Introduction

Thank you for using AC-Hunter!

This guide will walk you through installing an AC-Hunter virtual machine for VMWare.

This guide does not cover how to install AC-Hunter from a ".tar" file using the script install_acm.sh . If you have these, please see the "AC-Hunter Install Guide" instead.

Steps

Prerequisites

1. You'll need the AC-Hunter virtual machine. This is sent out as a zip file. A link to this zip file (and all other AC-Hunter CE resources) can be found at https://www.activecountermeasures.com/ac-hunter-community-edition/ .
2. Your computer must provide a 64-bit Intel or AMD architecture, commonly called "x86_64". Most systems fall in this category with the exception of computers with ARM chips or Apple systems with an M1 or M2 processor. If the command `uname -m` on a Linux or MacOS system returns `x86_64` you're all set.

3. Your computer will need a copy of VMWare installed. This can be VMWare Workstation (14.x or higher), Fusion (10.x or higher), or ESXi (6.7 or higher). It may work with VMWare Player as well.
4. If you plan to have regular feeds from a sensor, we recommend at least 300GB of drive space to hold the virtual machine and data. If you plan to use this for testing but won't have a regular feed from a sensor, we recommend at least 200GB of drive space.

Steps to install AC_Hunter

1. Create an empty directory for placing the virtual machine. We recommend "ac-hunter-vm" inside your home directory. On Linux or MacOS, run:

```
cd
mkdir -p ac-hunter-vm ac-hunter-storage
cd ac-hunter-vm
```

2. If you have not already done so, download the AC-Hunter virtual machine zip file to this directory.
3. Open up the zip file using a zip utility included with your operating system.
4. If it's not already running, start up VMWare on your host computer.
5. Choose "Open a virtual machine"; this may be an icon you'll double-click or the menu item "Open" under the File menu. Navigate to the "ac-hunter-vm" directory, and if there's an additional directory under that go into that as well. Select the file ending in "**.vmx**" and choose Open/Continue/Next/OK.
    a. **Do not start the virtual machine yet.**
    b. (As a side note, if you're running VMWare Fusion you may be able to replace the above instructions with "Drag and drop the .vmx file into the main VMWare window".)
6. Choose Edit Virtual Machine Settings. (If this is not visible, go to the "VM" menu and choose "Settings".)
    a. Under "Memory": This needs to be at least 12GB. If you intend to use this for light testing you may be able to set this to 12GB. For regular use we recommend at least 16GB. If you are monitoring a heavily loaded network you may need more memory, perhaps 32GB or more.
    b. Under "Processors": You should have at least 4 processor cores.
    c. Create the storage for AC-Hunter. This is a second virtual disk that will hold your incoming logs and AC-Hunter databases.
        i. Press "+ Add", select "Hard Disk", and press "Next".
        ii. The Virtual Disk Type should be "SCSI"; press "Next" again.
        iii. In most cases you'll select "Create a new virtual disk". If you're upgrading from a previous version of AC-Hunter you can select "Use an existing virtual disk", but first make sure that the previous version of AC-Hunter is shut down and the virtual disk is no longer attached to the old version.
        iv. Choose your maximum disk size. This should be well below the available drive space on your system. We recommend a minimum of 200GB, and

encourage much more if you have the space available. By leaving "Allocate all disk space now" **unchecked**, this will start very small and grow to your limit as needed. We recommend storing this virtual disk as a single file, though "multiple files" works too.

v. We recommend naming the virtual disk "ac-hunter-storage.vmdk" and placing it in ~/ac-hunter-storage/ (so it can be reused when you upgrade to a new virtual machine.) Press Finish.

d. You **should not** mount this drive - that is handled automatically.
e. Save your changes with the "Save" button.
f. If you have any questions about the values to use for any of the above, please see the Pre-Install Guide.

7. Start the AC-Hunter virtual machine with the light green "Play" button.
   a. The start will take a little longer than normal, and the system should reboot itself automatically after running some setup steps for your new storage.
   b. You may be asked "Do you want to create a new unique identifier (UUID) for the virtual machine or keep the old one?" If so, please answer "Create"
   c. You may also be asked whether this virtual machine was moved or copied. Please answer "I copied it."
   d. Look at the vmware console. You will see a message there with the automatically changed password for the dataimport account. **Please save this password in your password safe now**.
   e. Log in on the console as the dataimport user with the supplied password.
   f. The system will print out the IP addresses of this system - record the IPv4 address as you'll need it to set up the networking. If it scrolls off the screen, you can see it again by running:

```
ip addr show dev ens33 | grep 'inet '
```

   It'll be the 4 dot-separated numbers immediately before "/".

   g. Run:

```
manage_web_user.sh reset -u 'welcome@activecountermeasures.com'
```

   You'll be prompted for a password. Remember this, as you'll need it to log in to AC-Hunter's web interface later.

   h. Type:

```
exit
```

   to log out, then shut the virtual machine down with the red shutdown button.

