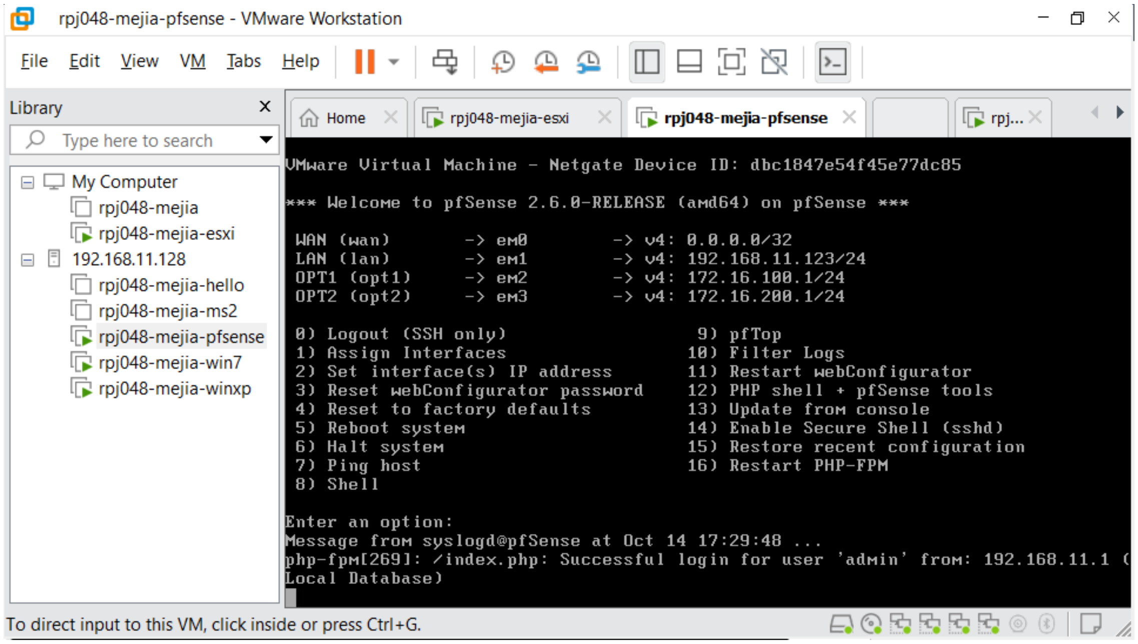
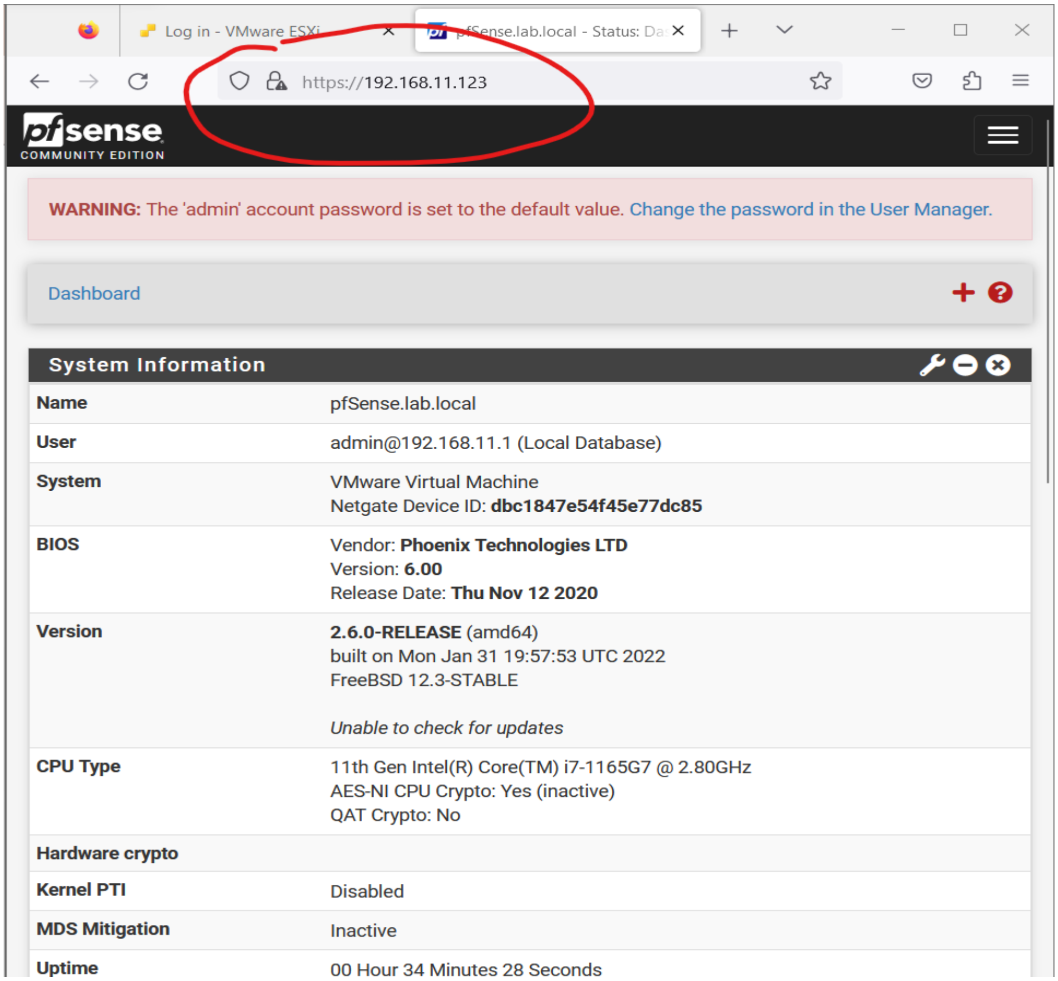
10/15/2023



```
VMware Virtual Machine - Netgate Device ID: dbc1847e54f45e77dc85

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

 WAN (wan)       -> em0        -> v4: 0.0.0.0/32
 LAN (lan)       -> em1        -> v4: 192.168.11.123/24
 OPT1 (opt1)     -> em2        -> v4: 172.16.100.1/24
 OPT2 (opt2)     -> em3        -> v4: 172.16.200.1/24

 0) Logout (SSH only)                  9) pfTop
 1) Assign Interfaces                 10) Filter Logs
 2) Set interface(s) IP address       11) Restart webConfigurator
 3) Reset webConfigurator password    12) PHP shell + pfSense tools
 4) Reset to factory defaults         13) Update from console
 5) Reboot system                     14) Enable Secure Shell (sshd)
 6) Halt system                       15) Restore recent configuration
 7) Ping host                         16) Restart PHP-FPM
 8) Shell

Enter an option:
Message from syslogd@pfSense at Oct 14 17:29:48 ...
php-fpm[269]: /index.php: Successful login for user 'admin' from: 192.168.11.1 (
Local Database)
```

