**Threat Intelligence Tools**

**Introduction**

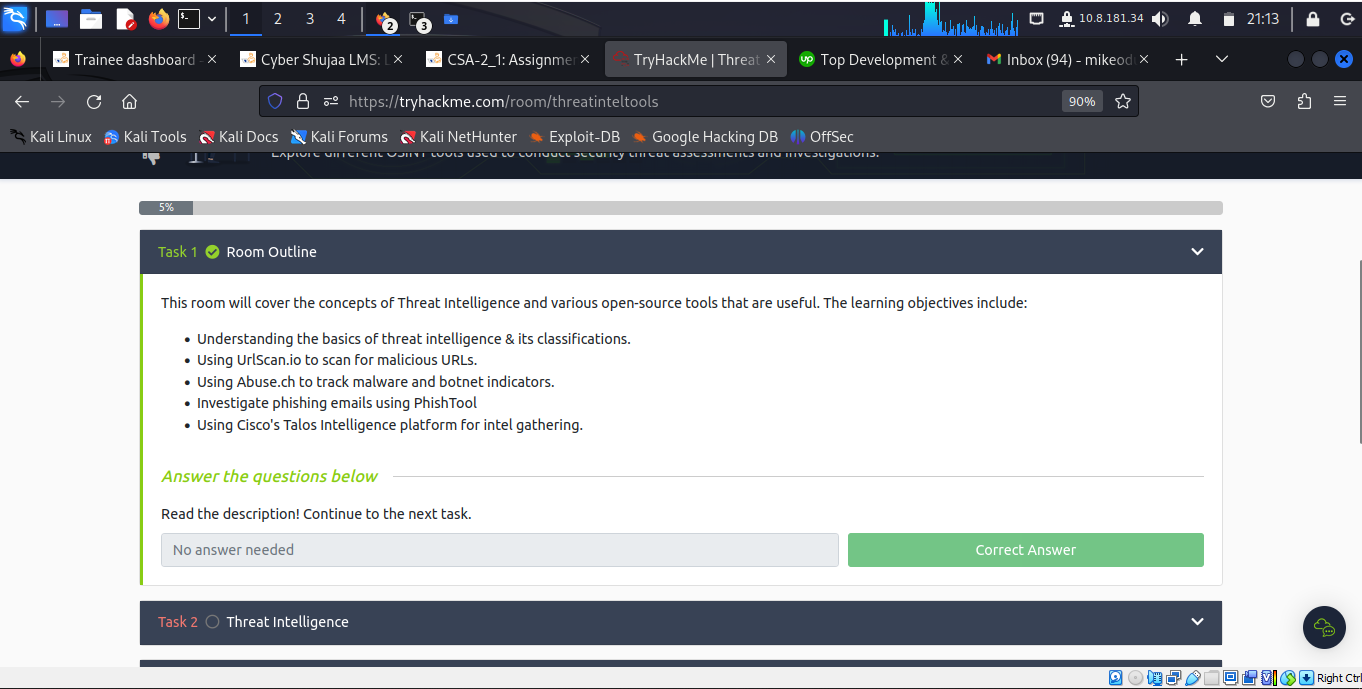
This task introduces the learner to the practical knowledge over the concepts of Threat Intelligence and various open-source tools that are useful. The learning objectives are:

* Understanding the basics of threat intelligence & its classifications.
* Using UrlScan.io to scan for malicious URLs.
* Using Abuse.ch to track malware and botnet indicators.
* Investigate phishing emails using PhishTool
* Using Cisco's Talos Intelligence platform for intel gathering.

***Activities***

***Task 1: Room Outline***

This section outlines objectives such as the understanding of building blocks of threat intelligence and the respective classifications.



***Task 2: Threat Intelligence***

Threat intelligence refers to the analysis of data and information using tools and techniques to generate meaningful patterns on how to mitigate against potential risks associated with existing or emerging threats targeting organizations, industries, sectors or governments.

The learner understands now about risk mitigation and can start by trying to answer the following:

* Who's attacking you?
* What's their motivation?
* What are their capabilities?
* What artefacts and indicators of compromise should you look out for?

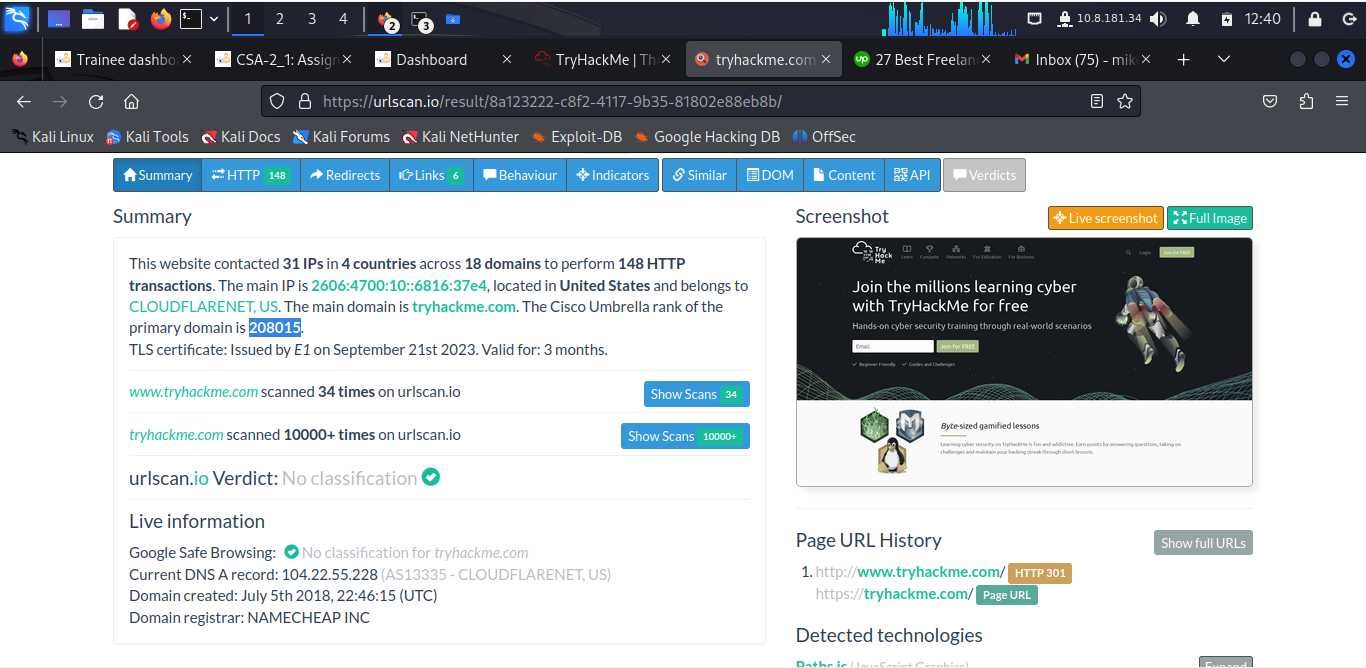
***Threat Intelligence Classifications:***

