



Colombia Hack Agent (CHackA)



### Colombia Hack Agent (CHackA)

```
[...] Developer:      Jairo A. García H.      [...]  
[...] Version:       1.0.                  [...]  
[...] Codename:      HACKLAB PARA CREAR METASPLOITABLE 2 EN VMWARE [...]  
[...] Report to:     chacka0101 @ gmail.com [...]  
[...] Homepage:      https://github.com/chacka0101/HACKLABS [...]  
[...] Publication Date: 2/Dec/2017          [...]
```

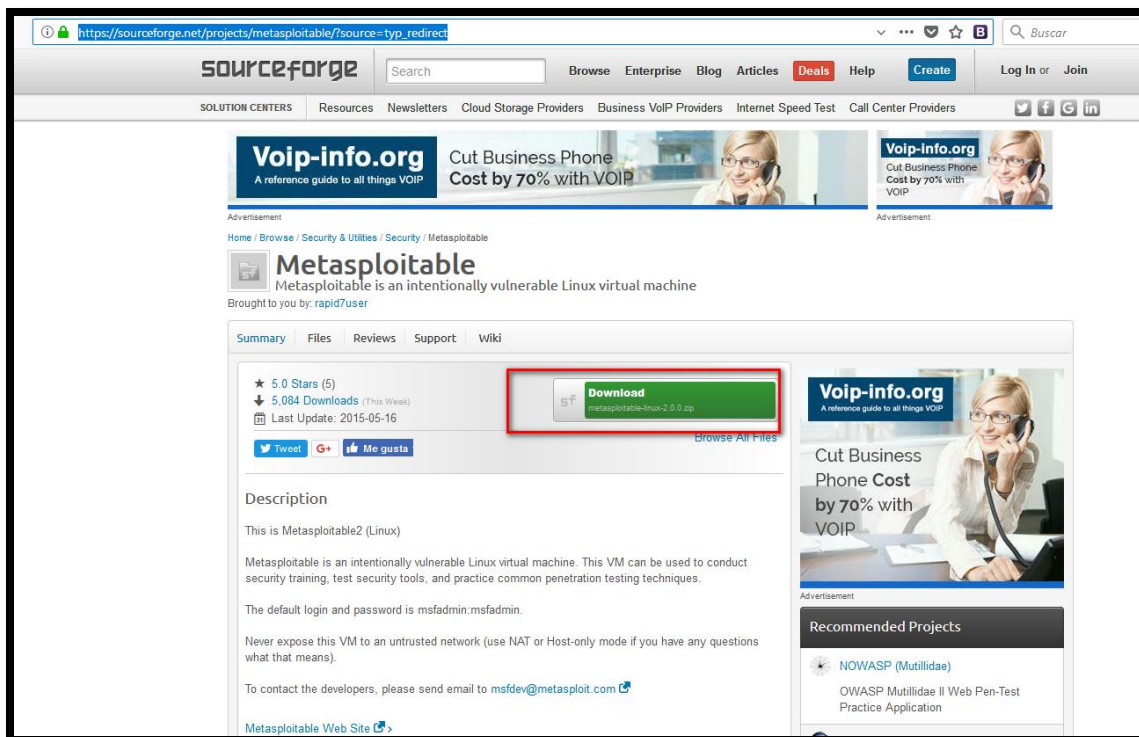
## HACKLAB PARA CREAR METASPLOITABLE 2 EN VMWARE

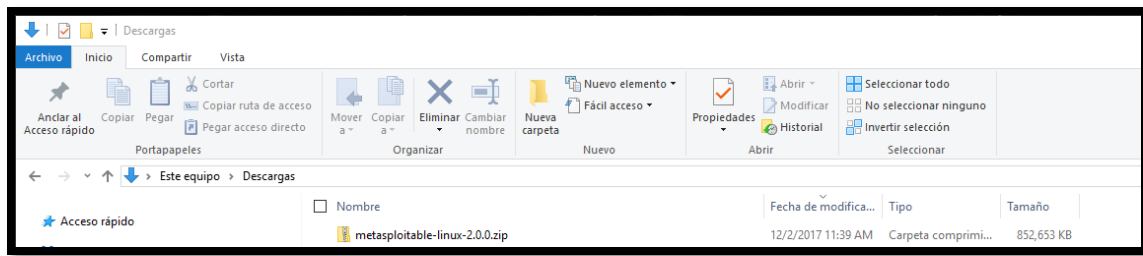
