Collection Methods and Sources & Threat Intelligence Hunting and Sharing

By: Keziah Rogers

Things learned from this project:
Know about Open Source Intelligence (OSINT)
Work with OSINT Tools
Employ Incident Response using SIEM
Use a Honeypot Tool
Use MITRE ATT&CK to Identify Tactics, Techniques, and Procedures (TTPs)
Access and Research Logs using Windows Event Viewer
Enable Firewall Logging

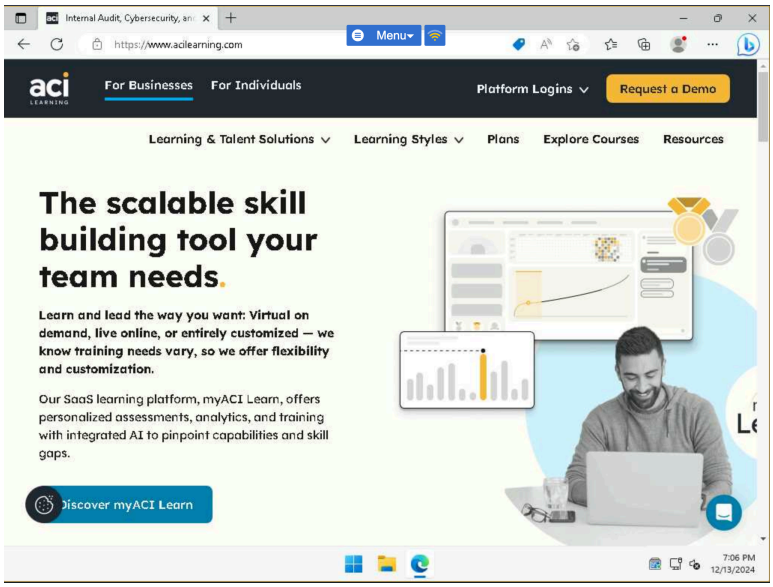
Collection Methods and Sources
Information such as news stories, magazine features, user-uploaded videos and photographs on social networking sites, blogs, forums, government bulletins, deep and dark web searches are all examples of sources used in OSINT. The use of OSINT is crucial in both governmental and private investigations. As the rate at which new data is being generated increases, it is more crucial than ever that analysts develop effective strategies for locating, cataloging, and analyzing the data at their disposal.

Analysts will look all over the Internet for readily available information anyone can access. Accessing this data also leaves no trace that can be used to figure out what happened. So, it is important for organizations to limit their digital footprint, which can expose the company to a cyber-attack. Exposure of priority information like executive email addresses, phone numbers, employee names, in-depth about pages, website code build analysis, wireless network analysis and packet inspection, image processing and other things that threats could use.

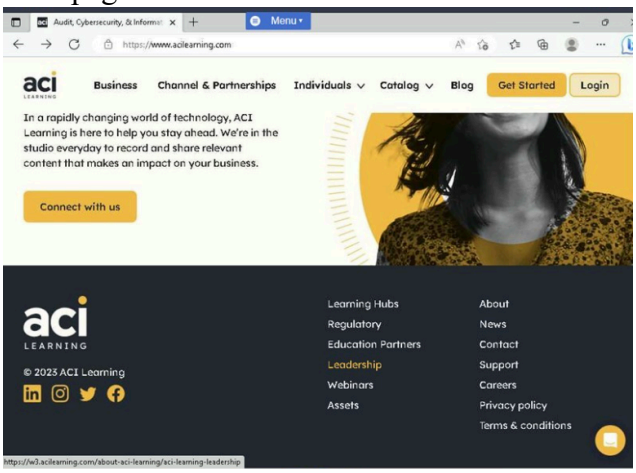
In this exercise, you will learn about collection methods and sources.

Task 1 - Know about Open Source Intelligence (OSINT)
In this task, you are going to manually explore the ACI learning website and look for potential pieces of information that are being shared that threat actors may be interested in. Some information will be necessary because customers need to contact us. Some of the information may be overshared and can be used to further research and find information on the company and its employees.

- Connected to ACIWIN11 (VM).
- Clicked the Microsoft Edge icon on the Taskbar.
- Microsoft Edge is displayed.
- In the address bar, I typed the following and press Enter: acilearning.com
- The ACI Learning webpage is displayed.

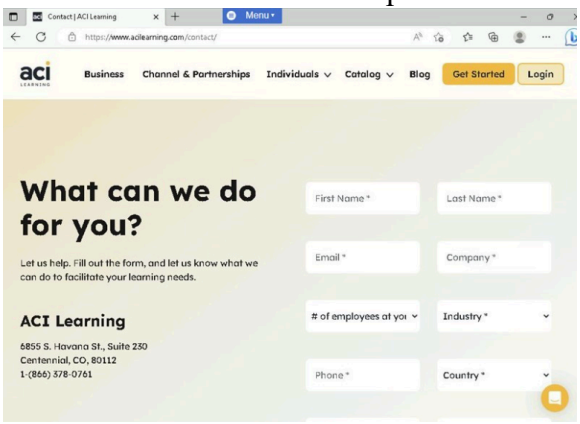


- Clicked Accept on the pop-up window.
- Scrolled down through the page and review the information.
- I understood that ACI is a multifaceted premium tech training company.
- I found there were clickable options for learning more about the company.
- This took me to a website pertaining to what that section of the company does.
- I scrolled to the bottom of the page & noticed the Leadership option.
- On the ACI Leadership page, you can view members who make up the management of ACI.
- Threat actors can use this page for web and social media searches to formulate social engineering attacks.