Figure 17: Configured pfSense console window ^



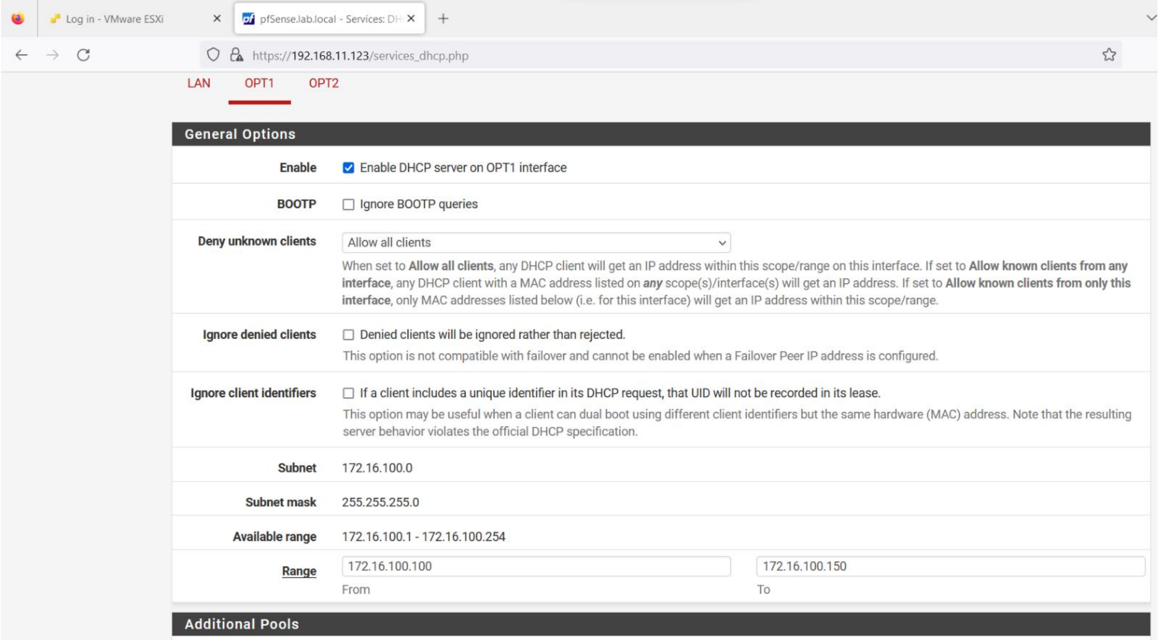
WARNING: The 'admin' account password is set to the default value. Change the password in the User Manager.

Dashboard

System Information

Name	pfSense.lab.local
User	admin@192.168.11.1 (Local Database)
System	VMware Virtual Machine Netgate Device ID: **dbc1847e54f45e77dc85**
BIOS	Vendor: **Phoenix Technologies LTD** Version: **6.00** Release Date: **Thu Nov 12 2020**
Version	**2.6.0-RELEASE** (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE *Unable to check for updates*
CPU Type	11th Gen Intel(R) Core(TM) i7-1165G7 @ 2.80GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Disabled
MDS Mitigation	Inactive
Uptime	00 Hour 34 Minutes 28 Seconds

Figure 18: Configured pfSense web interface


Log in - VMware ESXi
pfSense.lab.local - Services: DH
https://192.168.11.123/services_dhcp.php
LAN
OPT1
OPT2

General Options

Enable ☑ Enable DHCP server on OPT1 interface

BOOTP □ Ignore BOOTP queries

Deny unknown clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on ***any*** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients □ Denied clients will be ignored rather than rejected.

This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers □ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.