Resumen: El "Metasploitable 2" es un entorno de **Unix** "Vulnerable" que proporciona un ambiente controlado para realizar pruebas de Hacking y PenTest. Realizaremos la instalación del "Metasploitable 2" en una máquina virtual de VMWare.

Aplica para sistemas operativos: **WINDOWS**.

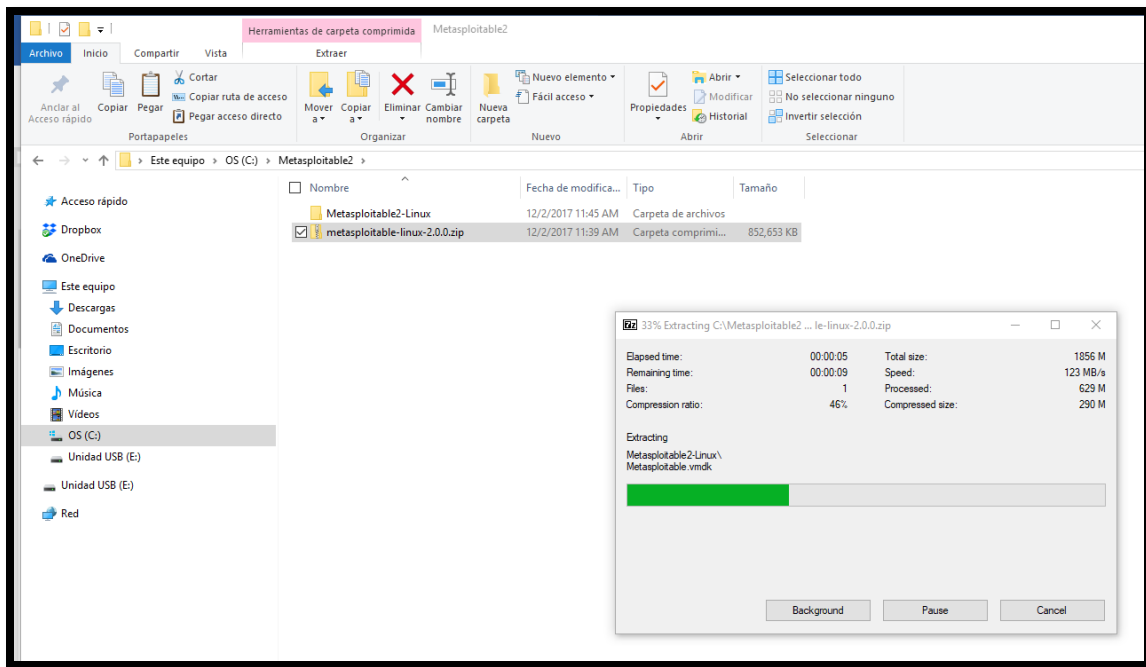
1. Descargar el "METASPLOITABLE 2" de alguna de las siguientes dos ubicaciones:

[https://sourceforge.net/projects/metasploitable/?source=typ\\_redirect](https://sourceforge.net/projects/metasploitable/?source=typ_redirect)

