AC HUNTER™

ANALYZE. IDENTIFY. HUNT.

Table of Contents

Greetings and welcome to the AC-Hunter^{tm} Pre-Install Guide. This document will identify all the things you need to know before you try to install AC-Hunter. If you have any questions or problems, please do not hesitate to contact support@activecountermeasures.com.

General Product Description

AC-Hunter helps you find the bad guys that have penetrated your network. It is designed to analyze millions of network connections and highlight the ones that indicate one or more of your internal systems have been compromised by an external entity. AC-Hunter is capable of doing the first pass at a threat hunt for you and sending you alerts. This helps you to quickly identify which systems require a deeper forensic analysis in order to take back control of your network.

System Components

AC-Hunter utilizes two primary components; Zeek (formally Bro) and AC-Hunter itself. Don't worry if you don't yet have Zeek installed. The AC-Hunter install process will take care of that.

AC-Hunter also includes three optional components. First, If you prefer to import your network data via Netflow records, we provide an additional module called Active-Flow. This accepts incoming Netflow records generated by your router(s) or switch(es) and presents them in AC-Hunter. Second, if you would like to discover which Windows programs and users created each network connection, we provide a way to track these called BeaKer. Finally, you can accept network connection information directly from Windows machines (as opposed to capturing them with Zeek) with Espy.

Here is a brief description of each of the components.

Zeek Network Security Monitor

Zeek is an open source network monitoring tool that has been released under BSD licensing. It captures the network traffic passing by on your network and converts this information into logs that can be analyzed. It is considered to be one of the best network analysis tools available. More information can be found at https://www.zeek.org/.

Active-Flow Netflow converter

The Active-Flow module, included with AC-Hunter, converts Netflow records into a form that AC-Hunter can ingest. It's an alternative in environments where it's impossible or impractical to run Zeek.

Active Countermeasures Hunter (AC-Hunter)

AC-Hunter is a Web based tool that provides a graphical front end for analysis. It is designed to simplify and expedite the process of finding compromised systems on your network. AC-Hunter is also capable of generating alerts to Slack or your centralized logging system so you know when systems need additional attention. AC-Hunter is a new class of security tool typically referred to as a "threat hunting analysis" tool.

BeaKer

The BeaKer module passively accepts reports from your Windows systems on each created connection. Monitored Windows systems notify the BeaKer server every time a connection is created, noting the time the connection was started, the program that opened it up, and the user that started the program.

When you later work with AC-Hunter and want to do research on a suspicious connection, you can click on the BeaKer icon on that connection's AC-Hunter page and be sent to the Beaker page for that connection, where you should see the connection details.

Espy

Instead of watching a network directly with Zeek or using Netflow records with the Active-Flow module, you have a third choice for importing the network connection information. Espy accepts connection information directly from Windows machines (that are configured to send it) and presents some of the same Threat Hunting screens you'd see if you were running a Zeek sensor.

System Requirements

AC-Hunter requires at least two systems, one running Zeek, Active-Flow, or Espy and the other running AC-Hunter. The following are the minimum system requirements for each.

Operating Systems

All systems are designed to run on 64 bit Linux operating systems. The preferred platforms are Ubuntu 18.04 LTS, Ubuntu 20.04 LTS, CentOS 7, and RHEL 7. The system should be patched and up-to-date using apt or yum. AC-Hunter will install all of the required dependencies.

If your operating system offers "server" and "desktop" versions, we encourage the server version as it frees up a little more ram and the desktop isn't required. That said, if you prefer the desktop for your uses, that's fine.

With the exception of the system running Zeek (see notes below under Zeek/Virtualization), all of the other components can be run on physical or virtual machines.

System running Zeek

Processor

Two cores plus an additional core for every 100 Mbps of traffic being captured. (three cores minimum). This should be dedicated hardware as opposed to virtual machines, as VM scheduling and resource congestion with other VMs can cause packets to be dropped or missed.

Memory

16GB minimum. 32GB if monitoring 1000Mb or more of network traffic.