This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 172.16.100.0

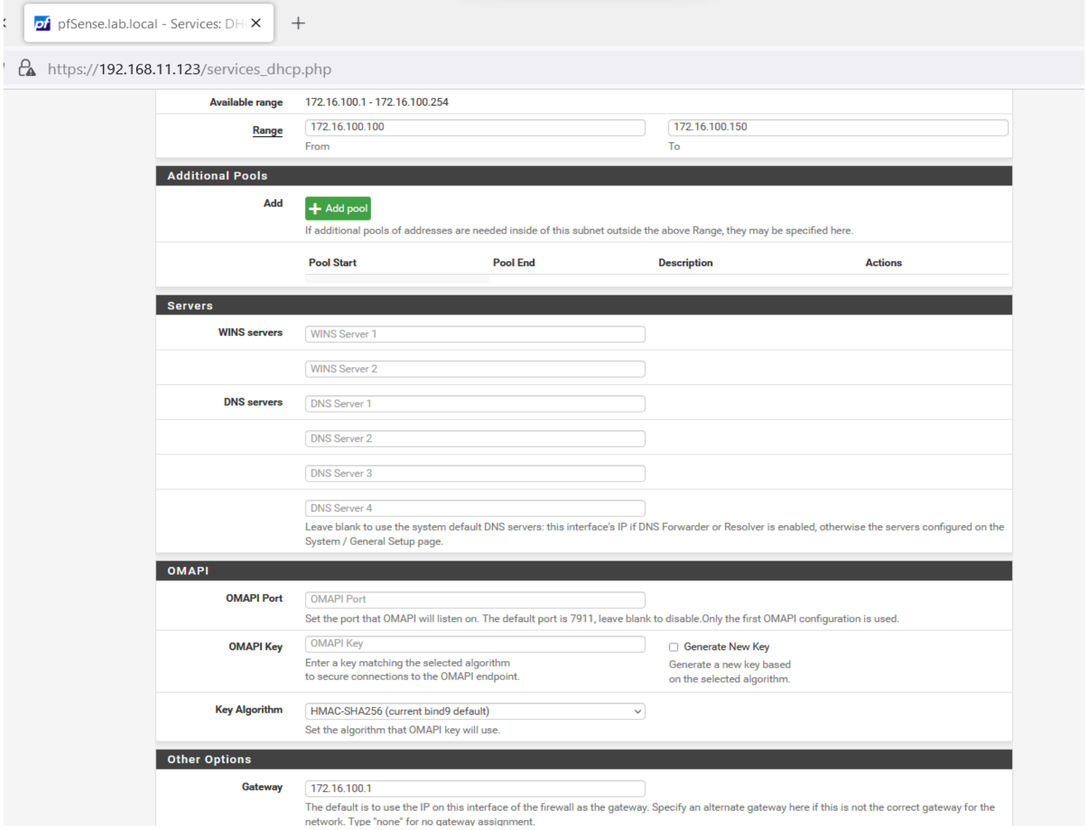
Subnet mask 255.255.255.0

Available range 172.16.100.1 - 172.16.100.254

Range 172.16.100.100 (From) 172.16.100.150 (To)

Additional Pools

Figure 19: Sample capture for enable and address pool for OPT1


pfSense.lab.local - Services: DH
https://192.168.11.123/services_dhcp.php
Add pool

Available range 172.16.100.1 - 172.16.100.254

Range 172.16.100.100 (From) 172.16.100.150 (To)

Additional Pools

Add Add pool

If additional pools of addresses are needed inside of this subnet outside the above Range, they may be specified here.

Pool Start	Pool End	Description	Actions

Servers

WINS servers WINS Server 1

WINS Server 2

DNS servers DNS Server 1

DNS Server 2

DNS Server 3

DNS Server 4

Leave blank to use the system default DNS servers: this interface's IP if DNS Forwarder or Resolver is enabled, otherwise the servers configured on the System / General Setup page.

OMAPI

OMAPI Port OMAPI Port

Set the port that OMAPI will listen on. The default port is 7911, leave blank to disable.Only the first OMAPI configuration is used.

OMAPI Key OMAPI Key

Enter a key matching the selected algorithm
to secure connections to the OMAPI endpoint.

□ Generate New Key

Generate a new key based
on the selected algorithm.

Key Algorithm HMAC-SHA256 (current bind9 default)

