Lab Assignment

Cybersecurity Professional Program

Digital Forensics & Incident Response

Threat Hunting & Intelligence

DFIR-11-L2
Exploit Hunting

Lab Objective

Understand how to perform exploit hunting using AlienVault.

Lab Mission

Create an AlienVault account. Search for information about common indicators of compromise.

Lab Duration

30–60 minutes

Requirements

Basic working knowledge of searching for information on the internet

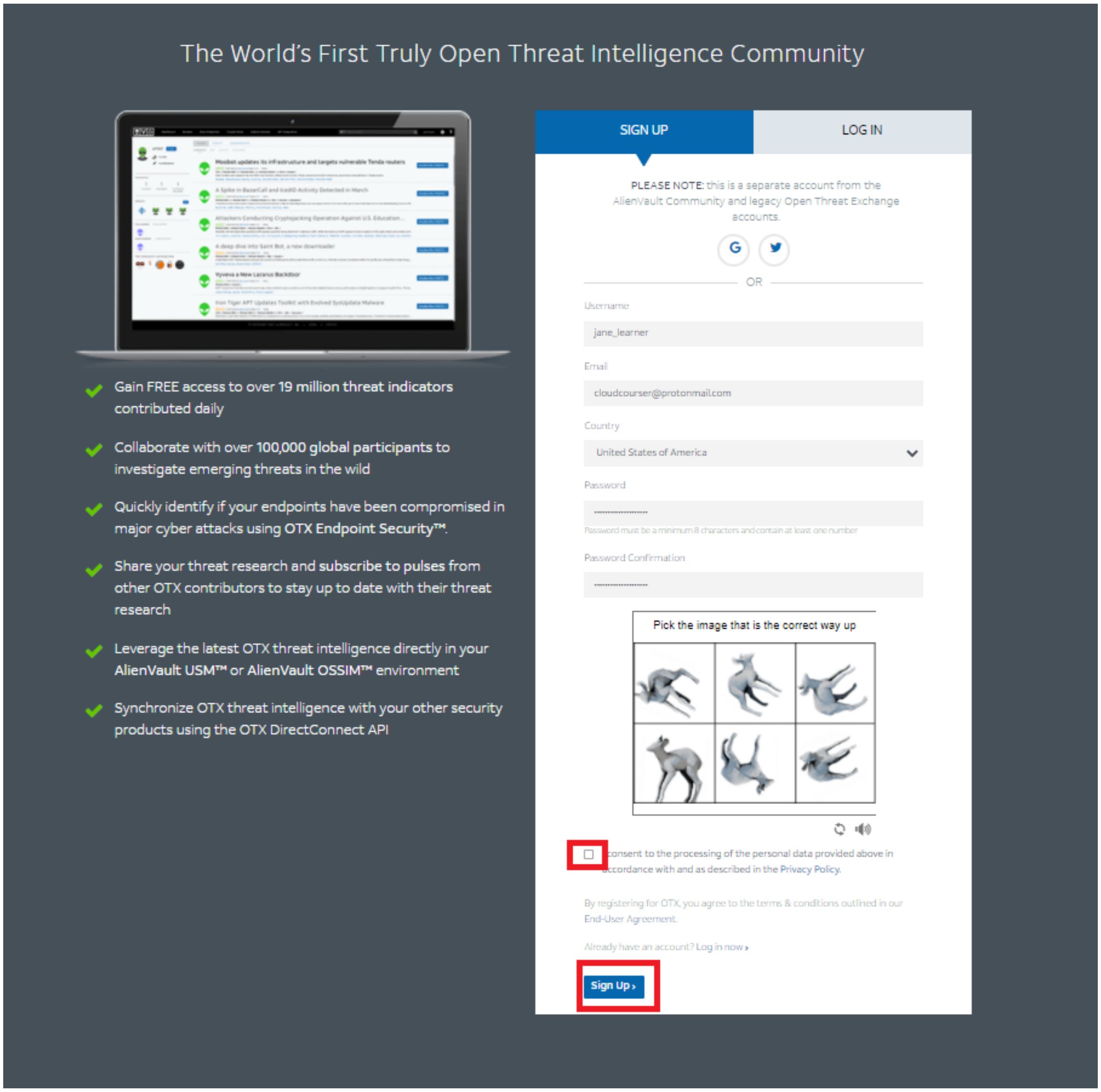
Resources

- Live internet connection

Lab Task 1: Create an AlienVault Account

Find information about well-known exploits using a threat exchange platform.