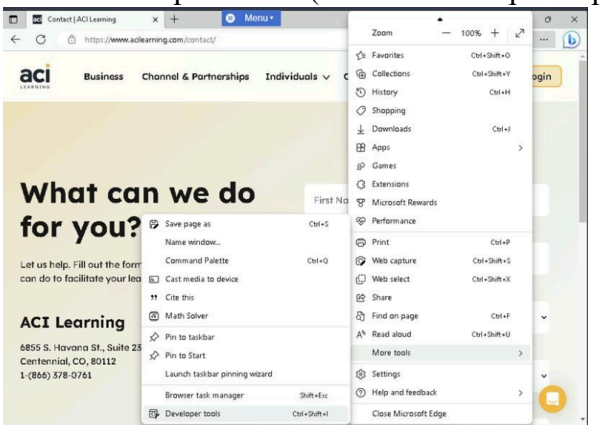


- Clicked Contact at the bottom of the page.
- The ACI Learning Contact page is displayed.
- Here you can see the address and phone number for the company.

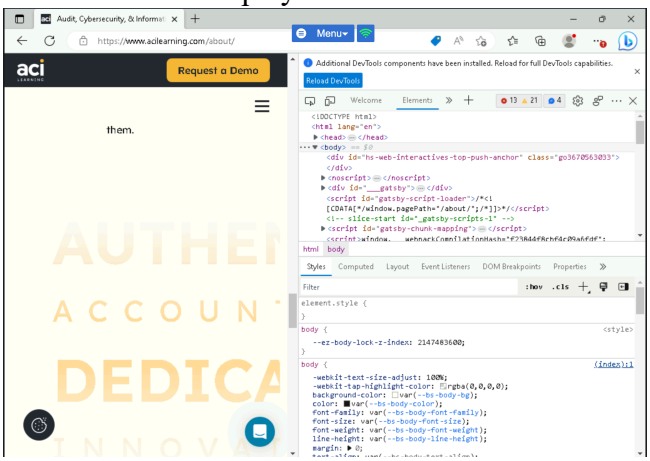
- You can also view the full addresses and phone numbers of each of the ACI Learning Locations.



- Clicked the … icon on the browser
- Clicked More Tools and the Developer Tools. (The DevTools pane appeared)



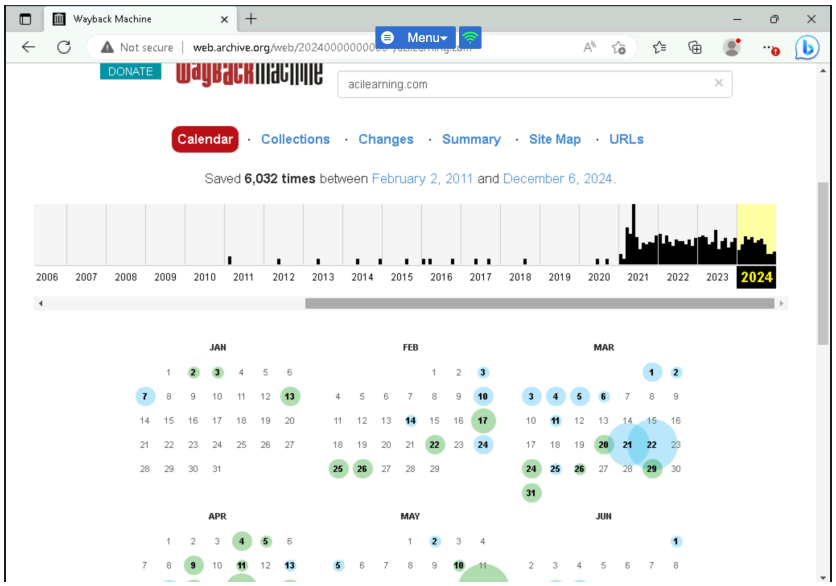
- Clicked on Elements.
- The HTML Code for the website is displayed.



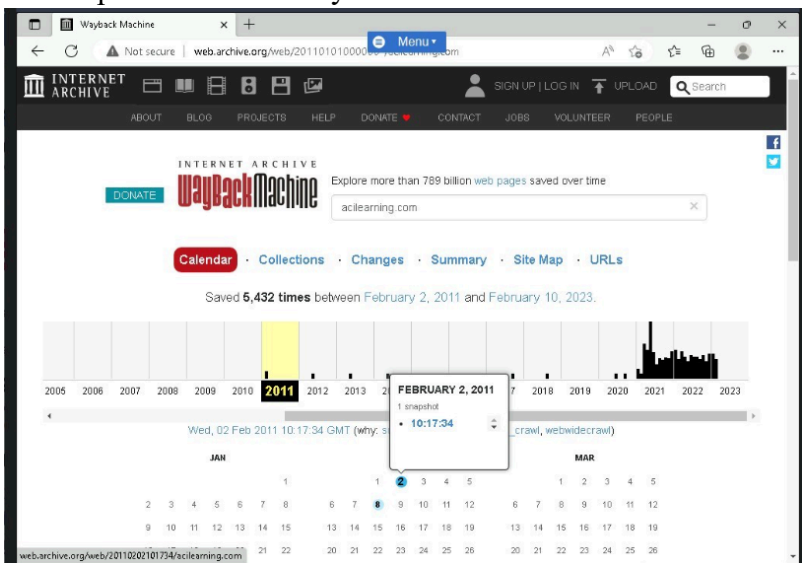
- As an analyst, I can use DevTools primarily for the detection of bugs, the execution of instructions, the verification of variable values, and so on.
- If there are flaws in the code, it can reveal unwanted information and present a vulnerability for those who are looking.
- Clicked Close on the DevTools pane.