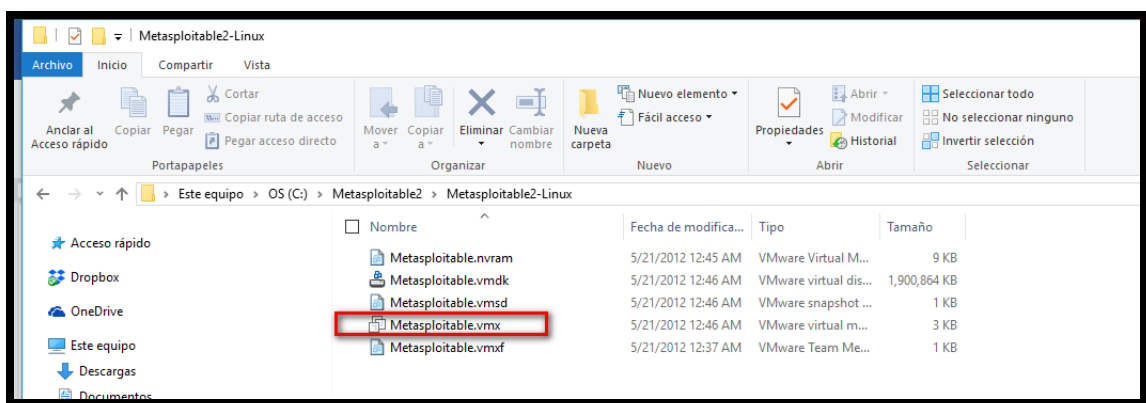


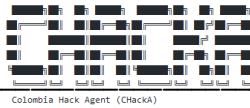


2. Copiamos él .zip a una nueva carpeta