Threat Intelligence Tools

Introduction

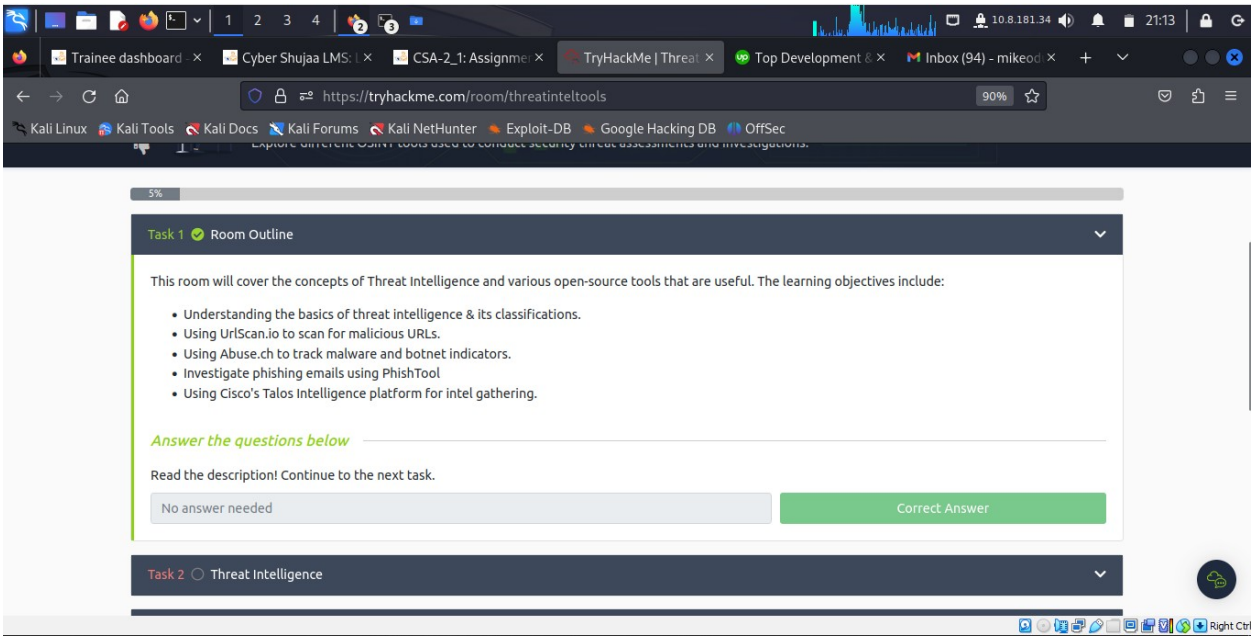
This task introduces the learner to the practical knowledge over the concepts of Threat Intelligence and various open-source tools that are useful. The learning objectives are:

- 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?

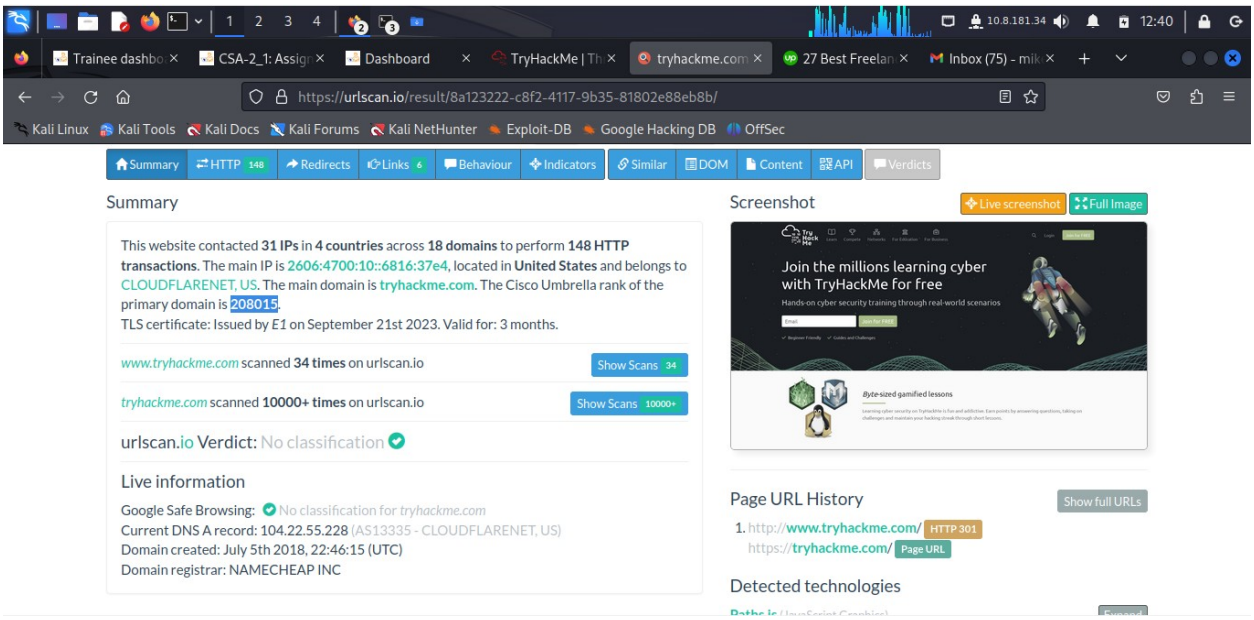
Threat Intelligence Classifications:

