Name: Kaushal Kotkar Department: CyberSecurity Div: BE-15 Roll No :54

Subject: OSINT

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Experiment No. – 6** | | | | |
| **Date of Performance:** | 15/10/2024 | | | |
| **Date of Submission:** | 17/10/2024 | | | |
| Program Execution/ formation/ correction/  ethical practices (06) | Timely Submission  (01) | Viva (03) | Experiment Total (10) | Sign with Date |
|  |  |  |  |  |

# Experiment No. 6

### Aim: To solving real-world challenges on the TryHackMe platform, using innovative tools and techniques to uncover hidden digital insights

**Lab Outcome:** Conduct advanced searches to gather intelligence and apply advance OSINT search techniques and tools.

**Theory:**

1. **Definition of OSINT**
   * OSINT refers to data collected from publicly accessible resources, including social media, websites, public records, forums, and more. It is often used in cybersecurity, intelligence analysis, and competitive analysis.

## OSINT Techniques

* + **Search Engines:** Using advanced search operators (e.g., Google Dorking) to find specific information.
  + **Social Media Analysis:** Investigating profiles, posts, and connections to gather insights.
  + **WHOIS Lookups:** Checking domain registration details to find information about website owners.
  + **Geolocation:** Using images or posts to determine the geographical location of an event or individual.

## Tools for OSINT

* + Tools like Maltego, theHarvester, and Shodan help automate the collection and analysis of OSINT data.
  + Browser extensions like Hunter can assist in finding email addresses associated with a domain.

## Data Validation

* + It's crucial to validate the accuracy of the information gathered, as OSINT can lead to false positives. Cross-referencing multiple sources can help ensure reliability.

## Ethical Considerations

* + While OSINT involves publicly available information, ethical considerations must be taken into account, especially concerning privacy and consent.

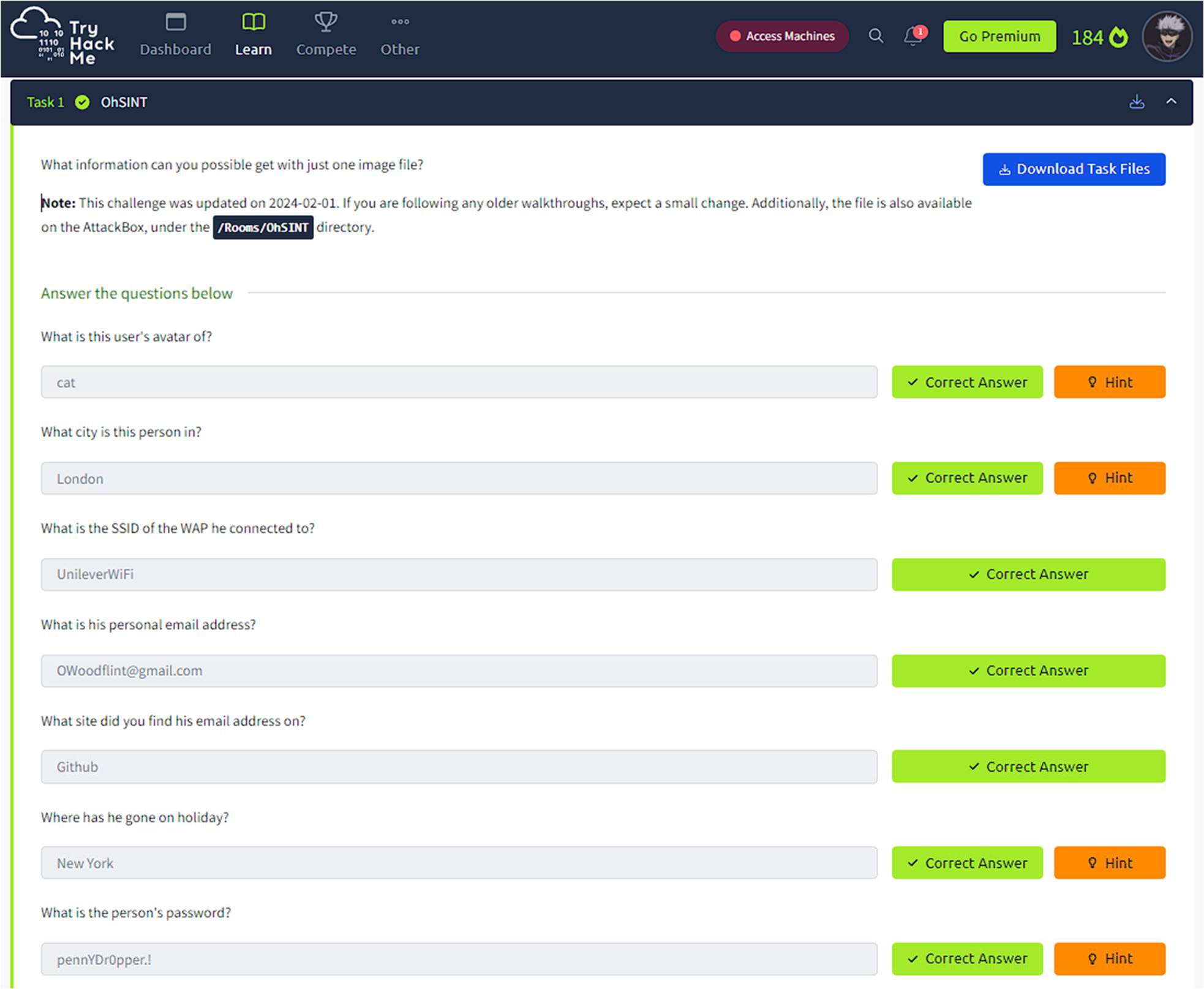
## Application in Cybersecurity

* + OSINT is valuable for threat intelligence, vulnerability assessments, and understanding potential attack vectors. Cybersecurity professionals use it to gather information about targets during penetration testing or red teaming.

## Challenges

* + The vast amount of data available can be overwhelming, making it difficult to identify relevant information quickly.
  + Staying up to date with changing privacy laws and platform policies is essential to ensure compliance during data collection.

**Output:**

****

**Conclusion:** Here we successfully completed the tryhackme room.