1 Enter AlienVault's website and sign up for an account: in your browser, go to ***https://otx.alienvault.com***, fill out the form, and solve the Captcha. Consent to the privacy policy and click **SIGN UP**.



The World's First Truly Open Threat Intelligence Community

- ✓ Gain FREE access to over 19 million threat indicators contributed daily
- ✓ Collaborate with over 100,000 global participants to investigate emerging threats in the wild
- ✓ Quickly identify if your endpoints have been compromised in major cyber attacks using OTX Endpoint Security™.
- ✓ Share your threat research and subscribe to pulses from other OTX contributors to stay up to date with their threat research
- ✓ Leverage the latest OTX threat intelligence directly in your AlienVault USM™ or AlienVault OSSIM™ environment
- ✓ Synchronize OTX threat intelligence with your other security products using the OTX DirectConnect API

PLEASE NOTE: this is a separate account from the AlienVault Community and legacy Open Threat Exchange accounts.

Username: jane_learner

Email: cloudcourser@protonmail.com

Country: United States of America

Password: ••••••••••••••••••••

Password must be a minimum 8 characters and contain at least one number

Password Confirmation: ••••••••••••••••••••

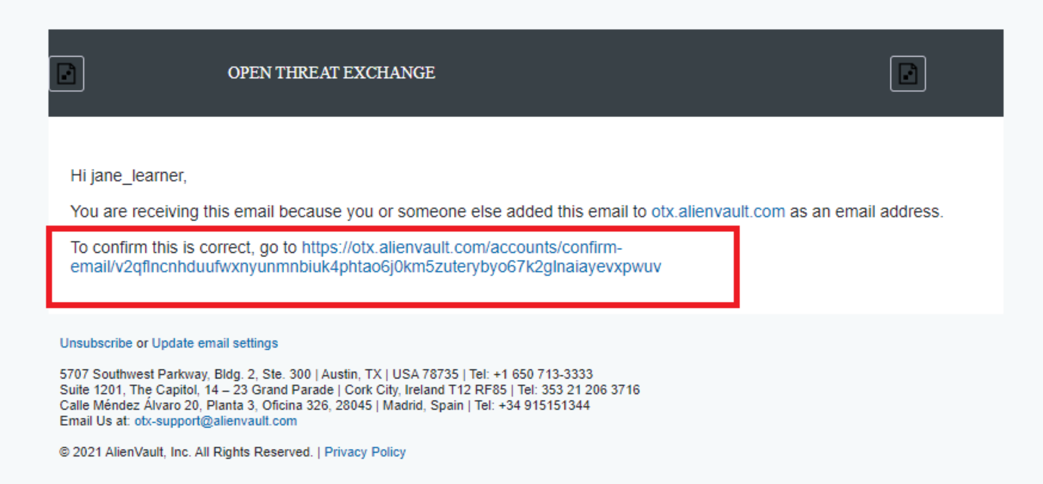
Pick the image that is the correct way up

□ consent to the processing of the personal data provided above in accordance with and as described in the Privacy Policy.

By registering for OTX, you agree to the terms & conditions outlined in our End-User Agreement.

Already have an account? Log in now ›

2 Open your email account and find the message from AlienVault. Find the hyperlink in the message and click through to activate your account (yours may look different than the screenshot below).



Hi jane_learner,

You are receiving this email because you or someone else added this email to otx.alienvault.com as an email address.