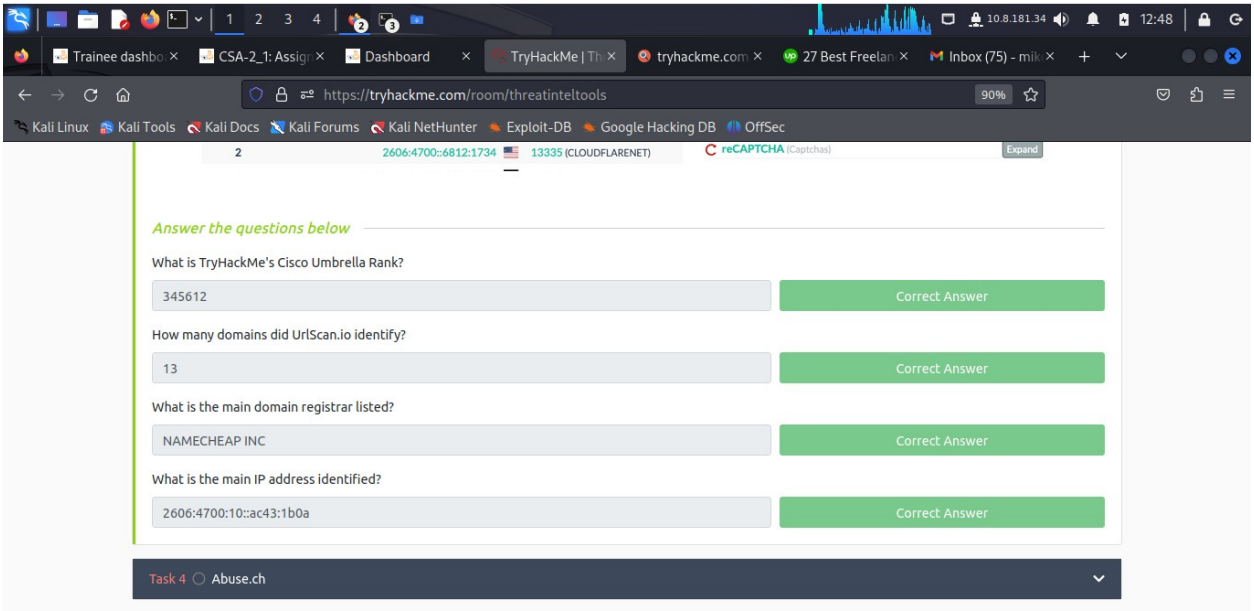
Threat Intel is geared towards understanding the relationship between an operational environment and the adversary. The learner can break down threat intel into the following classifications:

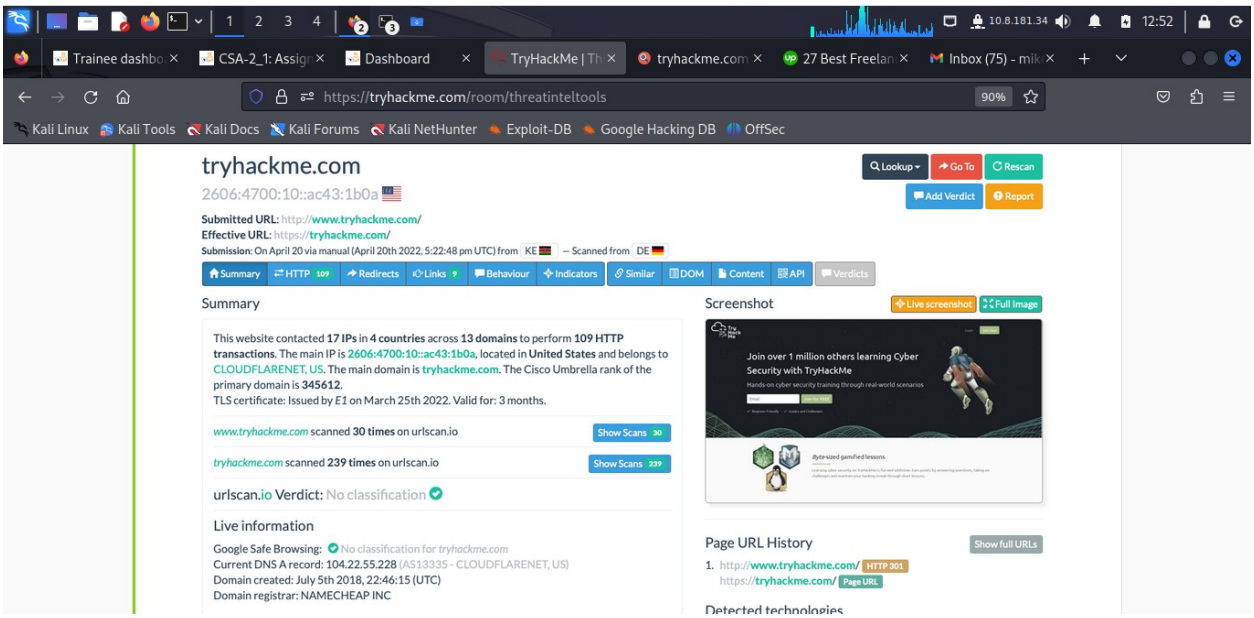
- **Strategic Intel:** High-level intel that looks into the organisation's threat landscape and maps out the risk areas based on trends, patterns and emerging threats that may impact business decisions.
- **Technical Intel:** Looks into evidence and artefacts of attack used by an adversary. Incident 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** 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.


https://urlscan.io/result/8a123222-c8f2-4117-9b35-81802e88eb8b/
Summary
HTTP 148
Redirects
Links 6
Behaviour
Indicators
Similar
DOM
Content
API
Verdicts
Summary
This website contacted 31 IPs in 4 countries across 18 domains to perform 148 HTTP transactions. The main IP is 2606:4700:10::6816:37e4, located in United States and belongs to CLOUDFLARENET, US. The main domain is tryhackme.com. The Cisco Umbrella rank of the primary domain is 208015.
TLS certificate: Issued by E1 on September 21st 2023. Valid for: 3 months.
www.tryhackme.com scanned 34 times on urlscan.io
Show Scans 34
tryhackme.com scanned 10000+ times on urlscan.io
Show Scans 10000+
urlscan.io Verdict: No classification
Live information
Google Safe Browsing: No classification for tryhackme.com
Current DNS A record: 104.22.55.228 (AS13335 - CLOUDFLARENET, US)
Domain created: July 5th 2018, 22:46:15 (UTC)
Domain registrar: NAMECHEAP INC
Screenshot
Live screenshot
Full Image
Join the millions learning cyber with TryHackMe for free
Hands-on cyber security training through real-world scenarios
Page URL History
Show full URLs
1. http://www.tryhackme.com/ HTTP 301
https://tryhackme.com/ Page URL
Detected technologies


https://tryhackme.com/room/threatinteltools
2606:4700::6812:1734
13335 (CLOUDFLARENET)
reCAPTCHA (Captchas)
Expand
Answer the questions below
What is TryHackMe's Cisco Umbrella Rank?
345612
Correct Answer
How many domains did UrlScan.io identify?
13
Correct Answer
What is the main domain registrar listed?
NAMECHEAP INC
Correct Answer
What is the main IP address identified?
2606:4700:10::ac43:1b0a
Correct Answer
Task 4 Abuse.ch



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:

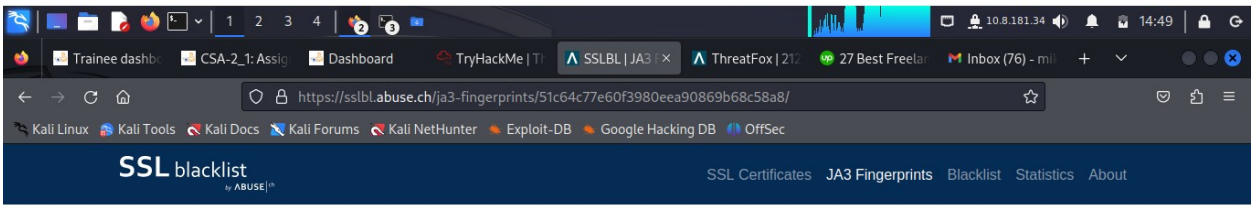
Malware Bazaar: A resource for sharing malware samples.

