Table of Contents

Greetings and welcome to the AC-Hunter[tm] Install Guide. This guide will walk you through the process of installing AC-Hunter and connecting for the first time. If you have any questions or problems, please do not hesitate to contact support@activecountermeasures.com.

Obtaining The Software

Once you purchase AC-Hunter you will receive an email with a link to download the software. If you later want to install updates, the latest version of the software will always be available at https://portal.activecountermeasures.com. Simply login with the account you created at the time of purchase. If you have trouble accessing the software, please contact support@activecountermeasures.com.

Initial Installation

The AC-Hunter install script is designed to run from a Linux or Mac system[1] and install Zeek[2] on one server and RITA and AC-Hunter on another. For the servers, you will need two Linux systems (see below for details about supported Linux distributions). They should also meet the minimum requirements specified in the "System Requirements" section of the Pre-Install Guide. The AC-Hunter install script will install all needed components. Both systems should be SSH accessible. Both systems should have a user account that is capable of executing sudo commands. Both systems will also require internet access at installation time in order to install the required dependencies.

Ubuntu Linux 18.04 and 20.04 LTS

Ubuntu 18.04 and 20.04 LTS (Long Term Support) are fully supported.

- The systems must be patched and up-to-date ("`sudo apt-get update && sudo apt-get -y upgrade`")

CentOS 7.x and RHEL 7.x

Centos 7.x and RHEL 7.x are fully supported. If you plan to use these, please note:

- The systems must be patched and up-to-date ("`sudo yum -y update`").
- On each Centos 7 or RHEL 7 system, make sure the user under which you plan to install this software can run commands under sudo - this is required for the install. To test, run the following as that user (entering your password if requested):

```
sudo whoami
```

If you get:

```
accountname is not in the sudoers file.  This incident will be reported.
```

[1] The install can also be run from the command line on a Windows system that has the ssh and scp command line tools installed.

[2] Formerly Bro; the two names are used interchangeably in these documents and the installation process

You need to edit /etc/group as root and add that username to the wheel group. That line in the file should look like:

```
wheel:x:10:accountname
```

, or, if other account names were already on that line, like:

```
wheel:x:10:aparker,jsmith,accountname
```

As that user, log out, log back in, and run the same "sudo whoami" command. You should now see:

```
root
```

- On Centos 7 and RHEL 7 systems, we strongly recommend checking that selinux is in permissive mode. To check, run

```
sestatus
```

If this shows:

```
Current mode:                   enforcing
```

We suggest you run:

```
setenforce permissive
```

For more information on disabling selinux see https://access.redhat.com/solutions/3176 .

Opening the Tar Archive

AC-Hunter is delivered as a tar file. Download the file to the home directory of the account you wish to use to install AC-hunter. Open the archive by running the command:

```
tar xvf <name of AC-Hunter tar file>
```

You can then move to the newly created directory by typing:

```
cd achunter
```

Before Running The Install Script

All components are installed by running the install script. Before you begin, make sure you have the following information handy:

- The IP address or fully qualified domain name of the systems that will be running Zeek, Active-Flow, BeaKer, and/or Espy. Note that the Zeek, Active-Flow and Espy modules conflict with each other, so you'll need separate machines for each you wish to use.
- The IP address or fully qualified domain name of the system that will be running AC-Hunter.
- Login names and passwords to access the servers over SSH. This allows the install script to log in remotely and complete the install. Passwords are not needed for the SSH connection if you have SSH keys already configured, though you'll still need the passwords to run commands with elevated privileges (sudo).

- Which network interfaces on the Zeek system will be used to capture packets. These interfaces should be configured and up before running the installer. They are usually an Ethernet interface such as eth0 or eth1.
- The IP address space in use on your internal network. These are usually private addresses (like 10.0.0.0/8) but in some cases may be legal addresses.
- The IP addresses of any internal name servers (DNS) forwarding DNS queries. Do not include any name servers on the Internet, such as your ISP's name servers. tar
- Bare minimum of 50 GB of free storage on all systems.