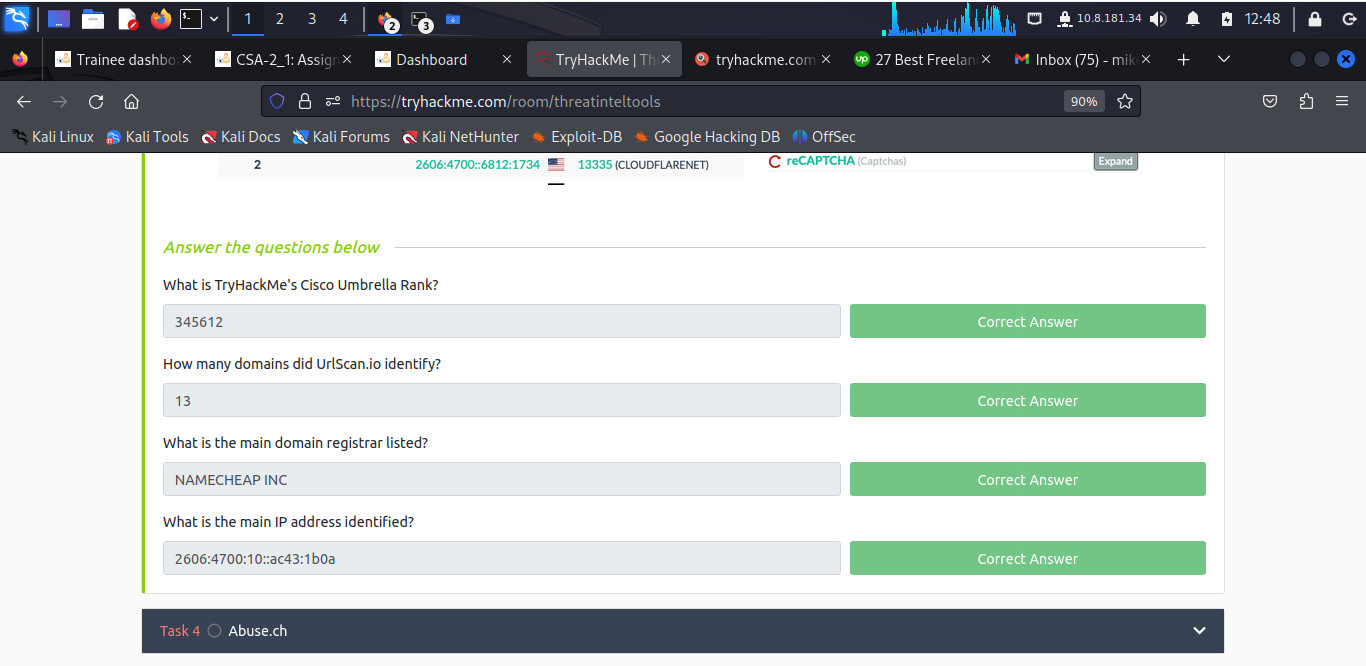
Threat Intel is geared towards understanding the relationship between an operational environment and the adversary. The learner can break down threat intel into the following classifications:

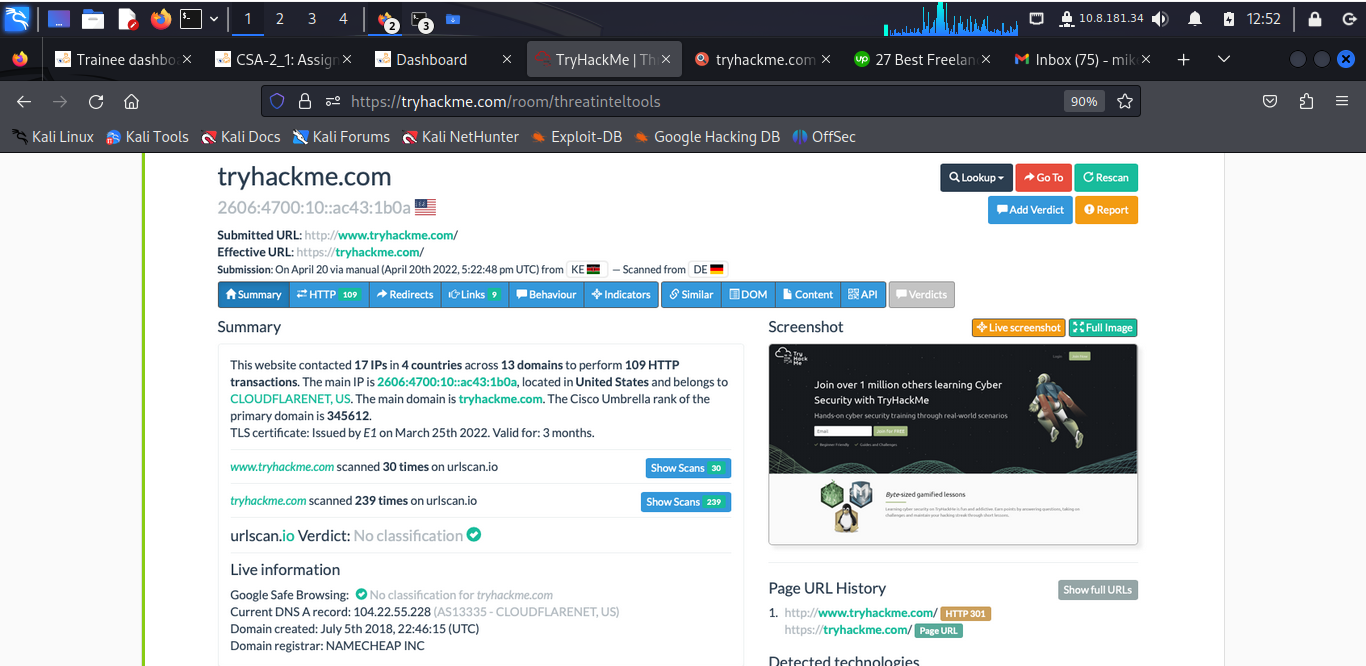
* **Strategic Intel:** High-level intel that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.
* **Technical Intel:** Looks into evidence and artefacts of attack used by an adversary. Incident Response teams can use this intel to create a baseline attack surface to analyse and develop defence mechanisms.
* **Tactical Intel:** Assesses adversaries' tactics, techniques, and procedures (TTPs). This intel can strengthen security controls and address vulnerabilities through real-time investigations.
* **Operational Intel:** Looks into an adversary's specific motives and intent to perform an attack. Security teams may use this intel to understand the critical assets available in the organisation (people, processes, and technologies) that may be targeted.

***Task 3: UrlScan.io***

The learner dives deeper into learning [**Urlscan.io**](https://urlscan.io) which is a free service developed to assist in scanning and analyzing websites. It is used to automate the process of browsing and crawling through websites to record activities and interactions.







***Task 4: Abuse.ch***

This is a tool developed to identify and track malware and botnets through several operational platforms. It’s a research project hosted by the Institue for Cybersecurity and Engineering at the Bern University of Applied Sciences in Switzerland.

The platforms developed under Abuse.ch are:

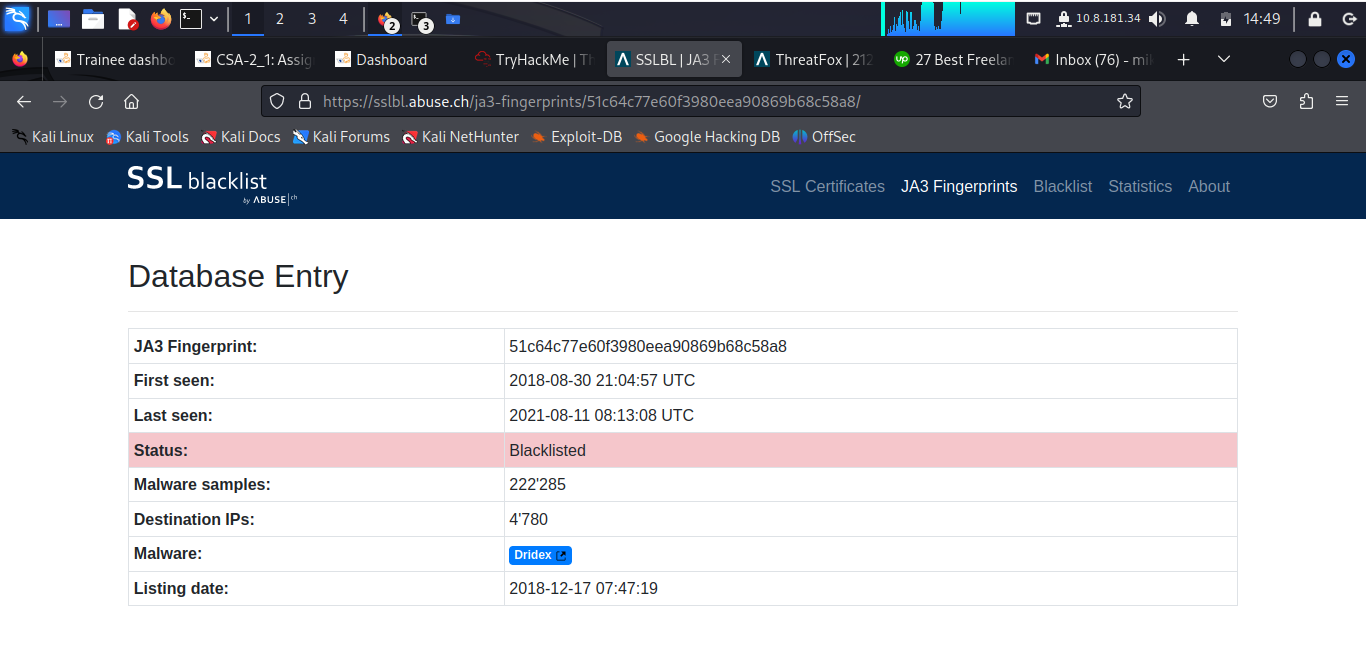
**Malware Bazaar:**  A resource for sharing malware samples.

