Perché i nomi computer o i nomi utente NULL vengono registrati nei log degli accessi?

Sommario

Domanda

- Perché i nomi computer o i nomi utente NULL vengono registrati nei log degli accessi?
- Come identificare le richieste utilizzando credenziali di workstation o NULL per l'esenzione di autenticazione successiva?

Ambiente

- Cisco Web Security Appliance (WSA) - tutte le versioni
- Schema di autenticazione NTLMSSP con surrogati IP
- Windows Vista e i nuovi sistemi operativi per PC desktop e portatili Microsoft

Sintomi

WSA blocca le richieste di alcuni utenti o si comporta in modo imprevisto.
Nei log degli accessi vengono visualizzati i nomi dei computer o il nome utente e il dominio NULL anziché gli ID utente.

Il problema si risolve dopo:

- Timeout surrogati (il valore predefinito per Timeout surrogati è 60 minuti)
- Riavvio del processo proxy (comando CLI > *diagnostica* > *proxy* > *avvio*)
- Scaricamento della cache di autenticazione (comando CLI > *authcache* > *flushall*)

Premesse

Nelle versioni più recenti del sistema operativo Microsoft non è più necessario che un utente effettivo sia connesso per consentire alle applicazioni di inviare le richieste a Internet. Quando tali richieste vengono ricevute dal server di servizi di distribuzione Windows e viene richiesta l'autenticazione, non sono disponibili credenziali utente da utilizzare per l'autenticazione da parte della workstation client, che potrebbero invece utilizzare il nome computer del computer per

un'alternativa.

Il server WSA accetta il nome di computer specificato e lo inoltra ad Active Directory (AD) che lo convalida.

Se l'autenticazione è valida, WSA crea un surrogato IP associando il nome della workstation del computer all'indirizzo IP della workstation. Per le ulteriori richieste provenienti dallo stesso IP verrà utilizzato il nome della workstation sostitutiva.

Poiché il nome della workstation non è membro di alcun gruppo AD, le richieste potrebbero non attivare i criteri di accesso previsti e quindi essere bloccate. Il problema persiste fino al timeout del surrogato e fino al rinnovo dell'autenticazione. Questa volta, con un utente effettivo connesso e credenziali utente valide disponibili, verrà creato un nuovo surrogato IP con queste informazioni e ulteriori richieste corrisponderanno ai criteri di accesso previsti.

Un altro scenario è quello in cui le applicazioni inviano credenziali non valide (nome utente NULL e dominio NULL) e non credenziali di computer valide. Questa operazione viene considerata come un errore di autenticazione e verrà bloccata oppure, se i criteri guest sono abilitati, l'autenticazione non riuscita viene considerata come un "guest".

Il nome della workstation termina con una **$** seguita da **@DOMAIN** che semplifica la traccia dei nomi delle workstation utilizzando il comando **grep** della CLI nei log degli accessi per **$@**. Per ulteriori informazioni, vedere l'esempio seguente.

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

La riga precedente mostra un esempio di un surrogato IP già creato per l'indirizzo IP 10.20.30.40 e il nome del computer **gb0000d01$.**

Per trovare la richiesta che ha inviato il nome del computer, è necessario identificare la prima occorrenza del nome della workstation per l'indirizzo IP specifico. A tal fine, il comando CLI seguente:

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

Cercare nel risultato la prima occorrenza del nome della workstation. Le tre prime richieste vengono comunemente riconosciute come handshake NTLM Single-Sin-On (NTLMSSP/NTLMSSP) come descritto di seguito e illustrato nell'esempio seguente:

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

Durante la risoluzione dei problemi, verificare che queste richieste siano relative allo stesso URL e vengano registrate in un intervallo di tempo molto breve, a indicare che si tratta di un handshake NTLMSSP automatico.

Nell'esempio precedente, le richieste precedenti vengono registrate con il codice di risposta HTTP 407 (autenticazione proxy richiesta) per le richieste esplicite, mentre le richieste trasparenti vengono registrate con il codice di risposta HTTP 401 (non autenticate).

In AsyncOS 7.5.0 e versioni successive è disponibile una nuova funzionalità che consente di definire un timeout alternativo diverso per le credenziali del computer. Può essere configurato utilizzando il seguente comando:

```
> 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]>.
```

Èpossibile utilizzare gli stessi passaggi per rilevare quali richieste ottengono le credenziali NULL inviate e individuare quale URL o agente utente sta inviando le credenziali non valide e le esenta dall'autenticazione.

Esenzione dell'URL dall'autenticazione

Per evitare che questa richiesta causi la creazione del falso surrogato, l'URL deve essere esentato dall'autenticazione.Oppure, invece di esentare l'URL dall'autenticazione, si potrebbe decidere di esentare l'applicazione che invia la richiesta stessa dall'autenticazione, assicurandosi di ottenere tutte le richieste per l'applicazione da esentare dall'autenticazione. A tale scopo, è possibile aggiungere l'agente utente da registrare nei log degli accessi aggiungendo il parametro aggiuntivo **%u** nei **campi personalizzati** facoltativi nella sottoscrizione del log degli accessi di WSA. Dopo aver identificato l'agente utente, deve essere esentato dall'autenticazione.