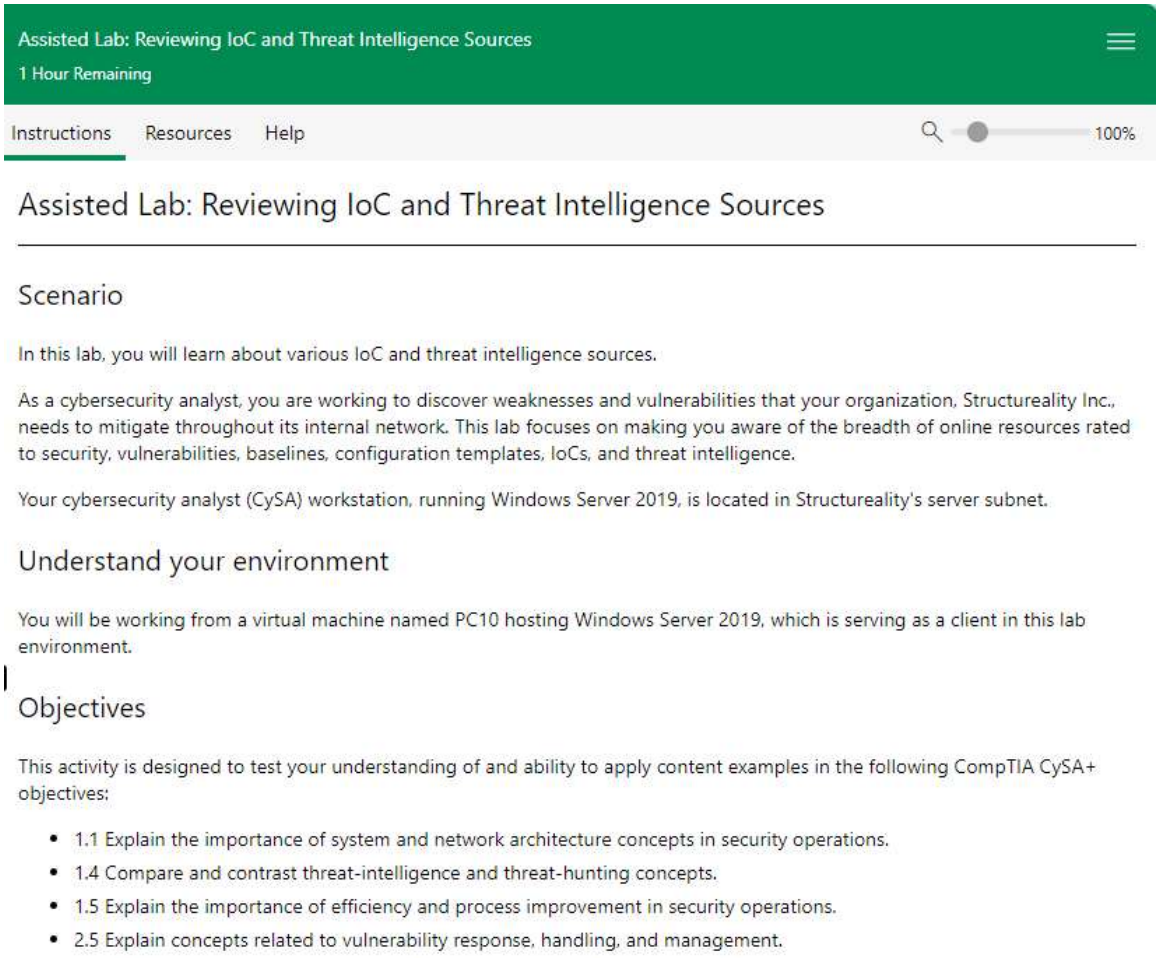


Understanding IoC and threat intelligence Sources

Sources of IoC (Indicators of Compromise) and threat intelligence feeds are available from numerous open-source community groups, commercial entities, and government agencies. An IoC and/or threat intelligence source / feed can provide you with actionable intelligence to defend against future attacks or discover evidence of previous compromise (i.e., threat hunting).

However, most of these information sources require registration or a paid subscription. This is because an attacker can use the information they provide to avoid detection, so the providers and vendors want to minimize access to this data by the malicious and limit it to those deemed benign. Therefore, these services do not lend themselves to a lab demonstration.

Instead, in this exercise, you will view the introduction to the real-time cyber threat intelligence indicator feeds from CIS.

The CySA+ Skillable lab environment does not have direct internet access. Therefore, you must perform some tasks using your local browser. The links in this task will open in a new browser window. Arrange both windows so that you can refer to the content in the external site and to these instructions.

