为什么是计算机机器名字或NULL用户名登陆的accesslog ？

目录

问题

- 为什么是计算机机器名字或NULL用户名登陆的accesslog ？
- 如何识别请求使用工作站或最新验证免税的NULL凭证？

环境

- 思科Web安全工具(WSA) -所有版本
- 与IP代理人的认证机制NTLMSSP
- Windows比斯塔和更新的桌面和移动Microsoft操作系统

症状

WSA拒绝从一些用户的请求或意外地正常运行。
accesslog显示计算机机器名字或NULL用户名和域而不是用户标识。

问题以后解决自己：

- 代理人计时(代理人超时的默认值是60分钟)
- 重新启动代理进程(CLI命令> *诊断*> *代理*> *反撞力*)
- 冲洗的验证缓存(CLI命令> *authcache* > *flushall*)

背景信息

在Microsoft操作系统中最新版本，没有要求一个实际用户再登陆为了应用程序能再发送请求到互联网。当那些请求由WSA接收和请求验证时，用户凭证不是可用使用验证由可能采取计算机的机器名字对于替代品的客户端工作站。

WSA将采取提供的机器名字并且寄验证它的它给激活目录(AD)。

使用有效验证， WSA创建IP代理人绑定机器的工作站名称对工作站IP地址。来自同样IP的进一步请

求将使用代理人和因而工作站名称。

当工作站名称是任何AD组的成员，请求不可以触发预计访问策略和因而阻塞。问题持续，直到代理人计时了，并且验证必须被更新。这时，当一个实际用户登陆和有效用户凭证联机，一个新的IP代理人将创建与此信息，并且请求进一步将匹配预计访问策略。

被看到的另一个方案是，当应用程序发送凭据无效(NULL用户名和NULL域)时和无效计算机凭证。这认为认证失败，并且阻塞或者，如果访客策略启用，失败的验证考虑作为"访客"。

工作站名称以使工作站名称容易跟踪通过使用在accesslog的CLI命令**grep $@的@DOMAIN**跟随的一**$**结束。参见下面示例关于说明。

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

以上的线路显示为IP地址10.20.30.40和机器名字已经创建的IP代理人的示例**gb0000d01 $**

为了查找发送机器名字的请求，工作站名称的第一出现对于特定IP地址必须识别。以下CLI命令完成此：

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

搜索结果工作站名称的第一出现。 三第一请求在下面示例通常被认可作为单一罪孽在(NTLMSSP/NTLMSSP)握手的一NTLM如描述此处和显示：

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

当排除故障时，请保证这些thee请求是为同样URL和登陆indicatiting非常短时间的时间间隔它是自动化的NTLMSSP握手。

在以上示例中，先于的请求记录与明确请求的HTTP响应代码407 (要求的代理验证)，而透明请求将记录与HTTP响应代码401 (未经鉴定)。

有在AsyncOS 7.5.0的一新特性联机和更加高您能定义计算机凭证的地方一不同的代理人超时。使用以下命令，它可以配置：

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

您能使用请求获得NULL凭证发送的同样步骤检测并且发现哪个URL或用户代理发送凭据无效并且从验证豁免他们。

豁免从验证的URL

为了防止造成错误代理人的此请求创建， URL必须从验证被豁免。或者，而不是豁免从验证的URL，您也许决定豁免发送从验证的应用程序请求，确保获得所有要求应用程序从验证被豁免。这通过添加添加将登陆的accesslog用户代理是可能的在可选**自定义菲尔茨的**其它参数**%u** WSA的accesslog订阅的。在识别用户代理以后，它必须从验证被豁免。