DESENVOLVIMENTO DE UMA HONEYNET EM UMA INSTITUIÇÃO DE ENSINO SUPERIOR[1]

Carlos Alfredo Weissheimer Junior[2], *Eduardo Leivas Bastos*[3]

O desenvolvimento da Internet tem gerado um avanço sem precedentes no compartilhamento de informações e aplicações. Esse avanço traz consigo inúmeros riscos de ataques virtuais. Cabe aos profissionais de TI (Tecnologia da Informação) encontrar soluções para que as informações não sejam acessadas e muito menos destruídas por pessoas não autorizadas. Portanto, é extremamente importante conhecer os mecanismos e as táticas dos ataques antes mesmo que eles sejam empregados e causem prejuízos. As *honeynets* foram imaginadas tendo este objetivo em mente. O objetivo principal deste trabalho é a implantação de uma *Honeynet* de interatividade média em uma instituição de ensino superior a fim de obter informações sobre o perfil dos ataques sofridos. Para a implantação da mesma, primeiramente foi instalado um *notebook* modelo Acer 5102WLI com processador turion 1.6Ghz 1GB de memória e disco rígido 100GB ao roteador *Enterasys* X PEDITION XP-2400-256 da Instituição de Ensino Superior. O *notebook* respondia pelo IP 200.19.250.86 e estava posicionado antes do controle de segurança da IES, não passando assim por nenhum *proxy* ou pelo *firewall*. Em seguida, o *daemon Honeyd* foi instalado e teve seus scripts de configuração personalizados para emular dois *honeypots*, um simulando uma máquina com sistema operacional *Linux* e outra Windows contendo alguns serviços como POP3, SMTP, FTP entre outros. A partir dos logs registrados, seguindo a topologia e os *scripts* mencionados anteriormente, foi possível com a ajuda da ferramenta *Honeyd sum*-v0.3 uma análise dos resultados obtidos em forma de gráficos e tabelas. Foram registradas 3712 tentativas de conexões ao protocolo TCP e mais 19 ao protocolo UDP sendo divididas entre os dois *honeypots*. Observou-se uma preferência pela máquina que simulava o SO Windows que registrou 2360 tentativas. Refinando mais a análise foram registradas 1251 tentativas na porta 445 (Serviço de compartilhamento de arquivos) sendo a de maior preferência dessas pessoas mal intencionadas. Além disto, o endereço IP mais registrado foi o 89.185.245.146 com 496 registros e a hora preferida pelos invasores com 606 tentativas foi às 16:00. Portanto, o uso de uma ferramenta que identifique e capture este tráfego mal intencionado para posteriormente analisá-lo tem uma grande importância para os profissionais que primam pela segurança da informação. A importância de uma *honeynet* em uma organização ficou bem clara com os resultados obtidos pelo trabalho. O número de tentativas de conexões alto para o tempo que ela passou em funcionamento, remete a uma constante busca de informações por pessoas mal intencionadas. E com registros dos gráficos que apontam serviços, protocolos, hora de preferência desta comunidade e também com os registros de ataques sofridos, fica mais fácil a análise das deficiências das ferramentas de defesas.

[1] WEISSHEIMER JÚNIOR, Carlos Alfredo. Hoynet: Um estudo Teórico e Prático. Novo Hamburgo, 2007. (Trabalho de Conclusão de Curso - Ciências da Computação) Centro Universitário Feevale, 2007.

[2] Aluno graduado Feevale em ciência da computação, pós-graduando Feevale.
[3] Mestrando Unisinos, pós-graduado em ciência da computação UFRGS e graduado em ciência da computação UFRGS.