en C:, o donde ustedes consideren:

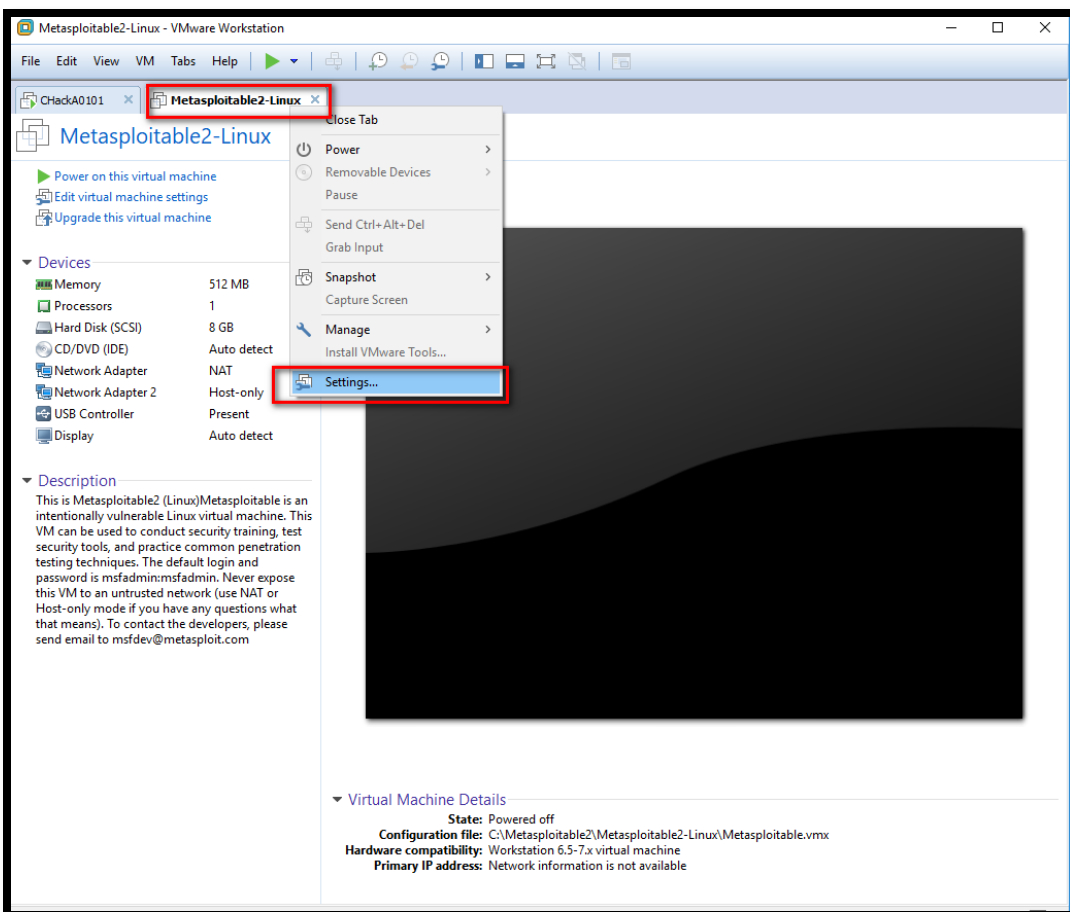
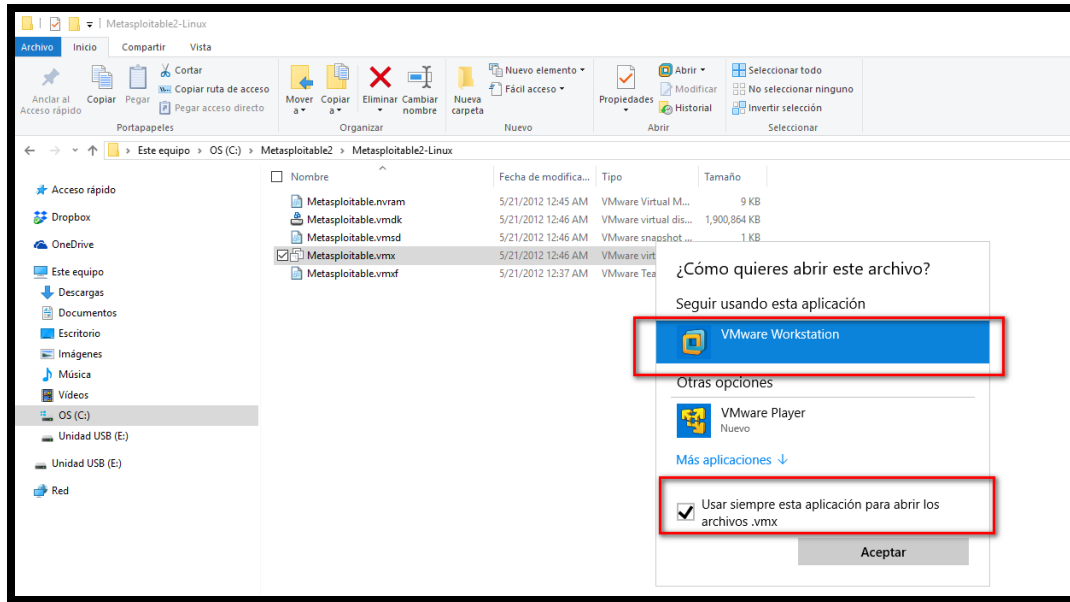


