7
Conclusão

Este trabalho apresentou, inicialmente, a necessidade e importância – tendo em vistas aspectos de segurança da informação - de processos de monitoração e detecção de incidentes e intrusões. As organizações e corporações modernas estão cada vez mais dependentes de sistemas de informação e de redes que os interliguem. A Internet, em especial e como uma rede universal, tem se tornado instrumento e meio para realização das mais diversas operações antes realizadas apenas fisicamente. O conjunto de protocolos e aplicações que suportam estas redes e todas estas operações não considerou, na época do seu desenvolvimento, uma série de aspectos relacionados à segurança da informação e a redução de vulnerabilidades, hoje considerados essenciais, para um ambiente "hostil" como o da Internet atual. Investimentos crescentes em produtos, soluções e serviços que melhorem os processos e tecnologias associadas a segurança vem sendo realizados por organizações em todo o mundo. Entretanto a maioria dos recursos tem sido destinados a medidas preventivas. Apesar de sua importância, é vital que as organizações reconheçam que medidas preventivas por si só não são suficientes. Medidas preventivas, por melhores que sejam, podem falhar. É preciso estar preparado para detectar quando e se determinada medida preventiva falhar.

Sistemas de detecção de intrusão são ferramentas essenciais no auxílio a etapa de detecção de falhas não previstas e mesmo de falhas em medidas preventivas adotadas. Este trabalho apresentou a classificação de sistemas de detecção de intrusão bem como realizou revisão bibliográfica de trabalhos da área. Apresentou em seguida, taxonomia para padrões de ataques e intrusões em sistemas computacionais, proposta em projeto desenvolvido em projeto DARPA/MIT.

A maioria dos sistemas de detecção de intrusão existentes depende de conhecimento humano especialista codificado para funcionar. São sistemas especialistas, que apresentam uma enorme desvantagem: a incapacidade de detectar novos padrões de ataques e intrusões. Explorar a capacidade de generalização das redes neurais artificiais, em especial as redes Perceptron de

múltiplas camadas, como solução para detecção de intrusão em redes de pacotes foi o objetivo deste trabalho. O grande desafio para realização de um estudo como este reside na necessidade de uma base de dados realista e identificada de padrões normais e anômalos (representando as mais variadas técnicas de intrusão e ataque). O projeto DARPA/MIT realizado em 1998/1999 para avaliação de sistemas de detecção de intrusão existentes gerou a base de dados utilizada neste trabalho.

A análise de diversos cenários, com variações nas entradas utilizadas para a rede neural, no conjunto de treinamentos e na determinação da resposta da rede provou a viabilidade do emprego desta ferramenta para o problema de detecção de intrusão. Foi apresentado ainda um cenário em que as redes treinadas tinham suas respostas agrupadas para fornecer uma resposta final, criando assim um comitê de redes neurais especialistas. Mecanismos clássicos de avaliação de respostas de várias redes para elaboração de uma resposta única, com decisão por voto majoritário e pela média, foram analisados. Finalmente um algoritmo adaptativo para seleção das respostas a serem utilizadas e dos pesos de cada resposta foi desenvolvido e apresentado com o objetivo de aumentar a taxa de acerto e reduzir a taxa de falso positivo. A base para o desenvolvimento deste método consiste na análise dos resultados obtidos com as redes simuladas juntamente com a análise dos principais erros por elas cometidos. A combinação de redes neurais MLP com o algoritmo proposto gera um sistema de detecção híbrido: combina características de inteligência computacional (sistema de detecção baseado em comportamento) com características de um sistema especialista (baseado em conhecimento prévio). Mesmo com a obtenção de bons índices para os classificadores analisados e propostos, acredita-se que sistemas como estes teriam melhores resultados em situações práticas se combinados com sistemas comerciais tradicionais.

Adaptar este problema para a utilização de redes neurais RBF (função de base radial), em especial redes PNN (Probabilistic Neural Networks) e avaliar o desempenho destas redes é uma sugestão para trabalhos futuros. O desenvolvimento de um sistema de geração automatizada de padrões (normais e de ataque) para renovar o treinamento das redes, mantendo seu aprendizado útil, também é uma extensão possível para este trabalho.