Anmeldung bei einem Remote-Desktop mit RDP zum Ändern des einer IP-Adresse zugeordneten Benutzers

Inhalt

Einleitung

Wenn Sie sich mit dem Remote Desktop Protocol (RDP) bei einem Remote-Host anmelden und sich der Remote-Benutzername von dem Ihres Benutzers unterscheidet, ändert das FireSIGHT-System die IP-Adresse des Benutzers, der Ihrer IP-Adresse im FireSIGHT Management Center zugeordnet ist. Sie bewirkt eine Änderung der Berechtigungen für den Benutzer in Bezug auf die Zugriffskontrollregeln. Sie werden feststellen, dassFalscher Benutzer ist mit Workstation verbunden. Dieses Dokument bietet eine Lösung für dieses Problem.

Voraussetzungen

Cisco empfiehlt, Kenntnisse über das FireSIGHT-System und den Benutzer-Agenten zu erwerben.

> **Hinweis**: Die Informationen in diesem Dokument stammen von den Geräten in einer bestimmten Laborumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Ursache

Dieses Problem tritt auf, weil Microsoft Active Directory (AD) RDP-Authentifizierungsversuche an die Windows-Sicherheitsprotokolle auf dem Domänencontroller protokolliert. AD protokolliert den Authentifizierungsversuch für die RDP-Sitzung anhand der IP-Adresse des ursprünglichen Hosts

und nicht anhand des RDP-Endpunkts, mit dem Sie eine Verbindung herstellen. Wenn Sie sich mit einem anderen Benutzerkonto beim Remote-Host anmelden, ändert dies den Benutzer, der mit der IP-Adresse Ihrer ursprünglichen Workstation verknüpft ist.

Verifizierung

Um sicherzustellen, dass dies der Fall ist, können Sie überprüfen, ob die IP-Adresse des Anmeldeereignisses Ihrer ursprünglichen Workstation und der RDP-Remotehost über dieselbe IP-Adresse verfügen.

Um diese Veranstaltungen zu finden, müssen Sie die folgenden Schritte befolgen:

Schritt 1: Bestimmen Sie den Domänencontroller, für den sich der Host authentifiziert:

Führen Sie den folgenden Befehl aus:

```
nltest /dsgetdc:<windows.domain.name>
```

Beispiel:

```
C:\Users\WinXP.LAB>nltest /dsgetdc:support.lab
DC: \\Win2k8.support.lab
Address: \\192.X.X.X
Dom Guid: XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
Dom Name: support.lab
Forest Name: support.lab
Dc Site Name: Default-First-Site-Name
Our Site Name: Default-First-Site-Name
Flags: PDC GC DS LDAP KDC TIMESERV WRITABLE DNS_DC DNS_DOMAIN DNS_FOREST
CLOSE_SITE FULL_SECRET WS 0x4000
The command completed successfully
```

Die Zeile, die mit "DC:" beginnt, ist der Name des Domänencontrollers, und die Zeile, die mit "Address:" beginnt, ist die IP-Adresse.

Schritt 2: Verwenden des RDP-Protokolls beim in Schritt 1 angegebenen Domänencontroller

Schritt 3: Gehen Sie zu **Start > Verwaltung > Ereignisanzeige**.

Schritt 4: Navigieren Sie zu **Windows-Protokolle > Sicherheit**.

Schritt 5: Filtern Sie nach der IP-Adresse Ihrer Workstation, indem Sie auf Aktuelles Protokoll filtern, auf die Registerkarte XML klicken und auf Abfrage bearbeiten klicken.

Schritt 6: Geben Sie die folgende XML-Abfrage ein, und ersetzen Sie **<IP-Adresse>** durch Ihre IP-Adresse.

```
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">
*[EventData[Data[@Name='IpAddress'] and(Data='<IP address>')]]
</Select>
</Query>
</QueryList>
```

Schritt 7: Klicken Sie auf das **Anmeldeereignis** und anschließend auf die Registerkarte **Details**.

Ein Beispiel für die Ausgabe:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
<Provider Name="Microsoft-Windows-Security-Auditing"
Guid="{XXXXXXXX-XXX-XXXX-XXX-XXXXXXXXXXXX}"/>
<EventID>4624</EventID>
<Version>0</Version>
<Level>0</Level>
<Task>12544</Task>
<Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime="2014-07-22T20:35:12.750Z" />
<EventRecordID>4130857</EventRecordID>
<Correlation />
<Execution ProcessID="576" ThreadID="704" />
<Channel>Security</Channel>
<Computer>WIN2k8.Support.lab</Computer>
<Security />
</System>
- <EventData>
<Data Name="SubjectUserSid">S-1-0-0</Data>
<Data Name="SubjectUserName">-</Data>
<Data Name="SubjectDomainName">-</Data>
<Data Name="SubjectLogonId">0x0</Data>
<Data Name="TargetUserSid">S-X-X-XX-XXXXXXXXXX-XXXXXXXXXX-XXXXXXXXX-XXXX</Data>
<Data Name="TargetUserName">WINXP-SUPLAB$</Data>
<Data Name="TargetDomainName">SUPPORT</Data>
<Data Name="TargetLogonId">0x13c4101f</Data>
<Data Name="LogonType">3</Data>
<Data Name="LogonProcessName">Kerberos</Data>
<Data Name="AuthenticationPackageName">Kerberos</Data>
<Data Name="WorkstationName" />
<Data Name="LogonGuid">{XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX}</Data>
<Data Name="TransmittedServices">-</Data>
<Data Name="LmPackageName">-</Data>
<Data Name="KeyLength">0</Data>
<Data Name="ProcessId">0x0</Data>
<Data Name="ProcessName">-</Data>
<Data Name="IpAddress">192.0.2.10</Data>
<Data Name="IpPort">2401</Data>
</EventData>
```

Führen Sie nach der Anmeldung über RDP die gleichen Schritte aus, und Sie werden feststellen, dass Sie ein weiteres Anmeldeereignis (Ereignis-ID 4624) mit der gleichen IP-Adresse erhalten, wie in der folgenden Zeile aus den XML-Daten des Anmeldeereignisses aus der ursprünglichen Anmeldung dargestellt:

```
<Data Name="IpAddress">192.x.x.x</Data>
```

Lösung

Wenn Sie User Agent 2.1 oder höher verwenden, können Sie Konten ausschließen, die Sie werden hauptsächlich für RDP in der Konfiguration des Benutzer-Agents verwendet.

Schritt 1: Melden Sie sich beim Benutzer-Agent-Host an.

Schritt 2: Starten Sie die Benutzeroberfläche des Benutzer-Agents.

Schritt 3: Klicken Sie auf die Registerkarte **Ausgeschlossene Benutzernamen**.

Schritt 4: Geben Sie alle Benutzernamen ein, die Sie ausschließen möchten.

Schritt 5: Klicken Sie auf **Speichern**.

Benutzer, die in diese Liste eingegeben werden, generieren keine Anmeldeereignisse im FireSIGHT Management Center und werden
die IP-Adressen zugeordnet sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.