(Version: 202104121338)

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

The webcast starts at 11:00am eastern time (15:00 UTC, 08:00 Pacific) on Tuesday April 13th 4/13/2021:
11:00 eastern/15:00 UTC: Setup questions
11:30 eastern/15:30 UTC: Pre-show banter
12:00 eastern/16:00 UTC: start of class
17:00 eastern/21:00 UTC: approximate end of class.

Links

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

Discord server for discussion: https://discord.gg/AxHJRrRz
Questions related to the material: "Questions" window in Gotowebinar
General chat about the webcast: #live-webcast-chat
Course material and FAQ download: #acm-webcast-content

Problems (audio/video): #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 a single processor.
To do the labs, make sure you create the machine with at least 5120MB. If you're not able to spare that much, use Zeek to solve "C2 over DNS" and skip trying to use tshark.
Also, make sure you have plenty of free space on the drive that holds the virtual machines - 24G 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!

Download

You need one of the following; either download a full virtual machine or the script that will try to install the tools.

Option 1 - full virtual machine

For the vmware virtual machine, download:
https://threat-huntiing.s3.amazonaws.com/thunt-202102.zip
Note that the "ii" is correct.

To verify that the download finished successfully, check the md5 checksum of the file you downloaded:

```
md5sum thunt-202102.zip
```

Which should return:

```
f6ee1e3bb4a7c9bdfb1e6108a046784c  thunt-202102.zip
```

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

```
get-filehash -alg MD5 .\thunt-202102.zip
Algorithm Hash Path
--------- ---- ----
MD5 F6EE1E3BB4A7C9BDFB1E6108A046784C thunt-202102.zip
```

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-202102.zip ./
```

Now that you have the image downloaded, import the image into your virtual machine software (vmware).

In VMware, please find the menu option to import a virtual machine and point it at your opened directory.

Here are some alternate steps for VMWare Fusion (courtesy of Dante Smith!). Your steps may vary;

1) You've already opened the zip file.
2) Go to VMWare
3) Click on New -> Create a custom VM
4) Under Custom VM, select Ubuntu 64-bit
5) Select Legacy Bios
6) Under Virtual Disk, select "Use an existing Virtual DIsk" and select "Choose Virtual Disk".
7) In the dropdown menu choose the directory that contains thunt-202102.vmx .
8) Select the thunt-202102.vmdk file and select choose. Step through the remaining defaults and enter the login information provided.

Name: thunt-202102.zip
Size: 2193726370 bytes (2092 MiB)
CRC32: C8E75210
CRC64: CB1CCD83D0FAFE1A
SHA1: EB38C2CC4E5074A11DE231945A2447A8179E108B
SHA256:
50A1A2CFC431777B7EDF25553072BE15D9E7359861A2D3C8EBB071C9CA553DC4

Option 2 - install tools on existing Centos/Ubuntu system

If you are running Centos/RHEL 7 or Ubuntu Linux 16.04 or 18.04, you can install the needed tools and the sample data files with a shell script. Download:

```
https://threat-huntiing.s3.amazonaws.com/install-tools.v0.2.3.sh
```

(note that the "ii" in hunting is correct), make it executable with:

```
chmod +x install-tools.v0.2.3.sh
```

, and run it:

```
./install-tools.v0.2.3.sh
```

Name: install-tools.v0.2.3.sh
Size: 7943 bytes (7 KiB)
CRC32: 40246E46
CRC64: 9ED640DA78F8681A
SHA1: 8EBFC7573B42AD793E84116F35C0575BA5F16098
SHA256:
00A1CC67013E0ABD4DC116E2AB5389061701796CDA93AD81F8DCF0D1D1FEB0C9

Option 3 - Run the entire thing on a Cloud instance

If neither of the above work for you, you have the option of doing all the labs in a DigitalOcean cloud server (they call these "droplets"). Since DigitalOcean offers a $100 credit for first time users for the first 2 months (at the time of this writing), you should be able to do the labs at no cost.

See "Setting_up_a_cloud_lab_VM.pdf" in the #acm-webcast-content channel of the Threat Hunter Community Discord server.

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: thunt
Pass: aybab2u
```

