Wie blockiert die Layer-4-Datenverkehrsüberwachung den Datenverkehr?

Frage:

Wie blockiert die Layer-4-Datenverkehrsüberwachung Datenverkehr, wenn sie nur gespiegelten Datenverkehr empfängt?

Umgebung:

Layer-4-Datenverkehrsüberwachung - L4TM-Konfiguration zur Blockierung von verdächtigem Datenverkehr

Lösung:

Die Cisco Web Security Appliance (WSA) verfügt über einen integrierten Layer 4 Traffic Monitor (L4TM)-Service, der verdächtige Sitzungen über alle Netzwerk-Ports (TCP/UDP 0-65535) blockieren kann.

Um diese Sitzungen überwachen oder blockieren zu können, muss der Datenverkehr entweder über ein TAP-Gerät (Test Access Port) oder einen Spiegelport auf Netzwerkgeräten (SPAN-Ports auf Cisco Geräten) an die WSA umgeleitet werden. Der In-Line-Modus von L4TM wird noch nicht unterstützt.

Obwohl der Datenverkehr nur von den ursprünglichen Sitzungen zur Appliance gespiegelt (kopiert) wird, kann die WSA verdächtigen Datenverkehr dennoch blockieren, indem sie entweder eine TCP-Sitzung zurückstellt oder ICMP-Nachrichten für UDP-Sitzungen sendet, die nicht erreichbar sind.

Für TCP-Sitzungen

Wenn das WSA L4TM ein Paket an oder von einem Server empfängt und der Datenverkehr mit einer Blockaktion übereinstimmt, sendet L4TM je nach Szenario ein TCP-RST-Datagramm (Reset) an den Client oder Server. Ein TCP-RST-Datagramm ist nur ein reguläres Paket, bei dem das TCP-RST-Flag auf 1 festgelegt ist.

Der Empfänger eines RST validiert diesen zuerst und ändert dann den Zustand. Wenn sich der Empfänger im LISTEN-Status befand, wird er ignoriert. Wenn sich der Empfänger im Status SYN-RECEIVED befand und sich zuvor im Status LISTEN befunden hatte, kehrt der Empfänger in den Status LISTEN zurück. Andernfalls bricht der Empfänger die Verbindung ab und wechselt in den Status CLOSED. Wenn sich der Empfänger in einem anderen Zustand befindet, wird die Verbindung abgebrochen, der Benutzer wird informiert und der CLOSED-Status wird angezeigt.

Es sind zwei Fälle zu berücksichtigen (in beiden Fällen befinden sich Benutzer/Clients hinter einer Firewall):

Erstens, wenn das verdächtige Paket von außerhalb der Firewall zu einem Client im internen Netzwerk kommt. Der RST wird an den Server gesendet und in diesem Fall an die Firewall, die normalerweise den RST nicht weiterleitet, die Sitzung jedoch beendet, da der RST vermutlich vom Client stammt. In diesem Fall ist die Quell-IP des RST die gefälschte IP des Clients. Der Client beendet die Sitzung.

Ein zweiter Fall wäre der Fall, wenn das Paket vom Client im internen Netzwerk kommt und an einen externen Server (außerhalb der Firewall) weitergeleitet wird. Der RST wird dann an den Client gesendet, und die RST-Quell-IP ist die gefälschte IP-Adresse des Servers.

Für UDP-Sitzungen

Ein ähnliches Verhalten wird von der WSA ausgeführt, wenn der verdächtige Datenverkehr aus einer UDP-Sitzung stammt. Anstatt jedoch TCP RST zu senden, sendet L4TM nicht erreichbare ICMP-Hosts (ICMP-Typ 3-Code 1) entweder an den Client oder an den Server. In diesen Fällen gibt es jedoch kein IP-Spoofing, da die ICMP-Meldung angibt, dass der Host nicht erreichbar ist, sodass er keine Pakete senden kann. Die Quell-IP in diesem Fall ist die IP-Adresse der WSA.

Diese RSTs und ICMP-Pakete werden je nach Bereitstellung entweder über M1, P1 oder P2 von der WSA mithilfe der Datenrouting-Tabelle gesendet.