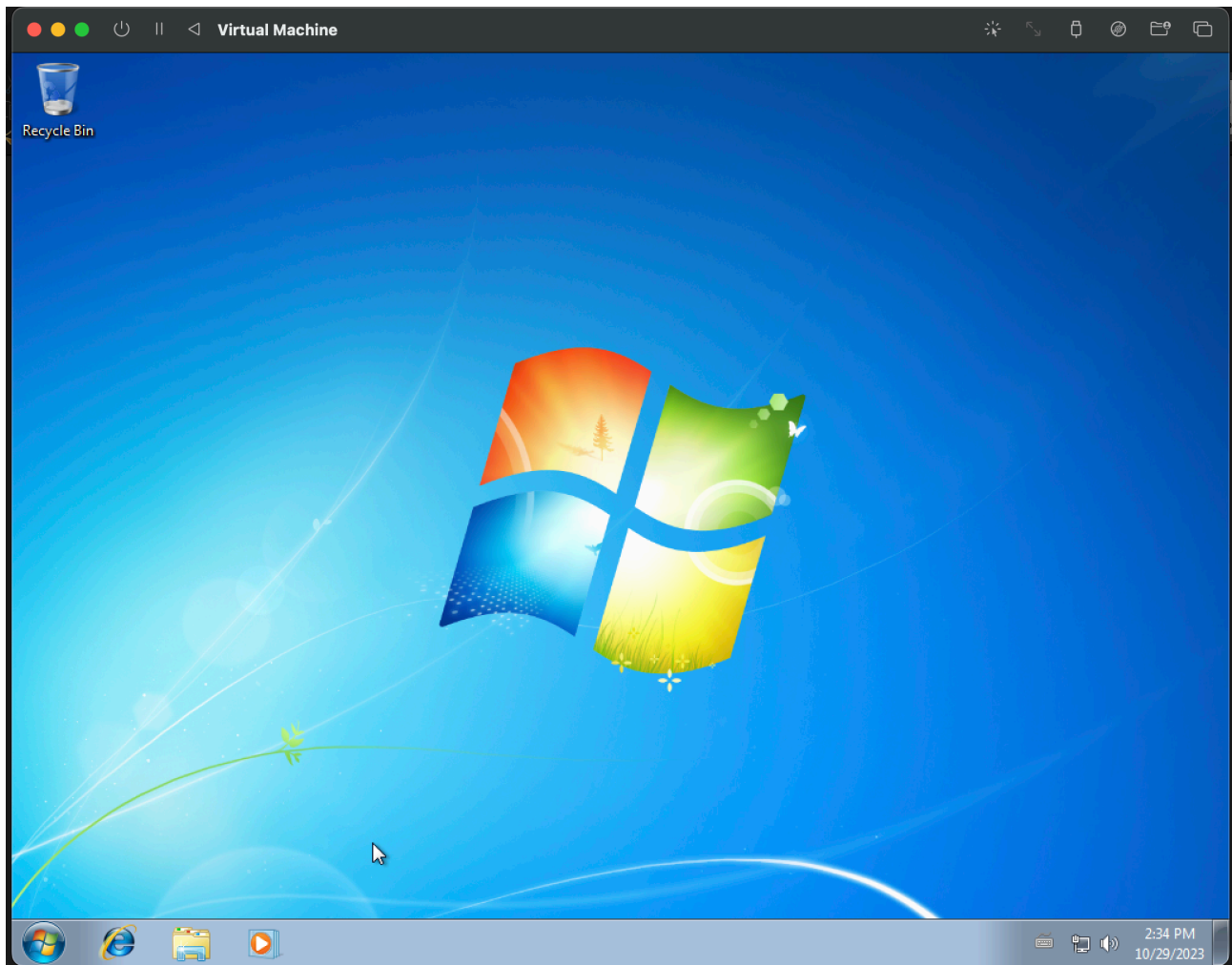


## EPICODE VIRTUAL LAB

Di seguito gli screenshot delle macchine virtuali utilizzando il software UTM e loro configurazione IP come da richiesta