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.

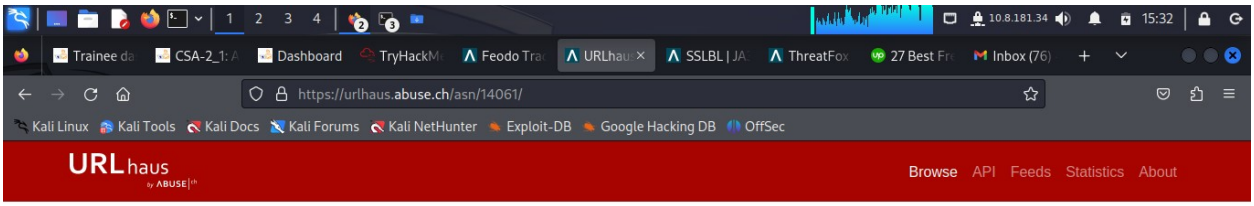
URL Haus: A resource for sharing malware distribution sites.

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



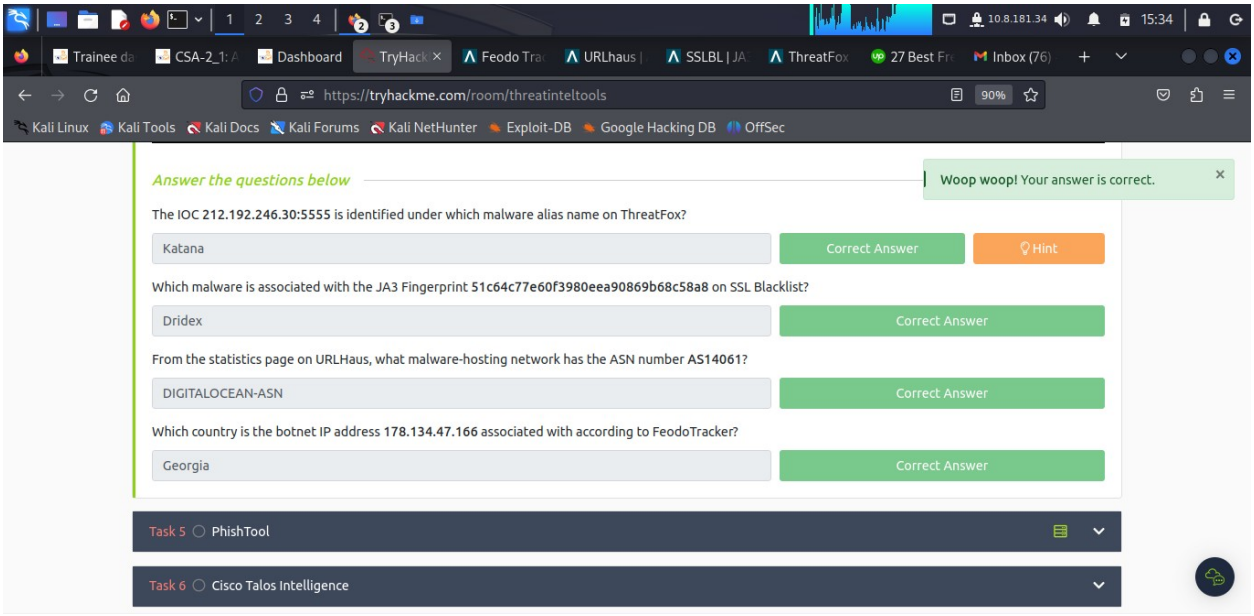
Database Entry

JA3 Fingerprint:	51c64c77e60f3980eea90869b68c58a8
First seen:	2018-08-30 21:04:57 UTC
Last seen:	2021-08-11 08:13:08 UTC
Status:	Blacklisted
Malware samples:	222'285
Destination IPs:	4'780
Malware:	Dridex
Listing date:	2018-12-17 07:47:19



Database Entry

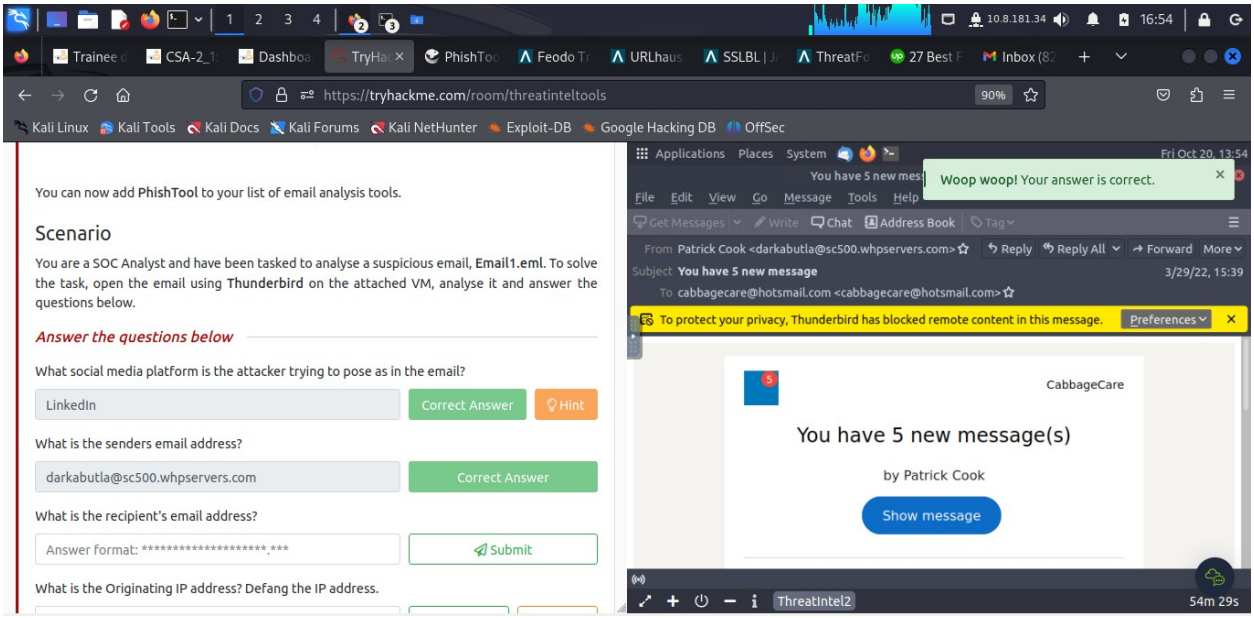
AS number:	AS14061
AS name:	DIGITALOCEAN-ASN
Country:	DE
Total IPs observed ⓘ:	1'099
Online malware site ⓘ:	37 (0%)
Offline malware site ⓘ:	57'418 (100%)
Oldest active malware site ⓘ:	2018-10-04 23:26:01 UTC (Age: 5 years, 1 months, 11 days, 13 hours, 5 minutes)
Newest active malware site ⓘ:	2023-10-19 12:43:04 UTC
Average takedown time ⓘ:	5 days, 4 hours, 28 minutes - That's a very poor abuse desk reaction time! 😵
First seen:	2018-03-14 07:54:01 UTC

