cs-sa07-24019
John_Mbithi_Mutave

Threat Intelligence Tools

1. Introduction to Threat Intelligence

Threat intelligence is the process of gathering, analyzing, and utilizing information about current and potential cyber threats. This information helps organizations understand the risks they face and develop strategies to protect against these threats. The main goals of threat intelligence are to identify threat actors, their methods, and their targets to better defend against cyberattacks.

2. Classifications of Threat Intelligence

Threat intelligence can be classified into several categories based on the type and scope of information provided:

Strategic Threat Intelligence

Focus: High-level information about cyber threats and trends.

Audience: Executives and decision-makers.

Purpose: To inform long-term security strategies and investment decisions.

Example: Reports on emerging cyber threats and their potential impact on specific industries.

Tactical Threat Intelligence

Focus: Specific information about threat actors and their tactics, techniques, and procedures (TTPs).

Audience: Security operations teams.

Purpose: To aid in the development of detection and mitigation strategies.

Example: Analysis of a malware family, including its indicators of compromise (IOCs) and attack vectors.

Operational Threat Intelligence

Focus: Information about specific, ongoing attacks.

Audience: Incident response teams.

Purpose: To provide actionable insights for immediate response to threats.

Example: Real-time alerts about a phishing campaign targeting the organization.

Technical Threat Intelligence

Focus: Detailed technical data about threats.

Audience: Security analysts and researchers.

Purpose: To support in-depth analysis and the development of detection tools.

Example: Hashes of malicious files, IP addresses of command-and-control servers.

3. Open-Source Threat Intelligence Tools

UrlScan.io

UrlScan.io is a free service designed to scan and analyze websites. It provides insights into how a website behaves, including its interactions and any potential security risks.

Key Features

Website Analysis: Provides detailed information about a website’s behavior and structure.

Threat Detection: Identifies potentially malicious URLs and phishing sites.

Integration: Can be integrated with other security tools for automated scanning.

Usage

Scanning a URL: Users can submit a URL to be scanned. UrlScan.io will analyze the URL and provide a detailed report.

Reviewing Results: The results include information about the website’s IP addresses, domain names, and any detected malicious activity.

Integration with Other Tools: UrlScan.io offers APIs that can be integrated with SIEM (Security Information and Event Management) systems for automated threat detection.

Abuse.ch

Abuse.ch is a platform dedicated to tracking malware and botnet activities. It provides various feeds and tools to help security professionals stay updated on the latest threats.

Key Features

Malware Feeds: Provides real-time feeds of malware samples and indicators.

Botnet Tracking: Monitors and reports on botnet command-and-control servers.

Threat Intelligence Sharing: Enables sharing of threat data among security professionals.

Usage

Accessing Feeds: Users can subscribe to different feeds, such as the URLhaus or the MalwareBazaar feed, to receive updates on malicious URLs and malware samples.

Investigating Threats: Analysts can use the data provided by Abuse.ch to investigate and mitigate threats within their networks.

Contributing Data: Security researchers can submit their findings to Abuse.ch to contribute to the community’s knowledge base.

PhishTool

PhishTool is a specialized tool for analyzing and investigating phishing emails. It helps identify phishing attempts and gather evidence for further action.

Key Features

Email Analysis: Provides detailed analysis of phishing emails, including header and body content.

Threat Indicators: Identifies indicators of phishing, such as malicious links and attachments.

Collaboration: Allows for sharing analysis results with other team members or organizations.

Usage

Submitting Emails: Users can upload suspected phishing emails to PhishTool for analysis.

Reviewing Analysis: PhishTool provides a comprehensive report on the email's content and any identified threats.

Taking Action: Based on the analysis, users can take appropriate actions to block the phishing attempt and mitigate any potential impact.

Cisco's Talos Intelligence Platform

Cisco's Talos Intelligence platform is a leading threat intelligence service that provides in-depth insights into various cyber threats. It leverages Cisco's extensive network and research capabilities to deliver actionable intelligence.