Per la macchina windows il download è stato fatto dalla UTM gallery e poi il software viene emulato invece che virtualizzato così si può eseguire software per x86/x64



Per la macchina metasploitable è stato necessario installare ( aggiornare ) homebrew e poi utilizzare una conversione da vmdk a qcow2 che potesse essere digerita da utm

```
Metasploitable
* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

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

metasploitable login:
```

Kali aveva invece la versione preconfezionata

```
kali@kali: ~
File Actions Edit View Help
GNU nano 7.2 /etc/network/interfaces *
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

auto eth0
iface eth0 inet static
address 192.168.50.100/24
gateway 192.168.50.1

KALI LINUX
"the quieter you become, the more you are able to hear"

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify
```

```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.50.100 netmask 255.255.255.0 broadcast 192.168.50.255  
    inet6 fe80::e8f0:2fff:fe00:113a prefixlen 64 scopeid 0x20<link>  
    inet6 fd7d:eb20:58e9:cb6c:e8f0:2fff:fe00:113a prefixlen 64 scopeid  
    0x0<global>  
    ether ea:f0:2f:00:11:3a txqueuelen 1000 (Ethernet)  
    RX packets 2 bytes 284 (284.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 21 bytes 3349 (3.2 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 6 bytes 430 (430.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 6 bytes 430 (430.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
(kali@kali)-[~]  
$
```

```
Metasploitable  
GNU nano 2.0.7 File: /etc/network/interfaces Modified  
# This file describes the network interfaces available on your system  
# and how to activate them. For more information, see interfaces(5).  
  
# The loopback network interface  
auto lo  
iface lo inet loopback  
  
# The primary network interface  
auto eth0  
iface eth0 inet static  
address 192.168.50.101  
netmask 255.255.255.0  
network 192.168.50.0  
broadcast 192.168.50.255  
gateway 192.168.50.1_  
  
^G Get Help ^O WriteOut ^R Read File ^Y Prev Page ^K Cut Text ^C Cur Pos  
^X Exit ^J Justify ^W Where Is ^V Next Page ^U UnCut Text ^T To Spell
```

```
Metasploitable
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 1e:bd:d4:c8:f1:75
          inet addr:192.168.50.101  Bcast:192.168.50.255  Mask:255.255.255.0
          inet6 addr: fd7d:eb20:58e9:cb6c:1cbd:d4ff:fec8:f175/64 Scope:Global
          inet6 addr: fe80::1cbd:d4ff:fec8:f175/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3 errors:0 dropped:0 overruns:0 frame:0
          TX packets:69 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:438 (438.0 B)  TX bytes:4942 (4.8 KB)
          Base address:0xc000  Memory:feb00000-feb00000

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:117 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:25153 (24.5 KB)  TX bytes:25153 (24.5 KB)

msfadmin@metasploitable:~$ _
```

# Internet Protocol Version 4 (TCP/IPv4) Properties



## General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 50 . 102

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 50 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK

Cancel

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

C:\Users\Mc>ipconfig

Windows IP Configuration

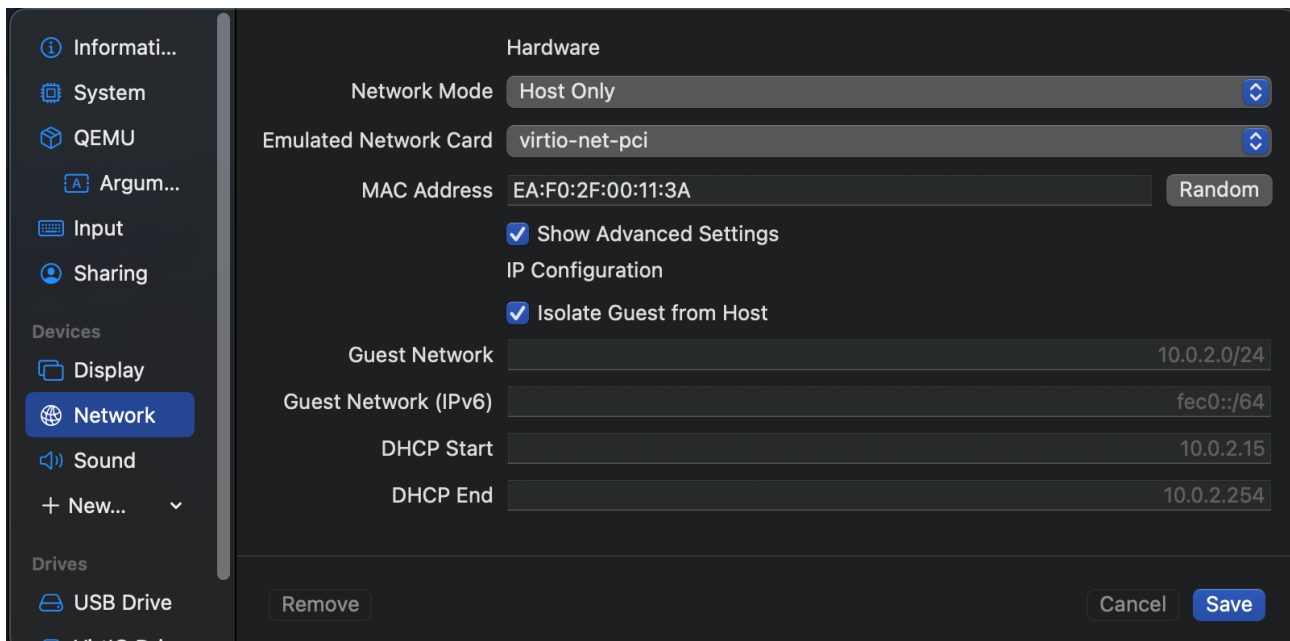
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : fd7d:eb20:58e9:cb6c:c920:78bb:50f9:a2f5
    Temporary IPv6 Address. . . . . : fd7d:eb20:58e9:cb6c:81a1:2655:2aaf:3dcf
    Link-local IPv6 Address . . . . . : fe80::c920:78bb:50f9:a2f5%11
    IPv4 Address. . . . . : 192.168.50.102
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.50.1

Tunnel adapter isatap.{3DEDA546-F1E0-486E-938B-8D0573FB38B1}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\Mc>
```



Senza togliere la spunta da “ Isolate Guest from Host “ le macchine non parlano tra loro

Viene lasciata la configurazione Host only senza la seconda spunta

Qui sotto esempio di raggiungimento altra macchina virtuale e di non raggiungimento server google



kali@kali: ~



File Actions Edit View Help

```
PING 192.168.50.101 (192.168.50.101) 56(84) bytes of data.  
64 bytes from 192.168.50.101: icmp_seq=1 ttl=64 time=3.17 ms  
64 bytes from 192.168.50.101: icmp_seq=2 ttl=64 time=2.53 ms  
64 bytes from 192.168.50.101: icmp_seq=3 ttl=64 time=2.50 ms  
64 bytes from 192.168.50.101: icmp_seq=4 ttl=64 time=5.42 ms  
64 bytes from 192.168.50.101: icmp_seq=5 ttl=64 time=2.49 ms  
64 bytes from 192.168.50.101: icmp_seq=6 ttl=64 time=2.44 ms  
64 bytes from 192.168.50.101: icmp_seq=7 ttl=64 time=3.55 ms  
64 bytes from 192.168.50.101: icmp_seq=8 ttl=64 time=3.01 ms  
64 bytes from 192.168.50.101: icmp_seq=9 ttl=64 time=2.70 ms
```

^Z

zsh: suspended ping 192.168.50.101

(kali@kali)-[~]

\$ ping 8.8.8.8

```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
From 192.168.50.100 icmp_seq=1 Destination Host Unreachable  
From 192.168.50.100 icmp_seq=2 Destination Host Unreachable  
From 192.168.50.100 icmp_seq=3 Destination Host Unreachable  
From 192.168.50.100 icmp_seq=4 Destination Host Unreachable  
From 192.168.50.100 icmp_seq=5 Destination Host Unreachable  
From 192.168.50.100 icmp_seq=6 Destination Host Unreachable
```

^Z

zsh: suspended ping 8.8.8.8

(kali@kali)-[~]

\$