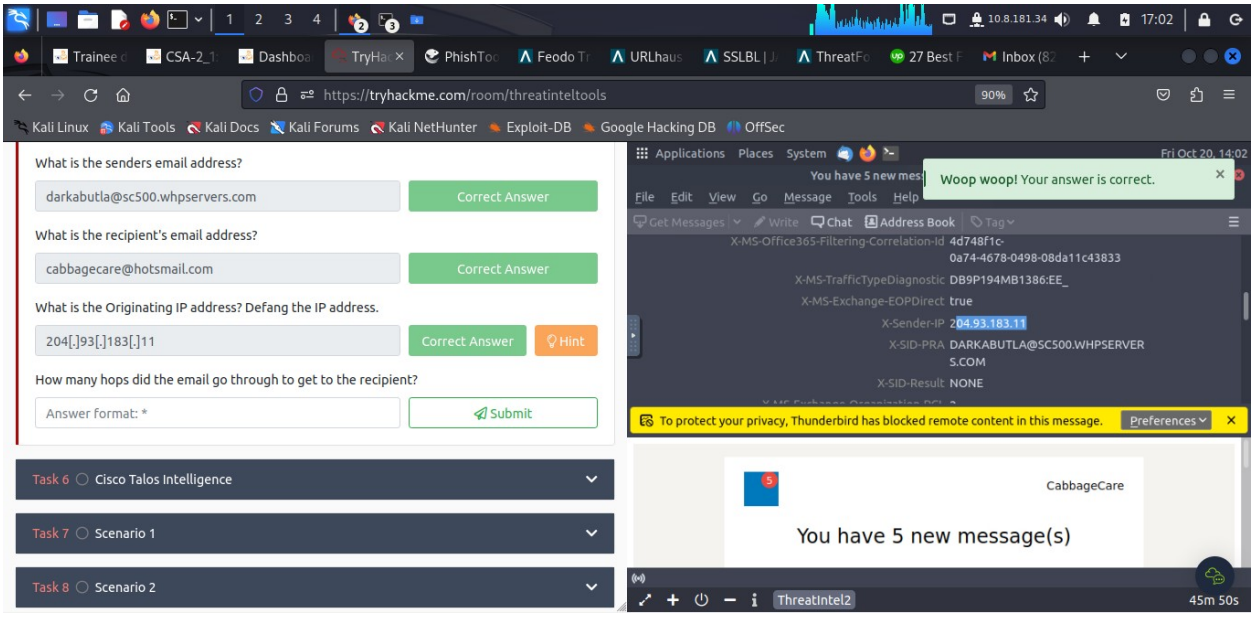


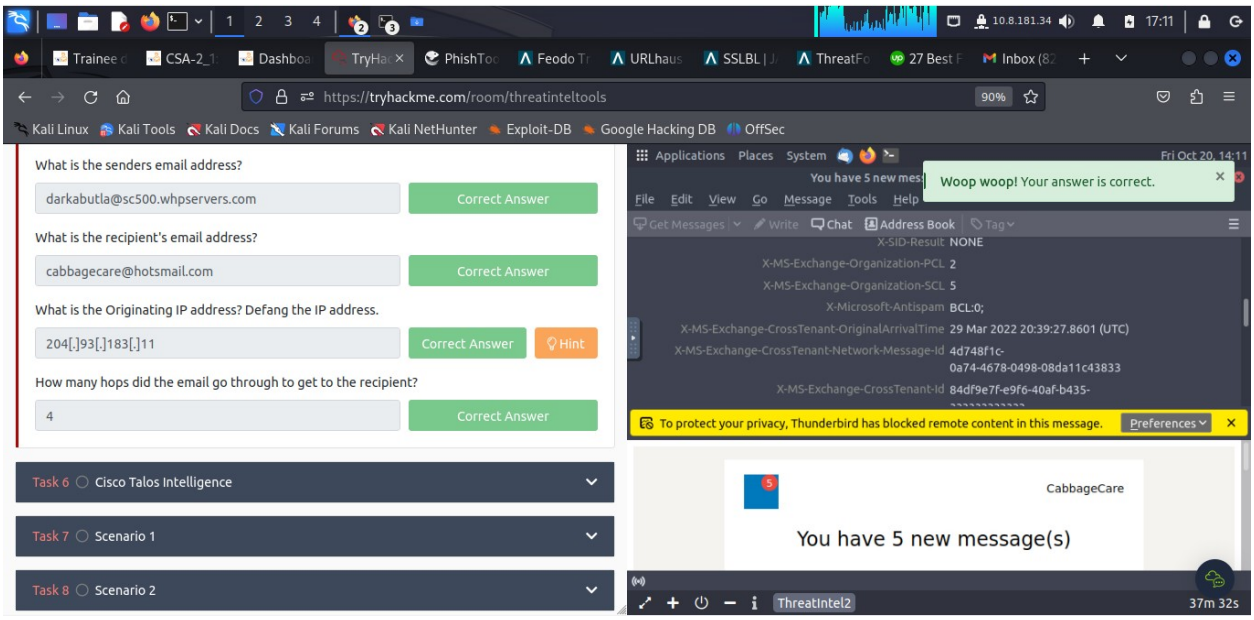
Task 5: PhishTool

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 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.