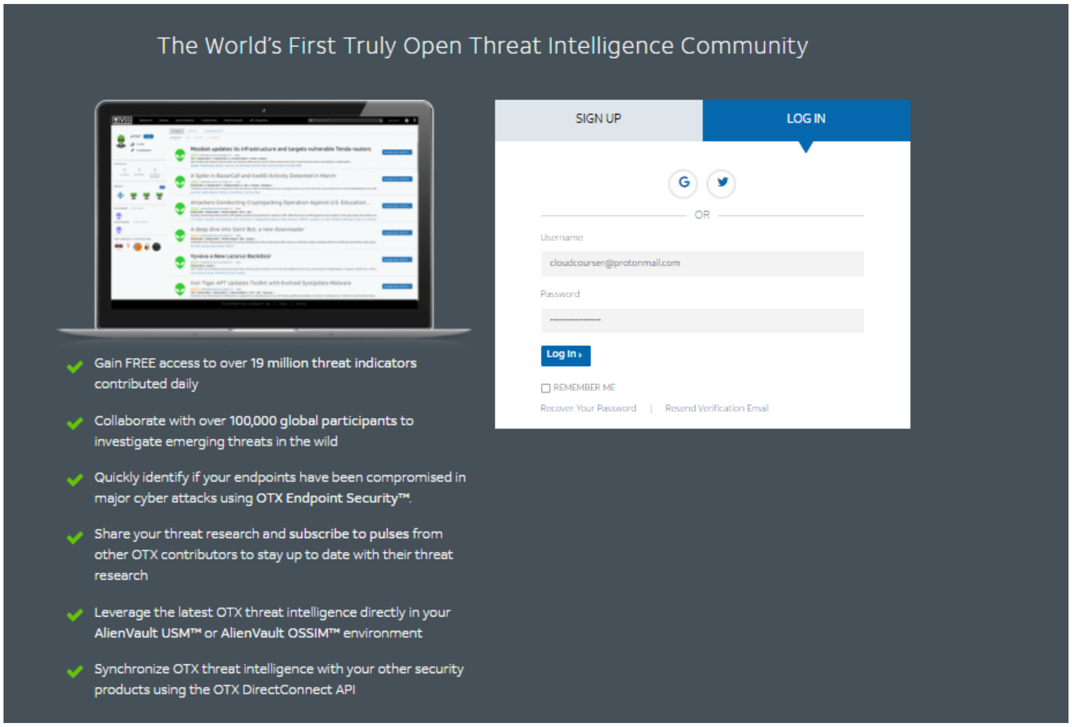
To confirm this is correct, go to https://otx.alienvault.com/accounts/confirm-email/v2qflncnhduufwxnyunmnbiuk4phtao6j0km5zuterybyo67k2glnaiayevxpwuv

Unsubscribe or Update email settings

5707 Southwest Parkway, Bldg. 2, Ste. 300 | Austin, TX | USA 78735 | Tel: +1 650 713-3333
Suite 1201, The Capitol, 14 – 23 Grand Parade | Cork City, Ireland T12 RF85 | Tel: 353 21 206 3716
Calle Méndez Álvaro 20, Planta 3, Oficina 326, 28045 | Madrid, Spain | Tel: +34 915151344
Email Us at: otx-support@alienvault.com

© 2021 AlienVault, Inc. All Rights Reserved. | Privacy Policy

3 The link will take you back to AlienVault with a popup that your account is activated. You can now click **LOG IN** and enter your credentials.



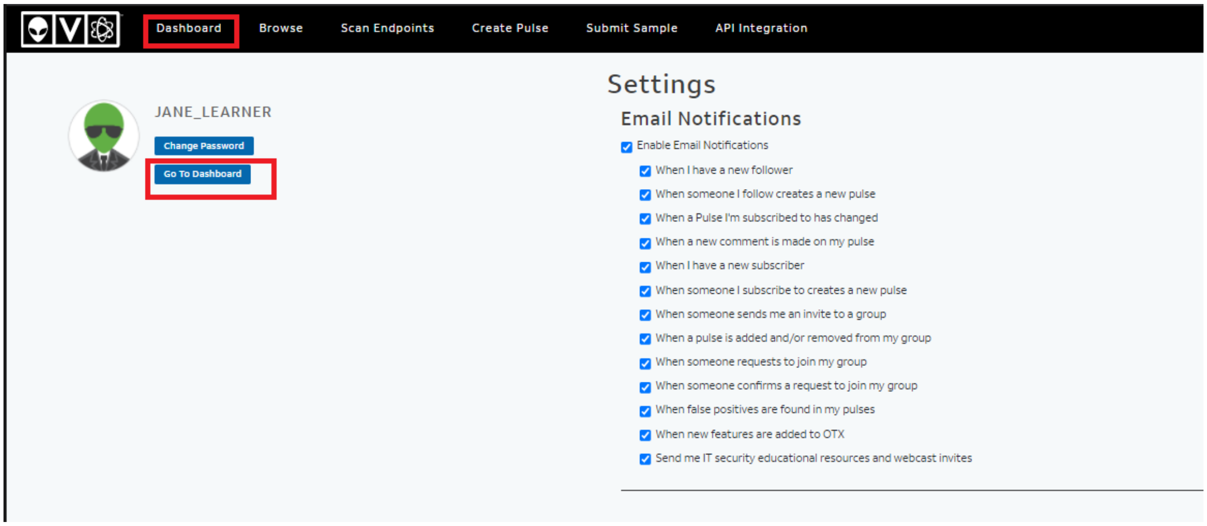
The World's First Truly Open Threat Intelligence Community

