Como o bloco do monitor de tráfego da camada 4 trafica?

Pergunta:

Como o monitor de tráfego da camada 4 obstrui o tráfego se está recebendo somente o tráfego espelhado?

Ambiente:

Monitor de tráfego da camada 4 - L4TM configurado para obstruir o tráfego suspeito

Solução:

A ferramenta de segurança da Web de Cisco (WSA) tem um serviço incorporado do monitor de tráfego da camada 4 (L4TM) que possa obstruir sessões suspeitos através de todas as portas de rede (TCP/UDP 0-65535).

Para poder monitorar ou obstruir o tráfego destas sessões deve ser reorientado ao WSA, usando um dispositivo da TORNEIRA (porta de acesso do teste), ou configurando uma porta do espelho nos dispositivos de rede (portas span em dispositivos Cisco). A em-linha modo L4TM não é apoiada ainda.

Mesmo que o tráfego seja espelhado somente (copiado) das sessões original ao dispositivo, o WSA pode ainda obstruir o tráfego suspeito descansando uma sessão de TCP ou enviando mensagens do “host inalcançável” ICMP para sessões de UDP.

Para sessões de TCP

Quando o WSA L4TM recebe um pacote a ou de um server e o tráfego combina uma ação do bloco, L4TM enviará uma datagrama TCP RST (restauração) ao cliente ou ao server segundo a encenação. Uma datagrama TCP RST é apenas um pacote regular com a bandeira TCP RST ajustada a 1.

O receptor de um RST primeiramente valida-o, a seguir muda-o o estado. Se o receptor estava no estado da ESCUTA, ignora-o. Se o receptor estava no estado SYN-RECEIVED e tinha estado previamente no estado da ESCUTA, a seguir o receptor retorna ao estado da ESCUTA, se não o receptor aborta a conexão e vai ao estado fechado. Se o receptor estava em qualquer outro estado, aborta a conexão e recomenda o usuário e vai ao estado fechado.

Há dois casos a considerar (em ambos os casos os usuários/clientes são atrás de um Firewall):

Primeiro um é quando o pacote suspeito está vindo fora do Firewall para um cliente na rede interna. O RST será enviado ao server e neste caso obterá ao Firewall que geralmente não enviará o RST mas terminará a sessão porque acreditará que o RST veio realmente do cliente. Neste caso o IP da fonte do RST será o IP falsificado do cliente. O cliente terminará a sessão.

Um segundo caso seria quando o pacote está vindo do cliente na rede interna e está indo a um servidor interno (fora do Firewall). O RST é enviado então ao cliente e o IP da fonte RST será o IP falsificado do server.

Para sessões de UDP

Um comportamento similar está executado por WSA quando o tráfego suspeito é de uma sessão de UDP, mas em vez de enviar TCP RST, o L4TM enviará mensagens ICMP host inalcançável (tipo 3 código 1 ICMP) ao cliente ou ao server. Contudo, não há falsificação de IP nesses casos porque o mensagem ICMP indica que o host é inacessível assim que não pode enviar pacotes. O IP da fonte neste caso será o IP de WSA.

Estes RST e pacotes ICMP são enviados do WSA usando a tabela de roteamento dos dados, através do M1, do P1, ou do P2, segundo o desenvolvimento.