Storage

300GB minimum. 1TB or more is recommended to reduce log maintenance (see the User Guide). SSD storage is **strongly** recommended as this can cut processing time significantly. We also recommend that you do not run RAID 5 (or 6) as this doubles (or triples) the number of read/writes per block, thus degrading I/O performance.

We recommend putting all the drive space into / (with the possible exception of 500MB-1GB in /boot if your linux distribution recommends it) and to format the partition with XFS. If your system is partitioned differently please check that you have the majority of the space (at least 300GB) in /opt/ .

Network

In order to capture traffic with Zeek, you will need at least 2 network interface cards (NICs). One will be for the management of the system and the other will be the dedicated capture port. Intel NICs perform well and are recommended.

When you're installing the operating system, do not assign an IP address to the capture port. This includes manually assigning an address and automatically assigning an address via DHCP or any other method; don't do either. The capture port does not need an address, and in fact, you may run into problems if you assign one.

Zeek is capable of handling network speeds above 1Gbps, but will commonly need some combination of additional tuning, performance optimizations, filtering, and/or capture card(s) with the ability to offload processing onto the network card itself. If you need speeds above 1Gbps, we encourage you to consider either a Corelight system with Zeek pre-installed and tuned, or a Napatech network card if you prefer to do your own setup. Get in touch if you'd like to go over these options.

Running an Underpowered System

Note that capturing packets is extremely resource intensive. If you dramatically underspec this system, it can result in failed data transfers to the AC-Hunter system or slow processing to where high levels of packet loss may be experienced.

Virtualization

We discourage running Zeek inside a virtual machine for the following reasons:

1. Packet capture and analysis are time sensitive. This can be difficult to support on a heavily loaded virtual machine host.
2. The virtualization layer introduces additional work to process each packet. At high packet rates this can be enough to raise the percent of packets lost.
3. A Zeek sensor that works well under normal load can fall behind if other virtual machines call for more memory or processing power. Tracking down a problem like this can be terribly difficult.
4. The configuration that allows you to capture packets off a physical network card in promiscuous mode can be complicated and/or poorly documented.

System running Active-Flow or Espy

The Active-Flow and Espy modules can run either on their own system or on the same machine as AC-Hunter. However, you cannot use Active-Flow and Espy simultaneously on the same machine. Either needs:

- Processors: 2 (additional) processor cores

- Memory: 2GB (additional) memory
- Storage: similar requirements to a Zeek node: 300GB minimum, 1TB recommended

Active-Flow details

As of AC-Hunter version 5.0, we are able to process Netflow V9 records only. Netflow V5 was limited to IPv4, so we do not intend to support Netflow v5.

IPFix support is not available at this time but may be added in the future.

The initial development was performed with Cisco ISR routers. Other Cisco Flexible Netflow (Netflow V9 implementation) devices are likely to work well. For other routers, we have a document that lists the needed fields; contact support@activecountermeasures.com for a copy. At a minimum, the router needs to send the following fields in Netflow records: tos, protocol, source address, destination address, source port, destination port, TCP flags, bytes, packets, absolute last timestamp, end-reason, and absolute first timestamp.

The routers providing the Netflow records need to capture and report on traffic in both directions.

If there is a firewall on the Active-Flow system, it needs to allow incoming traffic to UDP port 2055. We strongly encourage placing the Active-Flow module on a system in the same network as the routers feeding it. Netflow data from network devices is sent unencrypted and is carried in UDP packets, so there is a very good chance of the data being discarded if it traverses the Internet (UDP, unlike TCP, provides no guarantees for delivery and the chance of packet loss is greater when traversing the Internet which could cause a loss of accuracy in AC-Hunter).

If the Active-Flow system is on a different host than the AC-Hunter system and there's a firewall on either, SSH traffic from Active-Flow to AC-Hunter must also be allowed.

It's fine to do an install where a Zeek sensor is set up on one system and Active-Flow is set up on another - both will feed their information to AC-Hunter to separate databases so you can switch back and forth. While the Active-Flow module can be placed on the AC-Hunter system, it **cannot** be placed on the Zeek system - there's a conflict between the two modules.