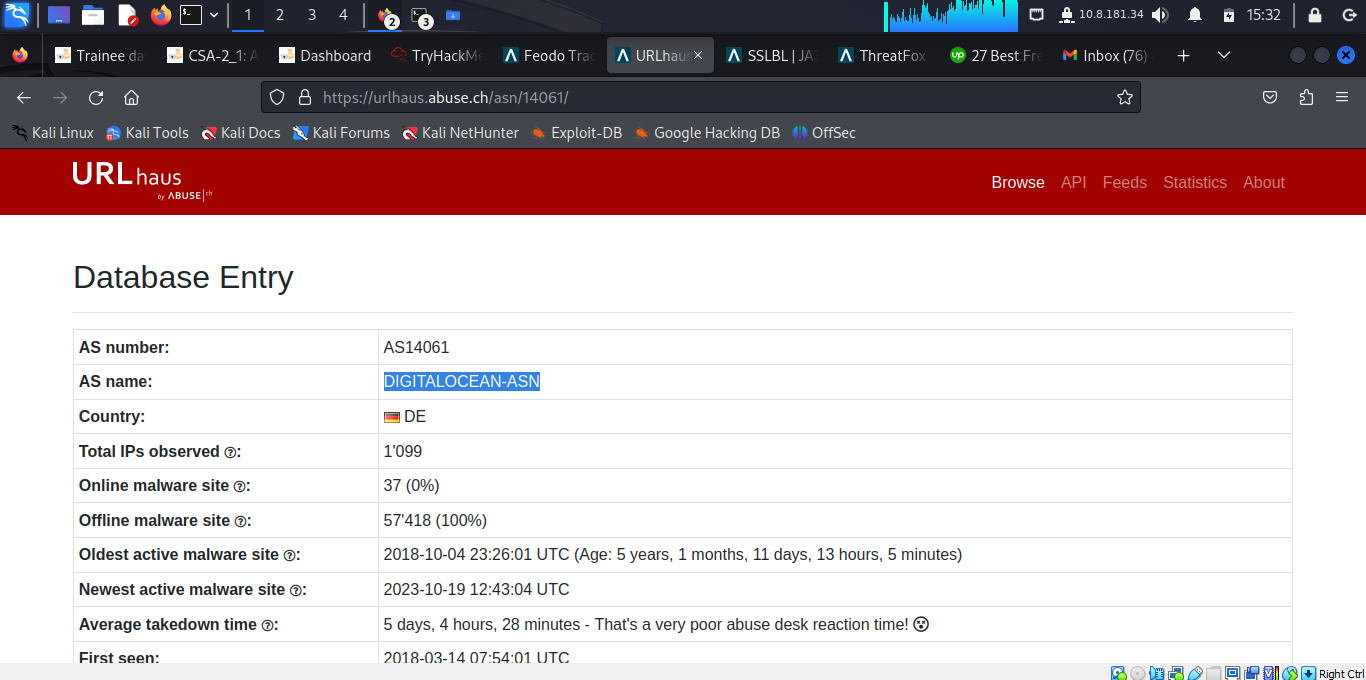
**Feodo Tracker:**  A resource used to track botnet command and control (C2) infrastructure linked with Emotet, Dridex and TrickBot.

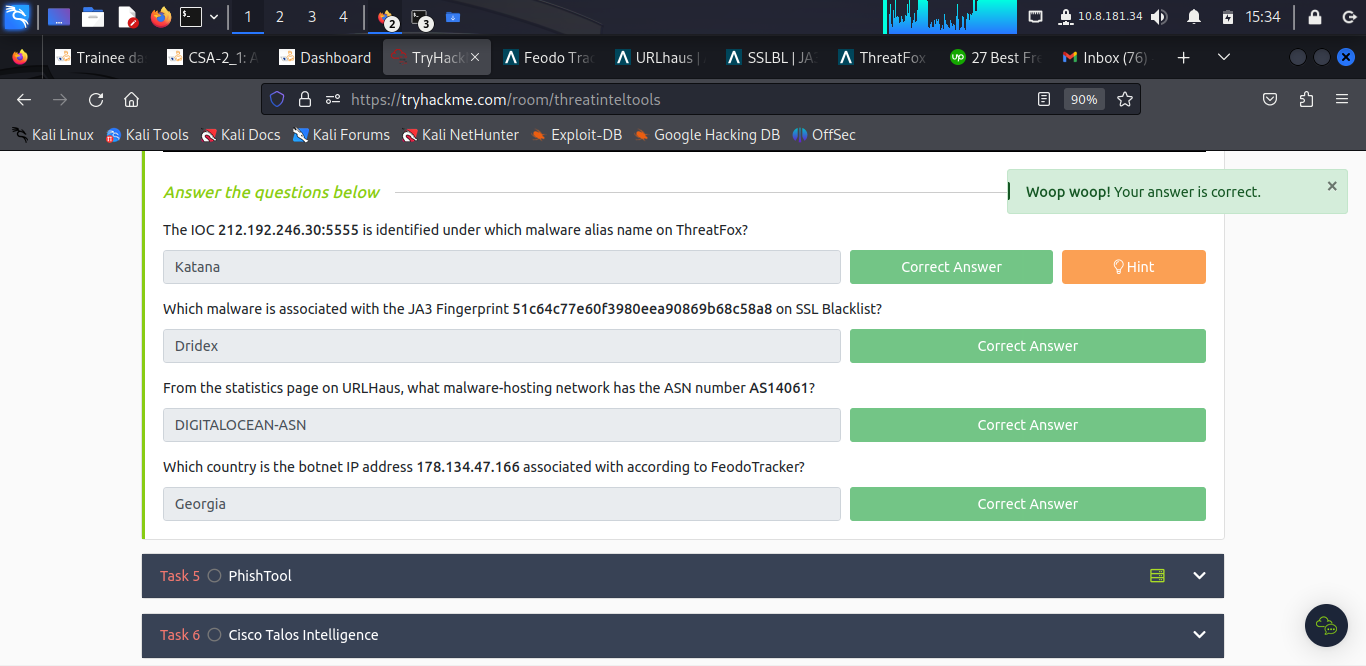
**SSL Blacklist:**  A resource for collecting and providing a blocklist for malicious SSL certificates and JA3/JA3s fingerprints.