3. Doble clic en "Metasploitable.vmx":



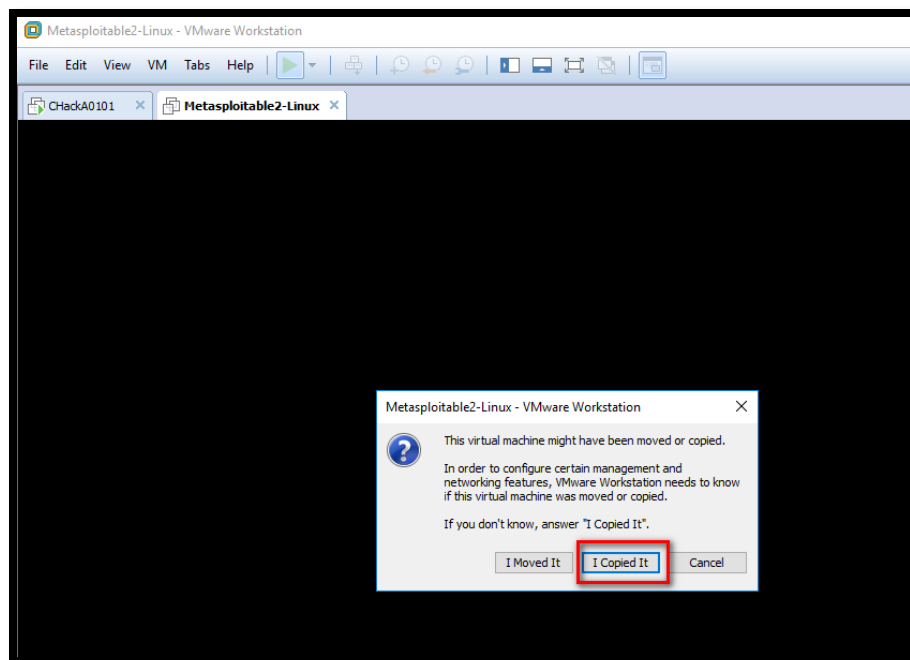
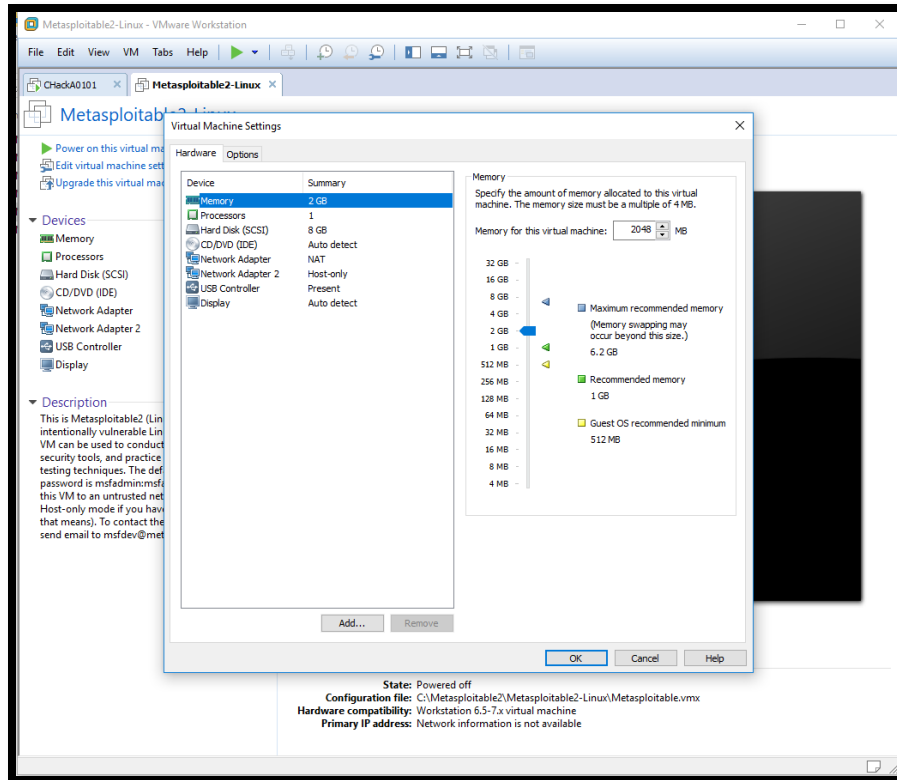