Espy details

Espy needs one or more windows machines that have been configured to send their network connection data to the Espy server. While the Espy module can be placed on the AC-Hunter system, it **cannot** be placed on the Zeek system - there's a conflict between the two modules. For more information on how to set this up, see the "Espy Agent" section of https://github.com/activecm/espy/ .

System Running AC-Hunter

Can be run as a virtual machine if provided sufficient resources.

Processor

Two cores minimum. Four are recommended.

Memory

16GB minimum. 32GB or more recommended.

Storage

300GB minimum. Additional storage - a terabyte or more - is recommended if you plan to keep data for an extended period of time (more than a few weeks). We recommend using XFS for the file system partition type, though ext4 works too. SSD storage is **required** as this can cut processing time significantly.

If your system is partitioned differently please check that you have at least 300GB in /opt/ and at least 300GB in /var/lib/docker/ .

Network

Standard Ethernet network card interface (physical or virtual).

System running BeaKer

Processor

Two or more cores. Elasticsearch uses parallel processing and benefits from more CPU cores.

Memory

8-64GB. Monitoring more hosts requires more RAM.

Storage

Ensure `/var/lib/docker/volumes` has free space for the incoming network logs.

Network

As the amount of connection metadata transferred is far less than the connections themselves, a 100 megabit/second or 1 gigabit/second ethernet connection should be fine.

Choices to make during operating system install

We recommend the following settings on all systems if prompted during the operating system install:

1. Select UTC (Greenwich Mean Time) as your time zone.
2. Disable selinux. Selinux, if available with your linux distribution, can impose limitations that can disrupt AC-Hunter's operation.
3. Place all storage in the filesystem root. With the exception of 500MB commonly used for the /boot/ partition, all remaining disk space should be placed in the root (also called "/") partition.
4. Avoid the use of software or hardware RAID 5 and 6, especially on the Zeek system. The performance penalty for writes with RAID 5 and 6 slows packet storage down immensely.
5. Install and enable the openssh server during the installation. The installation process needs to access all systems via ssh.

Required Internet Connectivity

6. If the installation enables a firewall, make sure you allow at least the following incoming traffic:
    a. Incoming to the AC-Hunter system, allow incoming TCP ports 22, 80, 443.
    b. Incoming to the Zeek system, allow incoming TCP port 22.   For the interface(s) used to sniff traffic, there should be no incoming firewall at all.
    c. If you're setting up a third Active-Flow system to process netflow records, that system should accept incoming TCP port 22 and UDP port 2055.
    d. You can further restrict the above ports so that only machines owned by administrators and the Zeek and Active-Flow nodes can access port 22, only machines that should see the AC-Hunter web interface can access ports 80 and 443 on the AC-Hunter computer, and only the routers feeding netflow records can access UDP port 2055 on Active-Flow.
    e. All systems should be able to place UDP port 53 and TCP ports 53, 80, and 443 requests out to the Internet to retrieve patches and pull down supporting information used in AC-Hunter's web UI.
    f. Incoming traffic summary:

System	Traffic from	Ports	Note
AC-Hunter	Admin systems	TCP 22	
AC-Hunter	All Zeek systems	TCP 22	For transferring logs
Zeek	Admin systems	TCP 22	
Active-Flow	Admin systems	TCP 22	

AC-Hunter	All analyst systems	TCP 80, 443	
Zeek	anywhere	all	On sniff interfaces
AC-Hunter	Active-Flow	TCP 22	If importing netflow
Active-Flow	Netflow routers	UDP 2055	If importing netflow
BeaKer or Espy	Admin systems	TCP 5601	Web interface
BeaKer or Espy	Monitored Windows systems	TCP 9200	Connection info from Windows

g. Outgoing traffic summary

System	Traffic to	Ports	Note
All systems	DNS servers	UDP 53, TCP 53	
All systems	Internet	TCP 80,443	Patches, updates, live lookups

System Examples

Active Countermeasures does not endorse or recommend any one specific hardware vendor. However for completeness, we wanted to include a real life example system to help you estimate hardware acquisition costs. This example is based on the Dell PowerEdge R630. Feel free to use an equivalent server from your preferred vendor.