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

```
thunt@thunt-one-day:~$ pwd
/home/thunt
thunt@thunt-one-day:~$ ls -Al lab[123]/
lab1/:
-rw-r--r-- 1 thunt thunt  1769129 Feb 17 12:25 conn.log
-rw-r--r-- 1 thunt thunt    48722 Feb 17 12:25 dhcp.log
-rw-r--r-- 1 thunt thunt  1529159 Feb 17 12:25 dns.log
-rw-r--r-- 1 thunt thunt   169343 Feb 17 12:25 files.log
-rw-r--r-- 1 thunt thunt  1444115 Feb 17 12:25 http.log
-rw-r--r-- 1 thunt thunt      819 Feb 17 12:25 ntp.log
-rw-r--r-- 1 thunt thunt      254 Feb 17 12:25 packet_filter.log
-rw-r--r-- 1 thunt thunt   109204 Feb 17 12:25 ssl.log
-rwxr-xr-x 1 thunt thunt 85294077 Jun 10  2020 trace1.pcap
-rw-r--r-- 1 thunt thunt    15630 Feb 17 12:25 weird.log
-rw-r--r-- 1 thunt thunt   235138 Feb 17 12:25 x509.log

lab2/:
-rw-r--r-- 1 thunt thunt   1281 Jan 22 11:01 conn.log
-rw-r--r-- 1 thunt thunt 453834 Jan 22 11:01 dns.log
-rw-r--r-- 1 thunt thunt    253 Jan 22 11:01 packet_filter.log
-rw-r--r-- 1 thunt thunt    470 Jan 22 11:01 weird.log

lab3/:
-rw-r--r-- 1 thunt thunt   1294975 Feb 18 04:09 conn.log
-rw-r--r-- 1 thunt thunt     48738 Feb 18 04:09 dhcp.log
-rw-r--r-- 1 thunt thunt   1463736 Feb 18 04:09 dns.log
-rw-r--r-- 1 thunt thunt    176430 Feb 18 04:09 files.log
-rw-r--r-- 1 thunt thunt     26802 Feb 18 04:09 http.log
-rw-r--r-- 1 thunt thunt       254 Feb 18 04:09 packet_filter.log
-rw-r--r-- 1 thunt thunt    125354 Feb 18 04:09 ssl.log
-rw-r--r-- 1 thunt thunt 323949399 Feb 17 12:17 trace3.pcap
-rw-r--r-- 1 thunt thunt     15621 Feb 18 04:09 weird.log
-rw-r--r-- 1 thunt thunt    266437 Feb 18 04:09 x509.log
```

All of the labs will be performed from the command line, so if you can see the files you are set to go!

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 when you try to load the VMWare VM. Try this quick hack:
1) Open "thunt-202102.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

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

KVM

If you'd like to use KVM, please see
https://jensoroger.wordpress.com/2021/02/22/attending-cyber-threat-hunting-level-1-w-chris-brenton-4-hours-and-want-to-run-the-vm-in-qemu-kvm-this-is-how-i-got-it-to-work-activecmeasures-activecountermeasures-aihunter-threathunting-bea/ . (We've not reviewed this)

Mac

A good approach would be to 1) Install Virtualbox, 2) Create an Ubuntu 18.04 virtual machine from the Ubuntu 18.04 ISO file (download from https://releases.ubuntu.com/18.04.5/ubuntu-18.04.5-live-server-amd64.iso), and use the install-tools script (above) to install the needed tools and sample data files.

Other virtualization tools

If you cannot use VMWare for some reason, you're welcome to see if your existing virtualization package can import VMWare virtual machines.

Cloud

If none of the above approaches work for you, you can always create a cloud server at any provider you like. Pick Ubuntu 18.04 LTS, 64 bit, 5 or more GB of memory, 10 or more GB of disk, and any number of processors. Once it comes up, log in, download the install-tools script (see above), and run it to install the needed tools and sample data 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!)