**URL Haus:**  A resource for sharing malware distribution sites.

**Threat Fox:**  A resource for sharing indicators of compromise (IOCs).



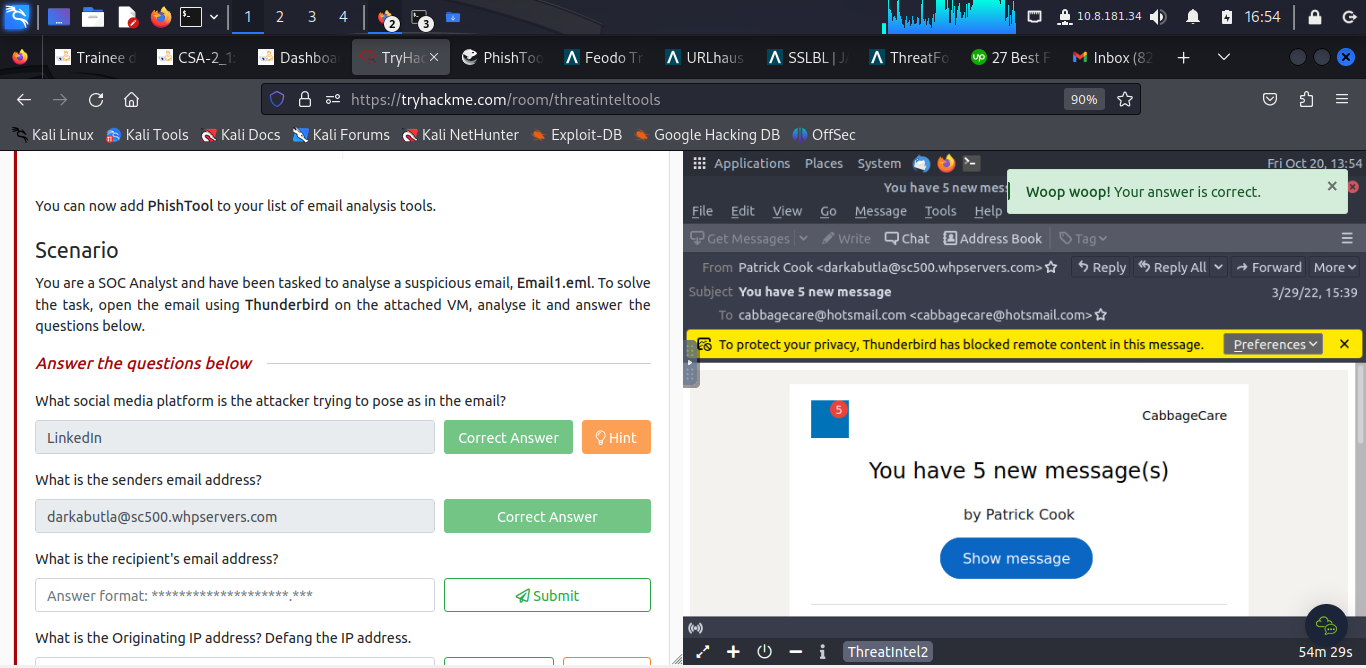


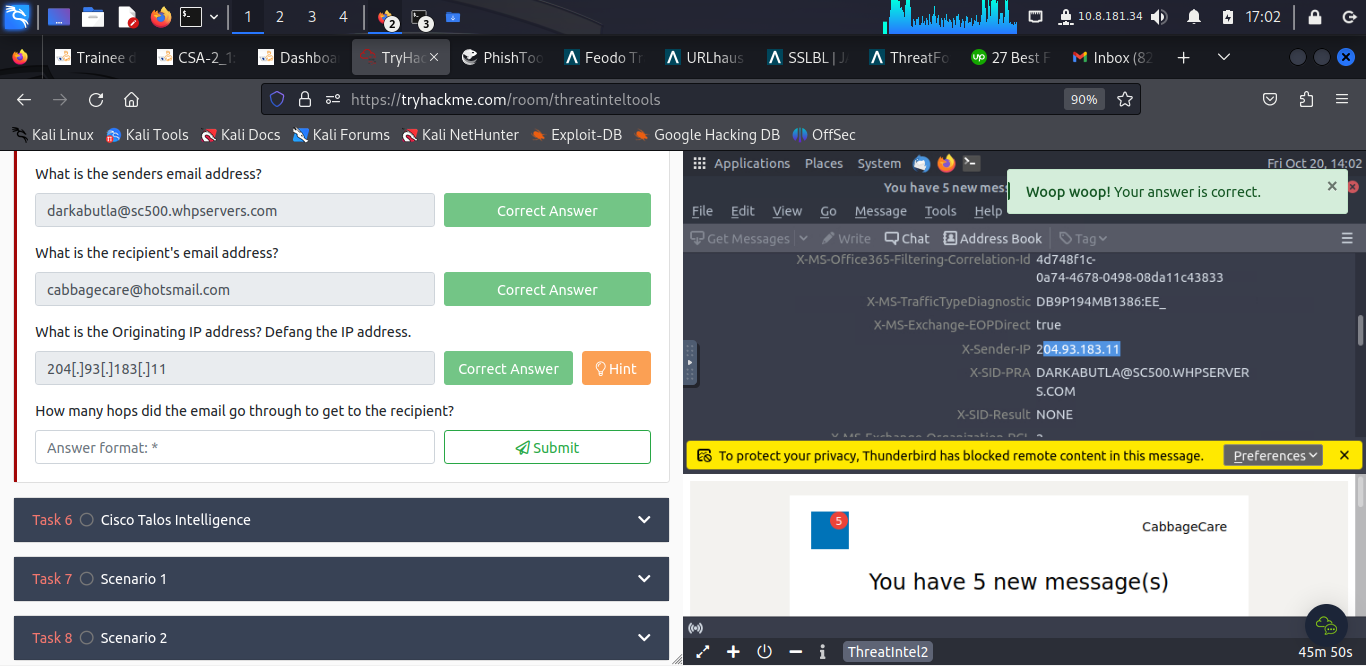


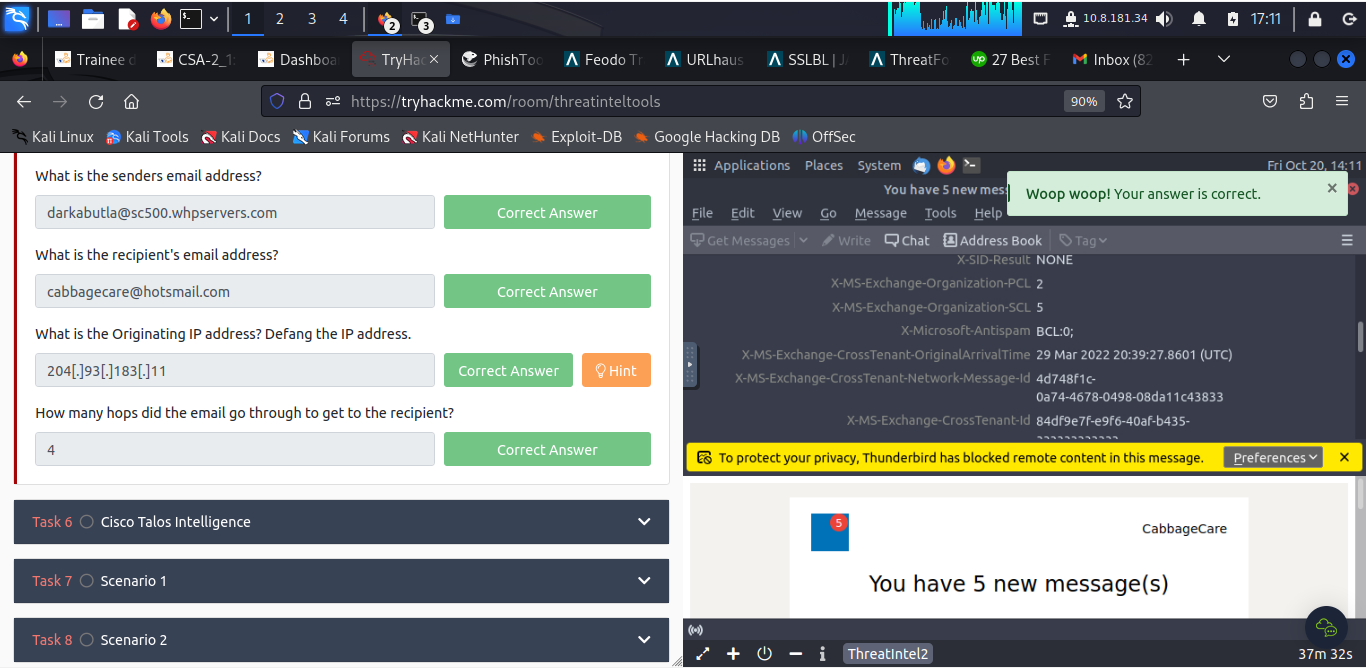
***Task 5: PhishTool***

The learner is introduced to phishing tool – **PhishTool** a toolkit for email analysis. Email phishing is one of the main precursors of any cyber attack. Unsuspecting users get duped into opening and accessing malicious files and links sent to them by email, as they appear to be legitimate. As a result, adversaries infect their victims’ systems with malware, harvesting their credentials and personal data and performing other actions such as financial fraud or conducting ransomware attacks.

