UM PROTÓTIPO PARA DETECÇÃO DE ANOMALIAS COM SYSTEMTAP

LIMA, Felipe da Silva (felipesl121@gmail.com) [1]; DE PAULA, Fabrício Sérgio (fabricio@comp.uems.br) [2]

[1] Aluno do curso de Ciência da Computação, bolsista PIBIC/UEMS

[2] Professor orientador do curso de Ciência da Computação da UEMS

Um sistema de detecção de intrusão (IDS do termo em inglês *Intrusion Detection System*) é importante no contexto da segurança computacional porque permite identificar ataques em andamento ou já realizados, sendo essencial no combate de ameaças internas e externas à segurança de corporações. Um sistema de detecção de intrusão automatiza o monitoramento e análise de eventos em um sistema em busca da ocorrência de problemas de segurança. Os sistemas de detecção de intrusão possuem três metas principais, que são: identificação, atribuição de responsabilidade e resposta. O objetivo geral deste projeto é utilizar a ferramenta SystemTap para construir um protótipo para detecção baseada em anomalia em processos do sistema operacional Linux. Durante o desenvolvimento do projeto, as atividades realizadas foram: estudos aprofundados sobre chamadas ao sistema operacional Linux; implementação de um mecanismo para especificação de políticas de monitoramento de processos usando SystemTap; Construção de um protótipo para detecção de anomalias em processos de acordo com políticas de monitoramento pré-observadas usando SystemTap; coleta dos resultados experimentais e elaboração das conclusões. Para os testes alguns programas foram especificados na política de monitoramento para então ao capturar as chamadas ao sistema e verificar a eficácia e o seu impacto. Os programas escolhidos para testar o protótipo foram: o *ls* (programa padrão Linux que lista o conteúdo de um diretório) utilizando uma listagem recursiva em um diretório definido na política e utilizando uma repetição da execução da listagem; um programa feito pelo próprio autor que faz diversas conexões com um servidor local e cria um processo filho para cada conexão. O impacto causado no sistema foi feito medindo o tempo gasto para executar os programas com e sem o protótipo de detecção em execução. O uso de memória RAM (*Random Access Memory*) pelo protótipo também foi verificado. Como o SystemTap trabalha em ambiente *kernel* e usa *scripts* que são traduzidos para linguagem C e então compilado em um módulo *kernel* a eficiência na captura dos dados é alta. A facilidade para criar os *scripts* também é notória. A dificuldade encontrada foi ao utilizar códigos em linguagem C embarcado no *script*. Os códigos embarcados foram utilizados essencialmente para implementar a obtenção dos dados da política de segurança. Embora o SystemTap permita que um código em linguagem C seja diretamente introduzido no *script*, ela impõe alguns limites de implementação como por exemplo, alocação de memória. O conhecimento adquirido em Sistemas de Computação mais precisamente em Segurança Computacional é de grande valia pois dá uma nova visão sobre o assunto ao bolsista. Os autores agradecem à UEMS pelo apoio financeiro recebido durante a execução deste projeto.

Palavras-Chave: segurança, detecção de intrusão, SystemTap.