Key Features

Comprehensive Threat Data: Offers a vast database of threat intelligence, including malware, vulnerabilities, and threat actors.

Real-Time Updates: Provides real-time updates on emerging threats and ongoing attacks.

Advanced Analytics: Uses advanced analytics to correlate threat data and identify patterns.

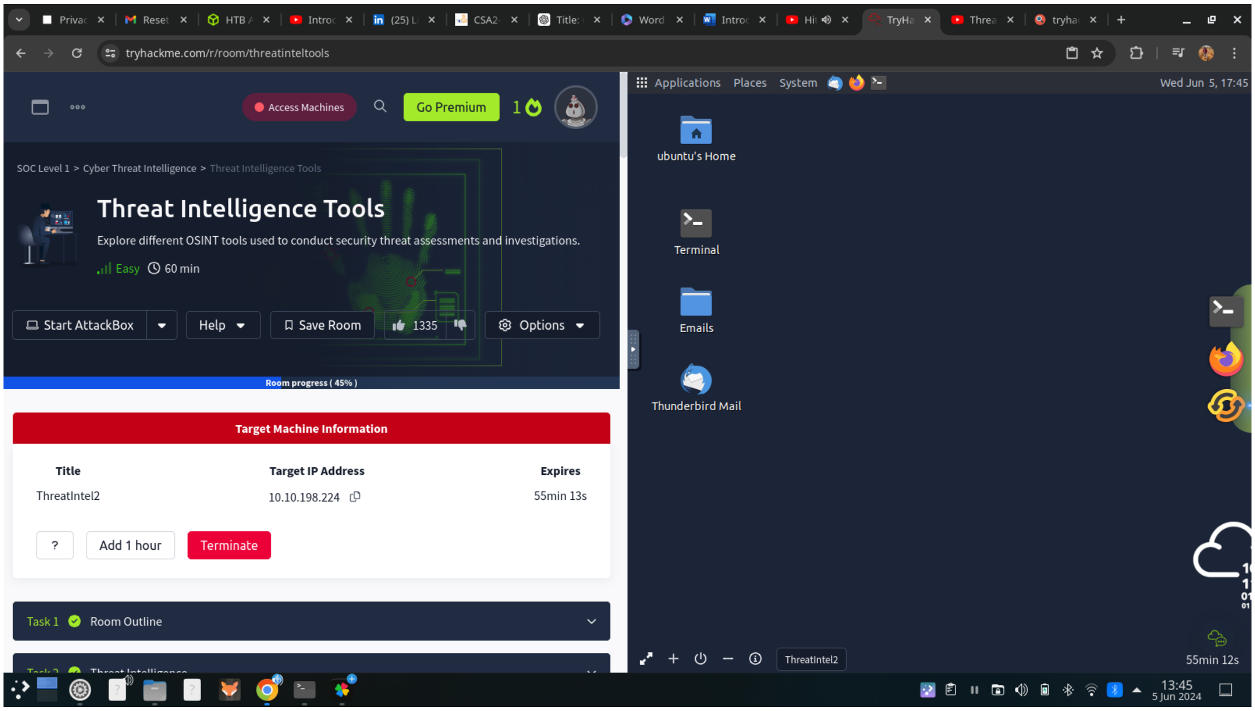
Usage

cs-sa07-24019
John_Mbithi_Mutave

Accessing Intelligence: Users can access Talos Intelligence through the Talos website or API.

Threat Research: Security analysts can use the platform to research specific threats and gather detailed information.

Implementing Defenses: Organizations can use the intelligence provided by Talos to enhance their security measures and defend against identified threats.



SOC Level 1 > Cyber Threat Intelligence > Threat Intelligence Tools

Threat Intelligence Tools

Explore different OSINT tools used to conduct security threat assessments and investigations.