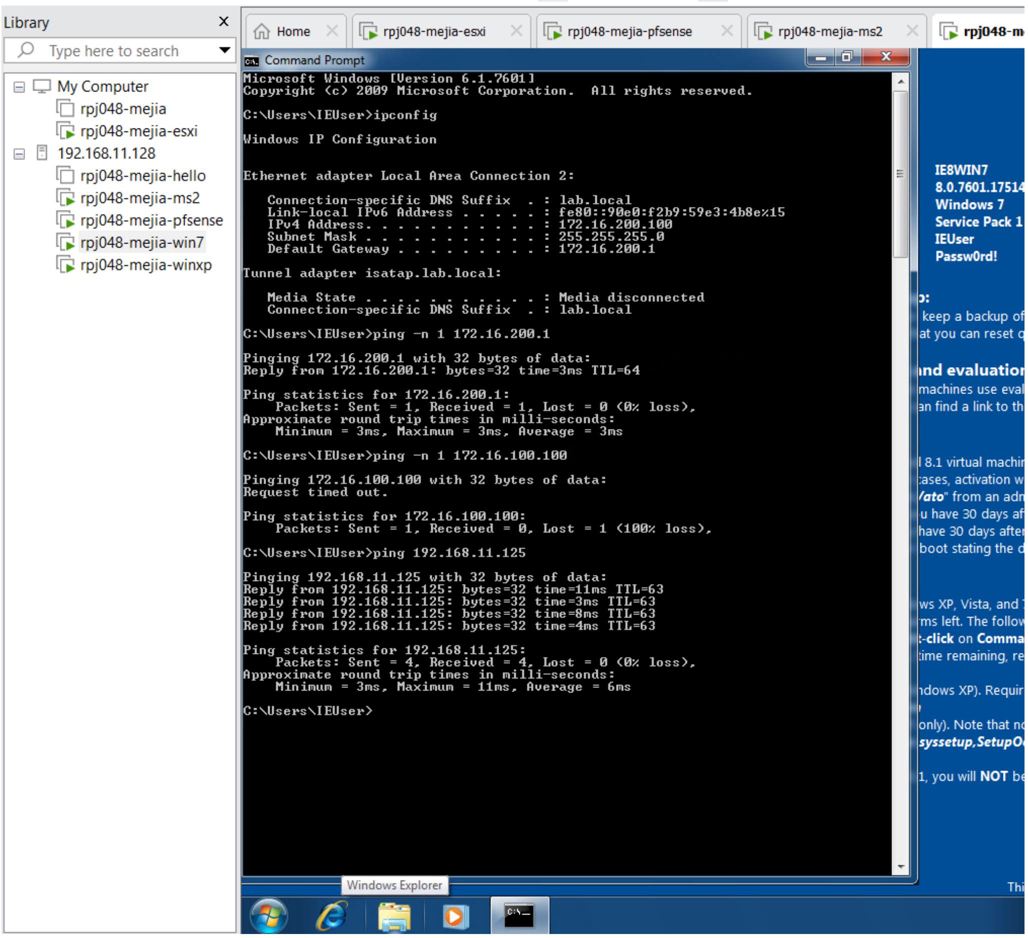
Set the algorithm that OMAPI key will use.

Other Options

Gateway 172.16.100.1

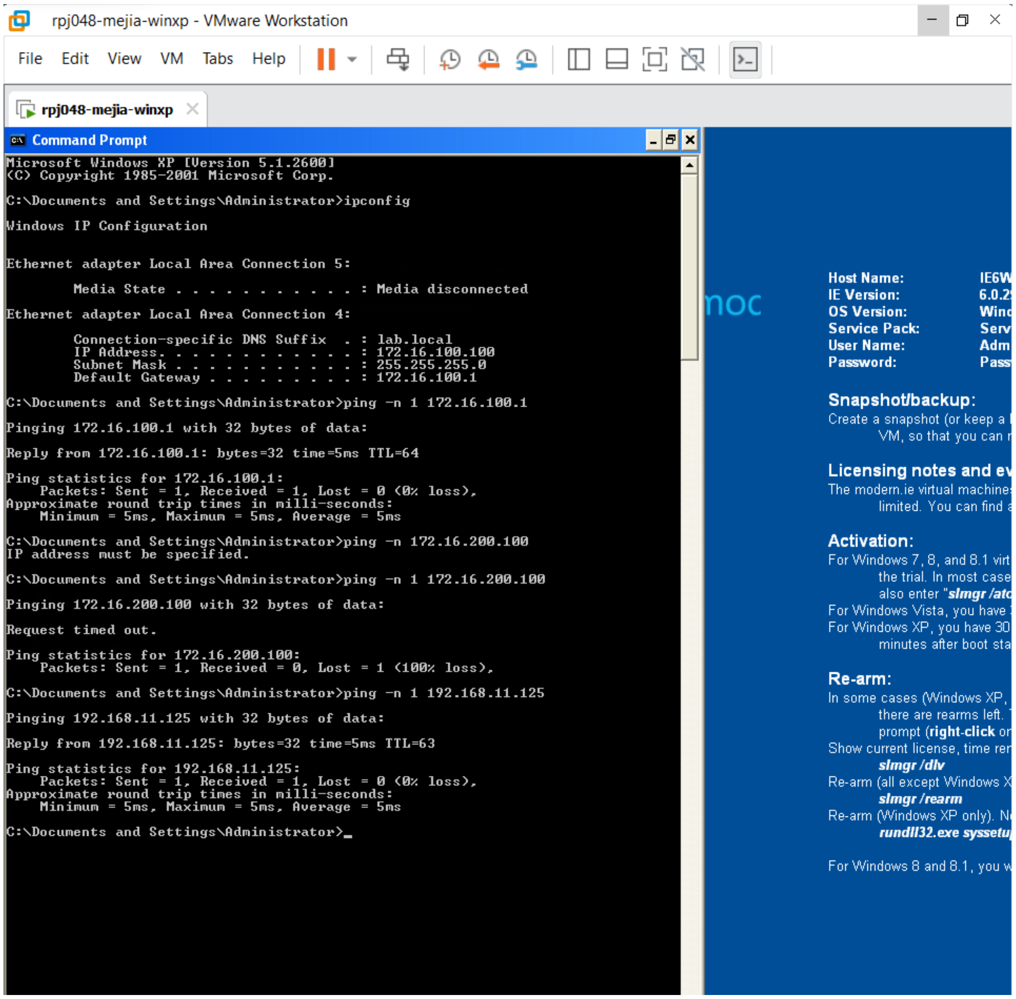
The default is to use the IP on this interface of the firewall as the gateway. Specify an alternate gateway here if this is not the correct gateway for the network. Type "none" for no gateway assignment.