Reviewed a few popular tools used in OSINT gathering

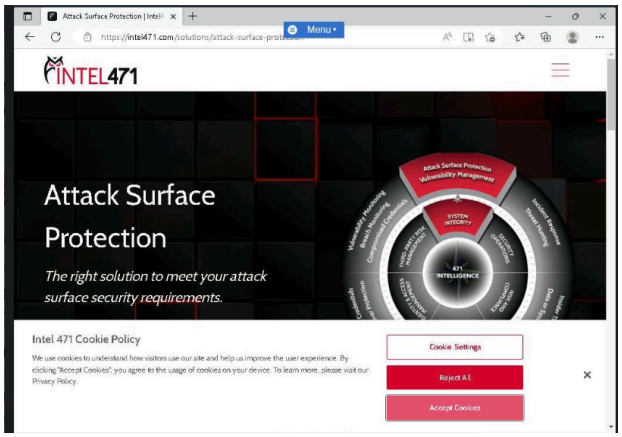
- Opened MS Edge & typed wayback.archive.org
- The Internet Archive Wayback Machine website is displayed.
- This site houses different versions of a website that may exist.
- This is a great way to see information exposure over time.
- Typed the following in the search bar and press Enter: acilearning.com
- You can see the site was saved a total of 6,032 times over the span of 13 years from 2011 to 2024.



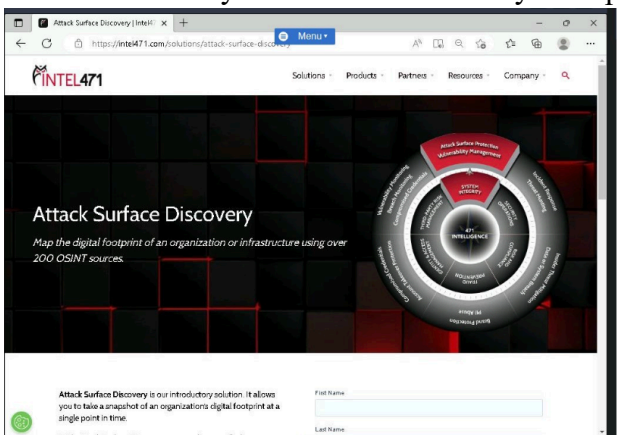
- Clicked 2011.
- Clicked February 2, 2011, and then click the time, 10:17:34, that appears to access the site snapshot from that day.



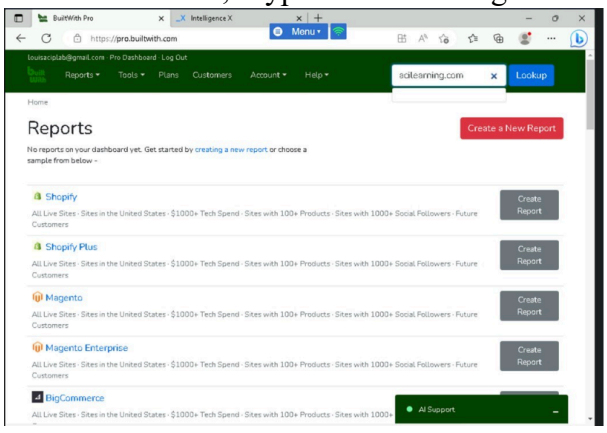
- In the address bar, I typed the following and press Enter: spiderfoot.net
- The Intel471 website is displayed.
- A prompt appeared, and I clicked Accept Cookies.
- This site houses several products that can help with cyber security needs.



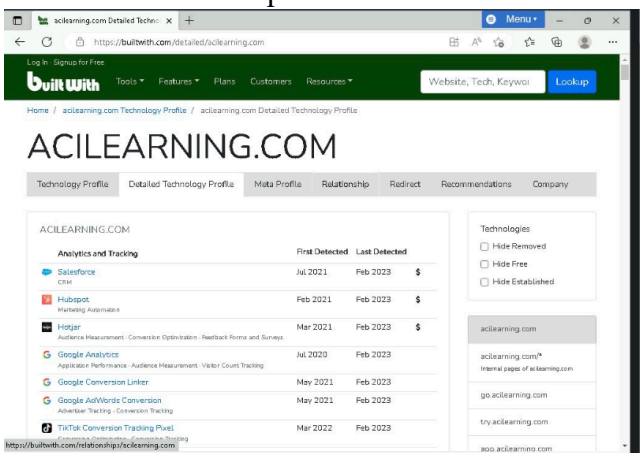
- I scrolled down the page and clicked Attack Surface Discovery.
- Here you can see this application uses over 200 OSINT sources to map out an organization's digital footprint.
- This can be a very useful tool as an analyst to speed up the research process.

