Hoe blokkeert Layer 4 Traffic Monitor het verkeer?

Vraag:

Hoe blokkeert Layer 4 Traffic Monitor het verkeer als het alleen gespiegeld verkeer ontvangt?

Milieu:

Layer 4 Traffic Monitor - L4TM ingesteld om verdachte verkeer te blokkeren

Oplossing:

Cisco Web Security Appliance (WSA) heeft een ingebouwde Layer 4 Traffic Monitor (L4TM) die verdachte sessies over alle netwerkpoorten kan blokkeren (TCP/UDP 0-65535).

Om deze sessies te kunnen bewaken of blokkeren moet het verkeer worden omgeleid naar de WSA, of door een TAP (Test Access Port)-apparaat te gebruiken of door een spiegelpoort op netwerkapparaten (SPAN-poorten op Cisco-apparaten) te configureren. L4TM-inline modus wordt nog niet ondersteund.

Hoewel het verkeer alleen gespiegeld (gekopieerd) is van de oorspronkelijke sessies naar het apparaat, kan de WSA nog steeds verdachte verkeer blokkeren door een TCP-sessie te resetten of door "host onbereikbaar" berichten van ICMP te verzenden voor UDP-sessies.

Voor TCP-sessies

Wanneer de WSA L4TM een pakket van of naar een server ontvangt en het verkeer past bij een Blokactie aan, zal L4TM een TCP RST (reset) datagram naar de client of server sturen, afhankelijk van het scenario. Een TCP RST-datagram is slechts een regelmatig pakket met de TCP RST-vlag ingesteld op 1.

De ontvanger van een RST bevestigt het eerst en verandert de staat. Als de ontvanger in de staat LISTEN was, negeert hij het. Als de ontvanger zich in SYN-ONTVANGEN toestand bevond en in het verleden in de staat LISTEN bevond, dan keert de ontvanger terug naar de staat LISTEN, anders sluit de ontvanger de verbinding af en gaat hij naar de staat CLOSED. Als de ontvanger in een andere staat was, sluit hij de aansluiting af, adviseert hij de gebruiker en gaat hij naar de CLOSED-staat.

Er zijn twee zaken in overweging te nemen (in beide gevallen bevinden gebruikers/klanten zich achter een firewall):

Ten eerste is het wanneer het verdacht pakket van buiten de firewall naar een client in het interne netwerk komt. De RST wordt naar de server verzonden en in dit geval komt deze naar de firewall die de RST meestal niet verstuurt, maar zal de sessie beëindigen omdat de RST daadwerkelijk van de klant afkomstig is. In dit geval zal de bron IP van de RST de gespoofde IP

van de client zijn. De cliënt zal de sessie beëindigen.

Een tweede geval zou zijn wanneer het pakket van de client in het interne netwerk komt en naar een externe server (buiten de firewall) gaat. RST wordt vervolgens naar de client verzonden en RST-bron IP wordt de gespoofde IP van de server genoemd.

Voor UDP-sessies

Een soortgelijk gedrag wordt uitgevoerd door WSA wanneer het verdachte verkeer van een UDP-sessie is, maar in plaats van TCP RST te verzenden, zal L4TM onbereikbare berichten van de ICMP-host (ICMP type 3 code 1) naar de client of de server sturen. Er is echter geen IP-spoofing in deze gevallen omdat het ICMP-bericht stelt dat de host onbereikbaar is, zodat deze geen pakketten kan verzenden. Bron-IP is in dit geval het IP van WSA.

Deze RSTs en ICMP pakketten worden van de WSA verzonden die de gegevens die tabel, via of M1, of P2, afhankelijk van de plaatsing, worden verzonden.