Zeek server for 1 Gbps Internet link speed

- No Trusted Platform Module (TPM)
- 8 2.5" HD chassis, 2 PCIe slots with riser
- 1 Intel Xeon E5-2650 v4 2.2ghz, 30M cache, 12C/24T
- 8x 16GB Performance optimized 2666 MT/s Dual rank rdimms
- Perc H730 raid controller with 1GB NV cache (drives arranged as raid 1)
- 2x 960GB Sata mixed use SSD's SM863a
- iDRAC remote access controller
- DVD-ROM
- standard bezel

- no rails
- performance bios
- 2x power cords
- dual hot-plug redundant 495W power supplies
- Intel ethernet I350 Quad port 1gb network daughter card
- PCIe riser
- no documentation, os, media, or additional software

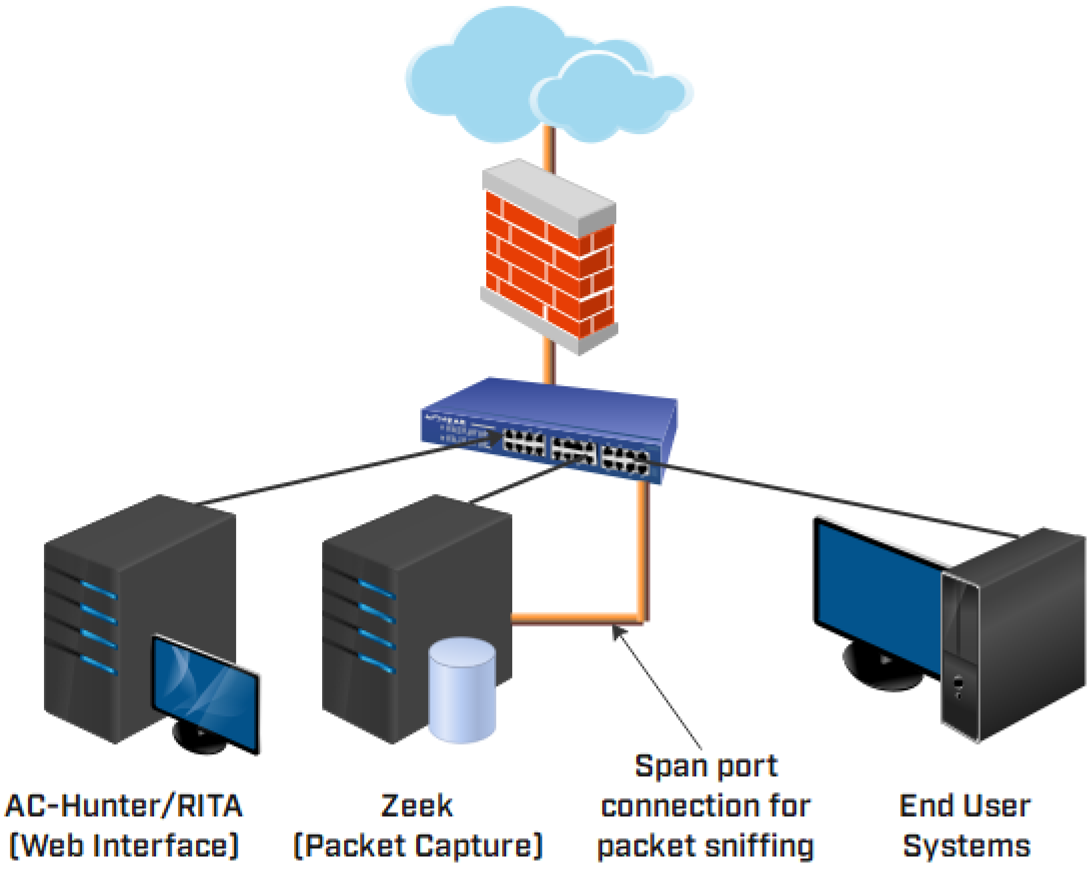
Base cost = $12,437
With coupon discount = $7,822.43