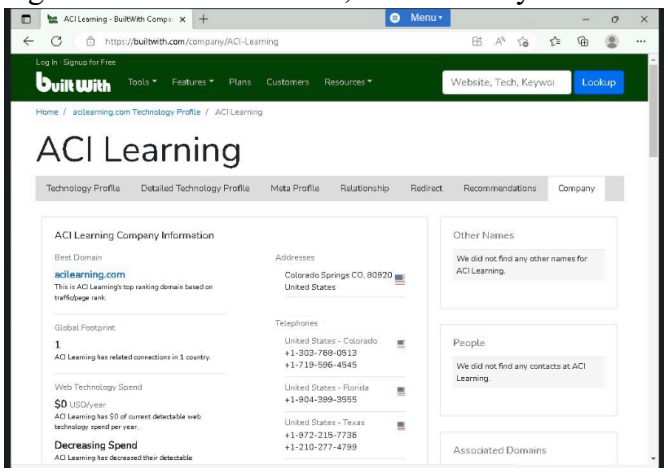


- In the address bar, I typed the following and press Enter: builtwith.com
- BuiltWith profiles a domain to quickly find internet assets associated with it and conduct passive surveillance.
- In the search box, I typed the following and clicked Lookup: acilearning.com

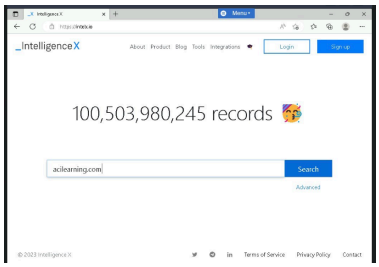


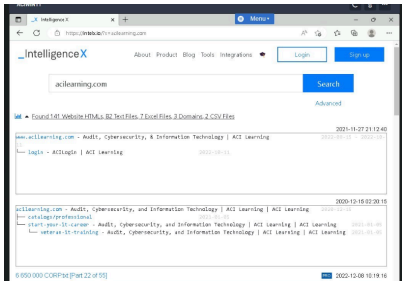
- The ACI Learning domain has been found.
- By scrolling down the page, you can see different companies and technologies that ACI is associated with.

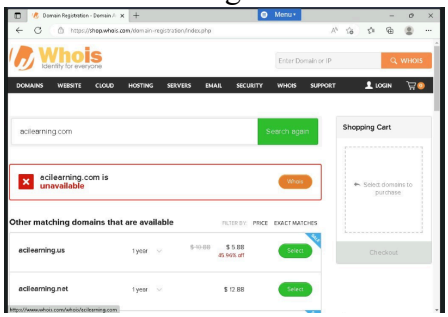
- I clicked the Detailed Technology Profile tab.
- The Detailed Technology Profile page is displayed.
- This is a free feature with up to 10 views in a day.
- Information about when the company was first detected using the service and when they used it last is available. It is a free or paid service.
- Each service can be clicked on to find out more about it.
- I clicked Relationship.
- 

- I completed the CAPTCHA.
- The Relationship page to acilearning.com is displayed.
- You can see the history of items like search tags, the website associated, and even the IP addresses associated with the URL.
- I clicked the Redirect tab.
- The Redirect page is displayed.
- Here you can see where internet traffic gets redirected to when accessing aspects of the website.
- I clicked Company. Here you can see where ACI Learning is active worldwide, organizational information, and how they use technologies over time.
- 

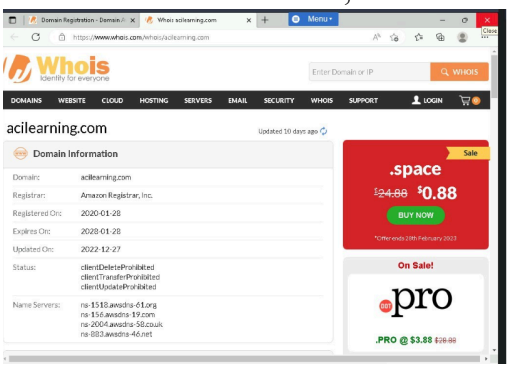
- In the address bar, I typed the following and press Enter: intelx.io
- The Intelligence X webpage is displayed.
- This is a search engine for domains.
- In the search box, I typed the following and clicked Search: acilearning.com

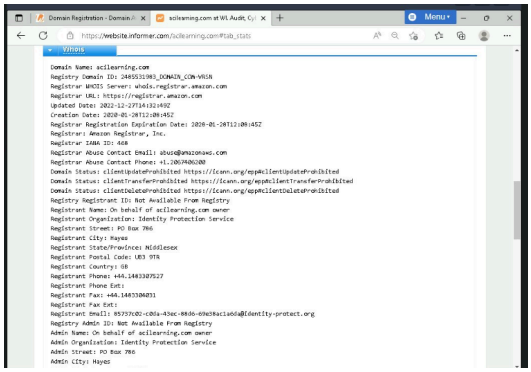
- 

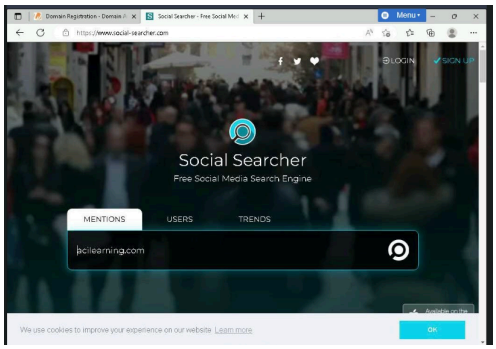
- Here you can see the search has found a wealth of information.
- I clicked on the link to the discovered information right below the search box.
- 

- Here you can see the results from the search.
- You can see logs, text files, excel files, .csv files and more information is available to gather information.
- In the address bar, I typed the following and press Enter: whois.com
- The Whois.com webpage is displayed.
- Whois is a popular Internet registry that shows who owns a domain, how to contact them, and information about the website and even the servers that house them.
- In the search box, I typed the following and clicked Search: acilearning.com
- I noticed that ACI Learning was unavailable, which means the URL was taken.
- I clicked the orange WHOIS for more information about acilearning.com.
- 

- The report for acilearning.com is displayed.

