post exploit part 1

الـPrivilege escalation هي عبارة عن أخذ صلاحيات أعلى.

يتم تقسيمها الى:

1-الـVertical : وهو عبارة عن الانتقال من Lower privilege الى Higher privilege .

2-الـHorizontal : وهو عبارة عن التبديل من مستخدم الى مستخدم أخر لهم نفس المسوى لكن عندة امكانيات أكثر.

بالبداية لازم نشيك على معلومات عن victim.

```
sysinfo
```

الـMaintaining : هي طريقه للحفاظ على الاتصال بعد الاختراق وذلك بتحقيق ثلاث أهداف:

1-الـStable

2-الـprivilege

3-الـpersistent

ليش نبغى نحصل على الـStable ؟

لأن وحدة من المشاكل عندنا كـPT عند الوصول للـ meterpreter session ممكن يقفل الـsession.

وعلشان يتم تحقيق الـ stable نستخدم مفهوم الـmigrate : وهي عبارة دمج process الىprocess أخرى.

يمكن عمل الـmigrate بشكل اوتماتيك باستخدام script بداخل الـmeterpreter او بشكل يدوي

```
1-Automatically
---------------------------------
getpid => see process before migrate

run post/windows/manage/migrate

getpid => see process after migrate
```

لاستعراض قائمه بكل الـprocesses المفتوحة.

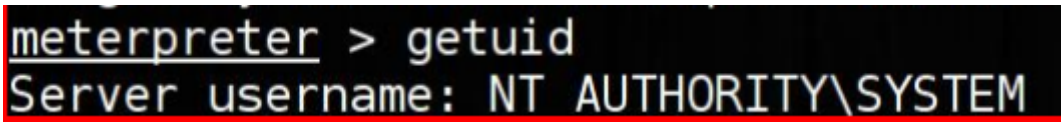
```
pc
```

```
2-manual
------------------------------
migrate -P <pid> |-N <name>
```

طيب الان نبغى اتصال دائم نستخدم مفهوم الـpersistent فعلشان نحققها لازم يكون عندنا Higher .privilege

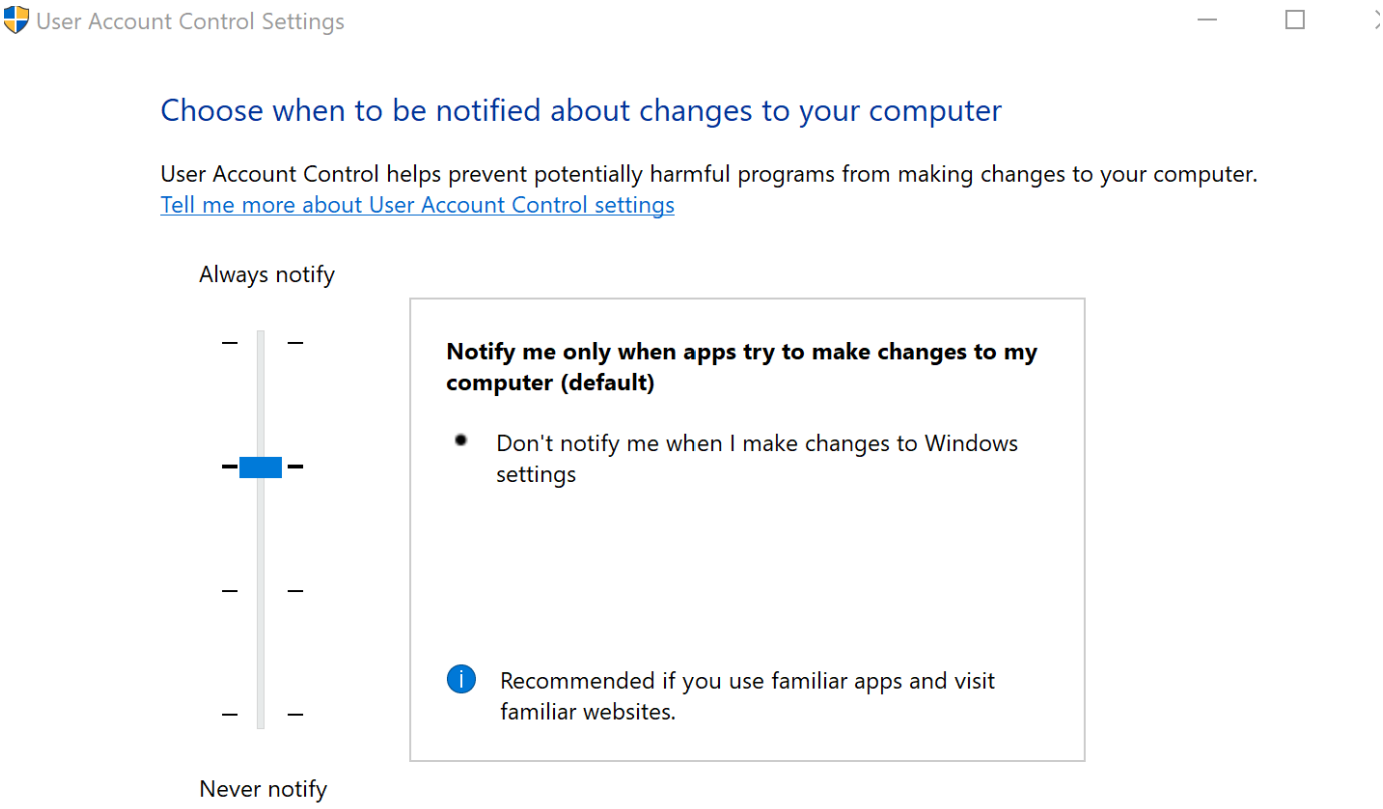
لو كان نظام التشغيل Windows نبدأ بـ أسهل طريقة للحصول على ترقية الصلاحيات وذلك باستخدام الأمر `getsystem` هذا بيشتغل اوتماتيك يجرب أفضل طريقة علشان يحصل على ترقية الصلاحيات.

```
getuid
getsystem
getuid
```



طبعا هذا الأمر ممكن أحيانا يشتغل وأحيانا لا !

حسب الـUser Account Control اذا كان enabled ماراح يزبط.



في حال كان الـUAC enabl نبع الخطوات :

1- نتأكد اذا الـUAC enabl من خلال هذا الـ Module

```
post/windows/gather/win_privs
```

```
meterpreter > run post/windows/gather/win_privs

Current User
============

 Is Admin  Is System  UAC Enabled  Foreground ID
 --------  ---------  -----------  -------------
 False     False      True         1
```

2-نبحث عن module يسمح بتخطي الـ UAC ونضع رقم الـ session ثم نشغل الـmodule

```
search bypassuac
```

All the best !

Asalah Mohammed..