Open the following URL: https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds

The Real-Time Indicator Feeds page from CIS: Center for Internet Security is displayed. Look over this document to learn about the information provided by CIS for free to US State, Local, Tribal, and Territorial entities (SLTTs) (i.e., US-based government entities).

CIS is an excellent source of information. However, their feed may be limited to US SLTT entities (which usually means government).

Open https://otx.alienvault.com/browse/global/pulses

Enter mirai in the Search OTX field at the top of the page.

The results should include any AlienVault Pulse related to the Mirai botnet and its related malware.

Pulses are collections of Indicators of Compromise, IPs, urls, and file hashes related to potentially malicious activity, contributed by the AlienVault Labs research team as well as other members of the OTX community.

Select any of Pulse results which includes Mirai in the title (such as Mirai Bonet IOCs).

Look over the page. Notice the colored bar of the various TYPES OF INDICATORS.

On the selected AlienVault Pulse page related to Mirai, what is one of the types of indicators?

Registrar

Host system

FileHash

Victim ID

Congratulations, you have answered the question correctly.

Notice that the first 10 of many pages of indicators are displayed. The display of indicators is sorted by ADDED date and time by default.

Select the item under the INDICATOR heading.

The Analysis Overview page for the selected indicator is displayed.

Scroll down the page to view the Analysis tab results.

Scroll back up and select the Related Pulses tab.

This tab lists other IoCs with elements in common with this selected indicator.

Use the back arrow button on Firefox to return to the AlienVault Pulse page.

In the Search: field above the indicator table, enter domain.

The results will be of indicators with domain names.

Select any indicator to view its Analysis Overview page. Then, return to the AlienVault Pulse page using the Back arrow button of Firefox.

Perform additional searching using the key terms of "URL", "IPv4", "IPv6", "hostname", and "hash".

Not all of these search terms will have indicator results for the selected Pulse.

Close the tab in your local browser focused on alienvault.com.

This exercise showed you an example of a US government IoC and threat intelligence feed description page and an older IoC page from AlienVault. There are many other IoC and threat intelligence sources to consider, but most require registration to access. Here are several to consider:

Cybersecurity and Infrastructure Security Agency:

https://www.cisa.gov/cybersecurity

NIST Computer Security Resource Center:

https://csrc.nist.gov/

FBI InfraGard:

https://www.infragard.org/

SANS Internet Storm Center:

https://isc.sans.edu/

Virus Total Intelligence:

https://www.virustotal.com/gui/intelligence-overview

Cisco Talos Intelligence:

https://www.talosintelligence.com/

SPAMHAUS:

https://www.spamhaus.org/

Crowdstrike:

https://www.crowdstrike.com/products/threat-intelligence/

AlienVault Open Source Threat Exchange:

https://otx.alienvault.com/

Anomali:

https://www.anomali.com/products/threatstream

Mandiant:

https://www.mandiant.com/advantage/threat-intelligence

Abuse.CH:

https://abuse.ch/

If you explore these URLs, open a new tab in your local browser.

There is a community-managed list of threat intelligence sources and sites maintained on GitHub under the awesome-threat-intelligence project. You can find this project by searching for it with "github awesome-threat-intelligence".

Check your work

Confirm that you looked over the CIS feed information.

Confirm that you explored an IoC page from AlienVault.

Assisted Lab: Reviewing IoC and Threat Intelligence Sources

46 Minutes Remaining

Explore The Exploit Database

The Exploit Database is a CVE-compliant archive of public exploits and corresponding vulnerable software developed for use by penetration testers and vulnerability researchers. The Exploit Database is maintained by Offensive Security, an information security training company that provides various information security certifications and high-end penetration testing services. The Exploit Database is a non-profit project offered by Offensive Security as a public service. They aim to serve the most comprehensive collection of exploits gathered through direct

submissions, mailing lists, and other public sources, and present them in a freely-available and easy-to-navigate database. The Exploit Database is a repository for exploits and proofs-of-concept rather than advisories, making it a valuable resource for those who need actionable data right away.

On your local computer, open another tab in your current browser or open a new browser.

Open https://www.exploit-db.com/

Be sure to leave the lab environment browser window open.

The Exploit Database main page should display listing posted exploit information in reverse chronological order (i.e., most recent at the top of the list).

Look over the list of exploits. Notice how many of the postings are very recent.

The default Exploits page provides the following information:

The *Date* column is sorted in reverse chronological posting order.

The *D* or *Download Exploit* column enables you to download the exploit file.