- Scrolling through, you can see when the site license was created and expired, a lot of DNS information, administrative information, technical contacts, and other information about the website. 

- In the address bar, I typed the following and press Enter: website.informer.com
- The Website Informer webpage is displayed.
- This site allows users to look up a website to gain more insight about the site.
- In the search box, I typed the following and clicked Search: acilearning.com
- General Info gives a general run down of what the organization that has the website does.
- I clicked on Stats & Details.
- Stats and Details of the website are shown.
- I clicked Whois to expand the menu.
- The Whois for the webpage is displayed.
- You can see the same info you saw when you searched for it.
- I scrolled down and clicked the IP Whois menu to expand it & it showed information that relates to the website.
- 
- I then typed and searched social-searcher.com.
- The Social Searcher webpage is displayed.
- This site allows users to search for a keyword, users, and trends on 11 social media platforms in one search.
- In the search box, I typed the following and click the Search icon: acilearning.com

- 

- Posts from Facebook.com, crunchbase.com, zoominfo.com, Twitter, Reddit and more can be seen.
- This very valuable tool demonstrates oversharing information in a quick and easy search.
- Account monitoring can be enabled so administrators can be notified if posts are created on acilearning.com.

<u>*Threat Intelligence Hunting & Sharing*</u>

- Threat hunting means looking for cyber-attacks and advanced persistent threats. Threat hunting is a deep search for the trail left by an individual who might have broken into the network and could be a threat. After getting into a network, an attacker can stay there for months gathering data, looking for confidential information, or getting login credentials that will let them pivot and move laterally across the environment. Once an attacker has avoided being found and gotten through an organization's defenses, many organizations don't have the advanced detection tools needed to stop persistent threats from staying in the network. Threat hunting should be an incorporated part of any defense plan. Companies try to keep up with the latest cyber threats and are ready to respond quickly to any possible attacks. There is a lot of information to sift through for just 1 computer; now consider a network. Analysts will look for indicators of compromise, which are bits of trace evidence that can be investigated to detect possible malicious activities on a system or network, such as data contained in system log entries or files. Like looking at a website in the previous exercise, this can be a manual process or be aided using tools. Common indicators of compromise include but are not limited to:
- Unusual Network Traffic
- Privilege Escalation
- Failed Login Attempts
- Off-Hour Login Attempts
- Increased Access to Files and Databases
- System File and Registry Changes
- Unusual DNS Activity
- Signs of DDOS
- Unusual IP Address Activity
- Log Clearing
    - Learning Outcomes:
        - Employ Incident Response using SIEM
        - Use a Honeypot Tool

- Use MITRE ATT&CK to Identify Tactics, Techniques, and Procedures (TTPs)
- Access and Research Logs using Windows Event Viewer
- Enable Firewall Logging

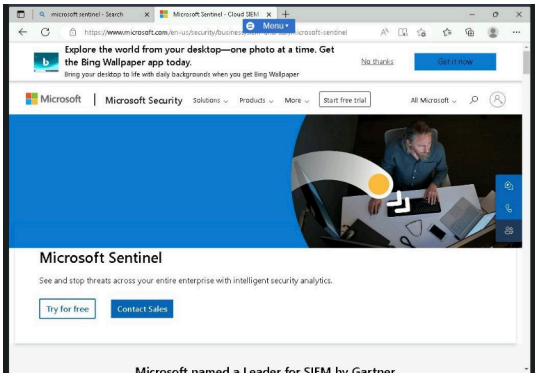
Task 1 - Employ Incident Response using SIEM

The term incident response refers to the steps taken by an organization after a privacy breach or cyberattack. The end objective of incident response is to reduce the damage, minimize recovery time and expenses, and prevent secondary effects like ruined brand reputation. It is essential for businesses to have a well-defined incident response strategy. Employees can go to this plan for clarity and direction on how to proceed when an event happens. It's also a good idea to have training exercises involving the teams, workers, or leaders who oversee the incident response program and carry out each action in the plan.

In this task, I employed incident response using Security Information and Event Management (SIEM).

- I connected to the VM.
- I clicked the Microsoft Edge icon on the taskbar.
- I typed the following into the browsers address bar and press Enter: microsoft sentinel
- I clicked the Microsoft Sentinel | Microsoft Security Solutions link.
- Here you can see Microsoft Sentinel is a feature offered by the Azure cloud.

