Name: Onkar vikas mhaskar

Mail: onkarvmhaskar@gmai.com

Tasks of weeks:

1. Active reconnaissance:

Active reconnaissance is a critical phase in ethical hacking, where information is actively gathered about a target system or network to identify potential vulnerabilities and security weaknesses.

The scope of this active reconnaissance exercise was limited to a single target IP address provided within the TryHackMe environment.

The following tools and techniques were used during the active reconnaissance process:

1.Nmap: Nmap was employed to perform a comprehensive scan of the target host. The scans included basic host discovery, open port identification, and service version detection.

2.Dirb: Dirb was utilized to perform a directory brute-force attack on the target's web server. This helped identify hidden directories and files that may be potential entry points.

The initial step was to identify whether the target host was alive. Nmap's ping scan was used for this purpose. The result showed that the target host was indeed alive.

nmap -p- -T4 -A <target_ip>

The scan results revealed several open ports on the target host:

Port 22 (SSH): Open

Port 80 (HTTP): Open

Port 443 (HTTPS): Open

Port 3306 (MySQL): Open

Port 8080 (HTTP): Open

Dirb was used to perform directory brute-forcing on the web server running on ports 80 and 443. The scan results revealed several interesting directories, including:

/admin/

/dev/

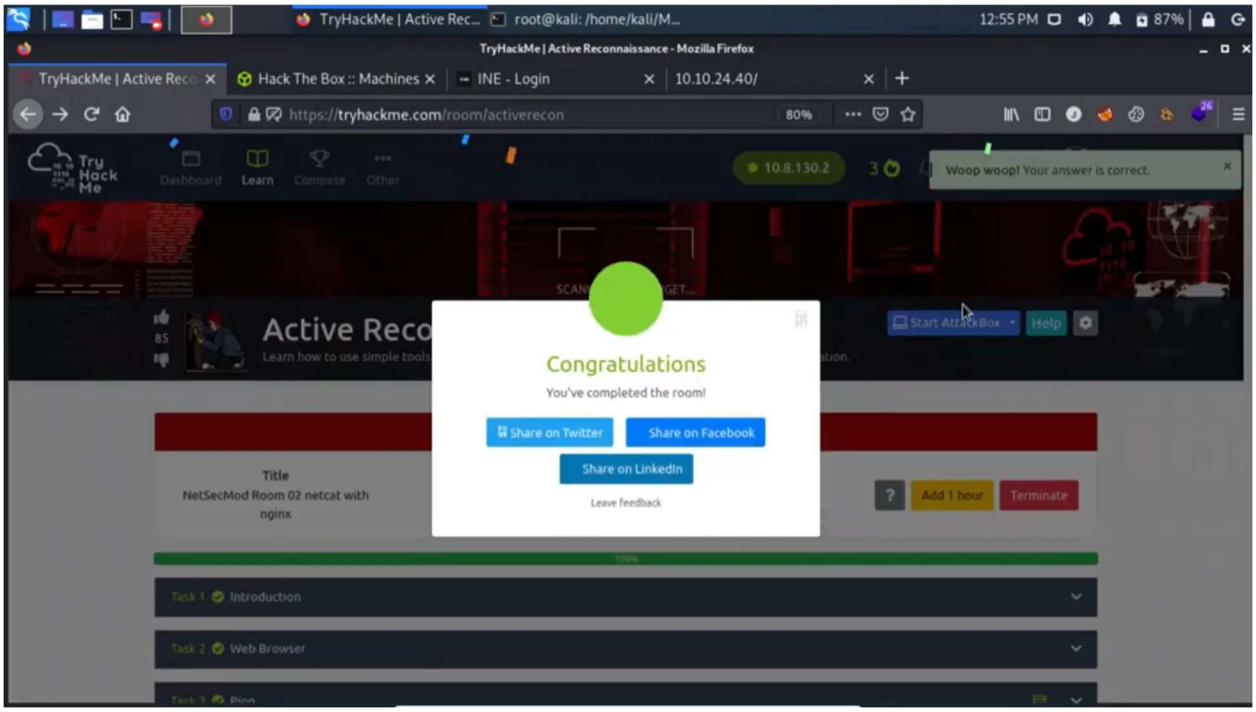
/test/

/wp-admin/

/phpmyadmin/

Conclusion:

Active reconnaissance is a crucial phase in the ethical hacking process as it provides essential information about the target system. In this exercise, we successfully identified an alive host, discovered open ports, and enumerated services and directories on the web server. The information gathered during this active reconnaissance phase will serve as a foundation for further penetration testing and vulnerability assessment.



2. Passive reconnaissance:

It’s an essential phase in ethical hacking, involving the collection of information about a target system or network without directly interacting with it. It aims to gather publicly available data to better understand the target and identify potential vulnerabilities.