https://tryhackme.com/room/threatinteltools
You can now add PhishTool to your list of email analysis tools.
Scenario
You are a SOC Analyst and have been tasked to analyse a suspicious email, Email1.eml. To solve the task, open the email using Thunderbird on the attached VM, analyse it and answer the questions below.
Answer the questions below
What social media platform is the attacker trying to pose as in the email?
LinkedIn
Correct Answer
Hint
What is the senders email address?
darkabutla@sc500.whpservers.com
Correct Answer
What is the recipient's email address?
Answer format: **********.***
Submit
What is the Originating IP address? Defang the IP address.
Woop woop! Your answer is correct.
Subject You have 5 new message
To cabbagecare@hotsmail.com
To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
CabbageCare
You have 5 new message(s)
by Patrick Cook
Show message
ThreatIntel2
54m 29s


https://tryhackme.com/room/threatinteltools
What is the senders email address?
darkabutla@sc500.whpservers.com
Correct Answer
What is the recipient's email address?
cabbagecare@hotsmail.com
Correct Answer
What is the Originating IP address? Defang the IP address.
204[.]93[.]183[.]11
Correct Answer
Hint
How many hops did the email go through to get to the recipient?
Answer format: *
Submit
Task 6 Cisco Talos Intelligence
Task 7 Scenario 1
Task 8 Scenario 2
Woop woop! Your answer is correct.
X-MS-Office365-Filtering-Correlation-Id 4d748f1c-0a74-4678-0498-08da11c43833
X-MS-TrafficTypeDiagnostic DB9P194MB1386:EE_
X-MS-Exchange-EOPDirect true
X-Sender-IP 204.93.183.11
X-SID-PRA DARKABUTLA@SC500.WHPSERVERS.COM
X-SID-Result NONE
To protect your privacy, Thunderbird has blocked remote content in this message.
Preferences
CabbageCare
You have 5 new message(s)
ThreatIntel2
45m 50s

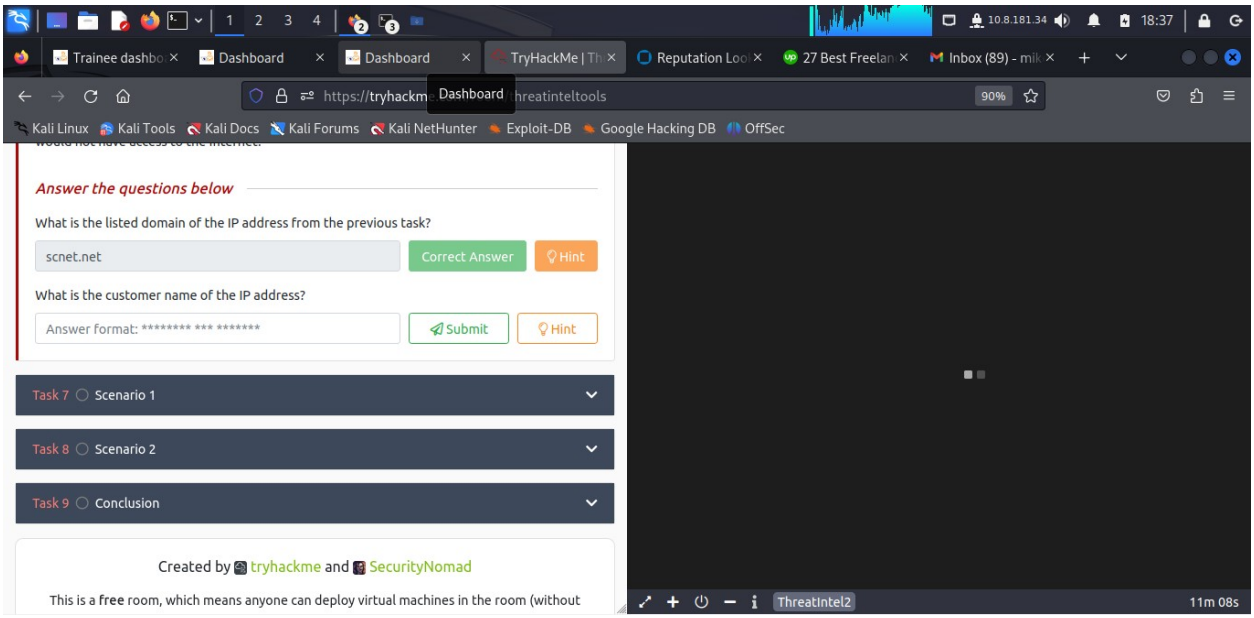


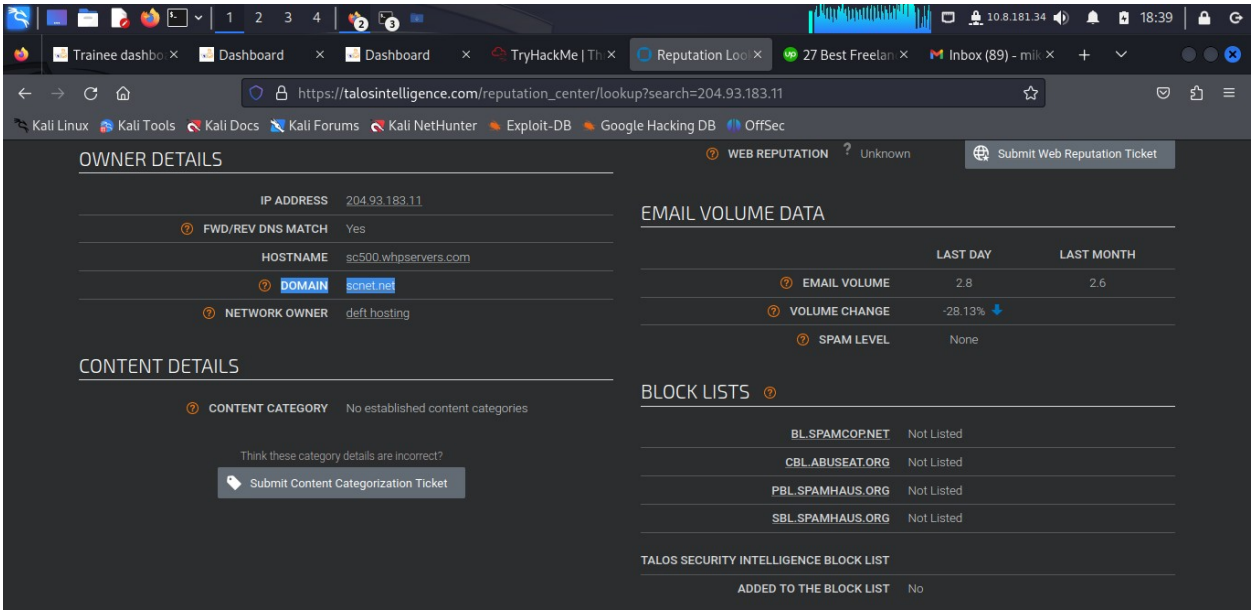
Task 6: Cisco Talos Intelligence Tool

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***.