By default, AC-Hunter looks for command and control (C&C) traffic originating from your internal network and headed for the Internet. We ignore internal to internal traffic as this can generate a very high false positive rate. During the installation you will be prompted to enter the IP addresses you use internally so we can properly analyze traffic patterns.

There is an exception to this analysis, which is command and control traffic that is using DNS as a communication channel. In this case, the endpoint (with an internal address) will be seen communicating with the local DNS resolver/forwarder (which may also have an internal address). In this case, we want to ensure we analyze this traffic pattern. Thus, during the install, you will be prompted to identify the IP addresses of your internal name servers. This entry will act as an exception for the above analysis.

Running the Install Script

Pro tip: Test connectivity prior to running the install script. Login to the Zeek system via SSH. From the command line, attempt to SSH to the AC-Hunter system. If the AC-Hunter system is accessible by both a private and a legal IP address, you should use the IP address that is reachable from the RITA system when running the install_acm.sh command.

Conversely, SSH directly into the AC-Hunter system. From the command line, connect to the Zeek system via IP address. Whichever IP address is successful (private or legal), that is the IP address to use in the script for the Zeek system.

Here's the command line syntax for the installer. In these examples, we'll show installing all components - leave off any you do not need:

```
./install_acm.sh zeek zeekuser@zeeksystem achunter achuser@achsystem
flow flowuser@flowsystem beaker beakeruser@beakersystem espy
espyuser@espysystem
```

Example:

```
./install_acm.sh zeek ubuntu@192.168.1.10 achunter ubuntu@192.168.1.11
flow ubuntu@192.168.2.7 beaker ubuntu@192.168.1.12
```

In the above example, the installer would place Zeek on 192.168.1.10, place AC-Hunter on 192.168.1.11, place Active-Flow on 192.168.2.7, place BeaKer on 192.168.1.12, and set up regular log transfers from Zeek and/or Active-Flow to AC-Hunter.

You can choose to install a Zeek sensor, an Active-Flow converter, or Espy. These modules conflict with each other so must be installed on separate systems. However, you may choose to install one of them on the same system running AC-Hunter.

In order for the script to run successfully, the IP addresses you specify must be accessible from the other system. For example, let's say AC-Hunter has a private address assigned of 192.168.100.10 but runs through a NAT device that maps the legal address 1.2.3.4 to this system. Which address you should use depends on which address the RITA system must use in order to connect to the system. If the AC-Hunter system is reachable via the private address, you can use that. If not, you should use the legal IP address.

During the installation, if you are using password authentication instead of SSH keys, you will be prompted to enter the remote system passwords. Since your password information is not cached by the script, you will be prompted multiple times for the same password information. This is by design in order to avoid saving passwords and thus increase security.

We make extensive use of Docker in order to isolate processes from each other, as well as the host system. During the install you will see that multiple Docker images are loaded and tested.

Defining internal IP addresses

If your network does not use the default internal subnets as defined in RFC1918:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Then you can customize your internal subnets by modifying the file /etc/AC-Hunter/rita.yaml (make sure you edit under "sudo" as the file is owned by root). This is to ensure that we properly monitor for command and control traffic.

Once you've made your changes, run:

```
hunt up -d --force-recreate
```

Analyzing incoming traffic

In some cases it may make sense to analyze incoming connections from the Internet. AC-Hunter, by default, lets you to focus on outgoing traffic by ignoring the incoming connections.

To process incoming connections, edit /etc/AC-Hunter/rita.yaml with your preferred editor under "sudo". This file will have a "Filter:" section. Leaving the existing lines as they are, add "`FilterExternalToInternal: false`". Ensure that the spacing in front of the new entry matches the spacing of the entries above it. The resulting section will look like:

```
Filtering:
  AlwaysInclude: ["8.8.8.8/32"]
  InternalSubnets: ["192.168.0.0/16","172.16.0.0/12","10.0.0.0/8"]
  FilterExternalToInternal: false
```

Your entries for AlwaysInclude and InternalSubnets may differ, of course.