[PhishTool](https://www.phishtool.com) seeks to elevate the perception of phishing as a severe form of attack and provide a responsive means of email security. Through email analysis, security analysts can uncover email IOCs, prevent breaches and provide forensic reports that could be used in phishing containment and training engagements.





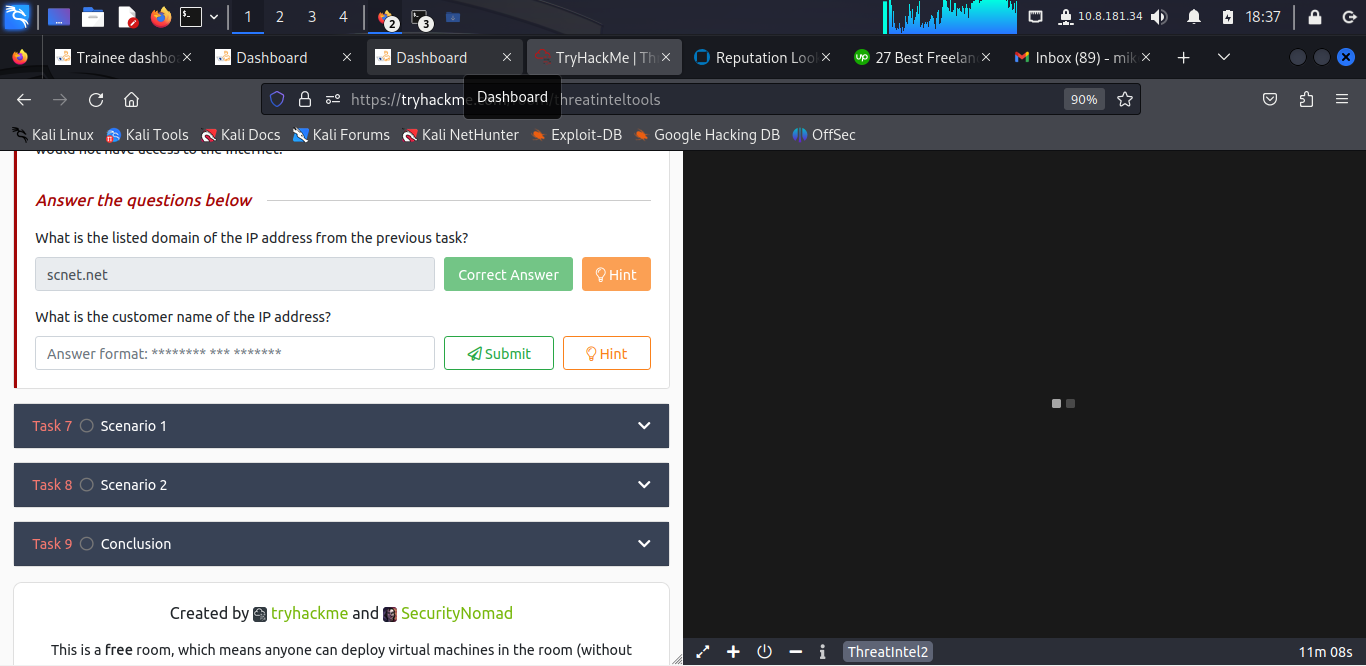


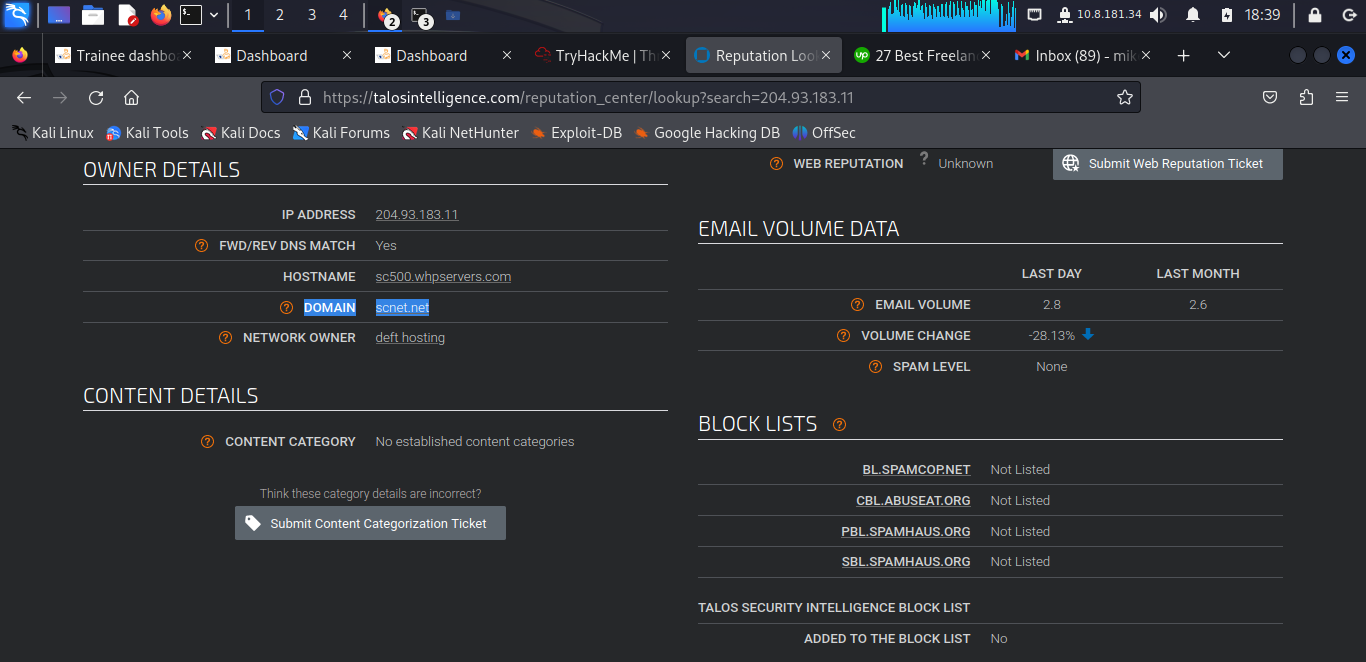
***Task 6:***  ***Cisco Talos Intelligence Tool***