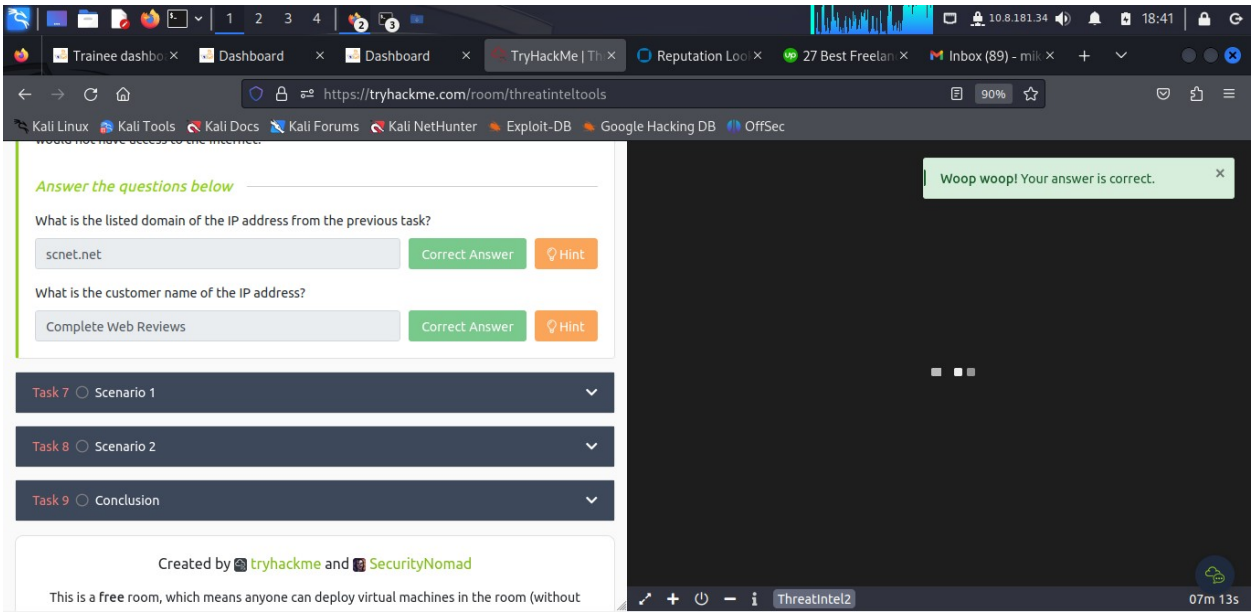
In this task the learner interacts with Talos Dashboard to conduct email traffic across the world.

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

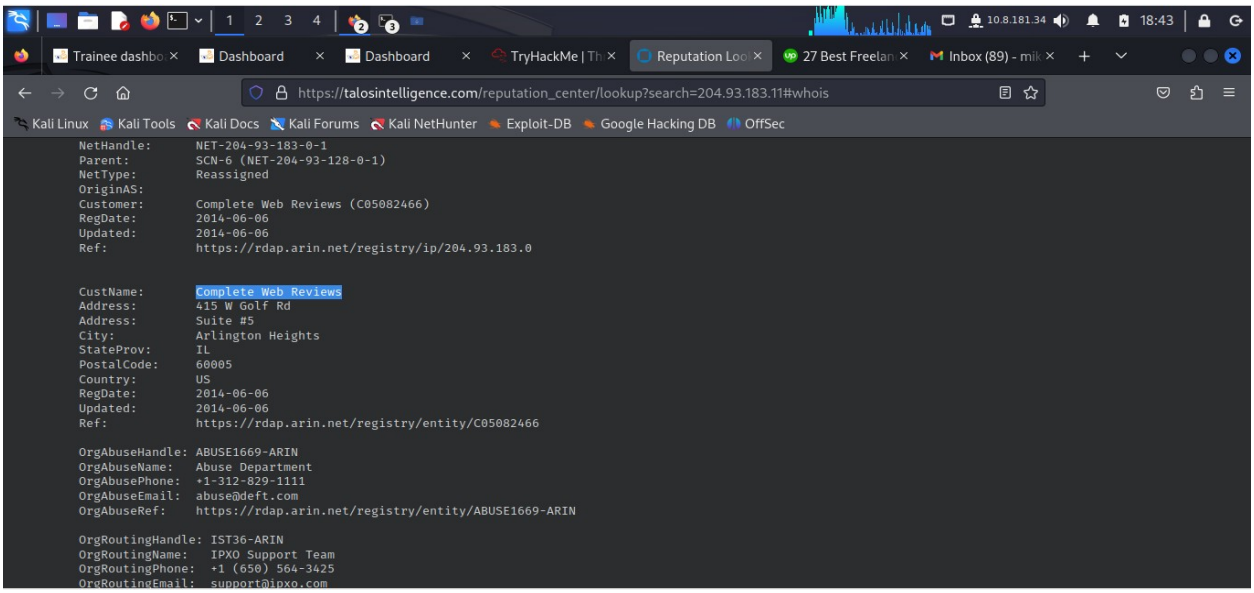




Customer name of the IP address is ***Complete Web Reviews.***



From Talos Dashboarding tool:



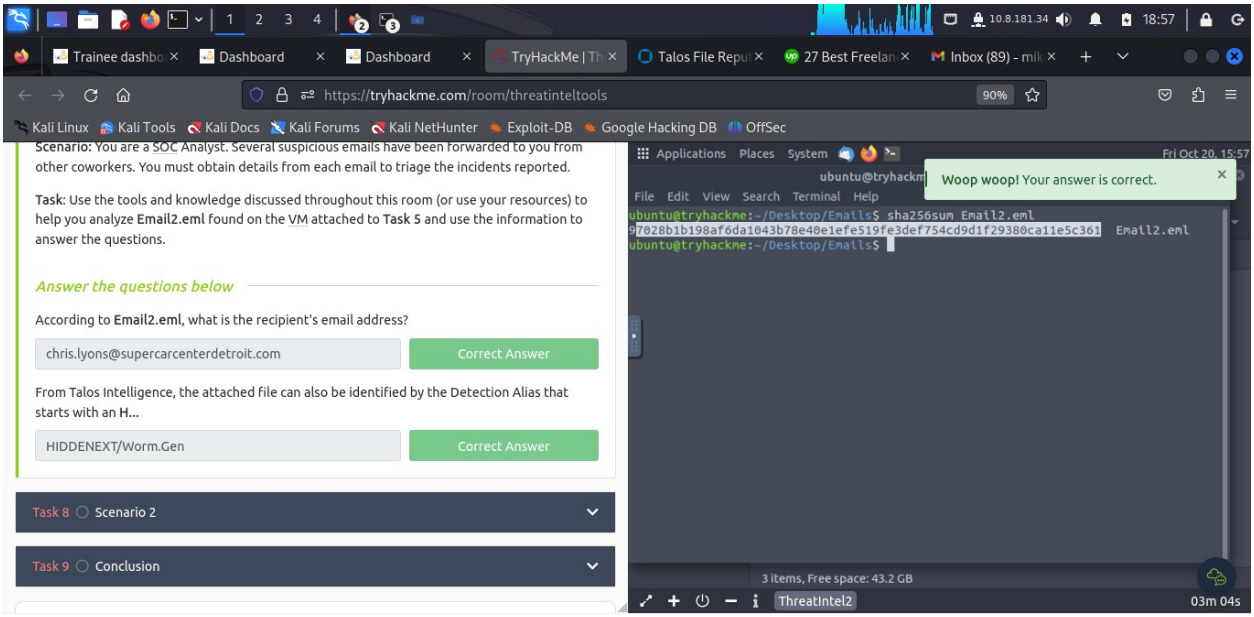
The learner used Cisco Talos Intelligence to answer questions from files provided in Task 5.