Zeek server for less than 1 Gbps Internet link speed

Same as above, except with 64 GB RAM instead of 128 GB
Base cost = $9,881
With coupon discount = $6,214.79

Deployment Architecture

The following is a general diagram on how all of the components of AC-Hunter should be deployed on your network:



Architecture Requirements

Zeek needs to be connected so that it can monitor passing network traffic. This is typically performed by connecting Zeek to a span or monitoring port on the network switch handling the traffic. Since compromised systems call home to Command and Control (C&C) servers on the Internet, you want to set your span port to capture all traffic going in and out of your firewall's internal interface.

Some routers offer an alternate approach to span ports called ERSPAN. This wraps up each of the captured packets in a special header and sends them off to a sniffer listening on a non-span port. Unfortunately, Zeek is not able to process all ERSPAN traffic types, so we do not recommend this.

The Zeek and AC-Hunter server can be located on your internal network or an isolated VLAN. This is a personal choice depending on your requirements.

Alternative Architectures

While you could connect Zeek to a spanning port outside of your firewall, you may lose visibility of which internal systems are communicating. This is because most firewalls perform Network Address Translation (NAT) which changes the source IP address to a fixed legal IP address. While AC-Hunter can still operate in this configuration, you would need to cross reference all detections against your firewall's outbound traffic logs to determine which systems are potentially compromised. This adds a huge layer of complexity to the threat hunting process. It is for this reason that this configuration is not recommended.

If you have external links besides an Internet connection, Zeek can be deployed there as well to monitor passing traffic. This would ensure that any threat traffic passing through the link is quickly detected. Typically however, it is a network's connection to the Internet that poses the highest risk.

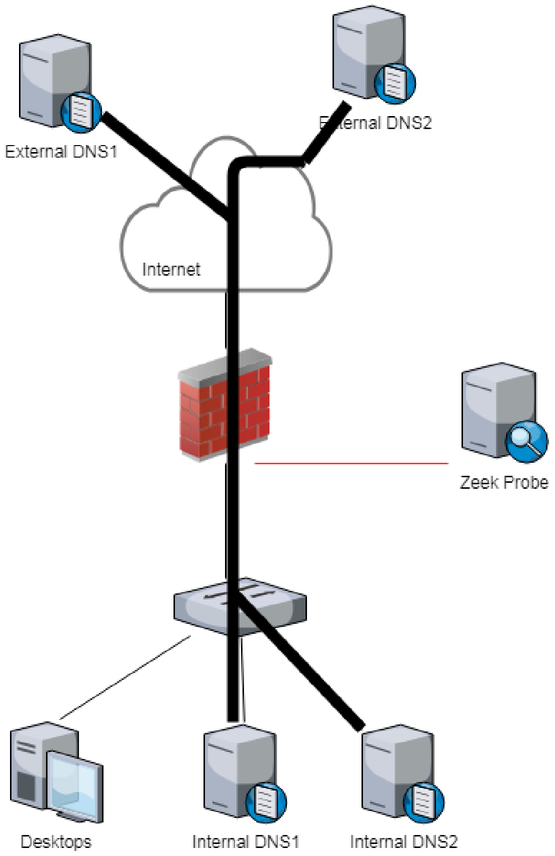
HTTP proxy analysis

If you use an HTTP proxy you'll want to have a Zeek sensor placed where it can see the traffic from your internal systems to the proxy. You'll need to use the Zeek package supplied with AC-Hunter 5.3.0 or above in order to analyze HTTP proxy traffic.