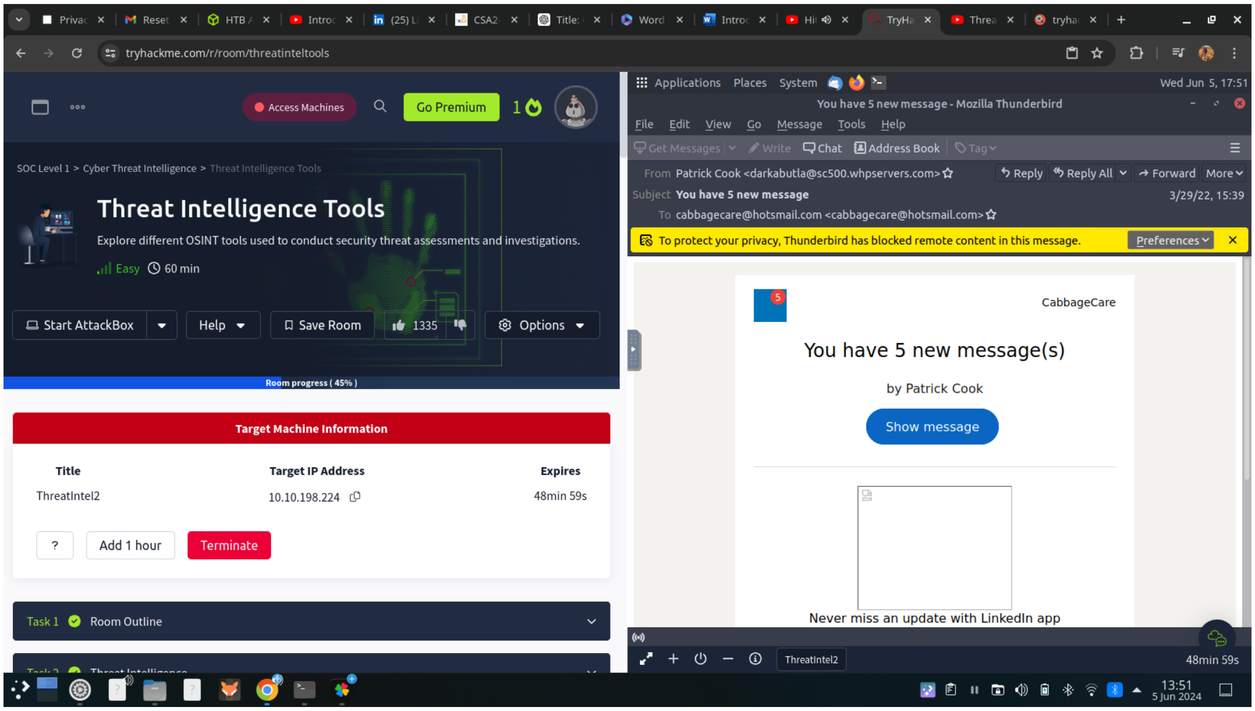
Easy 60 min

Target Machine Information

Title	Target IP Address	Expires
ThreatIntel2	10.10.198.224	55min 13s

Task 1 Room Outline

cs-sa07-24019
John_Mbithi_Mutave


tryhackme.com/r/room/threatinteltools

SOC Level 1 > Cyber Threat Intelligence > Threat Intelligence Tools

Threat Intelligence Tools

Explore different OSINT tools used to conduct security threat assessments and investigations.

Easy 60 min

Room progress (45%)

Target Machine Information

Title	Target IP Address	Expires
ThreatIntel2	10.10.198.224	48min 59s

Task 1 Room Outline

From Patrick Cook <darkabutla@sc500.whpservers.com>
Subject You have 5 new message 3/29/22, 15:39
To cabbagecare@hotmail.com <cabbagecare@hotmail.com>

To protect your privacy, Thunderbird has blocked remote content in this message.