Task 7: Scenario 1

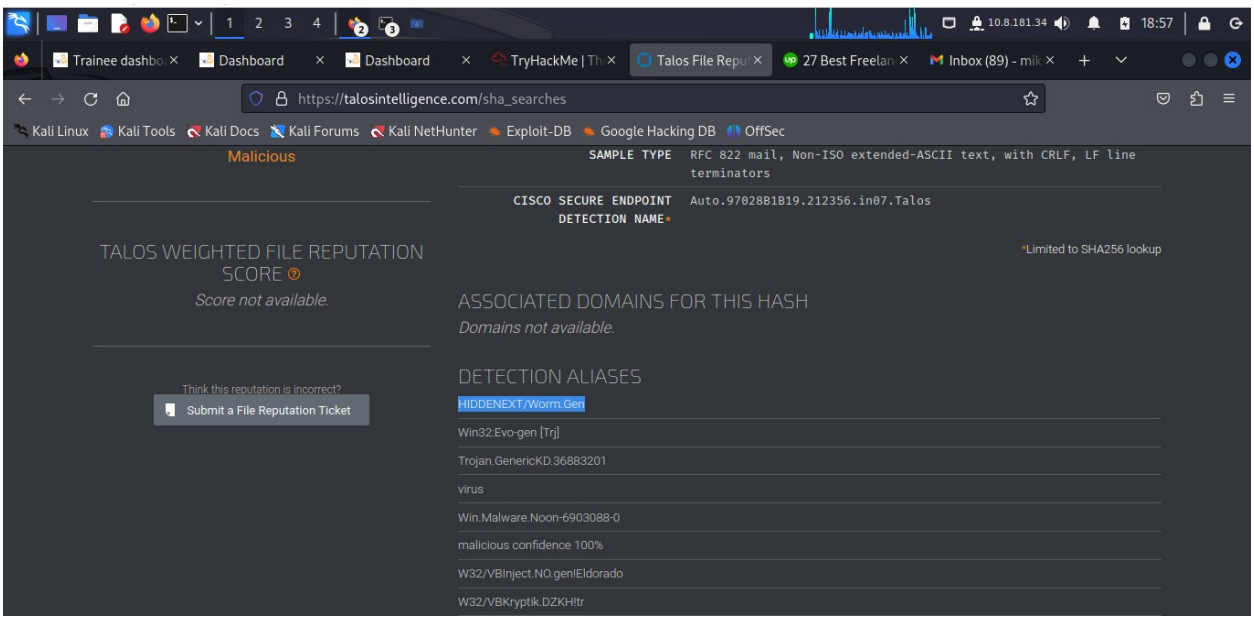
The learner - as SOC Analyst, the case is: there is suspicious emails forwarded from other coworkers. The learner must obtain details from each email to triage the incidents reported.

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.



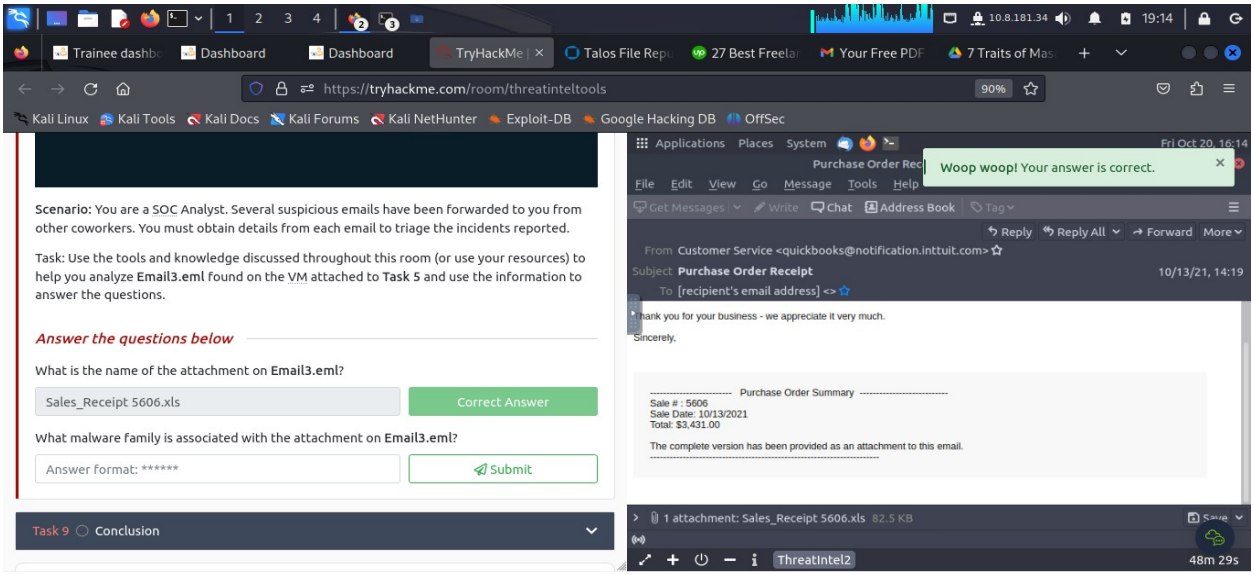
Task 8: Scenario 2

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.