Figure 20: Sample capture for address pool and gateway for OPT1



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : lab.local
   Link-local IPv6 Address . . . . . : fe80::90e0:f2b9:59e3:4b8e%15
   IPv4 Address. . . . . . . . . . . : 172.16.200.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.200.1

Tunnel adapter isatap.lab.local:

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

C:\Users\IEUser>ping -n 1 172.16.200.1

Pinging 172.16.200.1 with 32 bytes of data:
Reply from 172.16.200.1: bytes=32 time=3ms TTL=64

Ping statistics for 172.16.200.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms

C:\Users\IEUser>ping -n 1 172.16.100.100

Pinging 172.16.100.100 with 32 bytes of data:
Request timed out.

Ping statistics for 172.16.100.100:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Users\IEUser>ping 192.168.11.125

Pinging 192.168.11.125 with 32 bytes of data:
Reply from 192.168.11.125: bytes=32 time=11ms TTL=63
Reply from 192.168.11.125: bytes=32 time=3ms TTL=63
Reply from 192.168.11.125: bytes=32 time=8ms TTL=63
Reply from 192.168.11.125: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.11.125:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 11ms, Average = 6ms

C:\Users\IEUser>
```

Figure 21: Sample turn-in artifact for the Windows 7 VM



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 5:

        Media State . . . . . . . . . . . : Media disconnected

Ethernet adapter Local Area Connection 4:

        Connection-specific DNS Suffix  . : lab.local
        IP Address. . . . . . . . . . . . : 172.16.100.100
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 172.16.100.1

C:\Documents and Settings\Administrator>ping -n 1 172.16.100.1

Pinging 172.16.100.1 with 32 bytes of data:

Reply from 172.16.100.1: bytes=32 time=5ms TTL=64

Ping statistics for 172.16.100.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Documents and Settings\Administrator>ping -n 172.16.200.100
IP address must be specified.

C:\Documents and Settings\Administrator>ping -n 1 172.16.200.100

Pinging 172.16.200.100 with 32 bytes of data:

Request timed out.

Ping statistics for 172.16.200.100:
    Packets: Sent = 1, Received = 0, Lost = 1 (100% loss),

C:\Documents and Settings\Administrator>ping -n 1 192.168.11.125

Pinging 192.168.11.125 with 32 bytes of data:

Reply from 192.168.11.125: bytes=32 time=5ms TTL=63

Ping statistics for 192.168.11.125:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

C:\Documents and Settings\Administrator>_
```

moc

Host Name: IE6W
IE Version: 6.0.2
OS Version: Winc
Service Pack: Serv
User Name: Adm
Password: Pass