Special Considerations with DNS

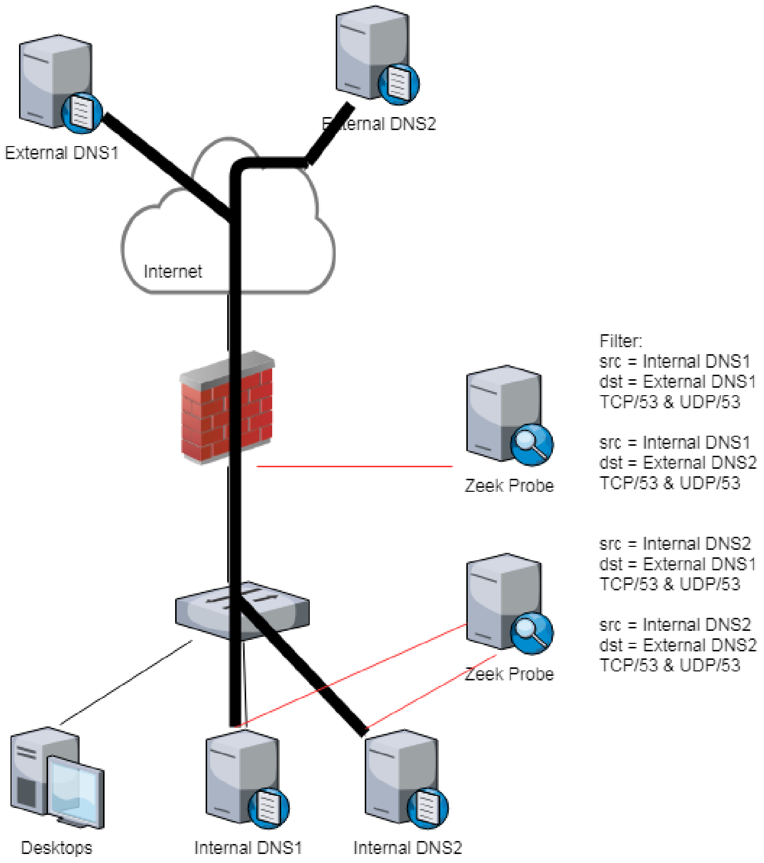
In some environments, the internal DNS server acts as a DNS forwarder that sends all traffic to an external DNS resolver. This may be the case if you have subscribed to a DNS blacklisting service. With this setup, special steps must be taken if you wish to leverage AC-Hunter's ability to detect endpoints that are using DNS as a command and control (C&C) channel.

Consider the following network drawing. Dark thick lines represent forwarder to resolver DNS traffic.



AC-Hunter analyzes communications between IP pairs to see if they exhibit beacon-like behavior. Since all internal DNS queries appear to be sent through the internal DNS forwarders, from the perspective of the Zeek probe a majority of DNS traffic involves the two specified internal DNS forwarders, and the two specified external DNS resolvers. This creates a problem when attempting to detect the endpoint responsible for C&C traffic, as the probe will only see the resolver's IP address (not the endpoint that originated the query).

The recommendation is to deploy an additional Zeek probe so that it can monitor DNS queries from the endpoints to the internal DNS forwarders. We further recommend implementing some filtering to prevent packet capture duplication. A possible deployment is shown in the following drawing:



Filter:
src = Internal DNS1
dst = External DNS1
TCP/53 & UDP/53

src = Internal DNS1
dst = External DNS2
TCP/53 & UDP/53

src = Internal DNS2
dst = External DNS1
TCP/53 & UDP/53

src = Internal DNS2
dst = External DNS2
TCP/53 & UDP/53

In this configuration, an additional Zeek probe is added so that it can collect DNS queries as they travel from internal systems to each of the internal DNS forwarders. This will permit the second probe to monitor each endpoint for beacon activity, as well as analyze DNS queries for suspect C&C behavior. **Both probes** should be configured to ignore all DNS traffic between the four above mentioned IP pairs. This should be implemented via a BP filter within Zeek. Since endpoint queries will be collected by the second Zeek probe, the forwarder queries can be safely ignored as they travel from the internal server to the external resolver. Further, the filters will help eliminate the high IP connection pair rates that provide no real useful data.

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.

Installing The Software

The version of AC-Hunter that you download will include the Install Guide which will always contain the latest and greatest installation instructions. If you would like to get a feel for the installation process, we have an 18 minute video on our Website that will walk you through the process.

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