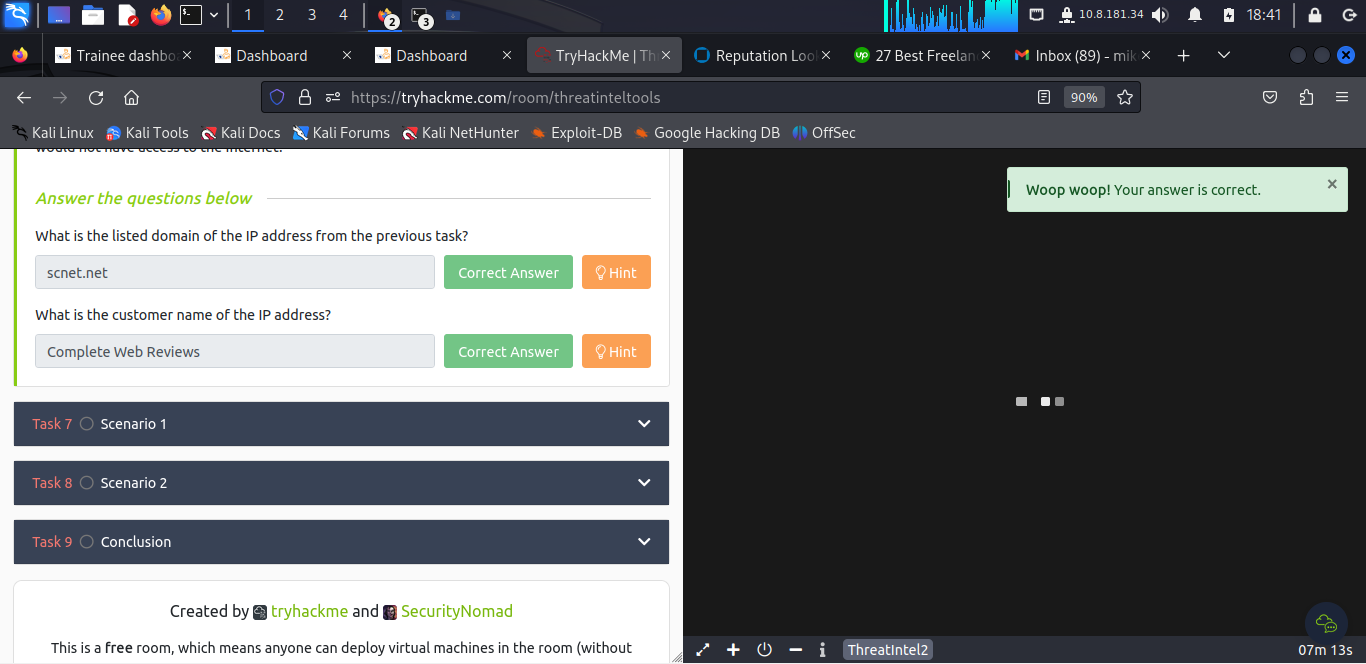
Cisco Talos is a team of security practitioners from Cisco that provide actionable intelligence, visibility on indicators, and protection against emerging threats through data collected from ***Talos Intelligence***.

In this task the learner interacts with Talos Dashboard to conduct email traffic across the world.

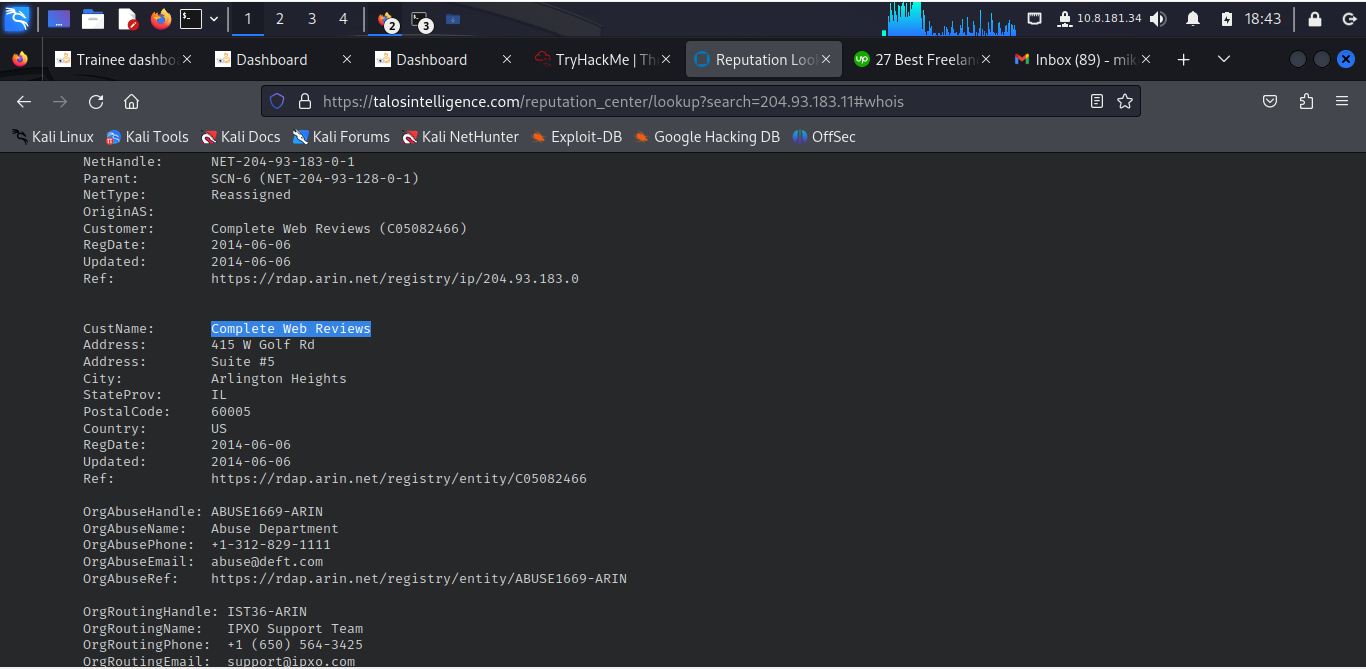
The questions – listed domain of IP and customer name of IP address were answered successfully by learner.





Customer name of the IP address is ***Complete Web Reviews.*** 

From Talos Dashboarding tool:



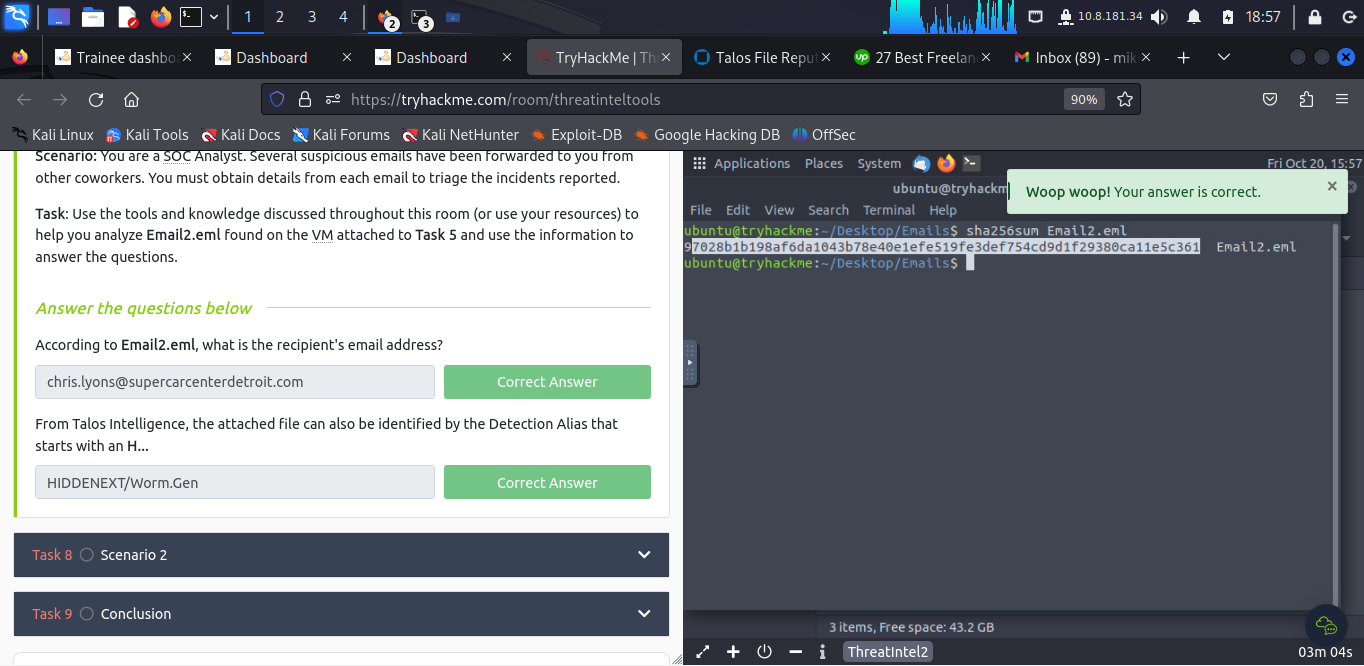
The learner used Cisco Talos Intelligence to answer questions from files provided in Task 5.