Snapshot/backup:
Create a snapshot (or keep a
VM, so that you can r

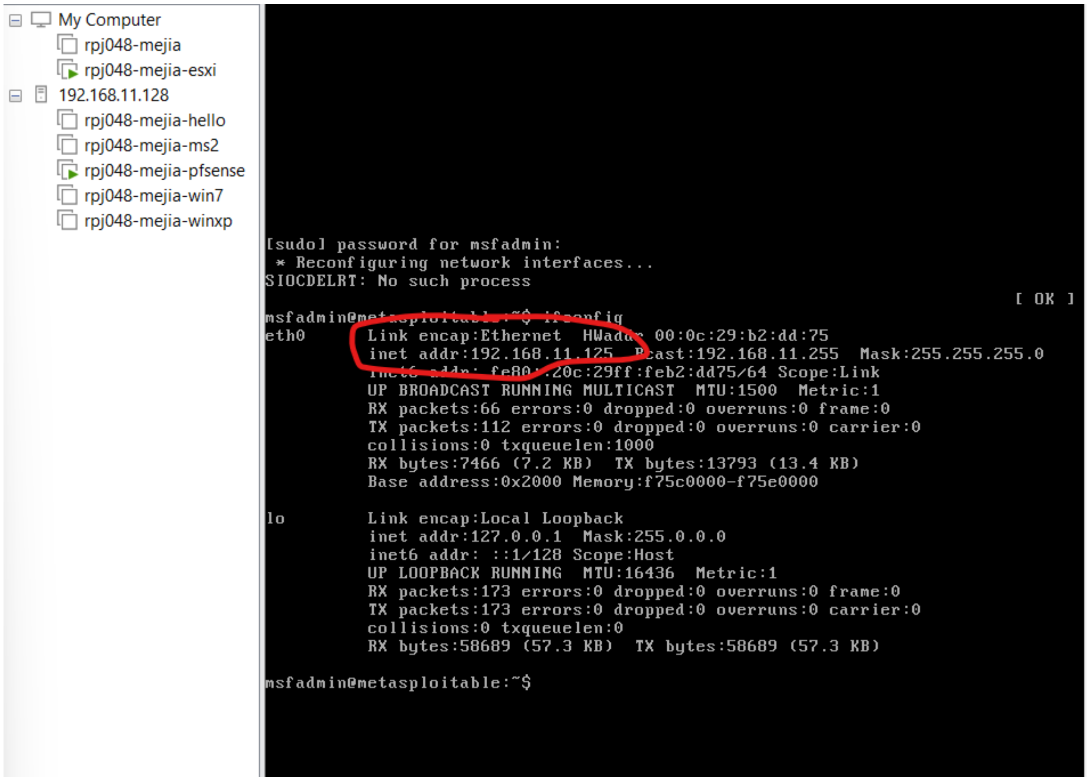
Licensing notes and ev
The modern.ie virtual machine
limited. You can find a

Activation:
For Windows 7, 8, and 8.1 virt
the trial. In most case
also enter "***slmgr /atc***
For Windows Vista, you have
For Windows XP, you have 30
minutes after boot sta

Re-arm:
In some cases (Windows XP,
there are rearms left.
prompt (**right-click** or
Show current license, time rer
slmgr /dlv
Re-arm (all except Windows X
slmgr /rearm
Re-arm (Windows XP only). N
rundll32.exe sysset

