(Version: 202403121054)

Welcome to the one-day threat hunting course!
We'll be placing longer answers here, short answers in the webcast chat.

Most commonly asked questions

- **Will there be a recording**? Yes, and it will be up in a few weeks at https://www.activecountermeasures.com/hunt-training/
- **Will I get a certificate**? Yes, it will be emailed to you in 2-3 days at the email address you used to sign up for the class. Please check your spam folder if you don't see it after 3 business days.
- **Where do I ask questions**? In the "Threat Hunter Community" discord (https://discord.gg/threathunter/), in the "#live-webcast-chat" channel.
- **Where do I get the slides**? In the "Threat Hunter Community" discord (https://discord.gg/threathunter/), in the "#acm-webcast-content" channel.
- **Where do I get the labs**? https://www.activecountermeasures.com/hunt-training/
- **But my company won't let me run the Discord app**. You can join discord in your web browser: https://discord.gg/threathunter/ .
- **Do I need to patch/update the virtual machine?** It's a good idea to patch it.

Class

The webcast starts at 11:00AM US eastern time (15:00 UTC, 08:00 US Pacific) on Friday Apr 12th, 2024:
10:30 eastern/14:30 UTC/07:30 US Pacific: Setup questions and Pre-show banter
11:00 eastern/15:00 UTC/08:00 US Pacific: Start of class
17:00 eastern/21:00 UTC/14:00 US Pacific: Approximate end of class.

Links

Course details, lab downloads:
https://www.activecountermeasures.com/cyber-threat-hunting-training-course/

Join us in the #live-webcast-chat channel on Discord for chat during the training:
https://discord.gg/threathunter/
Questions related to the material: #live-webcast-chat
General chat about the webcast: #live-webcast-chat
Course material and FAQ download: #acm-webcast-content
Problems (audio/video): #discord-feedback
Demo/more information requests: #acm-general

Future classes; see https://www.activecountermeasures.com/events/

Labs

The labs are distributed as a virtual machine for vmware. Please download it well in advance of the webcast, install them, and test that you can successfully log in.

Your virtual machine only needs 2 processors, though giving it 4 may help.
To do the labs, make sure you create the machine with at least 16GB (could drop to 12GB for the labs).
Also, make sure you have plenty of free space on the drive that holds the virtual machines - 200G should be fine.

To run more than one command at once, you can switch between consoles with ctrl-alt-f2 , ctrl-alt-f3, etc if you're typing a Windows or Linux system, or fn-option-f2, fn-option-f3 on a Mac.

Don't worry if you don't have network access once you load the VM. All labs will be done within the VM itself. We have some cool pcaps and Zeek files to play with. There is no GUI. We're going commando line on this one!

Option 1: Download

You need one of the following; either download a full virtual machine or the script that will try to install the tools. The details on these virtual machines are at https://www.activecountermeasures.com/hunt-training/ .

We supply the class VM in three formats: virtualbox virtual machine, VMWare virtual machine, and generic OVA (appropriate for virtualbox, vmware, and other virtualization packages, respectively.) **Please download these in advance - they take a while to download and install**.

For a some more background on how to work with virtual machines, see: https://carleton.ca/scs/tech-support/virtual-machines/virtual-machine-technical-support/virtual-machine-step-by-step-guide/

Option 2 - share a cloud server with the labs loaded.

We have 2 cloud instances loaded with the labs. They are:
https://ach1.aihhosted.com
https://ach2.aihhosted.com

You're welcome to use either of these. Please remember these are shared with other students, so we ask you not to create safelist entries or delete databases.

The web login to each is:
Name: **threat@activecountermeasures.com**
Password: hunting2

Using

If your virtual machine hangs with one or more "uninitialized urandom read" messages on the console and never gives you a login prompt, try pressing lots and lots of keys randomly. Seriously. The kernel is looking for random input to serve different services that need a random number to start correctly; pressing keys over and over should give it that information. (unconfirmed fix)

Login details:

```
Login: threat
Pass: hunting
```

This next block needs to be rechecked against the current lab VM:

Data files are in /home/threat/lab* . Verify that you can see the lab files:

```
thunt@thunt-one-day:~$ pwd
/home/threat
thunt@thunt-one-day:~$ cd labs
thunt@thunt-one-day:labs$ls -Al lab[123]
lab1:
total 5456
-rw-rw-r-- 1 threat threat    4419 Sep 28  2022 capture_loss.log
-rw-rw-r-- 1 threat threat  182813 Sep 28  2022 certs-remote.pem
-rw-rw-r-- 1 threat threat 1760057 Sep 28  2022 conn.log
-rw-rw-r-- 1 threat threat   48716 Sep 28  2022 dhcp.log
-rw-rw-r-- 1 threat threat 1529137 Sep 28  2022 dns.log
-rw-rw-r-- 1 threat threat  221275 Sep 28  2022 files.log
-rw-rw-r-- 1 threat threat 1444128 Sep 28  2022 http.log
-rw-rw-r-- 1 threat threat     205 Sep 28  2022 known_hosts.log
-rw-rw-r-- 1 threat threat     269 Sep 28  2022 known_services.log
-rw-rw-r-- 1 threat threat   28230 Sep 28  2022 loaded_scripts.log
-rw-rw-r-- 1 threat threat   27253 Sep 28  2022 notice.log
-rw-rw-r-- 1 threat threat     821 Sep 28  2022 ntp.log
-rw-rw-r-- 1 threat threat     254 Sep 28  2022 packet_filter.log
-rw-rw-r-- 1 threat threat     847 Sep 28  2022 software.log
-rw-rw-r-- 1 threat threat  135368 Sep 28  2022 ssl.log
-rw-rw-r-- 1 threat threat   26364 Sep 28  2022 stats.log
-rw-rw-r-- 1 threat threat  131521 Sep 28  2022 x509.log
lab2:
total 544
-rw-rw-r-- 1 threat threat  91626 Feb 27  2023 conn.log
-rw-rw-r-- 1 threat threat 453834 Jan 22  2021 dns.log
-rw-rw-r-- 1 threat threat    253 Jan 22  2021 packet_filter.log
-rw-rw-r-- 1 threat threat    470 Jan 22  2021 weird.log
lab3:
total 6116
-rw-rw-r-- 1 threat threat    4501 Feb 27  2023 capture_loss.log
-rw-rw-r-- 1 threat threat  208450 Feb 27  2023 certs-remote.pem
-rw-rw-r-- 1 threat threat 2058759 Feb 27  2023 conn.log
-rw-rw-r-- 1 threat threat   49321 Feb 27  2023 dhcp.log
```

```
-rw-rw-r-- 1 threat threat 1439748 Feb 27  2023 dns.log
-rw-rw-r-- 1 threat threat  393317 Feb 27  2023 files.log
-rw-rw-r-- 1 threat threat 1455144 Feb 27  2023 http.log
-rw-rw-r-- 1 threat threat     269 Feb 27  2023 known_hosts.log
-rw-rw-r-- 1 threat threat     416 Feb 27  2023 known_services.log
-rw-rw-r-- 1 threat threat   28230 Feb 27  2023 loaded_scripts.log
-rw-rw-r-- 1 threat threat   31924 Feb 27  2023 notice.log
-rw-rw-r-- 1 threat threat     819 Feb 27  2023 ntp.log
-rw-rw-r-- 1 threat threat     254 Feb 27  2023 packet_filter.log
-rw-rw-r-- 1 threat threat     727 Feb 27  2023 software.log
-rw-rw-r-- 1 threat threat  276112 Feb 27  2023 ssl.log
-rw-rw-r-- 1 threat threat   26741 Feb 27  2023 stats.log
-rw-rw-r-- 1 threat threat  242051 Feb 27  2023 x509.log
```

Keyboard layout

If you need a keyboard layout other than English/US, run:

```
sudo dpkg-reconfigure keyboard-configuration
```

VMware

If you do not have VMWare installed, see https://www.vmware.com/products/workstation-player.html for details about VMWare Player.

If you are running an older version of VMWare (like 14), you may get a version error such as "The virtual machine is using a hardware version that is not supported by this version of VMware Workstation." when you try to load the VMWare VM. Try this quick hack:
1) Open "thunt-1-day-v2-vmware.vmx" with Notepad or a similar text editor
2) Search for the line: virtualHW.version = "16" (should be towards the top)
3) Change this line to read = virtualHW.version = "14"
4) Save your changes
5) Launch the VM
Reference: https://kb.vmware.com/s/article/1003746

If you get error messages like:
VMware Workstation and Device/Credential Guard are not compatible.
VMware Workstation can be run after disabling Device/Credential Guard
, take a look at
https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/dg-readiness-tool

If you've never installed a VMWare virtual machine, we have an instruction video at https://www.youtube.com/watch?v=MzkFLcwnZbo . Note that the video is for installing AC-Hunter CE via VMWare (as opposed to the lab virtual machine for this class) so some of the instructions may differ.