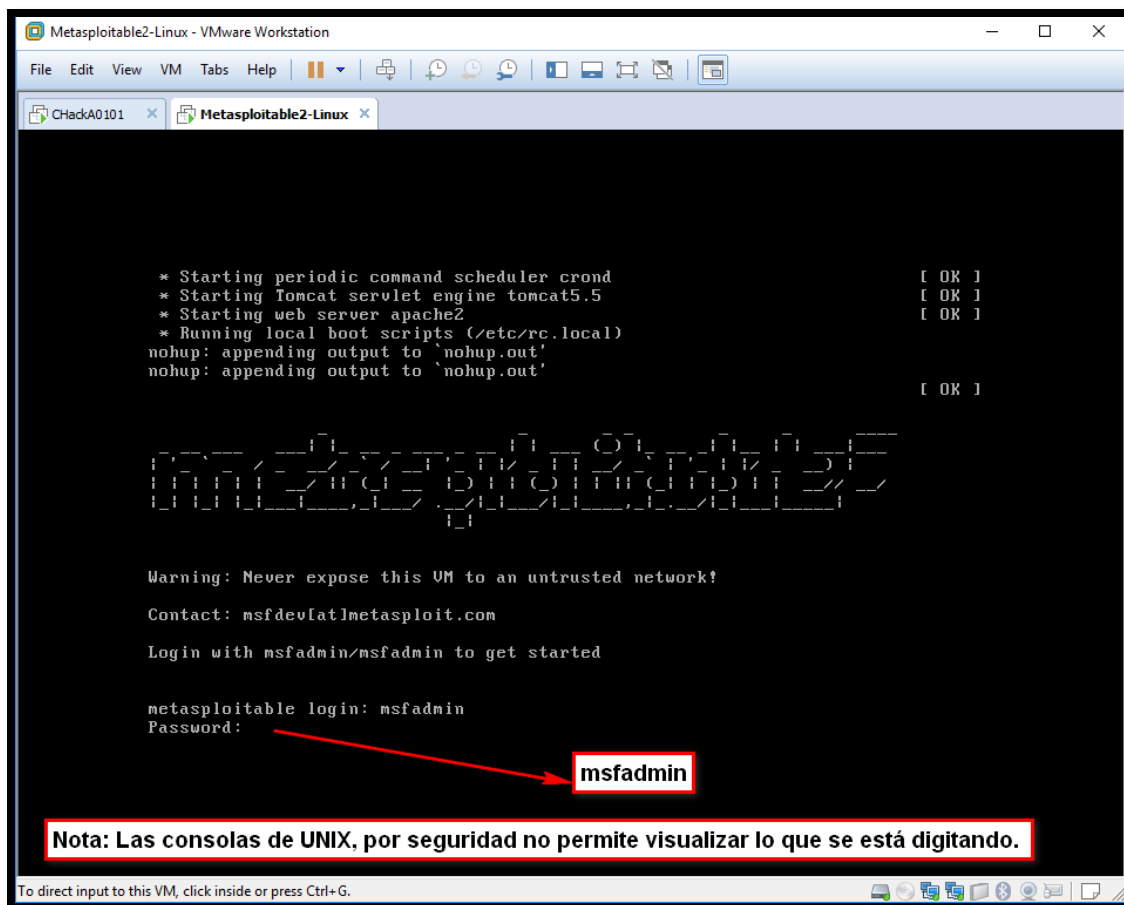
Colombia Hack Agent (CheckA)





Colombia Hack Agent (CheckA)





```

* Starting periodic command scheduler cron
* Starting Tomcat servlet engine tomcat5.5
* Starting web server apache2
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out'

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password: msfadmin

Nota: Las consolas de UNIX, por seguridad no permite visualizar lo que se está digitando.

```

```

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login: msfadmin
Password:
Last login: Mon May 21 01:44:38 EDT 2012 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$

```

4. Para finalizar digitamos el comando "ifconfig" con el fin de identificar la dirección IP que está asociada al "Metasploitable 2":

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:8f:cb:60
          inet addr:192.168.23.129  Bcast:192.168.23.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe8f:cb60/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:94 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:9648 (9.4 KB)  TX bytes:8678 (8.4 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:138 errors:0 dropped:0 overruns:0 frame:0
          TX packets:138 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:42061 (41.0 KB)  TX bytes:42061 (41.0 KB)

msfadmin@metasploitable:~$ _
```

Ya está lista la máquina para que sea atacada o vulnerada.

Puede consultar el **HACKLAB PARA EXPLOTACIÓN METASPLOITABLE 2**.

Agradecimientos a:

Rapid7 - <https://metasploit.help.rapid7.com/v1.1/docs/metasploitable-2>  
VMware - <https://www.vmware.com/>

**-END-**