ESTUDO DAS ASSINATURAS DE PORTSCANS

Clayton Kendy Nakahara Passos
CESUMAR - CESUMAR, Maringá - Paraná

Fabrício Ricardo Lazilha (Orientador)
CESUMAR - CESUMAR, Maingá - Paraná

Com a "explosão" da Internet, há também um aumento nos sistemas dedicados a ela, infelizmente as empresas não têm uma preocupação adequada no quesito segurança, preocupando-se apenas com o aumento dos lucros. Porém, há aquelas que se preocupam com a segurança de seus sistemas, para estas torna-se necessário a utilização de uma ferramenta que possa evitar futuros ataques. Uma vez que a maioria dos ataques começa com um portscan, pode-se evitar muitos dos ataques bloqueando a ação destes portscans. Para tanto devemos encontrar "assinaturas" de cada método utilizado para efetuar um portscan, a fim de documentar e possibilitar a criação de uma ferramenta que identifique e bloqueie em tempo real, de acordo com as exigências do administrador de segurança. Tal estudo se faz necessário, pois sem esta base é impossível criarmos um "anti-portscan", e a falta desta solução facilita a ação do chamados crackes, que pode acabar com perda de dados, tempo e dinheiro. Para isto utilizamos o tcpdump em conjunto com o NMAP, para analisarmos os diversos métodos de portscans. Nestas análises encontramos reações interessantes e curiosas sobre o comportamento do protocolo TCP, que nos levou a identificação de seis assinaturas, ou seja, seis comportamentos que podem ser utilizados para detectar e bloquear a ação destas ferramentas.

netstart@brturbo.com; fabricio@cesumar.br