Waarom zijn de computernamen of de NULL-gebruikersnamen aangemeld bij de accessoires?

Inhoud

vraag

- Waarom zijn de computernamen of de NULL-gebruikersnamen aangemeld bij de accessoires?
- Hoe identificeert u de verzoeken met werkstations of NULL-geloofsbrieven voor latere authenticatievrijstelling?

Omgeving

- Cisco web security applicatie (WSA) - alle versies
- NTLMSSP-verificatieregeling met IP-surrogaat
- Windows Vista en nieuwere desktop en mobiele Microsoft Operating Systems

Symptomen

De WSA blokkeert verzoeken van sommige gebruikers of gedraagt zich onverwacht.
Acclogs tonen computernamen of NULL-gebruikersnaam en -domein in plaats van gebruikerIDs.

De kwestie lost zichzelf op na:

- Surrogante time-out (standaardwaarde voor tijdelijke oplossing is 60 minuten)
- Herstart van het proxy-proces (CLI-opdracht > *diagnostiek* > *proxy* > *schop*)
- Flushing Authentication cache (CLI-opdracht > *authcache* > *flushall*)

Achtergrondinformatie

In recente versies van Microsoft Operating System is het niet vereist dat een echte gebruiker meer inlogt zodat toepassingen aanvragen naar het internet kunnen verzenden. Wanneer deze verzoeken door de WSA worden ontvangen en om authenticatie worden verzocht, zijn er geen gebruikersaanmeldingsgegevens beschikbaar voor gebruik voor authenticatie door het clientwerkstation, dat in plaats daarvan de machinenaam van de computer mag gebruiken voor

een substituut.

De WSA zal de meegeleverde machinenaam nemen en het naar de Actieve Map (AD) doorsturen die het geldig verklaren.

Met een geldige authenticatie creëert de WSA een IP surrogaat die de werkstationnaam van de machine aan het IP adres van het werkstation bindt. Verdere verzoeken die afkomstig zijn van hetzelfde OT zullen het surrogaat en dus de naam van het werkstation gebruiken.

Aangezien de werkstationnaam geen lid is van een AD-groep, kunnen verzoeken niet het verwachte toegangsbeleid starten en dus worden geblokkeerd. Het probleem blijft bestaan totdat het surrogaat is gestopt en de authenticatie moet worden verlengd. Deze keer, met een echte gebruiker die inlogt en geldige gebruikersreferenties beschikbaar is, wordt er een nieuw IP-surrogaat gemaakt met deze informatie en worden verdere verzoeken ontvangen volgens het verwachte toegangsbeleid.

Een ander scenario dat wordt gezien is wanneer toepassingen ongeldige geloofsbrieven (NULL gebruikersnaam en NULL-domein) en NIET geldige machinegeloofsbrieven verzenden. Dit wordt gezien als een mislukking van de authenticatie en zal worden geblokkeerd of als het gastbeleid wordt geactiveerd, wordt de mislukte autoriteit beschouwd als een "gast".

De naam van het werkstation eindigt met een $ gevolgd door @DOMAIN, waarmee werkstationnamen eenvoudig kunnen worden getraceerd met behulp van de CLI-opdrachtregel op de accessoires voor $@. Zie het voorbeeld hieronder voor meer informatie.

```
> 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,-,"-","-"> -
```

De bovenstaande lijn geeft een voorbeeld van een IP-surrogaat dat al is gemaakt voor het IP-adres 10.20.30.40 en de machinenaam gb0000d01$.

Om het verzoek te vinden dat de machinenaam heeft verzonden, moet het eerste exemplaar van de werkstationnaam voor het specifieke IP-adres worden geïdentificeerd. Met de volgende CLI-opdracht wordt dit bereikt:

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

Zoek het resultaat voor het eerste exemplaar van de werkstationnaam. De drie eerste verzoeken worden algemeen herkend als een NTLM Single-On (NTLMSSP/NTLMSSP)-handdruk zoals hier beschreven en in het onderstaande voorbeeld getoond:

```
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,-,"-","-"> -
```

Zorg er bij het oplossen van problemen voor dat deze verzoeken om dezelfde URL zijn en binnen een zeer kort tijdsinterval worden ingelogd om aan te geven dat het een geautomatiseerde NTLMSSP-handdruk is.

In het bovenstaande voorbeeld worden de bovenstaande verzoeken geregistreerd met de HTTP-responscode 407 (Proxy-verificatie vereist) voor expliciete verzoeken, terwijl transparante verzoeken worden vastgelegd met HTTP-responscode 401 (niet-geauthentiseerd).

Er is een nieuwe functie beschikbaar op AsyncOS 7.5.0 en hoger, waar u een verschillende surrogaat tijd kunt definiëren voor machine aanmeldingsgegevens. U kunt de configuratie als volgt configureren:

```
> 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]>.
```

U kunt dezelfde stappen gebruiken om te ontdekken welke verzoeken de NULL-referenties krijgen en te ontdekken welke URL of User Agent de ongeldige aanmeldingsgegevens verzenden en deze van verificatie vrijstellen.

De URL vrijstellen van verificatie

Om te voorkomen dat dit verzoek ertoe leidt dat het valse surrogaat wordt gecreëerd, moet de URL worden vrijgesteld van de echtheidscontrole.Of in plaats van de URL vrij te stellen van de authenticatie, kan u besluiten de aanvraag voor het verzenden van het verzoek zelf van de authenticatie vrij te stellen, zodat alle verzoeken om de toepassing van de authenticatie worden vrijgesteld. Dit is mogelijk door de gebruikersagent toe te voegen die in de toegangsbestanden moet worden ingelogd, door de extra parameter **%u** toe te voegen aan de optionele **Aangepaste velden** in het accessoire van de WSA. Na identificatie van de gebruikersagent moet het worden vrijgesteld van verificatie.