Analysis, 2017.

[13] BHUYAN, M. H.; BHATTACHARYYA, D. K.; KALITA, J. K. Surveying port scans and their detection methodologies. The Computer Journal, 2011.

[14] HOQUE, N. et al. Network attacks: Taxonomy, tools and systems. Journal of Network and Computer Applications, 2013.

[15] GOODRICH, M.; TAMASSIA, R. Introdução à Segurança de Computadores. [S.l.]: Bookman, 2013. ISBN 9788540701939.

[16] HERIYANTO, T.; ALLEN, L.; ALI, S. Kali Linux: Assuring Security By Penetration Testing. [S.l.]: Packt Publishing, 2014.

[17] STALLINGS, W. Criptografia E Segurança De Redes. [S.l.]: PEARSON BRASIL, 2014.

[18] HUSSAIN, A. et al. A framework for classifying denial of service attacks. In: SIGCOMM'03 Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications. [S.l.: s.n.], 2003. p. 99–110.

[19] SCARFONE, K. A.; MELL, P. M. SP 800-94. Guide to Intrusion Detection and Prevention Systems (IDPS). Gaithersburg, MD, United States, 2007.

[20] SOUZA, C. A. d. et al. Método híbrido de detecção de intrusão aplicando inteligência artificial. Universidade Estadual do Oeste do Paraná, 2018.