Other virtualization tools

If you cannot use VMWare or virtualbox for some reason, you're welcome to see if your existing virtualization package can import OVA files.

Errors

Datamash

If you get "invalid numeric value in line 1 field #" using datamash it's due to the language specific decimal separator. To fix this, execute "export LC_NUMERIC=en_US.UTF-8" before using datamash. (Thanks Bytewolf!)

Virtualbox

Getting a failed to attach to drive port 0 when trying to start the VM image on VirtualBox. What step am I missing?

Try deleting devices like floppy, usb, cdrom, sound card, and/or printer.

Followup

Within a few weeks we'll have a recording of the class at https://www.activecountermeasures.com/cyber-threat-hunting-training-course/ . Within a day or two we'll also email you a certificate for the class. Please check the spam folder for the account under which you registered for the class.

Miscellaneous

Is that PCAP or netflow data on the dashboard?

It's a pcap converted into Zeek logs and imported into AC-Hunter.

What data does AC hunter need, how do you "connect it"? Is it full mirror traffic, netflow, or something else?

You plug a Zeek sensor into a span/copy/mirror/tap . You then send the Zeek output (zeek logs) to AC-Hunter.

Do you need to configure port forwarding if you are logging in directly from the machine (not remotely)

It may work; if it doesn't, go back and configure port forwarding.

Are the datasets that come with the community edition the same as the class lab vm datasets?

The class labs include some additional lab datasets.

Windows users

To confirm a checksum on windows, get in to Powershell and run (example)

```
get-filehash -alg SHA256 .\thunt-L1-2023-r1-vbox.zip
```

or

```
get-filehash -alg SHA256 .\thunt-L1-2023-r1.ova
```

or

```
get-filehash -alg SHA256 .\thunt-L1-2023-r1-vmware.zip
```

which should return the right checksum for your downloaded file (see https://www.activecountermeasures.com/hunt-training/ for the correct checksums for those files).

Mac users

If you're on Mac OS and cannot unzip a file with unzip, the zip file cannot be opened by unzip supplied with Mac OS. To open, create a lab directory and use "ditto" (included with Mac OS) to open:

```
mkdir thuntclass
cd thuntclass
ditto -x -k /path/to/thunt-1-day-v2-vmware.zip ./
```

If you're on a mac with a non-intel processor (M1, M2, etc), the VMs won't work. You should use the online instances instead.

Extra links for class topics

- Site that explains long command lines: www.explainshell.com
- Level 2 Threat Hunting class (paid): https://www.antisyphontraining.com/live-courses-catalog/advanced-network-threat-hunting-w-chris-brenton/
- Excellent book on NotPetya: https://www.amazon.com/Sandworm-Cyberwar-Kremlins-Dangerous-Hackers-ebook/dp/B07GD4MFW2/
- Blogs on BPF: https://www.activecountermeasures.com/?s=BPF
- Next steps once you've found something interesting: https://www.activecountermeasures.com/suspicious-traffic-found-what-are-the-next-steps/
- Additional information about the connections from Microsoft systems: https://www.activecountermeasures.com/free-tools/beaker/
- Zcutter: https://www.activecountermeasures.com/free-tools/zcutter/
- Ngrep introduction: http://www.stearns.org/doc/ngrep-intro.current.html
- Rita :https://www.activecountermeasures.com/free-tools/rita/
    - Story about Rita Strand, John Strand's mom: https://darknetdiaries.com/episode/67/
- Bash scripting class: https://www.antisyphontraining.com/on-demand-courses/bash-scripting-for-server-administration-w-bill-stearns/
- Capinfos utility: https://www.wireshark.org/docs/man-pages/capinfos.html . If capinfos is not installed, run:

```
apt-get install wireshark-common
```

- More info about screen: http://www.stearns.org/doc/screen-for-detachable-sessions.html
- ACM blogs: https://www.activecountermeasures.com/blog/
- Youtube channel: https://www.youtube.com/@ActiveCountermeasures
- AC-Hunter Community Edition (CE): https://www.activecountermeasures.com/ac-hunter-community-edition/
- Module to add "open connection" logging to Zeek: https://github.com/activecm/zeek-open-connections
- Testing any Threat Hunting solution (not just AC-Hunter): https://www.activecountermeasures.com/threat-simulation-overview-and-setup/
- An (outdated) list of pcap analysis and capture tools: http://www.stearns.org/doc/pcap-apps.html