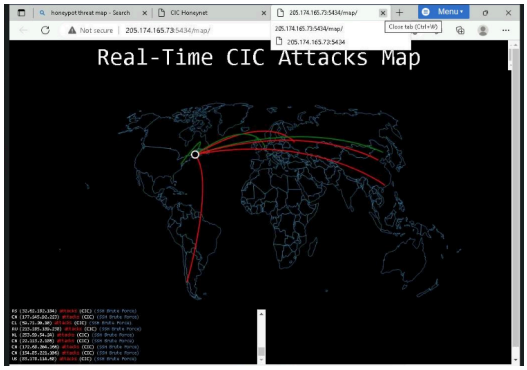
The acronym SIEM stands for "security information and event management," a technology that aids businesses in identifying, analyzing, and responding to security threats before they cause disruptions. A SIEM helps businesses respond quickly to security threats and maintain regulatory compliance by monitoring network activity. Over the past decade, advancements in SIEM technology have enabled faster and more accurate detection of threats and responses to incidents through the use of artificial intelligence. You can get a general idea of pricing per user and other highlights of using this SIEM. Like Microsoft, there are other SIEM options available that can help to analyze the logs and traffic in the network to cut down manual analysis. These are typically going to be paid services, however, due to the heavy investment in time by the program creators. I reviewed the information available on the webpage.



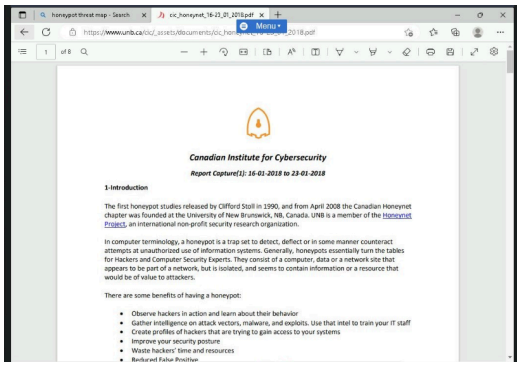
Task 2 - Use a Honeypot Tool

A honeypot is a hardened system connected to a network and is set up as a trick to catch threat actors trying to get into information systems without permission. A honeypot's job is to show up on the internet as a possible target for attackers, usually a server or other high-value asset, collect information, and let defenders know when unauthorized users try to get into the honeypot. Large businesses and companies researching cybersecurity often use Honeypots to find and defend against attacks from advanced persistent threats. To actively defend themselves from attackers, major enterprises often employ honeypots. Honeypots are also useful for cybersecurity researchers who are interested in learning more about the techniques, tools, and procedures used by attackers.

- I connected to the VM, where the Microsoft Edge browser window is open.
- I typed the following into the browser's address bar and pressed Enter: honeypot threat map
- I scrolled down the page and selected the CIC Honeynet search result.
- I scrolled down on the page to see the different clickable items to better help understand real-time attack behavior.
- I clicked REAL-TIME ATTACK MAP.
- A new browser tab opened with a Real-Time CIC Attacks Map. I noticed the attacks on the honeynet being recorded.
- I also noticed the number of attacks that are happening in a minute.
- I closed the tab.



- I clicked BI-WEEKLY REPORTS.
- The page with the reports is shown.
- I clicked the first available one to review and get an idea of the information the report contains.
- The report opened, and you can see information like the timeframe for the report, types of attacks that were performed, statistics about attacking countries and more.
- I reviewed the report.



Canadian Institute for Cybersecurity

Report Capture(1): 16-01-2018 to 23-01-2018

1-Introduction

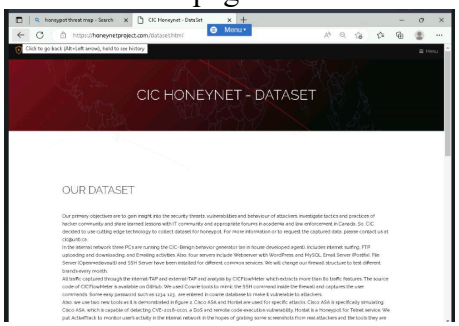
The first honeypot studies released by Clifford Stoll in 1990, and from April 2008 the Canadian Honeynet chapter was founded at the University of New Brunswick, NB, Canada. UNB is a member of the Honeynet Project, an international non-profit security research organization.

In computer terminology, a honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. Generally, honeypots essentially turn the tables for Hackers and Computer Security Experts. They consist of a computer, data or a network site that appears to be part of a network, but is isolated, and seems to contain information or a resource that would be of value to attackers.

There are some benefits of having a honeypot:

- Observe hackers in action and learn about their behavior
- Gather intelligence on attack vectors, malware, and exploits. Use that intel to train your IT staff
- Create profiles of hackers that are trying to gain access to your systems
- Improve your security posture
- Waste hackers' time and resources
- Reduced False Positive

- I clicked the back arrow on the browser window.
- I clicked OUR DATA SET.
- The build of the honeynet is shown, giving us an understanding of the equipment used.
- I reviewed the page and clicked the back arrow on the browser window.



CIC HONEYNET - DATASET

OUR DATASET

- I clicked HONEYPOT SOFTWARE.
- The software that is used in the honeypot is displayed.
- I reviewed the page and clicked the back arrow on the browser window.
- I clicked ATTACKER'S SOFTWARE.
- The software that attackers are using is listed.
- I reviewed the page and close the tab returning to the web search tab.
- I kept the Microsoft Edge browser window open.

