تسجيل الدخول إلى سطح مكتب بعيد باستخدام RDP يغير المستخدم المرتبط بعنوان IP

المحتويات

المقدمة

إذا قمت بتسجيل الدخول إلى مضيف بعيد باستخدام بروتوكول سطح المكتب البعيد (RDP)، وكان اسم المستخدم البعيد مختلفا عن المستخدم الخاص بك، فإن نظام FireSIGHT يقوم بتغيير عنوان IP الخاص بالمستخدم المرتبط بعنوان IP الخاص بك في مركز إدارة FireSIGHT. وهو يتسبب في تغيير أذونات المستخدم فيما يتعلق بقواعد التحكم بالوصول. ستلاحظون أنيالمستخدم غير الصحيح مقترن بمحطة العمل. يقدم هذا وثيقة حل لهذه المشكلة.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بنظام FireSIGHT ووكيل المستخدم.

ملاحظة: تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

سبب جذري

تحدث هذه المشكلة بسبب الطريقة التي يقوم بها Microsoft Active Directory(AD) بتسجيل محاولات مصادقة RDP لسجلات أمان Windows على وحدة التحكم بالمجال. AD تسجيل محاولة المصادقة لجلسة عمل RDP مقابل عنوان IP للمضيف الأصلي بدلا من نقطة نهاية RDP التي تتصل بها. إذا كنت تقوم بتسجيل الدخول إلى المضيف البعيد باستخدام حساب مستخدم مختلف، فإن ذلك سيؤدي إلى تغيير المستخدم المرتبط بعنوان IP الخاص بمحطة العمل الأصلية.

التحقق

للتحقق من ما يحدث، يمكنك التحقق من أن عنوان IP من حدث تسجيل الدخول من محطة العمل الأصلية ومضيف RDP البعيد لديهم نفس عنوان IP.

للعثور على هذه الأحداث، سيتعين عليك اتباع الخطوات التالية:

الخطوة 1: حدد وحدة التحكم بالمجال التي تقوم بمصادقة المضيف عليها:

قم بتشغيل الأمر التالي:

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

مثال الإخراج:

```
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
```

سيكون السطر الذي يبدأ "DC:" هو اسم وحدة التحكم بالمجال وسيبدأ السطر "العنوان:" في عنوان IP.

الخطوة 2: إستخدام سجل RDP في وحدة التحكم بالمجال المحددة في الخطوة 1

الخطوة 3: انتقل إلى **ابدأ > أدوات إدارية > عارض الأحداث**.

الخطوة 4: التنقل لأسفل إلى **سجلات Windows > الأمان**.

الخطوة 5: تصفية عنوان IP الخاص بمحطة العمل بالنقر فوق "تصفية السجل الحالي" والنقر فوق علامة التبويب XML والنقر فوق "تحرير الاستعلام.

الخطوة 6: أدخل استعلام XML التالي، مستبدلا عنوان IP الخاص بك من <ip address>

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

```
<QueryList/>
```
الخطوة 7: انقر فوق **حدث تسجيل الدخول** وانقر فوق علامة التبويب **تفاصيل**.

مثال للمخرجات:

```
<"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/>
```
أكمل هذه الخطوات نفسها بعد تسجيل الدخول عبر RDP وستلاحظ أنك ستحصل على حدث تسجيل دخول آخر (معرف الحدث 4624) بنفس عنوان IP كما هو موضح في السطر التالي من بيانات XML لحدث تسجيل الدخول من تسجيل الدخول الأصلي:

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

الحل

للحد من هذه المشكلة، إذا كنت تستخدم "وكيل المستخدم 2.1" أو إصدارا أعلى، يمكنك إستبعاد أي حسابات تريد إستخدامها
الاستخدام بشكل أساسي ل RDP في تكوين وكيل المستخدم.

الخطوة 1: سجل الدخول إلى مضيف وكيل المستخدم.

الخطوة 2: بدء تشغيل واجهة مستخدم وكيل المستخدم.

الخطوة 3: انقر فوق علامة التبويب **أسماء المستخدمين المستبعدة**.

الخطوة 4: أدخل جميع أسماء المستخدمين التي تريد إستبعادها.

الخطوة 5: انقر فوق **حفظ**.

لا يقوم المستخدمون الذين تم إدخالهم في هذه القائمة بإنشاء أحداث تسجيل دخول على FireSIGHT Management Center ولا يقومون بذلك
مقترن بعناوين IP.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).