CabbageCare

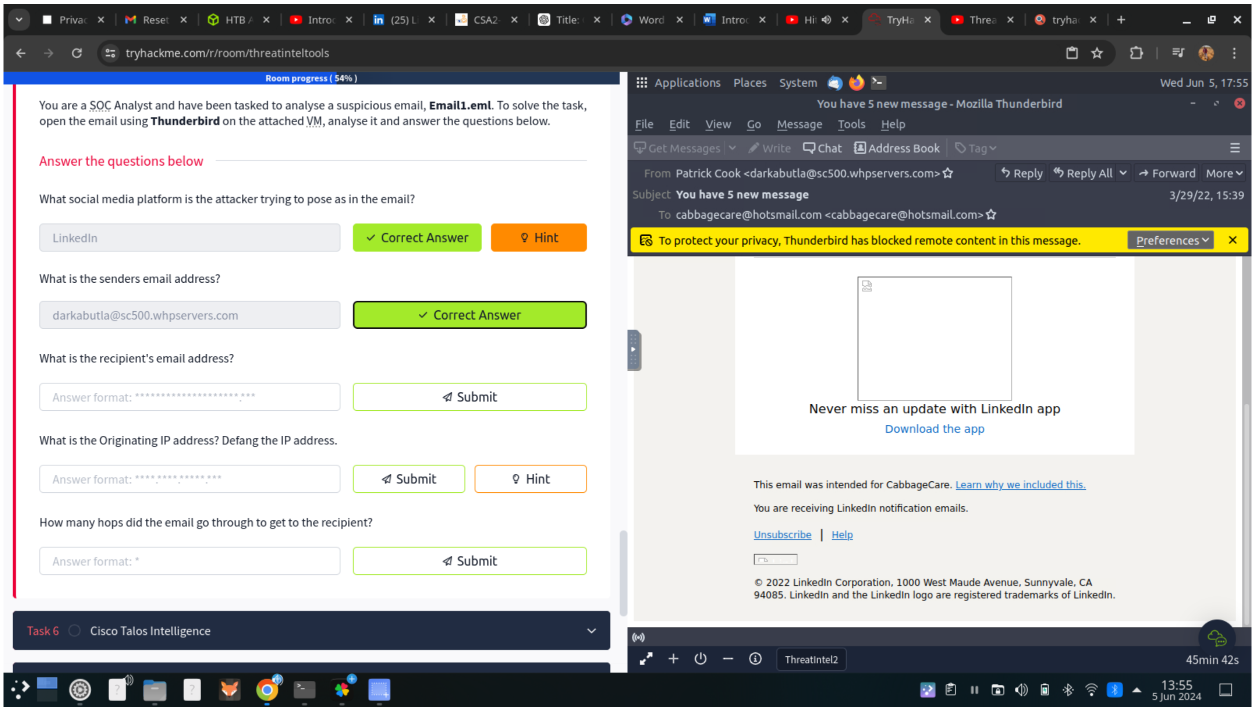
You have 5 new message(s)

by Patrick Cook

Show message

Never miss an update with LinkedIn app

Access Machines
Go Premium
Start AttackBox
Help
Save Room
1335
Options
Add 1 hour
Terminate
Applications Places System
Wed Jun 5, 17:51
You have 5 new message - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
Reply Reply All Forward More
Preferences
ThreatIntel2
48min 59s
13:51
5 Jun 2024


tryhackme.com/r/room/threatinteltools

Room progress (54%)

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

What is the senders email address?

darkabutla@sc500.whpservers.com ✓ Correct Answer

What is the recipient's email address?

Answer format: ********************.***

What is the Originating IP address? Defang the IP address.

Answer format: ****.****.*****.***

How many hops did the email go through to get to the recipient?

Answer format: *

Task 6 Cisco Talos Intelligence

From Patrick Cook <darkabutla@sc500.whpservers.com>
Subject You have 5 new message 3/29/22, 15:39
To cabbagecare@hotmail.com <cabbagecare@hotmail.com>

To protect your privacy, Thunderbird has blocked remote content in this message.