Username: cloudcourser@protonmail.com

Password: •••••••••••••••••••

- ✓ Gain FREE access to over 19 million threat indicators contributed daily
- ✓ Collaborate with over 100,000 global participants to investigate emerging threats in the wild
- ✓ Quickly identify if your endpoints have been compromised in major cyber attacks using OTX Endpoint Security™.
- ✓ Share your threat research and subscribe to pulses from other OTX contributors to stay up to date with their threat research
- ✓ Leverage the latest OTX threat intelligence directly in your AlienVault USM™ or AlienVault OSSIM™ environment
- ✓ Synchronize OTX threat intelligence with your other security products using the OTX DirectConnect API

4 Click **Dashboard** in the header or **Go To Dashboard** next to your avatar on the profile page.



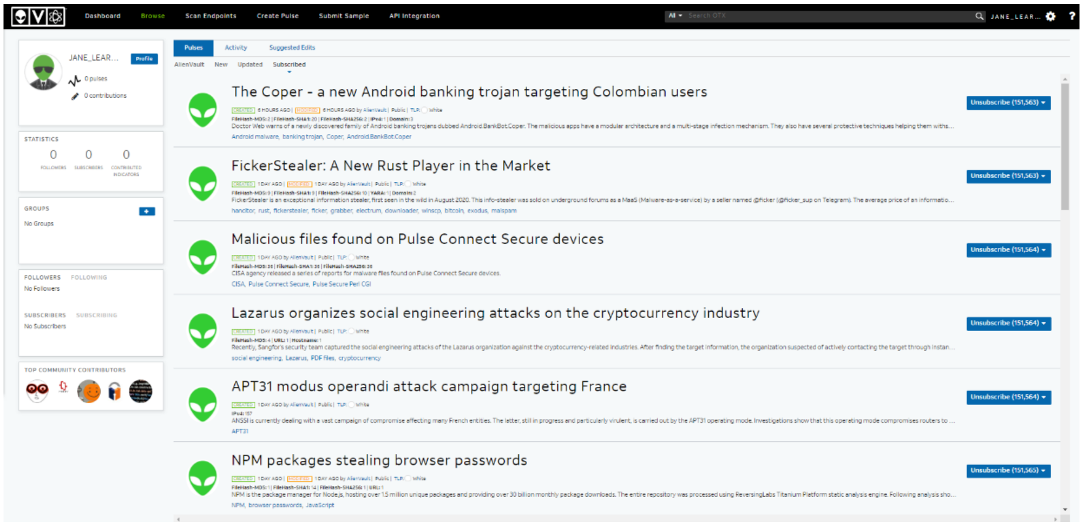
Settings

Email Notifications

☑ Enable Email Notifications

- ☑ When I have a new follower
- ☑ When someone I follow creates a new pulse
- ☑ When a Pulse I'm subscribed to has changed
- ☑ When a new comment is made on my pulse
- ☑ When I have a new subscriber
- ☑ When someone I subscribe to creates a new pulse
- ☑ When someone sends me an invite to a group
- ☑ When a pulse is added and/or removed from my group
- ☑ When someone requests to join my group
- ☑ When someone confirms a request to join my group
- ☑ When false positives are found in my pulses
- ☑ When new features are added to OTX
- ☑ Send me IT security educational resources and webcast invites

5 After the **Dashboard** page loads, note that you can subscribe to pulses, which are feeds related to malware, advanced persistent threats (APTs), or indicators of compromise (IOCs).