***Task 7:***  ***Scenario 1***

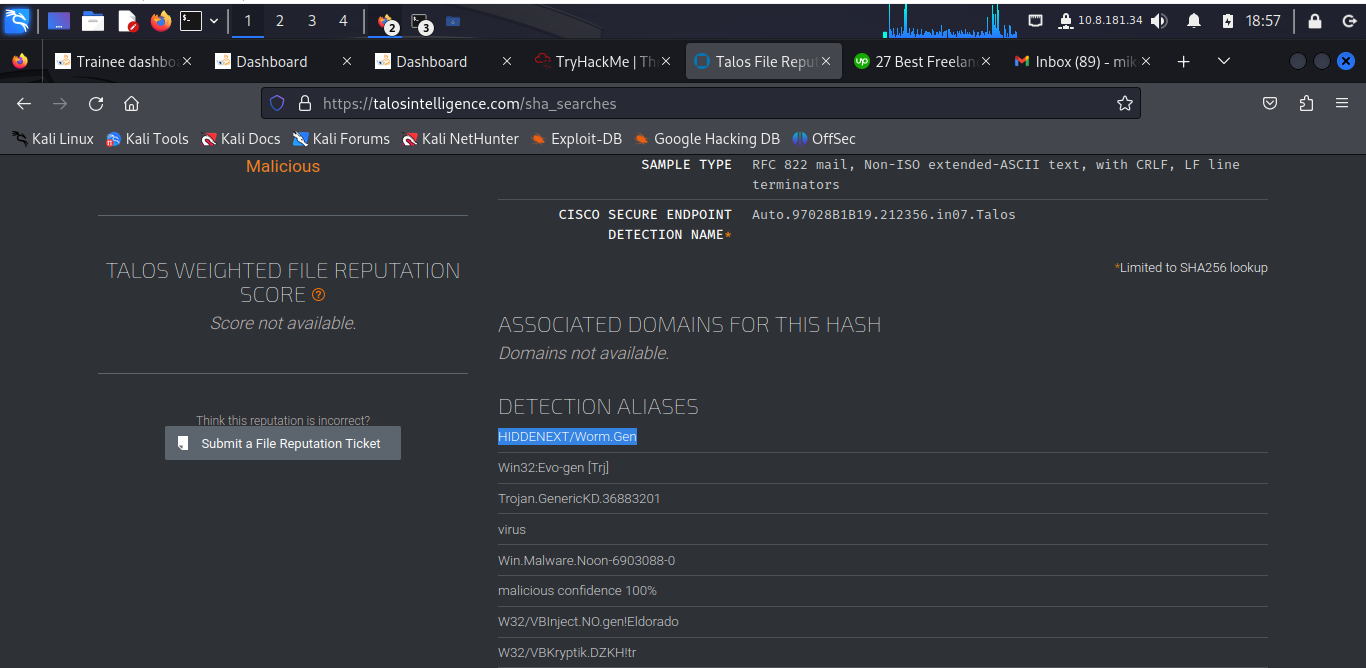
The learner - as SOC Analyst, the case is: there is suspicious emails forwarded from other coworkers. The learner must obtain details from each email to triage the incidents reported.

**Task**: Use the tools and knowledge discussed throughout this room (or use your resources) to aid analyze **Email2.eml**found on the VM attached to **Task 5** and use the information to answer the questions.

***Solution(s)***



On Talos File Reputation to Detect the alias.



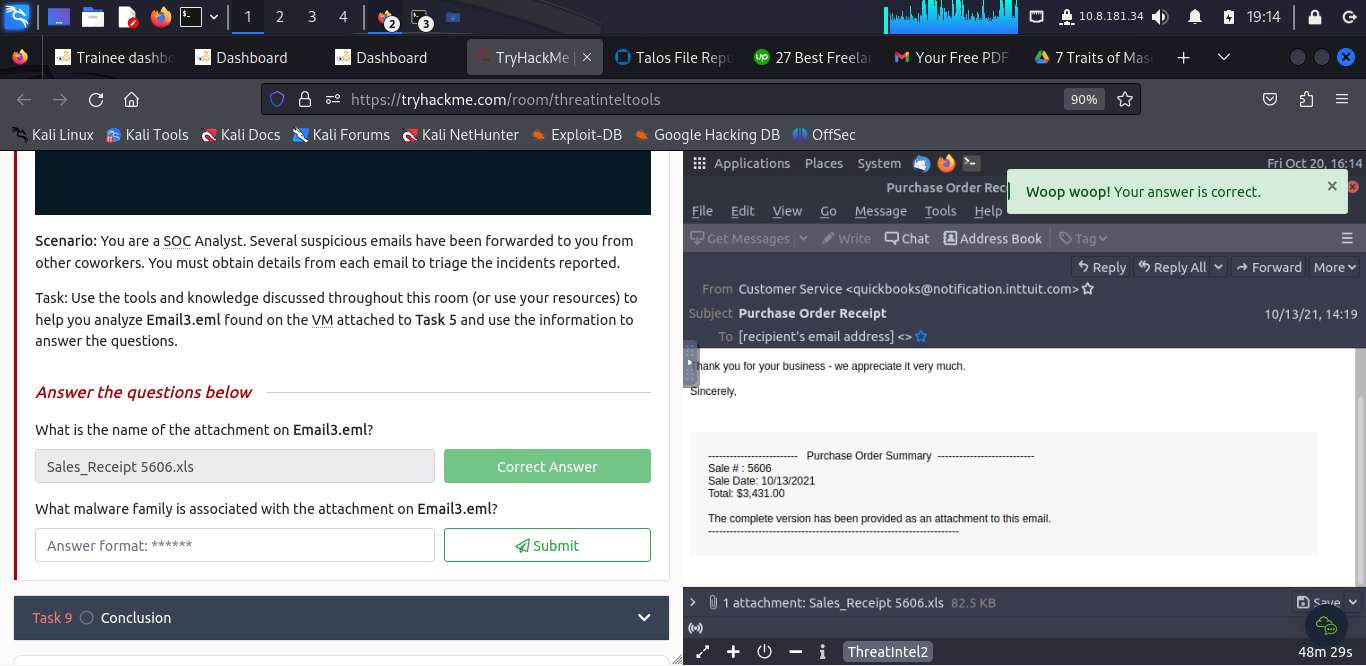
***Task 8:***  ***Scenario 2***

The learner – as SOC Analyst. Suspicious emails have been forwarded to you from other coworkers. You must obtain details from each email to triage the incidents reported.

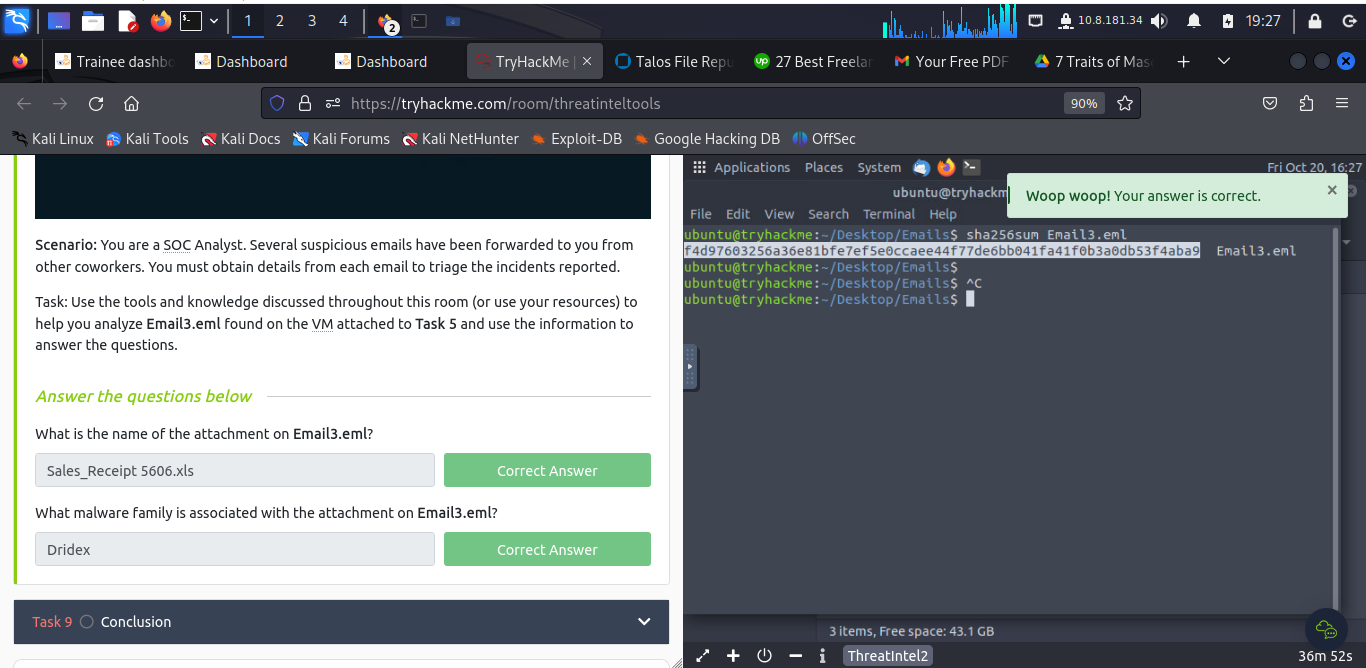
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze **Email3.eml**found on the VM attached to **Task 5** and use the information to answer the questions.