Never miss an update with LinkedIn app

Download the app

This email was intended for CabbageCare. Learn why we included this.

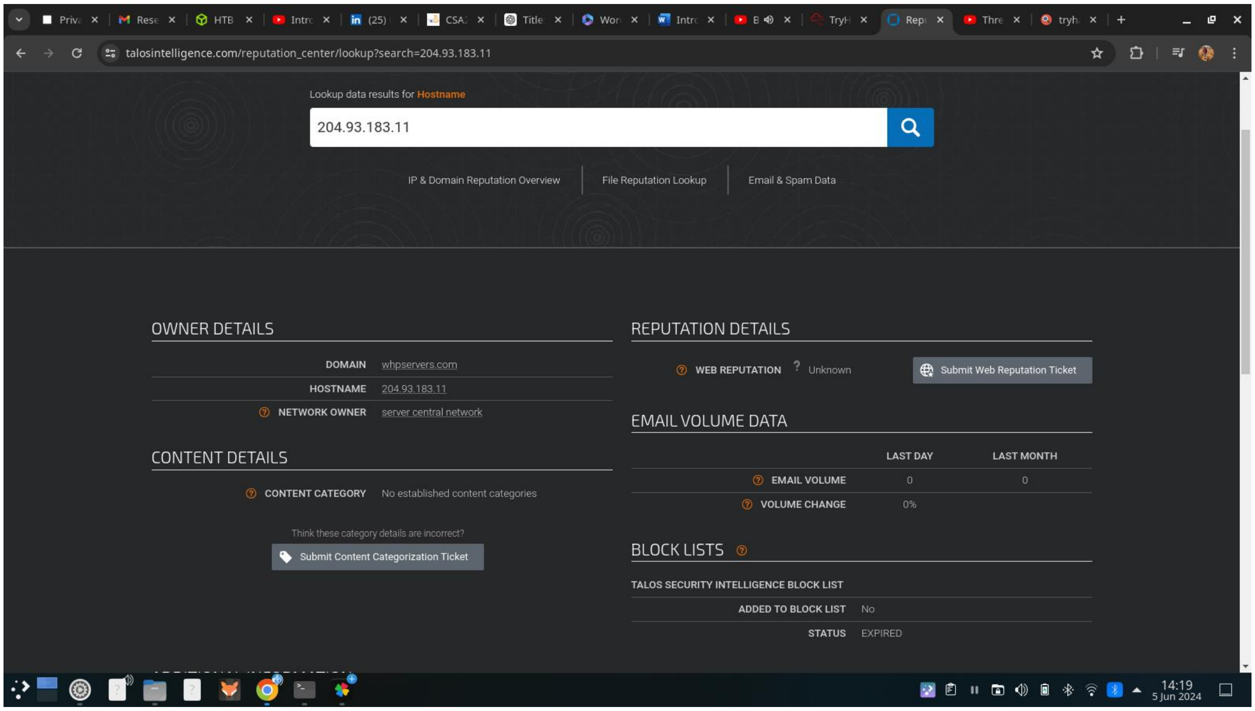
You are receiving LinkedIn notification emails.

Unsubscribe | Help

© 2022 LinkedIn Corporation, 1000 West Maude Avenue, Sunnyvale, CA 94085. LinkedIn and the LinkedIn logo are registered trademarks of LinkedIn.

Hint
Submit
Hint
Submit
Submit
Applications Places System
Wed Jun 5, 17:55
You have 5 new message - Mozilla Thunderbird
File Edit View Go Message Tools Help
Get Messages Write Chat Address Book Tag
Reply Reply All Forward More
Preferences
ThreatIntel2
45min 42s
13:55
5 Jun 2024

cs-sa07-24019
John_Mbithi_Mutave



talosintelligence.com/reputation_center/lookup?search=204.93.183.11

Lookup data results for Hostname

204.93.183.11

IP & Domain Reputation Overview
File Reputation Lookup
Email & Spam Data

OWNER DETAILS

DOMAIN	whpservers.com
HOSTNAME	204.93.183.11
NETWORK OWNER	server central network

CONTENT DETAILS

CONTENT CATEGORY	No established content categories

Think these category details are incorrect?