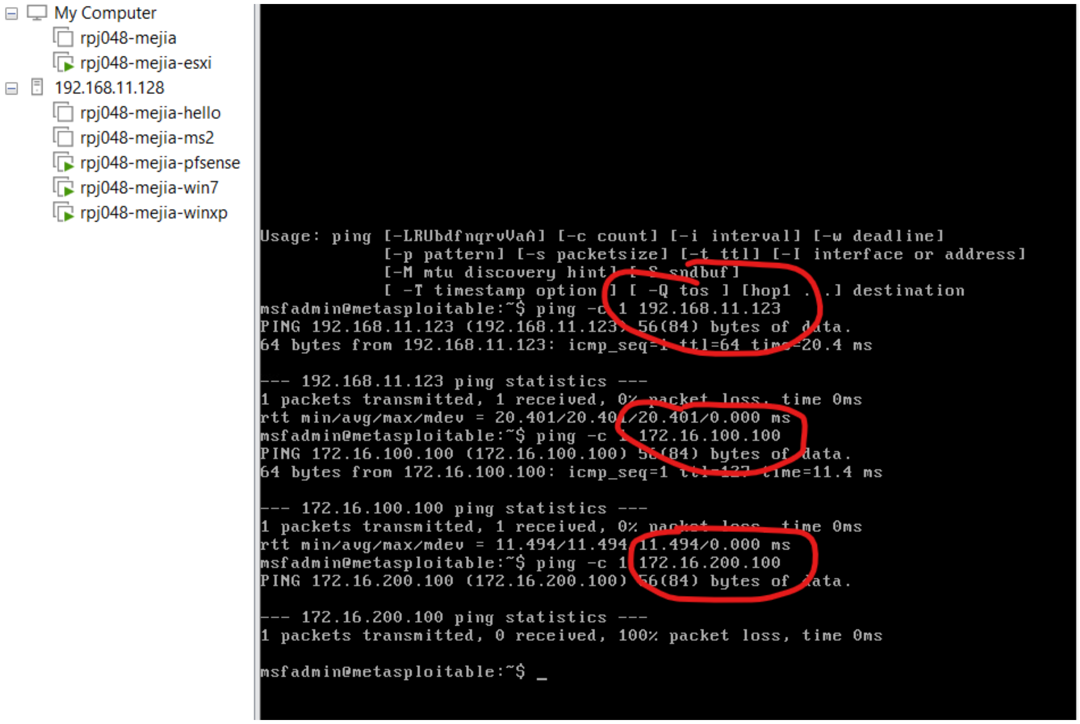
For Windows 8 and 8.1, you w

Figure 22: Sample turn-in artifact for Win XP virtual machine



```
[sudo] password for msfadmin:
 * Reconfiguring network interfaces...
SIOCDELRT: No such process
                                                                   [ OK ]
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:b2:dd:75
          inet addr:192.168.11.125  Bcast:192.168.11.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:feb2:dd75/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:66 errors:0 dropped:0 overruns:0 frame:0
          TX packets:112 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7466 (7.2 KB)  TX bytes:13793 (13.4 KB)
          Base address:0x2000 Memory:f75c0000-f75e0000

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:173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:173 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:58689 (57.3 KB)  TX bytes:58689 (57.3 KB)

msfadmin@metasploitable:~$
```

Figure 23: Screenshot showing MS2 virtual machine IP address



```
Usage: ping [-LRUbdfnqrvVaA] [-c count] [-i interval] [-w deadline]
            [-p pattern] [-s packetsize] [-t ttl] [-I interface or address]
            [-M mtu discovery hint] [-S sndbuf]
            [ -T timestamp option ] [ -Q tos ] [hop1 ...] destination
msfadmin@metasploitable:~$ ping -c 1 192.168.11.123
PING 192.168.11.123 (192.168.11.123) 56(84) bytes of data.
64 bytes from 192.168.11.123: icmp_seq=1 ttl=64 time=20.4 ms

--- 192.168.11.123 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 20.401/20.401/20.401/0.000 ms
msfadmin@metasploitable:~$ ping -c 1 172.16.100.100
PING 172.16.100.100 (172.16.100.100) 56(84) bytes of data.
64 bytes from 172.16.100.100: icmp_seq=1 ttl=127 time=11.4 ms

--- 172.16.100.100 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 11.494/11.494/11.494/0.000 ms
msfadmin@metasploitable:~$ ping -c 1 172.16.200.100
PING 172.16.200.100 (172.16.200.100) 56(84) bytes of data.

--- 172.16.200.100 ping statistics ---
1 packets transmitted, 0 received, 100% packet loss, time 0ms

msfadmin@metasploitable:~$ _
```

Figure 24: Screenshot showing sample MS2 virtual machine pings