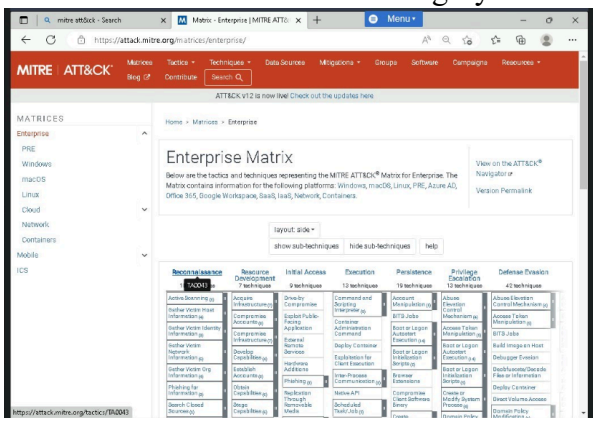
Task 3 - Use MITRE ATT&CK to Identify Tactics, Techniques, and Procedures (TTPs)

Cybersecurity experts use the term "TTPs" to describe the actions, processes, and strategies that a threat actor uses to create threats and launch cyberattacks. Tactics are the attack's main goals and the general plans that the threat actor used to carry out the attack. For instance, the threat actor may want to break into a website to steal PII about customers. Techniques describe how the attacker did the attack, like e-skimming or cross-site scripting (XSS). Procedures refers to creating a step-by-step explanation of how the attack was put together, including the tools and methods used. Most of the time, cybersecurity analysts use the steps of an attack to build an account or signature for a threat actor or threat group. A key part of a security program for information is knowing the TTPs of an attacker. In this task, I used MITRE ATT&CK to identify TTPs.

- In Microsoft Edge, I typed the following into the browser search box and pressed Enter: mitre att&ck
- I clicked the MITRE ATT&CK search result link.

The MITRE ATT&CK page is a repository of data detailing the methods and techniques that advanced persistent threat organizations have employed in actual intrusions. ATT&CK stands for Adversarial Tactics, Techniques, and Common Knowledge, and is a compilation of in-depth accounts of these threat actors' observed tactics, techniques, and procedures.

- I clicked Matrices on the upper menu pane of the webpage.
- The Enterprise Matrix page is displayed.
- There are several categories listed below that break down into subcategories.
- I clicked the Reconnaissance category.

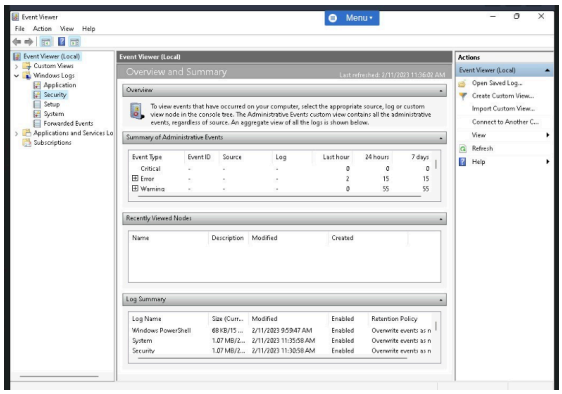


- Here, you can see a breakdown of techniques used in the reconnaissance phase.
- I clicked Active Scanning under the Techniques section.
- I reviewed the page discussing what active scanning is, how to detect it, and how to mitigate it.
- When I finished reviewing, I clicked Tactics and then selected Enterprise from the drop-down menu.
- I reviewed the options available and clicked Privilege Escalation.
- There are 13 Techniques listed with subcategories in each.
- I reviewed the option and clicked Abuse Elevation Control Mechanism at the top of the page.
- Here you can see mitigation recommendations and how to detect the act.
- You can view the depth this site offers to help understand how attackers attack and how organizations can protect themselves.
- I closed the browser window.

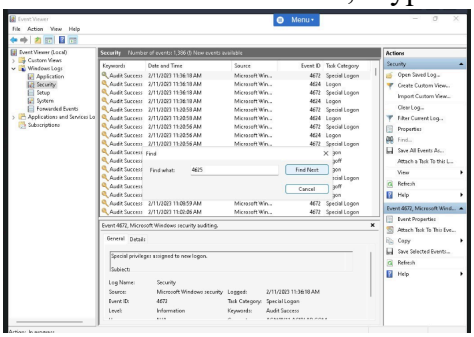
Task 4 - Access and Research Logs using Windows Event Viewer

Event Viewer logs, firewall logs, IDS logs, and protocol analyzers are a great way to look for unwanted activities. In this task, I accessed the Windows Event Viewer and searched for common Event IDs to be on the lookout for.

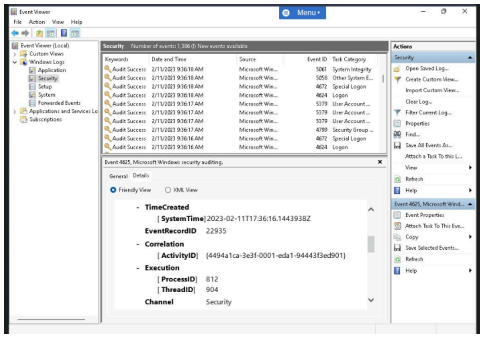
- I connected to the VM.
- I right clicked the Windows Start Charm and selected Event Viewer.
- In the Event Viewer window, I expanded the Windows Logs section and select Security.