Submit Content Categorization Ticket

REPUTATION DETAILS

WEB REPUTATION	? Unknown

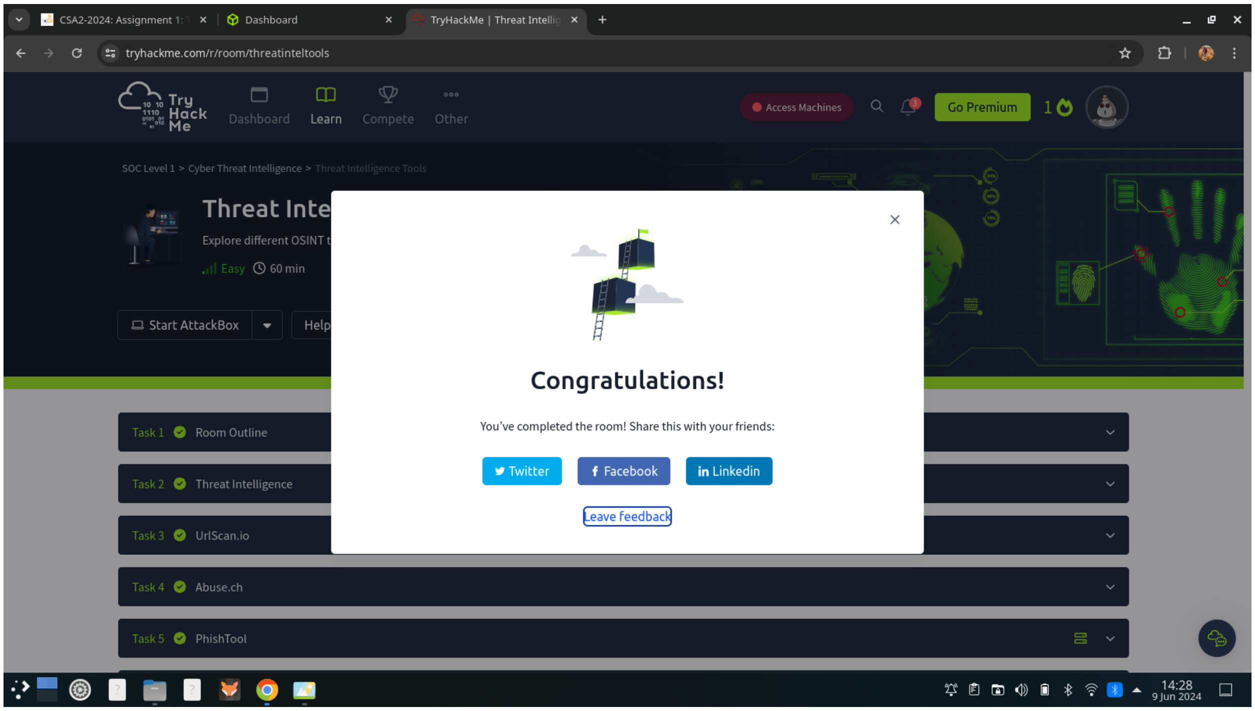
EMAIL VOLUME DATA

	LAST DAY	LAST MONTH
EMAIL VOLUME	0	0
VOLUME CHANGE	0%	

BLOCK LISTS

TALOS SECURITY INTELLIGENCE BLOCK LIST

ADDED TO BLOCK LIST	No
STATUS	EXPIRED



tryhackme.com/r/room/threatinteltools

SOC Level 1 > Cyber Threat Intelligence > Threat Intelligence Tools

Threat Inte

Explore different OSINT t

Easy 60 min

Congratulations!

