Estudos de Caso de Segurança em Redes Sem Fio Utilizando Ferramentas para Monitoramento e Detecção de Ataques

Lucas da Silva Carlessi[1], Paulo João Martins[1]

[1]Curso de Ciência da Computação – Departamento de Ciência da Computação – Universidade do Extremo Sul Catarinense (UNESC) – Criciúma, SC - Brazil

lucascarlessi@gmail.com, pjm@unesc.net

Abstract. *Wireless networks are everywhere and, constantly, are targets of attacks. To provide proactive actions to the managers of these networks, some tools that monitor and detect attacks have been developed. These tools can be effective if they are used properly, offering competent management of safety features and warnings of possible attacks. This paper aims to present and discuss the concepts of wireless networks, methods of security, vulnerabilities and some attacks. Based on these concepts, methods are tested for efficiency in monitoring and attack detection using open source tools for Linux, Kismet and Beholder.*

Resumo. *As redes sem fio estão por toda a parte e, constantemente, são alvos de ataques. Para prover ações pró-ativas dos administradores dessas redes, algumas ferramentas que monitoram e detectam ataques foram desenvolvidas. Estas ferramentas podem ser eficientes se utilizadas adequadamente, proporcionando um gerenciamento competente dos recursos de segurança e alertas de possíveis ataques. Este artigo apresenta e discute os conceitos de redes sem fio, os métodos de segurança, as vulnerabilidades e alguns ataques existentes. A partir destes conceitos, é testada a eficiência no monitoramento e detecção de ataques utilizando as ferramentas de código aberto para Linux, Kismet e Beholder.*

1. Introdução

Redes sem fio são redes de computadores que permitem interligar, ao menos, dois equipamentos utilizando-se de ondas eletromagnéticas, sem a necessidade de uma estrutura física de cabeamento. Elas estão, cada vez mais, presentes no mundo devido à necessidade constante de conexão a rede dos vários equipamentos móveis (como notebooks e Personal Digital Assistants - PDA's) existentes no mercado [SGUAREZI 2007].

Atendem tanto o cenário doméstico quanto empresarial devido ao baixo custo e facilidade de instalação sem precisar modificar as instalações já existentes. Além de poder interligar redes privadas, é crescente o número de estabelecimentos como aeroportos e universidades que também disponibilizam o acesso sem fio para seus usuários [TANENBAUM 2003].

Com sua popularização, as redes sem fio se tornaram uma importante alternativa às redes cabeadas, devido à possibilidade e facilidade de suprir a falta de infraestrutura nas empresas e residências. Assim, a questão de segurança deve ser tratada com muito mais importância dado o valor que as informações têm para os proprietários da rede [SILVA; SOUZA 2003].

2. Redes Sem Fio

Utilizam um meio totalmente diferente de redes convencionais, o ar. Devido a isso, é preciso utilizar-se de tecnologias específicas para garantir uma conexão eficiente entre os equipamentos da rede. Essas tecnologias devem compensar a impossibilidade de proteção física do meio utilizado nas redes wireless, fazendo com que estas obtenham um bom desempenho e estabilidade mesmo em ambientes poluídos [RUFINO, 2005].

3. Resultados Obtidos

Todos os testes foram realizados pelo menos cinco vezes cada para garantir que em todas as tentativas seria detectada a assinatura correta.

Ambas as ferramentas apresentaram resultados satisfatórios nos testes aplicados nesta pesquisa. A Tabela 5 demonstra os ataques e o resultado da detecção de cada um.

Tabela 1. Ataques testados no Kismet e Beholder

Ataque	Kismet	Beholder
APSPOOF	Detectado	Detectado
BCASTDISCON	Detectado	Não Detectado
BSSTIMESTAMP	Detectado	Detectado com outra assinatura
CHANCHANGE	Detectado	Detectado
CRYPTODROP	Detectado	Detectado
KARMA	Detectado	Detectado

As duas ferramentas pecaram no tratamento das informações coletadas, pois permitem somente que sejam gravados arquivos de log sem nenhum tipo de filtro por assinatura ou por rede. Enquanto essa funcionalidade não é agregada nas ferramentas, existem programas analisadores de log que auxiliam o administrador da rede nesta deficiência, como o Swatch e Logwatch para Linux.

Referências

ALVES, Walter F. Andrade. **Segurança em Redes Sem Fio: O caso da Assembléia Nacional de Cabo Verde.** Trabalho de Conclusão de Curso – Curso de Engenharia de Sistemas e Informática, Universidade Jean Piaget de Cabo Verde, 2009.

FRANCISCATTI, Vagner. **Segurança em Redes Sem Fio**. Trabalho de Conclusão de Curso – Curso de Especialização em Redes de Computadores e Comunicação de Dados, Universidade Estadual de Londrina, Londrina, Paraná, 2005.