Palestra sobre Segurança de Redes - Windows NT

Workshop: "Internet, Windows NT e Segurança de Rede"

Realizada em 13/05/1998

Palestrante:

Fabio C. Cunha Microsoft Systems Engineer

fccunha@flipflip.usp.br Microsoft Certified Trainer

FLIPFLOP

Resumo:

Adelino Domingos Conacci

Técnico em Redes

conacci@cirp.usp.br

Seção Técnica de Redes

Agenda

- Segurança
- Riscos
- Soluções
- Métodos
- Ferramentas

Resumo

Tipos de Ataque

- Passivos
  - Tapping ou Trace das comunicações.
  - É o mais difícil de detectar
  - Assumir que ele existe em qualquer comunicação através da Rede Internet
  - Exemplos: Programas Sniffer e TCP Port Scanners
- Ativos
  - Alguém está tentando entrar nas máquinas
  - Circulo de confiança
  - Exemplos: Equipamentos configurados com daemons de Telnet, FTP, etc. ou Recursos Compartilhados (Share para Rede Microsoft)

Regras Básicas

- Deverás negar qualquer serviço que não seja explicitamente permitido
  - Não instale serviços desnecessários, exemplo: "Simple TCT/IP Services" para Windows NT caso não tenha utilidade para o mesmo.
- Deverás impedir usuários externos de sua rede interna, sempre que possível
  - Utilize sempre que possível um Firewall para isolar sua Rede Interna de Rede Internet, ou seja, feche as portas.
- Deverás realizar auditoria e registro de todos os dias.
  - Crie e analise periodicamente arquivos de Log

Riscos

Onde estão os riscos?

- Furos do Sistema Operacional
  - Sempre efetuar a atualização do Sistema Operacional com os Patchs de Correção (Unix) ou Services Pack (S. O. Microsoft)
- IP não é confiável ou seguro
  - É um protocolo sem confirmação de conexão e sem garantia de entrega, ou seja, uma estação pode enviar um pacote a outra sem mesmo saber se a outra esta ou não conectada à rede.
- Serviços demais e erros de configuração

    - Exemplo: para que instalar e configurar o "Serviço de Compartilhamento de Arquivos e Impressoras" do Windows'95 em um equipamento que esta conectado diretamente à Rede Internet se o usuário que utiliza o mesmo não irá compartilhar seu equipamento com ninguém.
- Erros de projeto/implementação
    - Se for realmente necessário compartilhar recursos em um equipamento diretamente conectado à Rede Internet para que deixar o "Bind do NETBIOS com o TCP/IP", porque não deixar somente o "Bind do NETBIOS com o NETBeui".
- Erros de configuração
    - Para que deixar entrar em sua rede interna pacotes UDP 137.138 e TCP 139 oriundos da grande rede.
- TCP/IP não é seguro
    - É muito fácil monitorar os pacotes com auxílio de alguns programas como Sniffer's ou Port Scanners.
- Cavalos de Tróia
    - Uma vez detectada uma falha no Sistema Operacional (ex. Win'95), levando em consideração que o TCP/IP não é seguro e utilizando um Port-Scanner, podemos procurar em qualquer ponto da Rede Internet onde o administrador de rede local não configurou devidamente o seu Roteador e/ou não se preocupou em isolar sua rede interna com um Proxy/Firewall, por equipamentos mau configurados com TCP/IP e Compartilhamentos (Share). Uma vez satisfeitas todas estas condições, uma pessoa (hacker) com tempo disponível pode ter acesso aos dados contidos em seu disco rígido, e a partir daí fazer o que bem desejar com os mesmos.

Soluções

- Padronizar
- Treinamento
- Capacitação

Ataques conhecidos ao Windows NT

- Get Admin
  - Faz com que um usuário comum passe a ter privilégios de administrador.
- Ping of Death I e II
  - Consiste no envio de um "ping" com multiplos pacotes acima de 64K, após alguns pacotes o Windows NT/WIN'95 entra em "Lock-up" travando completamente. Método de proteção: bloquear toda entrada na rede interna de pacotes ICMP.
- RedButton
  - Através de uma conexão null-session (sem usuário e password), obtém os nomes de todos os usuários e dos compartilhamentos. Método de proteção: bloquear toda entrada na rede interna de pacotes ICMP.
- Out of Band Data
  - Também conhecido como "OOB Attack", consiste estabelecer uma conexão com um equipamento e enviar uma sequência qualquer de caracteres. O resultado deste ataque é uma quantidade enorme de entradas no "Event Log", e logo depois aparece aquela famosa tela BSOD (Blue Screen of Death) ai só reinicializando o servidor.
  - Alguns ataques conhecidos que utilizam "OOB Attack": WINS port 84, Deny of Service - DNS, Deny of Service - IIS (neste caso não são geradas entradas no "Event Log" o resultado é a queda do serviço, sendo necessário efetuar um "Shutdown").
  - Método de proteção: bloquear toda entrada na rede interna de pacotes destinados ao Port 139.
- Land Attack
  - Este tipo de ataque consiste em enviar pacotes "SYN" com o mesmo endereço de origem de destino e mesma porta de origem e destino, a um determinado equipamento. Isto faz com que o equipamento atacado passe a

responder as requisições para ele mesmo, com isso o Servidor Windows NT passa a funcionar cada vez mais lento.

- Pentium Bug
  - Quando um equipamento com um processador "Pentium Intel" recebe uma determinada sequência de instruções o mesmo para de responder. Para retornar ao normal é necessário desligar o equipamento e liga-lo novamente.
- Teardrop
  - Consiste no envio especificamente de 02 fragmentos do datagrama IP para a vitima. Isto causa um "Reboot" no servidor ou provoca a aparição da tela BSOD (Blue Screen of Death).

Ferramentas para "Scanners"

- Netzhack para MS-DOS
- Azmodeus para Micrsoft Windows NT
- Satan para Unix
- Internet Security Scanner
- NAT

Ferramentas para "Monitoração"

- Real Secure
- Performance Monitor com SNMP
- NetxRay
- eCAT