Warum sind Computernamen oder NULL-Benutzernamen in Zugriffsprotokollen angemeldet?

Inhalt

[Frage](#)
[Umgebung](#)
[Symptome](#)
[Hintergrundinformationen](#)

Frage

- Warum sind Computernamen oder NULL-Benutzernamen in Zugriffsprotokollen angemeldet?
- Wie identifizieren Sie die Anfragen mithilfe von Workstation oder NULL-Anmeldeinformationen für eine spätere Authentifizierungsfreistellung?

Umgebung

- Cisco Web Security Appliance (WSA) - alle Versionen
- Authentifizierungsschema NTLMSSP mit IP-Nachbarn
- Windows Vista und neuere Desktop- und mobile Microsoft Operations Systems

Symptome

Die WSA blockiert Anfragen einiger Benutzer oder verhält sich unerwartet.
Die Accesslogs zeigen Computernamen oder NULL-Benutzernamen und -Domäne anstelle von Benutzer-IDs an.

Das Problem wird wie folgt behoben:

- Surrogates Timeout (Standardwert für Surrogat Timeout beträgt 60 Minuten)
- Neustart des Proxyprozesses (CLI-Befehl > *diagnostisch* > *Proxy* > *Kick*)
- Löschen des Authentifizierungscaches (CLI-Befehl > *authcache* > *flushall*)

Hintergrundinformationen

Bei den neuesten Versionen des Microsoft-Betriebssystems ist es nicht mehr erforderlich, dass ein tatsächlicher Benutzer angemeldet ist, damit Anwendungen Anfragen an das Internet senden können. Wenn diese Anforderungen von der WSA empfangen und zur Authentifizierung

angefordert werden, stehen keine Benutzeranmeldeinformationen zur Verfügung, die für die Authentifizierung durch die Client-Workstation verwendet werden können. Stattdessen kann der Computername anstelle eines Ersatzgeräts verwendet werden.

Die WSA leitet den angegebenen Computernamen an das Active Directory (AD) weiter, das diesen validiert.

Mit einer gültigen Authentifizierung erstellt die WSA ein IP-Ersatz, das den Workstation-Namen des Computers an die IP-Adresse der Workstation bindet. Für weitere Anfragen, die von derselben IP-Adresse kommen, wird der Ersatz und damit der Workstation-Name verwendet.

Da der Workstation-Name nicht Mitglied einer AD-Gruppe ist, können Anfragen möglicherweise nicht die erwartete Zugriffsrichtlinie auslösen und daher blockiert werden. Das Problem besteht weiterhin, bis das Surrogat das Zeitlimit erreicht hat und die Authentifizierung erneuert werden muss. Dieses Mal wird ein neues IP-Surrogat mit diesen Informationen erstellt, sobald ein Benutzer angemeldet ist und gültige Benutzeranmeldeinformationen verfügbar sind. Weitere Anfragen stimmen mit der erwarteten Zugriffsrichtlinie überein.

Ein anderes Szenario wird gesehen, wenn Anwendungen ungültige Anmeldeinformationen (NULL-Benutzername und NULL-Domäne) und NICHT gültige Anmeldeinformationen des Computers senden. Dies gilt als Authentifizierungsfehler und wird blockiert. Wenn Gastrichtlinien aktiviert sind, wird die ausgefallene Authentifizierung als "Gast" betrachtet.

Der Workstation-Name endet mit einem **$** gefolgt von **@DOMAIN**, wodurch Workstation-Namen einfach nachverfolgt werden können, indem der CLI-Befehl **grep** in den Accesslogs für **$@** verwendet wird. Weitere Informationen finden Sie im folgenden Beispiel.

```
> grep $@ accesslogs

1332164800.0000 9 10.20.30.40 TCP_DENIED/403 5608 GET http://www.someURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_WEBCAT_11-DefaultGroup-Internet-NONE-NONE-
NONE-NONE <-,-,"-","-",-,-,-,"-","-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

Die Zeile oben zeigt ein Beispiel dafür, dass bereits ein IP-Ersatz für die IP-Adresse 10.20.30.40 und der Gerätename **gb0000d01$erstellt wurde.**

Um die Anforderung zu finden, die den Computernamen gesendet hat, muss das erste Vorkommen des Workstation-Namens für die spezifische IP-Adresse identifiziert werden. Mit dem folgenden CLI-Befehl wird Folgendes erreicht:

