MODELO DE DETECÇÃO DE INTRUSÃO POR BRUTE FORCE UTILIZANDO SCAPY

Alexandre Gomes Daniel (Acadêmica do Curso de Licenciatura em Computação - IFTO)
Adeilson Marques da Silva Cardoso (Orientador)
Email: alexandre.daniel@estudante.ifto.edu.br, Adeilson@ifto.edu.br

1.INTRODUÇÃO

Ao longo dos anos, a tecnologia progrediu rapidamente, penetrando cada vez mais na vida cotidiana das pessoas e mudando profundamente a forma como a sociedade funciona. Inserido num mundo de crescente autonomia, este contexto facilita a transmissão de dados, muitos dos quais são altamente sensíveis (Nursetyo, Setiadi e Rachamawanto). No entanto, esta evolução também resultou num aumento significativo e contínuo de tentativas de ataques cibercriminosos, resultando num cenário desafiador e em constante mudança.

Um ataque de força bruta ou “brute force attack” é baseado em uma abordagem de tentativa e erro acionando uma solicitação de acesso com valores possíveis, como métodos e chaves de acesso, combinações de conta e senha do sistema e assim por diante (Diorio, Serafim, Alves e Meira, 2019) . O objetivo é romper a barreira de segurança e ter acesso aos dados de interesse. Para atingir esse objetivo, o invasor cria uma lista contendo diversas combinações possíveis de letras, formando o chamado “dicionário”. Um agente malicioso testa diversas combinações desses dicionários até encontrar a ordem correta. Milhares de combinações podem ser testadas a cada segundo.

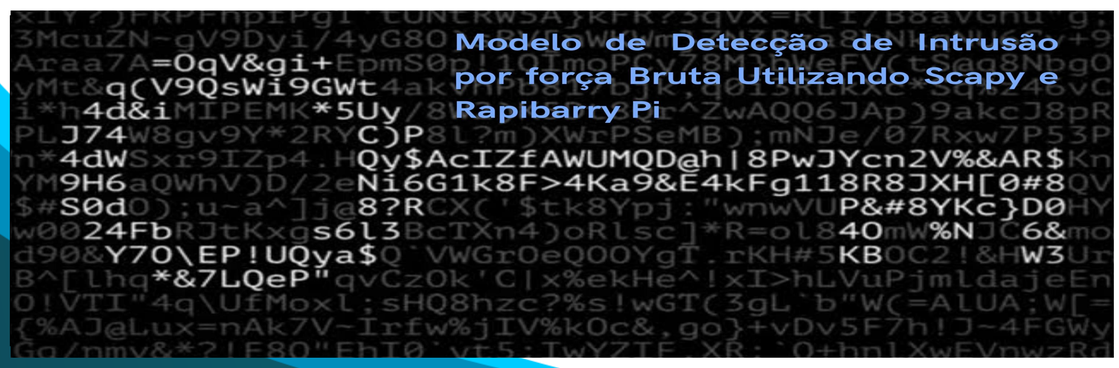
2. MATERIAIS E MÉTODOS

Para a realização dos testes para desenvolvimento do modelo foi feito uma configuração das redes virtualizadas consistindo em duas máquinas virtuais, cada uma desempenhando uma função específica no experimento. A primeira máquina virtual foi preparada com software Hydra e foi capaz de emular um ataque de força bruta. Enquanto isso, uma segunda máquina virtual foi configurada e instalada o openServer para executar um serviço exigia autenticação SSH, além suporte adicional para Scapy, uma ferramenta para captura e análise aprofundada de tráfego de rede. Posteriormente o Raspibarry Pi foi alocado dentro da rede para poder realizar a captura dos dados. O núcleo do experimento foi o desenvolvimento de algoritmos de análise de tráfego projetados usando a linguagem de programação Python. Este algoritmo é usado para identificar padrões suspeitos que aparecem nos fluxos de tráfego.

3. RESULTADOS E DISCUSSÃO

Nesta seção, discutiremos sobre o resultado do modelo de detecção de ataque de força bruta utilizando a biblioteca scapy e o Rapibarry Pi analisando a sua eficácia em proteger a vítima de um possível tentativa de intrusão utilizando brute force.

O computador atacante enviava os requerimentos de conexão para a vítima configurada com o IP 172.168.53.28 na porta padrão do SSH, porta 22. Ao ocorrer o envio dos requerimentos para esta porta, o modelo de detecção analisava cada pacote que estará passando na rede durante sua ativação com a função *sniff(),* usada para “farejar” os pacotes presentes na rede, filtrando para análise mais detalhada os pacotes do protocolo de rede TCP com destino na porta 22. Após capturar o primeiro pacote aplicado no filtro, o programa inicia um contador de tempo a partir do horário descrito na máquina, como também um segundo contador que irá aumentar de acordo com a quantidade de pacotes filtrados transitando pela rede contendo como limites de 10 tentativas de acesso por minuto, levando em consideração que o acesso remoto será utilizado com a taxa de quantidades de erros digitada por pessoas.



Antes de iniciar a tentativa de bloqueio, será verificado ser um arquivo chamado ssh_bruteforce.log está criado dentro do sistema, verificando de já aconteceu alguma outra tentativa de ataque do IP do invasor, caso não exista este arquivo ele será criado e irá guardar o IP do atacante para evitar futuras tentativas de atacar a vítima. Em seguida é mandado um comando de iptables para o firewall da vítima, recusando qualquer requerimento do IP atacante, notificando se a regra de iptables caso sucedida.

Como terceiro e último processo, foi configurado para enviar um e-mail pré-determinado via protocolo SMTP para o administrador da vítima avisando-o de uma possível tentativa de intrusão de ataque de força bruta, contendo dentro da mensagem o IP do atacante, e que foi tomado as devidas providências de bloqueios por parte de vítima.

4. CONCLUSÃO

Clonclui-se que o modelo de detecção de intrusão de ataque de força bruta utilizando a a biblioteca scapy e Rapibarry Pi se mostou funcional de forma eficiente conseguindo analisar os tráfegos presentes dentro da rede de computadores, protejendo a rede de ameaças ocacionadas por ataques de força bruta utilizando um processo rápido e otimizado reduzindos custos na implementação ocasionando na diminuição da utilização de recursos de um computador, máquina e servidores.

5. REFERÊNCIAS

WANJAU, Stephen K. WAMBUGU, Geoffrey M. KAMAU, Gabriel N. **SSH-Brute Force Attack Detection Model based on Deep Learning**, International Journal of Computer Applications Technology and Research, 2021. Volume 10, p. 42-50. Disponível em: <ijcatr10011008.pdf>. Acesso em: 23 maio 2023.

PARK, Jeonghoon. KIM, Junsu. GUPTA, B. B. PARK, Namje. **Network Log-Based SSH Brute-Force Attack Detection Model**, Tech Science Press, 2021. Computers, Materials & Continua, p. 887-901. Disponível em: <CMC | Network Log-Based SSH Brute-Force Attack Detection Model (techscience.com)>. Acesso em: 28 maio 2023.

DIORIO, Rafael F. SERAFIM, Edivaldo. ALVES, Karlan R. MEIRA, Matheus C. **Ataques de Força Bruta: Um Estudo Prático**, Brazilian Technology Symposium, 2019. Disponível em: <https://lcv.fee.unicamp.br/images/BTSym-19/Papers/040.pdf>. Acesso em: 13 jun 2023.