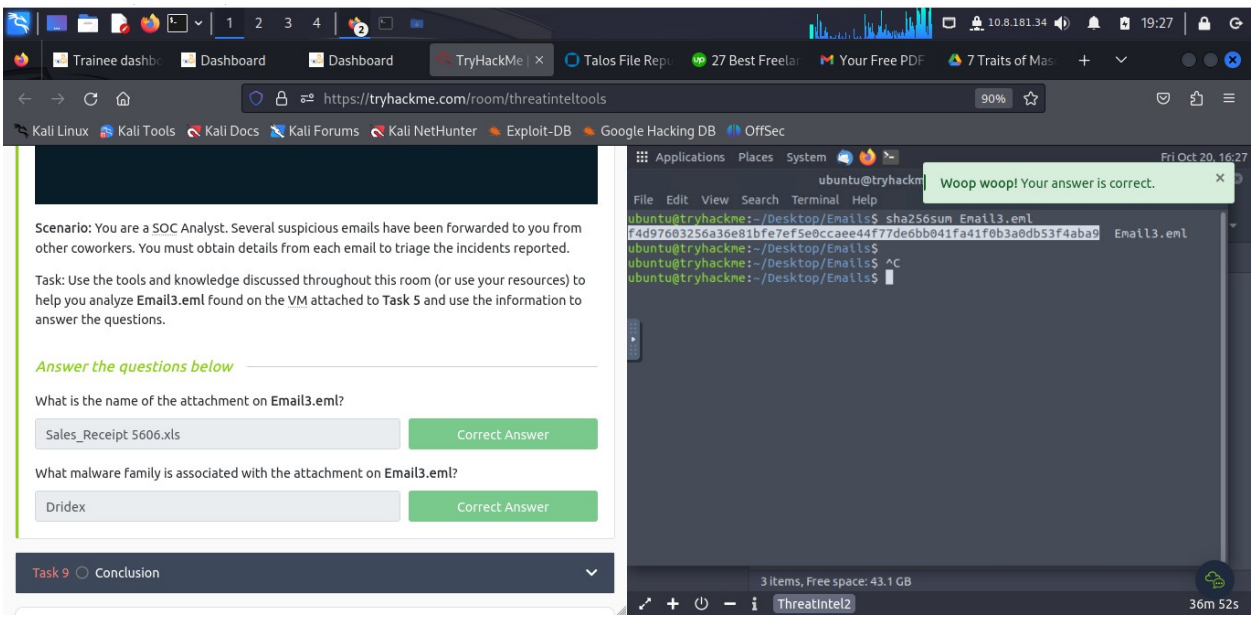
Task: Use the tools and knowledge discussed throughout this room (or use your resources) to help you analyze **Email3.eml** found on the VM attached to **Task 5** and use the information to answer the questions.

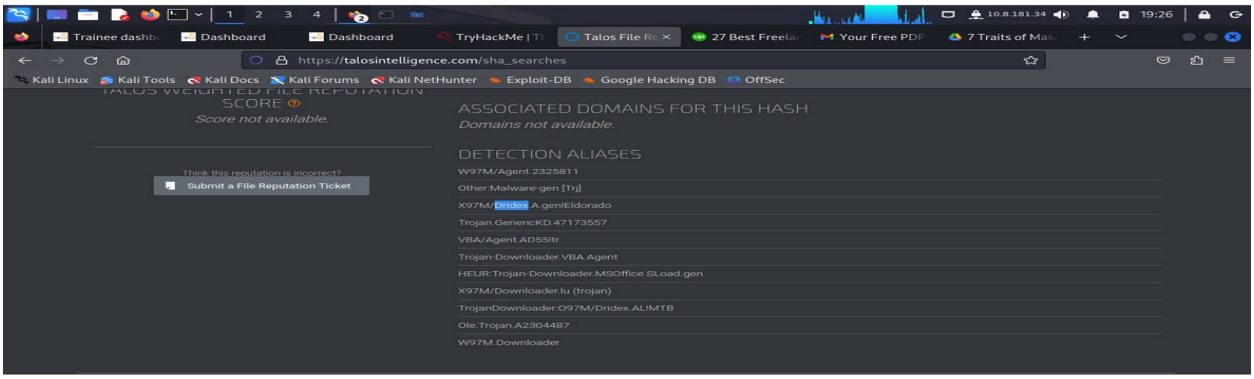
Solution(s)

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.

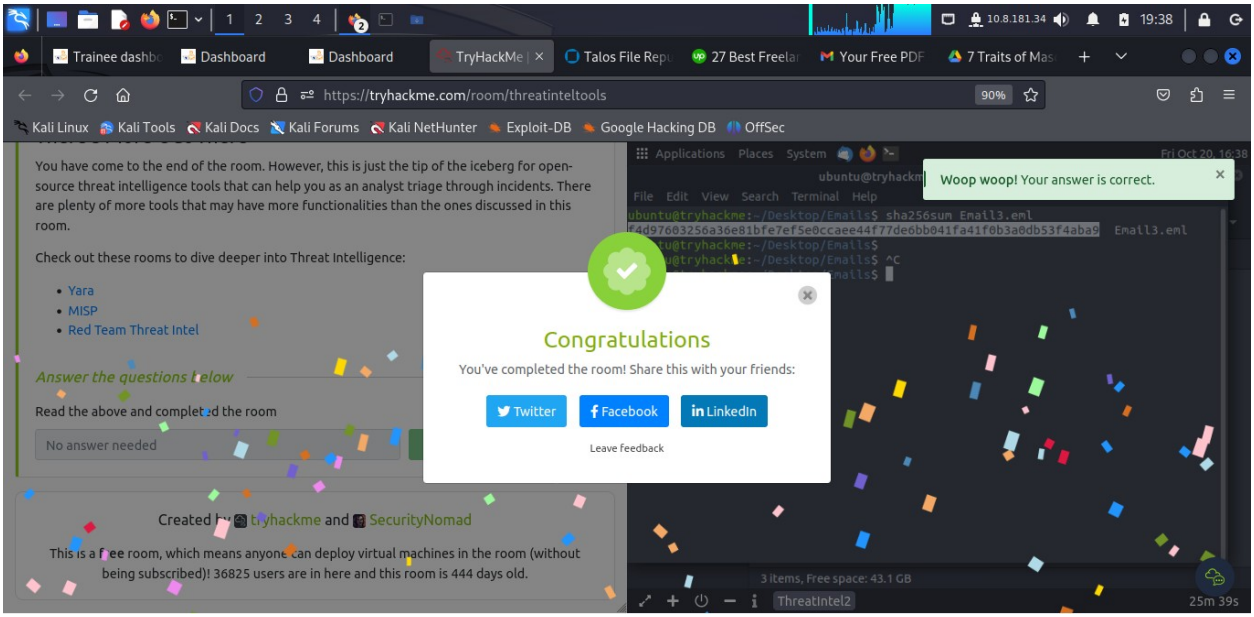
Task 9: Conclusion

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, MISP and Red Team Threat Intel

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