8. Under the "Edit" menu select "Virtual Network Editor". You will likely have to provide your user password to make the following changes.
   a. Select the network interface whose External Connection is labeled "NAT".
   b. Press the "NAT Settings" button.
   c. Go down to the table named "Port Forwarding"
   d. To allow you to ssh to the system:
      i. Press Add
      ii. Host port: 2222
      iii. Type: TCP
      iv. Virtual machine IP address: the address you noted above

v. Virtual machine port: 22
vi. Description: AC-Hunter SSH
vii. Press "Save"

e. To allow you to access the web interface
i. Press Add
ii. Host port: 8443
iii. Type: TCP
iv. Virtual machine IP address: the address you noted above
v. Virtual machine port: 443
vi. Description: AC-Hunter Web
vii. Press "Save"

f. To allow you to use the Cyber Deception module
i. Press Add
ii. Host port: 39839
iii. Type: TCP
iv. Virtual machine IP address: the address you noted above
v. Virtual machine port: 39839
vi. Description: AC-Hunter deception 1
vii. Press "Save"
viii. Press Add
ix. Host port: 39840
x. Type: TCP
xi. Virtual machine IP address: the address you noted above
xii. Virtual machine port: 39840
xiii. Description: AC-Hunter deception 2
xiv. Press "Save"

g. Press "Save" in the "NAT Settings" and "Virtual Network Editor" boxes.

h. To reach your AC-Hunter system you'll need to use the IP address of the **vmware host** system.
i. To reach the AC-Hunter web user interface, go to https://*vmware.host.ip.address*:8443
Since this copy of AC-Hunter only has a test certificate, you'll need to acknowledge this in most browsers to continue to the web interface.
ii. To ssh to the AC-Hunter system, use:

```
ssh -p 2222 dataimport@vmware.host.ip.address
```

9. To remember the port number and username for all future connections
a. On the Zeek sensor, edit /etc/ssh/ssh_config under sudo (`sudo nano /etc/ssh/ssh_config`). In that file, place the following block *above* a line starting with "Host *" (or if there isn't one, place this block at the end of the file):

```
Host achunter-vm
     Hostname              vmware.host.ip.address
     Port                  2222
     User                  dataimport
     HostKeyAlias          achunter-vm
```

b. To test this, run this on the Zeek sensor:

```
ssh achunter-vm
```

You may be asked to confirm the host key; if the value you're handed back matches the output from running

```
sudo ssh-keygen -l -f /etc/ssh/ssh_host_rsa_key
```

on the AC-Hunter VM, you can say yes.

c. From this point on whenever you need to enter the hostname or IP address of the AC-Hunter server, use "achunter-vm" instead.

d. If you run MacOS or Linux on your laptop, perform the previous steps (creating the new block inside /etc/ssh/ssh_config) again there. If you are using Windows or are using something other than a command line ssh, refer to your documentation for how to set up and remember an ssh connection with alternate username ("dataimport") and port ("2222").

10. Now log in to the AC-Hunter interface with the URL: https://*ip.address.of.host*:8443

When asked for a Username and Password, enter "welcome@activecountermeasures.com" and the password you entered above.

Steps to install Zeek

The Zeek software should be placed on a separate (physical) system. See the Pre-Install Guide for more details about the system needs for it. We recommend placing it on a physical system with an Intel or AMD 64-bit processor (if the command `uname -m` on a Linux or MacOS system returns `x86_64` you're all set.) We also recommend running Ubuntu Linux or Centos/RHEL Linux; see the Pre-Install Guide for more details about the supported Linux versions.

1. Log into the Zeek sensor system.
2. Pull down and install Zeek with the following commands. Note that the second command will wrap inside this document, but each of the 5 following commands should be run without linefeeds in the middle:

```
curl -fsSL https://get.docker.com | sh -

sudo wget -O /usr/local/bin/zeek
https://raw.githubusercontent.com/activecm/docker-zeek/master/zeek

sudo chmod +x /usr/local/bin/zeek

zeek pull
```

```
zeek start
```

3. If you have not yet edited /etc/ssh/ssh_config on the Zeek sensor, do that now (see above).
4. Connect the Zeek sensor to the AC-Hunter system so it can send over logs every hour with the following commands. Note that these will wrap inside this document, but each of the 4 following commands should be run without linefeeds in the middle:

```
curl -fsSL
https://raw.githubusercontent.com/activecm/zeek-log-transport/master/
connect_sensor.sh -O

curl -fsSL
https://raw.githubusercontent.com/activecm/shell-lib/master/acmlib.sh
-O

curl -fsSL
https://raw.githubusercontent.com/activecm/zeek-log-transport/master/
zeek_log_transport.sh -O

bash connect_sensor.sh achunter-vm
```