The *A* or *Vulnerable Application* column may include a link to download the vulnerable software (if licensing allows)

The *V* or *Verified* column indicates whether the site owners have verified the exploit works (with a checkmark) or have not been able to verify (with an X). Note: items that are proven not to work are removed entirely.

The *Title* column is a brief description of the target software and the type of exploit

The *Type* column indicates if the exploit is DOS, Local, Remote, or a WebApp.

The *Platform* column indicates the affected OS or host, such as Windows, Linux, Hardware, PHP, Python, or Multiple

The *Author* column indicates the entity creating or at least publishing the information.

The most valuable feature of Exploit Database is unique compared to other exploit information sites and services - namely, the ability to download the source code of listed exploits.

Select the Filters button.

The filter fields are displayed: Type, Platform, Author, Port, and Tag.

Select each of the filter fields' pull-down lists to view the options. You can make selections from the pull-down lists to immediately filter the results in the main list.

Which of the following is not an option in the list of Filters for exploits on The Exploit Database?

Authentication Bypass / Credentials Bypass

Code Injection

Deserialization

Evil Twin / Rogue Access Point

Heap Overflow

Congratulations, you have answered the question correctly.

On the left side of the page, there is a compressed side menu. Move your mouse over the side menu to expand it.

Select GHDB from the side menu.

The Google Hacking Database page is displayed.

The GHDB is a collection of search expressions that can be used to find vulnerabilities in websites via Google.

Select the Filters button.

Select the Category pull-down list to view all the groups/types of Google hacks (a.k.a., Google dorks). Then, select Files Containing Passwords from that list.

From the results, select any password-focused Google hacks to try.

Since the collection of Google hacks is always changing, we can't indicate a specific one to try. So, pick the first one that seems interesting to you.

A details page for the selected Google hack will be displayed. There are usually very few additional details on this page.

Select the Google hack code beside the Google Search: indicator.

This should open a new browser tab to google.com with the selected Google hack as a search term.

Look over the results. But do not visit any of the sites listed in the results at this time.

While visiting a site discovered through a Google search is often valid, there is always the possibility that the discovered site is itself malicious or hosting malicious content. Always perform Google hacking/dorking from a hardened system, such as one hosted in a VM which can be reset and restored to a known secure state in the event of malware exposure.

Close the local browser tab focused on the google.com search results to return to the tab focused on exploit-db.com.

There are other options to explore in the side menu.

Other features of Exploit Database to explore from the side menu include:

Security Papers - a collection of non-commercial papers on security and exploitation issues

Shellcodes - ready-to-run payload exploit scripts which may be used in combination with a delivery/intrusion exploit

SearchSploit: The Manual - a guide to using the Linux tool to search a downloaded cache of Exploit Database

Close the tab in your local browser focused on exploit-db.com.

Check your work

Confirm that you explored The Exploit Database

Evaluate security policy templates

Once you have reviewed IoCs and threat intelligence and performed threat hunting, you might need to update your security configurations to address the new concerns. As a cybersecurity analyst, you may need to use existing security templates from a reputable source, such as sans.org, which can be tailored and scoped to your environment's specific needs and requirements. In this exercise, you will be evaluating and customizing a security policy template.

Open https://www.sans.org/information-security-policy/

Be sure to leave the lab environment browser window open.

You may see the typical pop-up notification regarding the acceptance of cookies. This notification is due to the General Data Protection Regulation (GDPR). Select Accept All Cookies.

This site maintains security policy templates that anyone can use and customize. The security policy templates are grouped into various categories.

Under categories, select the Network Security check box.

You may need to scroll down to view the Categories list under the Filters: heading under the large graphical banner.

The security policy templates presented will only be those in the Network Security category.

Select the Wireless Communication Policy to expand its section.

Read the description of this security policy concept.

The PDF copy of this security policy has been pre-downloaded to a media container for use in the virtual lab environment.

Switch back to the browser window focused on the CySA+ Skillable virtual lab environment.

7. Connect to the PC10 virtual machine, send Ctrl+Alt+Delete, and sign in as T jamie using T Pa$$w0rd as the password.

8. Select the **Resources** tab from the lab interface's *Instructions* area. On the *Resources* tab, select the **DVD Drive** pull-down list and select **Student-Resources-L03.ISO**. Then, select the **Instructions** tab to return to the lab steps.

9. Select **Type here to search** magnifying glass icon from the taskbar, type T file, then select **File Explorer** from the results.

10. From the left pane, select **DVD Drive (D:)**.

11. Double-lick to open **Wireless_Communication_Policy**.

    This is a PDF document, but the pdf file extension will not be displayed as part of the filename.

