为什么计算机名或NULL用户名登录访问日志？

目录

问题

- 为什么计算机名或NULL用户名登录访问日志？
- 您如何使用工作站或NULL凭证识别请求，以便稍后进行身份验证免除？

环境

- 思科网络安全设备(WSA) — 所有版本
- 带IP代理的身份验证方案NTLMSSP
- Windows Vista和更新的桌面和移动Microsoft操作系统

症状

WSA会阻止某些用户的请求或意外地执行操作。
访问日志显示计算机名称或NULL用户名和域，而不是用户ID。

问题在以下情况下自行解决：

- 代理超时（代理超时的默认值为60分钟）
- 正在重新启动代理进程(CLI命令> *diagnostic* > *proxy* > *kick*)
- 刷新身份验证缓存(CLI命令> *authcache* > *flushall*)

背景信息

在Microsoft操作系统的最新版本中，实际用户不再需要登录，应用程序就可以向Internet发送请求。当WSA收到这些请求并请求进行身份验证时，客户端工作站将无法使用任何用户凭证进行身份验证，而客户端工作站可能会使用计算机的计算机名称来替代。

WSA将获取提供的计算机名称并将其转发到验证该名称的Active Directory(AD)。

使用有效身份验证时，WSA会创建IP代理，将计算机的工作站名称绑定到工作站的IP地址。来自同一IP的进一步请求将使用代理名称，从而使用工作站名称。

由于工作站名称不是任何AD组的成员，请求可能不会触发预期的访问策略，因此会被阻止。问题持续存在，直到代理超时且必须续订身份验证。此时，在实际用户登录且有效用户凭证可用的情况下，将使用此信息创建新的IP代理，并且进一步的请求将与预期的访问策略匹配。

出现的另一种情况是应用程序发送无效凭据（NULL用户名和NULL域）和无效计算机凭据。这被视为身份验证失败，将被阻止；如果启用访客策略，则失败的身份验证被视为“访客”。

工作站名称以$结尾，后跟@DOMAIN，通过在$@的访问日志上使用CLI命令grep ，可以轻松跟踪工作站名称。请参阅以下示例，了解说明。

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

上一行显示已为IP地址10.20.30.40和计算机名gb0000d01$创建的IP代理的示

要查找发送计算机名称的请求，必须确定特定IP地址的工作站名称的首次出现。以下CLI命令可实现此目的：

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

搜索工作站名称首次出现的结果。这三个第一个请求通常被识别为NTLM单次单机(NTLMSSP/NTLMSSP)握手，如此处所述，如以下示例所示：

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

排除故障时，请确保这些请求针对同一URL，并且记录在非常短的时间间隔内，表明这是自动NTLMSSP握手。

在上例中，对于显式请求，使用HTTP响应代码407（需要代理身份验证）记录上述请求，而使用HTTP响应代码401（未经身份验证）记录透明请求。

AsyncOS 7.5.0及更高版本上提供了一项新功能，您可以在其中为计算机凭证定义不同的替代超时。可以使用以下命令进行配置：

```
> 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]>.
```

您可以使用相同步骤检测哪些请求获取发送的NULL凭证，并发现哪些URL或用户代理正在发送无效凭证并免除这些凭证的身份验证。

免除URL身份验证

为防止此请求导致创建虚假代理，必须免除URL身份验证。或者，您可能决定免除发送请求本身的应用程序进行身份验证，确保获得免除身份验证的应用程序请求。通过在WSA的访问日志订阅中的可选自定义字段中添加附加参数**%u**，可以添**加要**登录到访问日志的用户代理。在识别用户代理后，它必须免除身份验证。