

Vulnerabilidade em Redes IP – Ataques por DoS

Introdução

Este tipo de ataque de Negação de Serviço pode desabilitar parcial ou completamente a rede local, além de um ou mais aplicativos de rede (web, mail, ftp) podendo ocasionar um problema ainda maior até a parada total da rede local. Geralmente, o método de ataque é sobrecarregar o sistema ou a rede. Tipicamente, os invasores enviam uma grande quantidade de requisições de serviços para um servidor/equipamento/aplicativo que é incapaz de tratar todas estas requisições. Muitas vezes os recursos do sistema se exaurem e o equipamento fica então sobrecarregado e incapaz de processar novas solicitações de usuários o que gera a Negação de Serviço (DoS). Existem diversas ferramentas que executam ataques e que estão livres na Internet não sendo mais privilégio de hackers o conhecimento necessário para fazê-los. Deve-se estar prevenido contra os ataques mais comuns e criar políticas de contingência:

Ataque de DoS por MAC Flooding:

É enviado a uma porta de um Switch frames Ethernet com endereços MAC randomicamente. O efeito deste ataque é que alguns switches podem começar a enviar o tráfego para todas as portas e o invasor pode fazer um sniffer (captura de informações) da rede.

Como dificultar o MAC Flooding com Switches Gerenciáveis:

- Implementar filtros de segurança L2 (MAC filter).
- Permitir que apenas um número limitado de MAC Address seja aprendido automaticamente por porta.
- Implementar Port Security com bloqueio automático de portas em caso de tentativa de intrusão.

Outras Funcionalidades de Segurança Suplementares:

- Segmentar a rede em grupos virtuais (VLAN).
- Desabilitar o acesso a serviços de gerenciamento e funcionalidades não utilizadas (SNMP, Telnet, WEB, etc).
- Restringir o acesso de gerenciamento (mng security filters) e/ou utilizar acesso criptografado (SSH, SSL).