```
> grep 10.20.30.40 -p accesslogs
```

Suchen Sie das Ergebnis nach dem ersten Vorkommen des Workstation-Namens. Die drei ersten Anforderungen werden allgemein als NTLM Single-Sin-On (NTLMSSP/NTLMSSP)-Handshake erkannt, wie hier beschrieben und im folgenden Beispiel gezeigt:

```
1335248044.836 0 10.20.30.40 TCP_DENIED/407 1733 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.839 0 10.20.30.40 TCP_DENIED/407 483 GET http://SomeOtherURL.com -
NONE/- - OTHER-NONE-DefaultGroup-NONE-NONE-NONE-NONE
```

```
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -

1335248044.845 10 10.20.30.40 TCP_DENIED/403 2357 GET http://SomeOtherURL.com
"gb0000d01$@DOMAIN" NONE/- - BLOCK_ADMIN_PROTOCOL_11-DefaultGroup-DefaultGroup-
DefaultGroup-NONE-NONE-NONE
<-,-,"-","-",-,-,-,"-","-",-,-,"-",-,"-","-",-,"-","-","-","-","-","-",
0.00,0,-,"-","-"> -
```

Stellen Sie bei der Fehlerbehebung sicher, dass diese Anforderungen für dieselbe URL gelten und in einem sehr kurzen Intervall protokolliert werden, was darauf hinweist, dass es sich um einen automatisierten NTLMSSP-Handshake handelt.

Im obigen Beispiel werden die vorhergehenden Anforderungen mit dem HTTP-Antwortcode 407 (Proxy-Authentifizierung erforderlich) für explizite Anforderungen protokolliert, während transparente Anforderungen mit dem HTTP-Antwortcode 401 (Nicht authentifiziert) protokolliert werden.

AsyncOS 7.5.0 und höher bieten eine neue Funktion, mit der Sie ein anderes Surrogat-Timeout für Anmeldeinformationen des Computers definieren können. Sie kann mit dem folgenden Befehl konfiguriert werden:

```
> advancedproxyconfigChoose a parameter group:- AUTHENTICATION - Authentication
related parameters- CACHING - Proxy Caching related parameters- DNS - DNS related
parameters- EUN - EUN related parameters- NATIVEFTP - Native FTP related parameters-
FTPOVERHTTP - FTP Over HTTP related parameters- HTTPS - HTTPS related parameters-
SCANNING - Scanning related parameters- WCCP - WCCPv2 related parameters-
MISCELLANEOUS - Miscellaneous proxy relatedparameters[]> AUTHENTICATION...Enter the
surrogate timeout.[3600]>Enter the surrogate timeout for machine credentials.[10]>.
```

Sie können die gleichen Schritte verwenden, um zu ermitteln, welche Anforderungen die NULL-Anmeldeinformationen erhalten, um herauszufinden, welche URL oder der Benutzer-Agent die ungültigen Anmeldeinformationen sendet und von der Authentifizierung ausnimmt.

URL von der Authentifizierung ausschließen

Um zu verhindern, dass diese Anforderung die Erstellung des falschen Surrogats bewirkt, muss die URL von der Authentifizierung ausgenommen werden.Anstatt die URL von der Authentifizierung zu befreien, können Sie die Anwendung, die die Anforderung selbst sendet, von der Authentifizierung ausnehmen. Stellen Sie sicher, dass alle Anforderungen für die Anwendung von der Authentifizierung ausgenommen werden. Dies ist möglich, indem Sie den Benutzer-Agent hinzufügen, der in den Accesslogs angemeldet werden soll, indem Sie den zusätzlichen Parameter **%u** in den optionalen **benutzerdefinierten Feldern** im AccessLog-Abonnement der WSA hinzufügen. Nachdem der User Agent identifiziert wurde, muss er von der Authentifizierung ausgenommen werden.