When you've completed the change, make sure you load it by running:

```
hunt up -d --force-recreate
```

Creating a Web interface user

The install script creates user accounts that can be used for accessing the GUI interface. The login name "welcome@activecountermeasures.com" will be created with a random password. You will be given the option to create an additional user account and password to access the GUI. The install script will pause and prompt you to record the passwords that have been assigned.

Creating the "dataimport" user

The logs generated by Zeek will need to be moved onto the RITA/AC-Hunter system for processing. The install script will setup a process to take care of this for you. We use rsync over SSH to both efficiently and securely move the files. This requires us to create a user called "dataimport" on the AC-Hunter system. During the install, you will be prompted to create a password for this user.

Please note that SSH keys will be generated for the dataimport user, and it will be the SSH keys that are used to authenticate to the AC-Hunter system when transferring logs. Our transfer process will never store the password created above nor use it for authentication.

Zeek install

The script will then move on to installing Zeek. When in doubt, choose the defaults. The installer analyzes the network interfaces on the target system. It looks for an active interface that does not have an IP address assigned. If one is found, Zeek is set to listen on that interface. If the script cannot determine which interface you will want to use for packet sniffing, you will be prompted to enter the interface name (eth0, eth1, etc.) it should use.

Upgrading to the Latest Version

If you are already running AC-Hunter and wish to upgrade to a newer version, the install process is nearly identical to performing a fresh install. You will use the same install script while identifying the same parameters:

```
./install_acm.sh zeek zeekuser@zeeksystem achunter achuser@achsystem
```

See Running the Install Script for verbose instructions. Some minor differences when performing an upgrade:

- When the install prompts you to create a user for the AC-Hunter GUI, it is okay to select "N" and skip this step. This will retain the current login credentials from your old install. If you say you do want to create a new user, and that user already exists, the old credentials will remain in place.
- The script will detect when Zeek is already installed and will skip this portion of the install process leaving all current settings in place.

Non-interactive mode

The acm installer can be run in a non-interactive mode **when upgrading** (this will not work on a first-time install.) This is especially for use under ansible, where user input is not possible. Because the first install requires input from the user, this is not intended for a first-time install; it's only intended for upgrades.

To run the install non-interactively, do one of the following:
- Run
`export acm_no_interactive='yes'`
  before running the install_acm.sh script, or
- Add the following command line option to ./install_acm.sh module1 target1 [module2 target2]...
`--no-interactive`

Both have exactly the same effect - the script will no longer ask for any input but run to completion (or error, if any detected.)

Notes

- If you are using ansible to perform the upgrade, ansible contains logic to provide a sudo password when required.
- **You must** configure sudo to run without requesting a password on the accounts in which you install any AC-Hunter modules. On *each* target system:
    - Identify the account name to which AC-Hunter will be installed. We'll use "jparker" in the example below; please replace it with the correct account name.
    - SSH to that system
    - edit /etc/sudoers with the command

```
visudo
```

    (Depending on your Linux setup, it may be necessary to run visudo under the root account.)
    - Modify the line that gives that user sudo privileges. it may look like this:

```
jparker          ALL=(root) ALL
```

    It needs to have the NOPASSWD keyword, so it will look like:

```
jparker          ALL=(root) NOPASSWD: ALL
```

    - If you're using the AC-Hunter for Azure installer, you *may* also have to add the line:

```
Defaults verifypw=any
```

    to /etc/sudoers .
    - Save and exit

Note that even when using ansible, the AC-Hunter installer may attempt to ssh to other systems to install individual modules, where ansible will not have the ability to provide sudo authentication. To avoid this, you will likely need to set up separate ansible requests for each target host in which an AC-Hunter module will be installed, and use "127.0.0.1" for the installer IP.

- This is not appropriate for first installs, where some questions like network settings need to be asked. It's appropriate for upgrades where the configuration stays the same.

- You must include the needed modules (achunter, zeek, etc) and the target IP/hostname for each on the command line. Obviously, it's not possible to ask the user for these interactively when this option is enabled.