More information

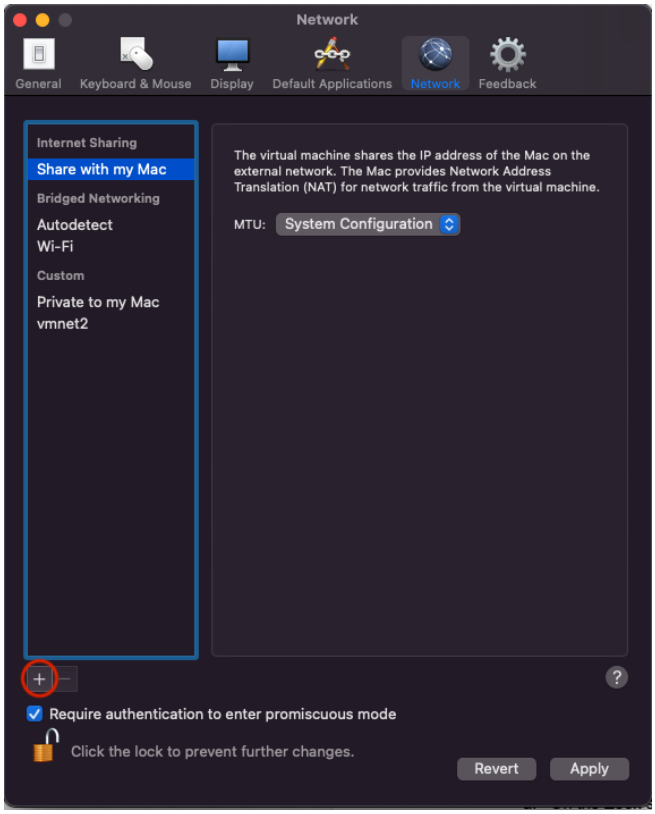
All the information about AC-Hunter CE can be found starting at https://www.activecountermeasures.com/ac-hunter-community-edition/ . This includes documentation and information on how to get and share support with other members of the AC-Hunter CE community.

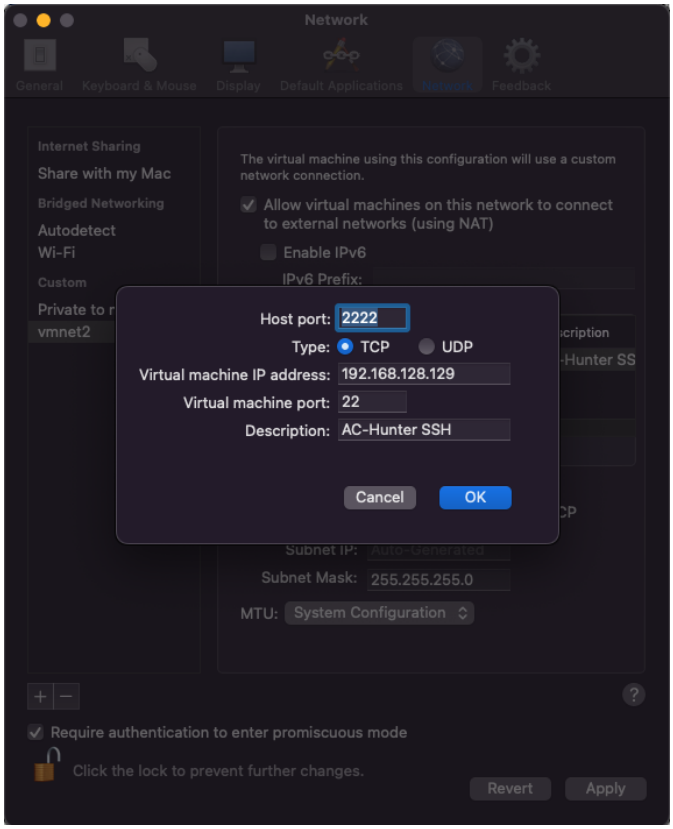
Appendix A - VMWare Fusion notes

First, we recommend users not note down their IP address at boot time. Instead, go to VMware Fusion > Preferences > Networking and create a new custom network, then go to the AC-Hunter VM's settings and assign the new network to the VM, restart the VM, then note down the IP address and enter the port forwarding values. The IP of the VM switches to a completely different subnet when changing the network.

Here are some screenshots of doing this:


VMware Fusion
File
Edit
View
About VMware Fusion
Preferences... ⌘ ,
License...
Check for Updates...
Services
Hide VMware Fusion ⌘H
Hide Others ⌥⌘H
Show All
Quit VMware Fusion ⌘Q


Network
General
Keyboard & Mouse
Display
Default Applications
Network
Feedback
Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
Custom
Private to my Mac
vmnet2
The virtual machine shares the IP address of the Mac on the external network. The Mac provides Network Address Translation (NAT) for network traffic from the virtual machine.
MTU: System Configuration
Require authentication to enter promiscuous mode
Click the lock to prevent further changes.
Revert
Apply


Network
Internet Sharing
Share with my Mac
Bridged Networking
Autodetect
Wi-Fi
Custom
vmnet2
The virtual machine using this configuration will use a custom network connection.
Allow virtual machines on this network to connect to external networks (using NAT)
Enable IPv6
IPv6 Prefix:
Host port: 2222
Type: TCP UDP
Virtual machine IP address: 192.168.128.129
Virtual machine port: 22
Description: AC-Hunter SSH
Cancel
OK
Subnet Mask: 255.255.255.0
MTU: System Configuration
Require authentication to enter promiscuous mode
Click the lock to prevent further changes.
Revert
Apply

AC-Hunter VMWare Image Install Guide v6.3