    File Explorer does not display known file extensions by default.

12. On the *How do you want to open this file?* window, select **OK** to open this PDF in Microsoft Edge.

13. The Wireless Communication Policy PDF document will display in the Microsoft Edge browser.

14. Review the major sections of this *Wireless Communication Policy*.

    Notice the sections or headings of Overview, Purpose, Scope, Policy, Policy Compliance, Related Standards, Policies and Processes, Definitions and Terms, and Revision History.

15. Close Microsoft Edge.

    You can view other examples of policy templates from SANS through your local system's browser.

Return to your local browser's tab focused on sans.org.

Select to clear the Network Security category checkbox.

Under categories, select the Application Security check box.

Locate and expand the Web Application Security Policy section within the Application Security category, then read the policy description.

Switch back to the browser tab focused on the CySA+ Skillable virtual lab environment.

File Explorer should still be open and focused on the media Student-Resources-L03.ISO as DVD Drive (D:).

Double-lick to open Web_Application_Security_Policy.

This is a Microsoft Word document, but the docx file extension will not be displayed as part of the filename.

LibreOffice Writer will open to display this document.

Select OK on the Tip of the Day window.

Assisted Lab: Reviewing IoC and Threat Intelligence Sources

30 Minutes Remaining

Instructions Resources Help 100%

☑ 25. Scroll down through the document to view each of the eight (8) section headings.

Which of the following is not one of the eight headings in the Web Application Security Policy template? (Select all that apply)

- ☑ Summary
- ☐ Overview
- ☐ Purpose
- ☐ Policy Compliance
- ☑ References
- ☐ Scope
- ☐ Revision History
- ☐ Definitions and Terms
- ☐ Policy
- ☐ Related Standards, Policies, and Processes
- ☑ Supplemental and Supporting Material

Score

✓ Congratulations, you have answered the question correctly.

☑ 26. Customize this policy template by replacing the Company Name placeholder with T CySA+ Lab Corp and craft an entry in the Revision History using today's date, use T SecManagement for responsibility, and using T Initial crafting and customization as the summary of changes.

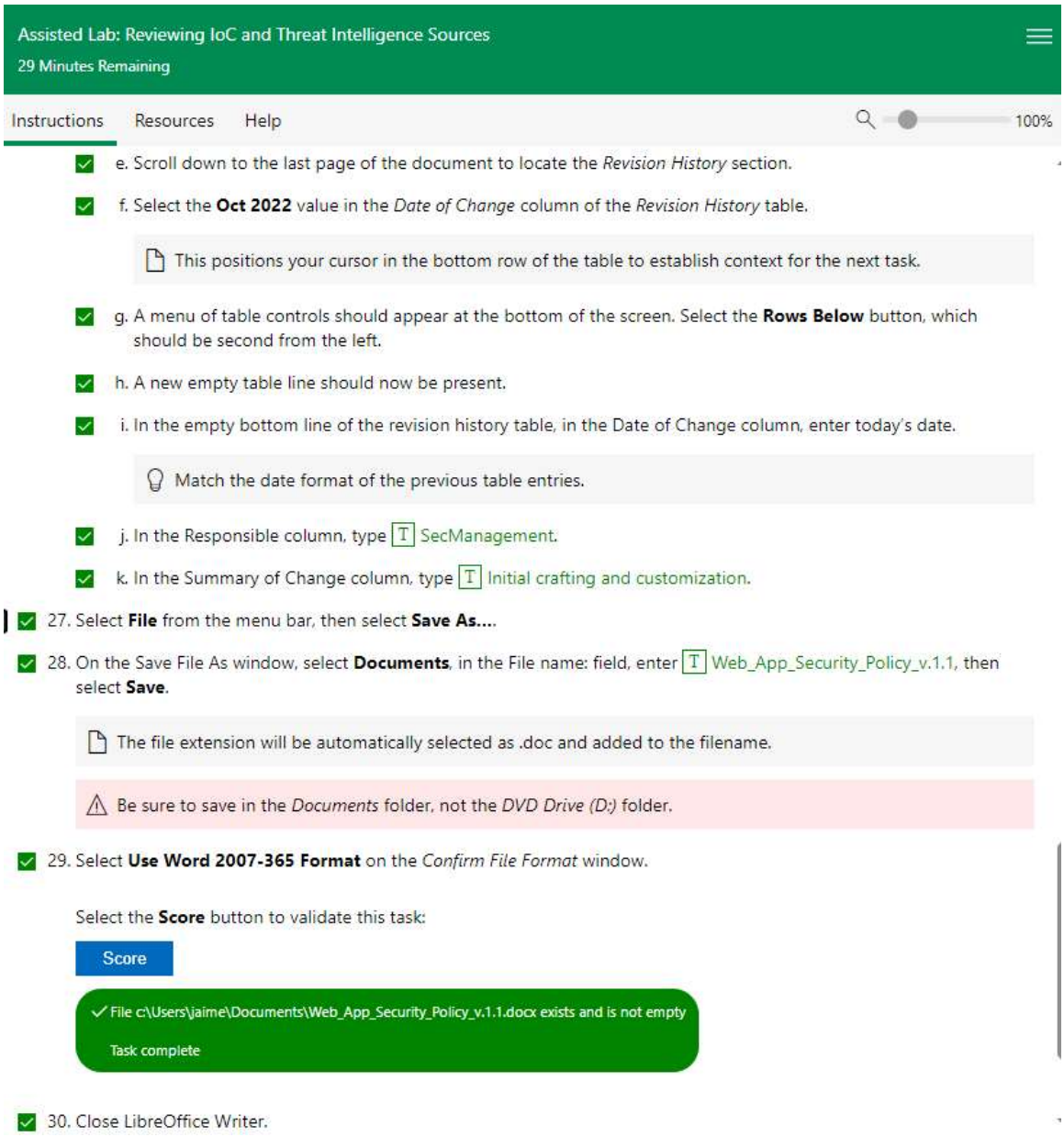
▼ Expand this hint for guidance.