Upgrading Incompatible Datasets

Newer versions of AC-Hunter sometimes introduce changes that provide improvements in performance or new features. Sometimes these updates require backend changes that cause previously processed datasets to no longer be compatible. If you simply install the latest version

without converting any previous datasets and then load AC-Hunter, you will see that all of your older datasets are displayed as incompatible or may not work correctly. After upgrading old datasets will need to be reanalyzed before the new version of AC-Hunter can use them.

During the update you will receive a prompt to automatically update incompatible datasets.

```
It appears there are older datasets on this system from the following sensors:
          dataset: rolling

If you would like to use the latest features with these older datasets, you will need to allow us
to re-analyze them. Depending on the size of your datasets this could take quite
a bit of time to complete. You can also choose to complete this action later
by following the AI-Hunter documentation.

If you do nothing, your rolling datasets will automatically be converted over 24 hours.
However, if you'd like, we can re-analyze your rolling datasets when AI-Hunter starts up.

Would you like to re-analyze the rolling datasets when AI-Hunter starts up (y/n)?
```

If you choose ‘yes,’ the necessary updates will be handled on the 7 most recent datasets that were imported automatically. When this finishes, you should now be able to login to the AC-Hunter interface and access your data.

If you choose ‘no,’ or cancel the upgrade before it completes you’ll have to manually run the upgrade script later using the following command:

```
hunt run --rm api /home/api/middleware upgrade-rita
```

You also might get a message telling you that you have older datasets that need to be manually updated.

```
It appears there are older datasets on this system which were manually imported.
If you would like to update the following datasets, you will need to manually re-analyze
them by following the AI-Hunter documentation:
        dataset1
        dataset2
```

To manually update these datasets you will need access to the original Zeek logs because you will have to delete and re-import them using the following command, replacing SENSORNAME, DATE, and DATASETNAME with your own values:

```
rita import --delete /opt/zeek/remotelogs/SENSORNAME/DATE DATASETNAME
```

Importing logs from additional sensors

Note that the Community Edition only supports accepting logs from a single sensor. To add a new sensor you'll have to remove the existing sensor first.

Zeek sensors

If you have a Zeek sensor and wish to feed it into AC-Hunter for processing, please follow the steps below.

1. Log in to your Zeek sensor as a user that can read the Zeek logs and can run commands under sudo.
2. Run the following commands. You'll need to replace "my.achunter.system" with the hostname or ip address of your AC-Hunter system. "[/zeek/log/top/dir/]" is an optional parameter pointing at the top level directory under which your Zeek logs can be found. You only need to specify this if it's not automatically detected.

```
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 my.achunter.system [/zeek/log/top/dir/]
```

* Note; common directories that hold Zeek logs include:

/opt/zeek/logs/	#Zeek prebuilt packages
/opt/bro/logs/	#Bro prebuilt packages
/usr/local/zeek/logs/	#Zeek compiled from source
/usr/local/bro/logs/	#Bro compiled from source
/var/lib/docker/volumes/var_log_bro/_data/	#Blue Vector
/nsm/bro/logs	#Security Onion

BeaKer sensors

If you've chosen to install the BeaKer server, you'll also need to send network event summaries to it. For each Windows system that you wish to monitor, do the following:

1. Download the file https://github.com/activecm/BeaKer/releases/latest/download/install-sysmon-beats.ps1 to the Windows machine(s) you wish to monitor.
2. Go to the download directory and run it as:

.\install-sysmon-beats.ps1 ip.or.hostname.of.beaker.server 9200

3. As this runs you'll be asked to enter the username and password to use. The username is "sysmon-ingest", and the password is the one you provided when you installed the BeaKer server for that account.
4. The agent will start feeding summaries of its network traffic to the BeaKer server, so you'll be able to search these events later.

Analysis Process

Once you have both systems configured, Zeek will start capturing traffic. Every hour AC-Hunter will process the logs from the preceding 24 hours. If you setup the system and immediately login to AC-Hunter, the only data available will be the sample datasets. Within a few hours you will be able to analyze real data from your network, and by the following day you'll have a full 24 hour block to work with.

Online FAQ: https://portal.activecountermeasures.com/support
Email Support: support@activecountermeasures.com