You've completed the room! Share this with your friends:

Task 1 Room Outline

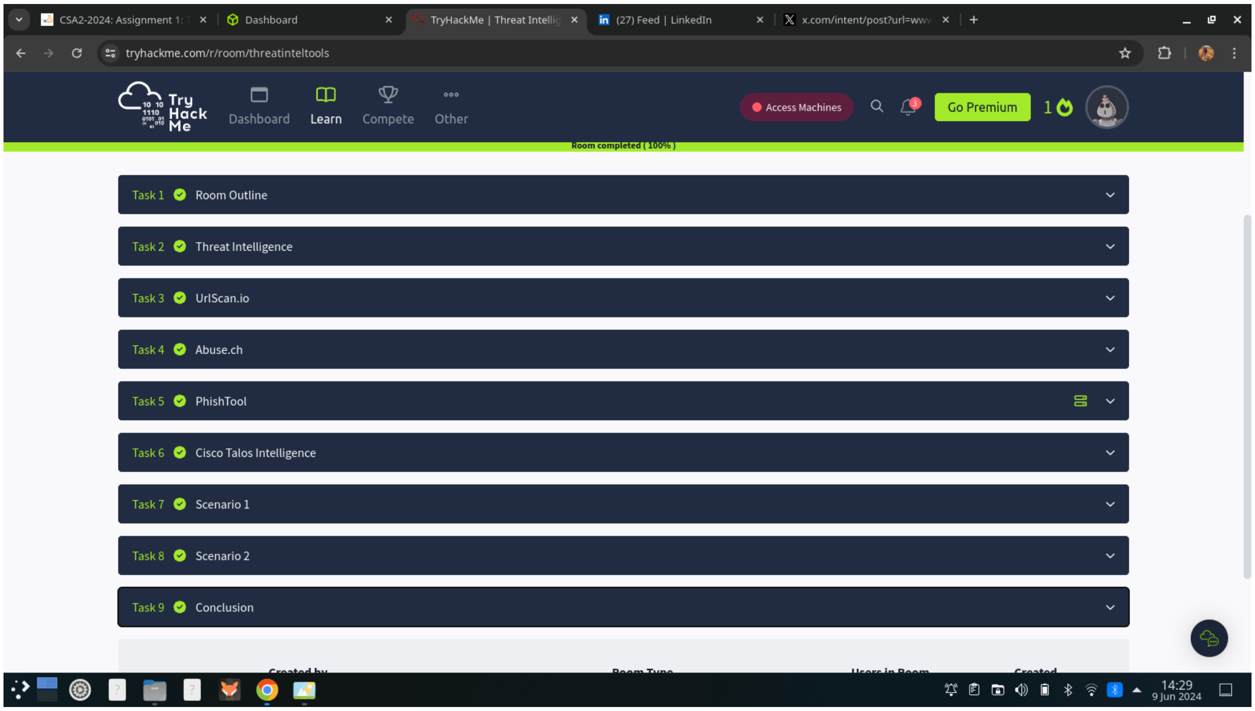
Task 2 Threat Intelligence

Task 3 UrlScan.io

Task 4 Abuse.ch

Task 5 PhishTool

cs-sa07-24019
John_Mbithi_Mutave



Task 1 Room Outline

Task 2 Threat Intelligence

Task 3 UrlScan.io

Task 4 Abuse.ch

Task 5 PhishTool

Task 6 Cisco Talos Intelligence

Task 7 Scenario 1

Task 8 Scenario 2

Task 9 Conclusion

Shareable link - www.tryhackme.com/r/room/threatinteltools

4. Conclusion

Threat intelligence is a critical component of modern cybersecurity strategies. By understanding the various classifications of threat intelligence and utilizing open-source tools such as UrlScan.io, Abuse.ch, PhishTool, and Cisco's Talos Intelligence platform, organizations can better protect themselves against the ever-evolving landscape of cyber threats. These tools provide valuable insights and actionable data that can enhance an organization's ability to detect, respond to, and mitigate cyber threats.