The Coper - a new Android banking trojan targeting Colombian users
CREATED 6 HOURS AGO | MODIFIED 6 HOURS AGO by AlienVault | Public | TLP: White
FileHash-MD5: 2 | FileHash-SHA1: 20 | FileHash-SHA256: 2 | IPv4: 1 | Domain: 3
Doctor Web warns of a newly discovered family of Android banking trojans dubbed Android.BankBot.Coper. The malicious apps have a modular architecture and a multi-stage infection mechanism. They also have several protective techniques helping them withs...
Android malware, banking trojan, Coper, Android.BankBot.Coper
Unsubscribe (151,563)

FickerStealer: A New Rust Player in the Market
CREATED 1 DAY AGO | MODIFIED 1 DAY AGO by AlienVault | Public | TLP: White
FileHash-MD5: 9 | FileHash-SHA1: 9 | FileHash-SHA256: 10 | YARA: 1 | Domain: 2
FickerStealer is an exceptional information stealer, first seen in the wild in August 2020. This info-stealer was sold on underground forums as a MaaS (Malware-as-a-service) by a seller named @ficker (@ficker_sup on Telegram). The average price of an informatio...
hancitor, rust, fickerstealer, ficker, grabber, electrum, downloader, winscp, bitcoin, exodus, malspam
Unsubscribe (151,563)

Malicious files found on Pulse Connect Secure devices
CREATED 1 DAY AGO by AlienVault | Public | TLP: White
FileHash-MD5: 36 | FileHash-SHA1: 36 | FileHash-SHA256: 36
CISA agency released a series of reports for malware files found on Pulse Connect Secure devices.
CISA, Pulse Connect Secure, Pulse Secure Perl CGI
Unsubscribe (151,564)

Lazarus organizes social engineering attacks on the cryptocurrency industry
CREATED 1 DAY AGO by AlienVault | Public | TLP: White
FileHash-MD5: 4 | URL: 1 | Hostname: 1
Recently, Sangfor's security team captured the social engineering attacks of the Lazarus organization against the cryptocurrency-related industries. After finding the target information, the organization suspected of actively contacting the target through instan...
social engineering, Lazarus, PDF files, cryptocurrency
Unsubscribe (151,564)

APT31 modus operandi attack campaign targeting France
CREATED 1 DAY AGO by AlienVault | Public | TLP: White
IPv4: 157
ANSSI is currently dealing with a vast campaign of compromise affecting many French entities. The latter, still in progress and particularly virulent, is carried out by the APT31 operating mode. Investigations show that this operating mode compromises routers to ...
APT31
Unsubscribe (151,564)

NPM packages stealing browser passwords
CREATED 1 DAY AGO | MODIFIED 1 DAY AGO by AlienVault | Public | TLP: White
FileHash-MD5: 1 | FileHash-SHA1: 14 | FileHash-SHA256: 1 | URL: 1
NPM is the package manager for Node.js, hosting over 1.5 million unique packages and providing over 30 billion monthly package downloads. The entire repository was processed using ReversingLabs Titanium Platform static analysis engine. Following analysis sho...
NPM, browser passwords, JavaScript
Unsubscribe (151,565)

Tip

Search results in the following section may vary, as AlienVault is a dynamic, community-fed source that contains up-to-date threat information. The fundamental ideas behind these tasks should remain consistent. Should the look of AlienVault change significantly, be sure to check out its documentation for guidance.

Lab Task 2: Search for Information About Common Indicators of Compromise

1. Use the search bar to look for the **Mimikatz** tool.
2. List some APTs that are associated with the use of **Mimikatz** in their campaigns (use your search results).
3. List some malware families associated with **Mimikatz**.
4. Take a deeper look at the **PowerShell/Mimikatz** report. Hover over each feature name for a tooltip that explains the item. Once done, click on **Process Visualization Steps** to see a map of the activity associated with this sample.
5. How many hashes are available to use as IOCs in your antivirus setup?
6. Click on one of the hashes and explore the **Analysis Overview** of the sample. Note the **Strings** section at the bottom of the screen. Recall from ***CIT-03*** the use of strings when creating YARA rules. Strings are also of significant value when performing memory analysis using **Volatility**, as we covered in the ***DFIR-07: Memory Analysis*** module.

Key Takeaways:

In this exercise, you were asked to do the following:

1. ***Create a new user account on AlienVault.***
2. ***Search for information about common indicators of compromise.***

Your organization's resources can be greatly enriched by using community-driven resources such as AlienVault, VirusTotal, and Anomali. New exploits, IOCs, and malware samples are discovered by the minute, and subscribing to the threat feeds provided by these sites can be an invaluable resource in your defense toolkit.

For further study, research and create your own YARA rules based on IOCs discovered on AlienVault, or consider writing your own pulse wiki based on research you perform.