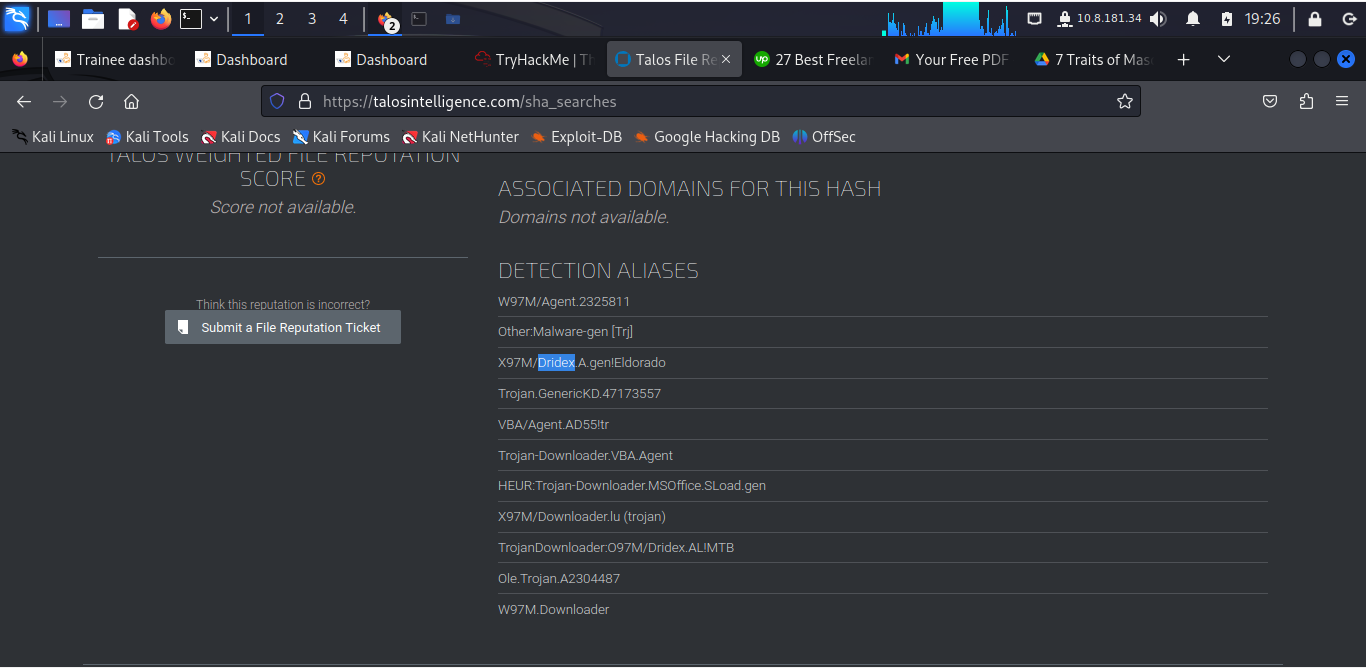
***Solution(s)***

The first question to the learner is answer correctly the name of the file attachment in email: ***Sales\_Receipt 5606.xls***



The second question to the learner is answer correctly the malware family is associated with the attachment on Email3.eml: ***Dridex***





This was about using Cisco’s Talo Intelligence tool as a Security Analyst to find or obtain details needed for analysis from emails.

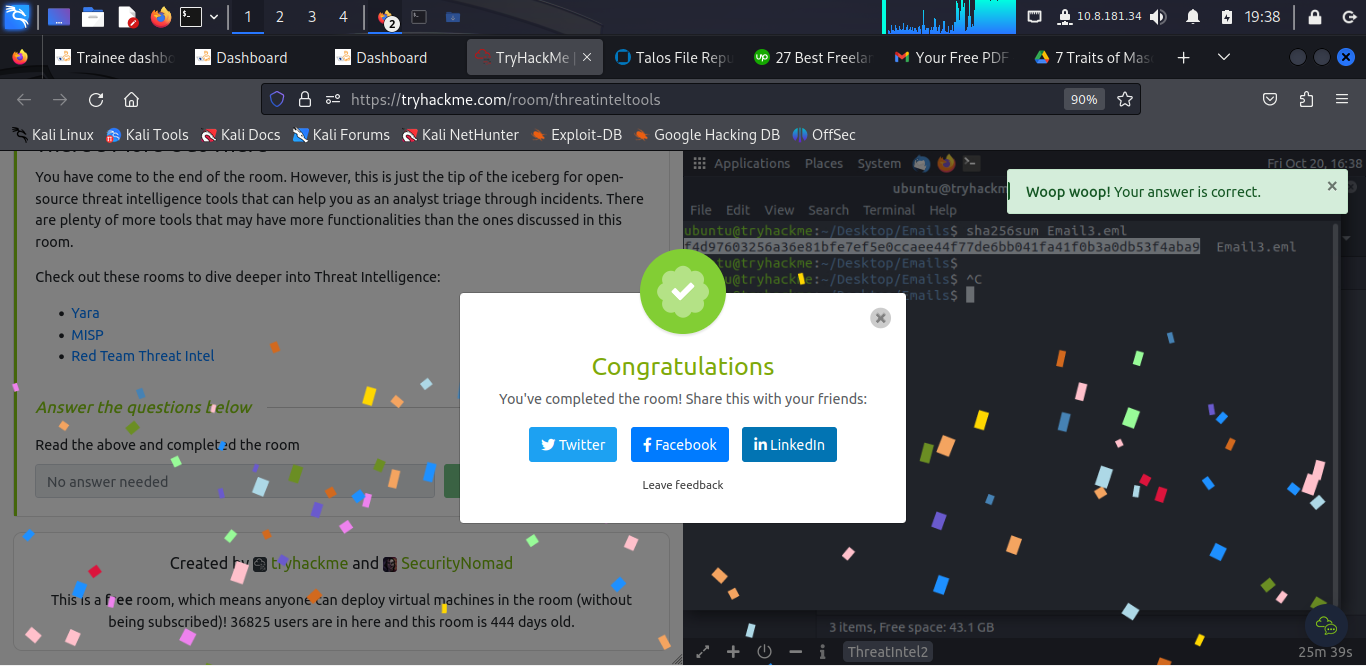
***Task 9:***  ***Conclusion***

As the learner comes to completion on the open source threat intelligence tools that can help them as an analyst triage through incidents. There are plenty of more tools that may have more functionalities like [Yara](https://tryhackme.com/room/yara), [MISP](https://tryhackme.com/room/misp) and [Red Team Threat Intel](https://tryhackme.com/room/redteamthreatintel)

**Conclusion**

The learner was able to walk through both theoretical and practical part of Threat Intelligence Tools like ***PhishTool, Cisco Talo Intelligence, Abuse.ch*** etc., this tools are key to the learner as an aspiring Security Analyst.

The learner was able to understand the basics of threat intelligence & its classifications and used ***UrlScan.io*** to scan for malicious URLs.



**Completion Link:** <https://tryhackme.com/room/threatinteltools>