☑ a. Select **Edit** from the toolbar of AbiWord, then select **Find and Replace...**.

☑ b. In the Find window, enter T <Company Name> in the Find what: field and enter T CySA+ Lab Corp in the Replace with: field, then select **Replace All**.

☑ c. Close the *Find and Replace* window.

☑ d. There should have been five (5) changes to the policy template based on the replacement operation. The first of which is present at the end of the first sentence under the *Purpose* heading.



Close the tab in your local browser focused on sans.org.

Check your work

Confirm that you viewed several security policy templates.

Confirm that you customized a security policy template.

Access security benchmarks and configuration guides

As a cybersecurity analyst, you may need to use existing security templates from a reputable source, such as CIS (Center for Internet Security). In this exercise, you will be evaluating security benchmarks and configuration guides.

On your local computer, open another tab in your current browser or open a new browser.

Be sure to leave the current local browser tab open, which is focused on the virtual lab environment. This will allow you to return to these instructions and perform additional steps.

In your local browser's address bar, enter https://www.cisecurity.org/cis-benchmarks/.

You may see the typical pop-up notification regarding the acceptance of cookies. This notification is due to the General Data Protection Regulation (GDPR). Select Accept.

CIS (Center for Internet Security) maintains security configuration guides and benchmarks that anyone can use and customize.

The CIS (Center for Internet Security) Benchmarks (a.k.a. configuration guides) are grouped into seven categories: Operating Systems, Server Software, Cloud Providers, Mobile Devices, Network Devices, Desktop Software, and Multi-Function Print Devices.

Scroll down the page of Benchmarks to locate the Microsoft Windows Server entry. The benchmarks are in alphabetical order.

Read over the list of available versions of this benchmark.

At the bottom of the section for Microsoft Windows Server, there is the statement "To further explore this Benchmark, click here.". Select that click here link.

A details page for the Microsoft Windows Server benchmarks is displayed.

This CIS Benchmark is the product of a community consensus process and consists of secure configuration guidelines developed for Microsoft Windows Server.

Select DOWNLOAD LATEST CIS BENCHMARK.

This opens a new page where the free PDF of the benchmark document can be obtained. However, there is a need to provide contact information to access the download. Do not fill out this form at this time – you are not required nor encouraged to distribute your private information as part of this exercise.

If you wish to download CIS benchmarks, you must provide some contact details to CIS, including name, organization, sector, role, email, and country.

Select the Back or left arrow on the Firefox toolbar to return to the previous web page (i.e., https://www.cisecurity.org/cis-benchmarks).

CIS has a benchmark document for which of the following products? (Select all that apply)

Firefox

Amazon Web Services

Discord

Apple MacOS

Docker

Congratulations, you have answered the question correctly.

Locate benchmark examples of the remaining categories: Server Software, Cloud Providers, Mobile Devices, Network Devices, Desktop Software, and Multi-Function Print Devices, and display their related content.

When you have finished exploring the CIS benchmarks or the rest of their site and offerings, close your local browser tab focused on cisecurity.org.

Check your work

Confirm that you explored the categories and topics of CIS benchmarks (a.k.a. configuration guides).