Como o Monitor de Tráfego de Camada 4 bloqueia o tráfego?

Pergunta:

Como o Monitor de Tráfego de Camada 4 bloqueia o tráfego se estiver recebendo apenas tráfego espelhado?

Ambiente:

Monitor de tráfego de camada 4 - L4TM configurado para bloquear tráfego suspeito

Solução:

O Cisco Web Security Appliance (WSA) tem um serviço L4TM (Monitor de Tráfego de Camada 4) incorporado que pode bloquear sessões suspeitas em todas as portas da rede (TCP/UDP 0-65535).

Para poder monitorar ou bloquear essas sessões, o tráfego deve ser redirecionado para o WSA, usando um dispositivo TAP (Test Access Port) ou configurando uma porta espelho em dispositivos de rede (portas SPAN em dispositivos Cisco). O modo em linha L4TM ainda não é suportado.

Mesmo que o tráfego seja espelhado (copiado) somente das sessões originais para o dispositivo, o WSA ainda pode bloquear o tráfego suspeito, quer restaurando uma sessão TCP, quer enviando mensagens ICMP "host inalcançável" para sessões UDP.

Para sessões TCP

Quando o WSA L4TM recebe um pacote de ou para um servidor e o tráfego corresponde a uma ação de bloqueio, o L4TM enviará um datagrama TCP RST (redefinição) para o cliente ou servidor, dependendo do cenário. Um datagrama TCP RST é apenas um pacote regular com o sinalizador TCP RST definido como 1.

O receptor de um RST primeiro o valida e, em seguida, altera o estado. Se o receptor estava no estado LISTEN, ele o ignora. Se o receptor estava no estado SYN-RECEIVED e estava anteriormente no estado LISTEN, o receptor retorna ao estado LISTEN, caso contrário, o receptor aborta a conexão e vai para o estado CLOSED. Se o receptor estiver em qualquer outro estado, ele aborta a conexão e avisa o usuário e vai para o estado FECHADO.

Há dois casos a considerar (em ambos os casos, os usuários/clientes estão por trás de um firewall):

- A primeira é quando o pacote suspeito está vindo de fora do firewall em direção a um cliente na rede interna. O RST será enviado ao servidor e, nesse caso, ele chegará ao firewall que normalmente não encaminhará o RST, mas encerrará a sessão, pois acreditará que o RST

realmente veio do cliente. Nesse caso, o IP de origem do RST será o IP falsificado do cliente. O cliente encerrará a sessão.

Um segundo caso seria quando o pacote vem do cliente na rede interna e vai para um servidor externo (fora do firewall). O RST é enviado ao cliente e o RST source IP será o IP falsificado do servidor.

Para sessões UDP

Um comportamento semelhante é executado pelo WSA quando o tráfego suspeito é de uma sessão UDP, mas em vez de enviar TCP RST , o L4TM enviará mensagens ICMP host inalcançável (código 1 do ICMP tipo 3) ao cliente ou ao servidor. No entanto, não há spoofing de IP nesses casos, pois a mensagem ICMP afirma que o host está inacessível, portanto, não pode enviar pacotes. O IP de origem nesse caso será o IP do WSA.

Esses RSTs e pacotes ICMP são enviados do WSA usando a tabela de roteamento de dados, através de M1, P1 ou P2, dependendo da implantação.