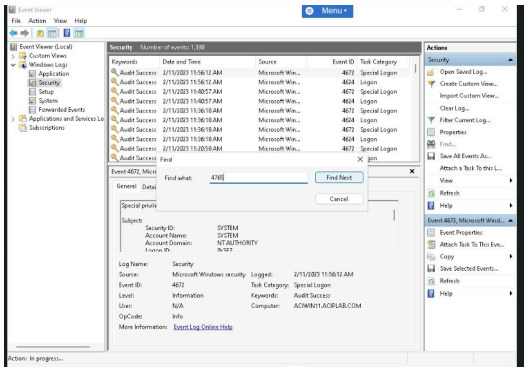
- In the Security tab, you can look for potential threats to security events like authentication.
- In the Actions pane, I clicked Find.
- In the Find window, I typed the following and clicked Find Next: 4625



- The results are displayed at the bottom of the page.
- I closed the Find pop-up window.
- I clicked Details and expanded any hidden information by clicking the + next to each category.
- The information displayed describes the event.
- The date & time the logon attempt failed, the computer used, the user account used, the logon type, and why the login failed.
- Many attempts and failures of logons can be an indication of brute force and dictionary attacks.



- In the Actions window, I clicked Find.
- In the Find pop-up window, I typed the following and clicked Find Next: 4765



- Event ID 4765 is for SID History being added to an account.
- This can be an indicator of privilege abuse and malicious activity.
- The search looks through the log and returns no events.
- I clicked OK on the EventViewer pop-up window.
- This same search process can be used for other Event IDs.
- Note: You can research the different types of Event IDs that are available on the Microsoft website.

Scripting and third-party monitoring tools can alert analysts to these events occurring and cut down on some of the false positives that may occur.
Close the Find pop-up window.

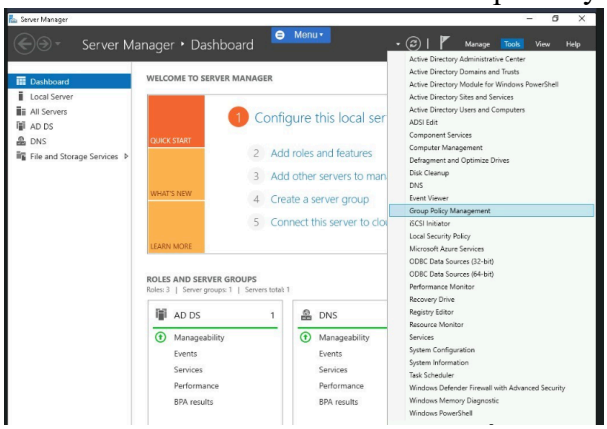
- I closed the Event Viewer window.

Task 5 - Enable Firewall Logging

Insight into network activity may be gained by reviewing firewall logs. You can watch your firewall's activities, verify the effectiveness of rules, and investigate any security breaches. This feature is not enabled automatically and will need to be turned on.

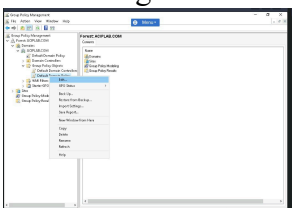
In this task, I accessed the domain group policy to turn on firewall logging.

- I connected to the VM.
- The Server Manager > Dashboard window is displayed.
- I clicked Tools and then selected Group Policy Management.

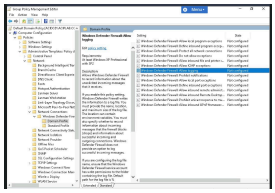


- In the Group Policy Management window, I expanded the following path: Forest:ACIPLAB.COM > Domains > Group Policy Objects.

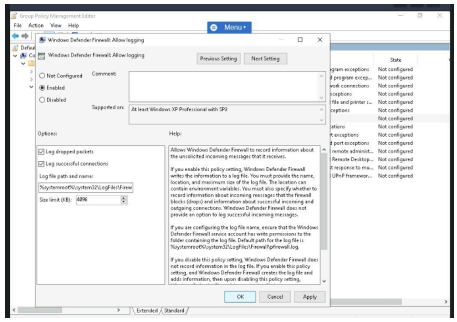
- I right-clicked Default Domain Policy and selected Edit.



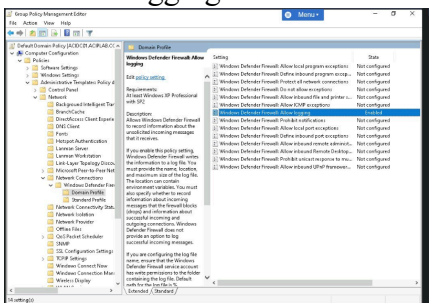
- The Group Policy Management Editor is opened for the Domains Default Policy.
- I expanded the following path: Computer Configuration > Policies > Administrative Templates > Network > Network Connections > Windows Firewall
- I selected Domain Profile.
- I double-clicked on Windows Defender Firewall: Allow Logging on the right pane.



- In the Windows Defender Firewall: Allow Logging window, I selected the Enabled option.
- I ticked the Log dropped packets and Log successful connections checkboxes under the Options section.
- There are additional options that can be configured below.
- I reviewed the Help pane to learn more about log locations and other information pertaining to this action.



- I clicked OK.
- I noticed logging has now been enabled for the Domain.



- I closed the Group Policy Management Editor window.
- I also closed the Group Policy Management window.