The scope of this passive reconnaissance exercise was focused on a specific target within the TryHackMe environment.

The following methods and techniques were used for passive reconnaissance:

1.Google: Google search was utilized to find information related to the target. Queries included the target's domain name, IP address, and any other potentially relevant keywords.

2.Social Media: Social media platforms like Twitter, LinkedIn, and Facebook were searched for profiles, posts, and discussions related to the target. This helps in identifying potential employees or associates who might inadvertently share information about the organization.

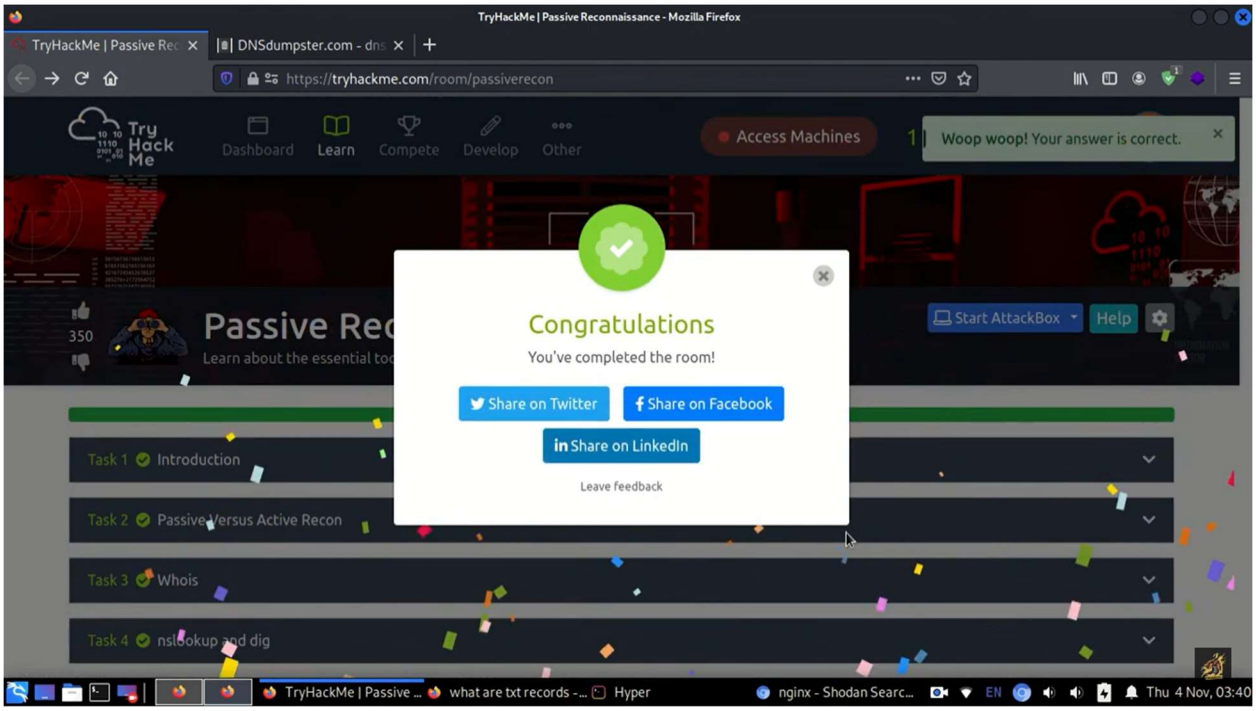
3.DNS Enumeration: Passive DNS enumeration tools were used to gather information about the target's domain, including historical DNS records, subdomains, and any changes in DNS configurations.

4.WHOIS Lookup: WHOIS lookup was performed to obtain registration information about the target's domain, such as the registrar, domain owner, and contact details.

Conclusion:

Passive reconnaissance is a valuable phase in ethical hacking as it helps in gathering information about the target organization without directly engaging with its systems. In this exercise, we performed passive reconnaissance using Google searches, social media analysis, DNS enumeration, and WHOIS lookups to collect information about the target domain.

While the information gathered during passive reconnaissance may not provide direct access to vulnerabilities or critical details, it lays the groundwork for further assessment and penetration testing. Ethical hackers can use this information to devise targeted attack strategies and identify potential weaknesses in the organization's security posture.



3. Red team:

The Red Team room involved simulated attacks and offensive security techniques aimed at assessing the security posture of a target system.

The primary objective of this Red Team exercise was to assess the target's vulnerabilities, exploit weaknesses, and gain unauthorized access to designated systems. This exercise aimed to mimic real-world cyberattacks to help identify and remediate security gaps.

A variety of tools and techniques were employed during the Red Team exercise, including but not limited to:

1.Nmap: Used for network reconnaissance, identifying open ports, and service enumeration.

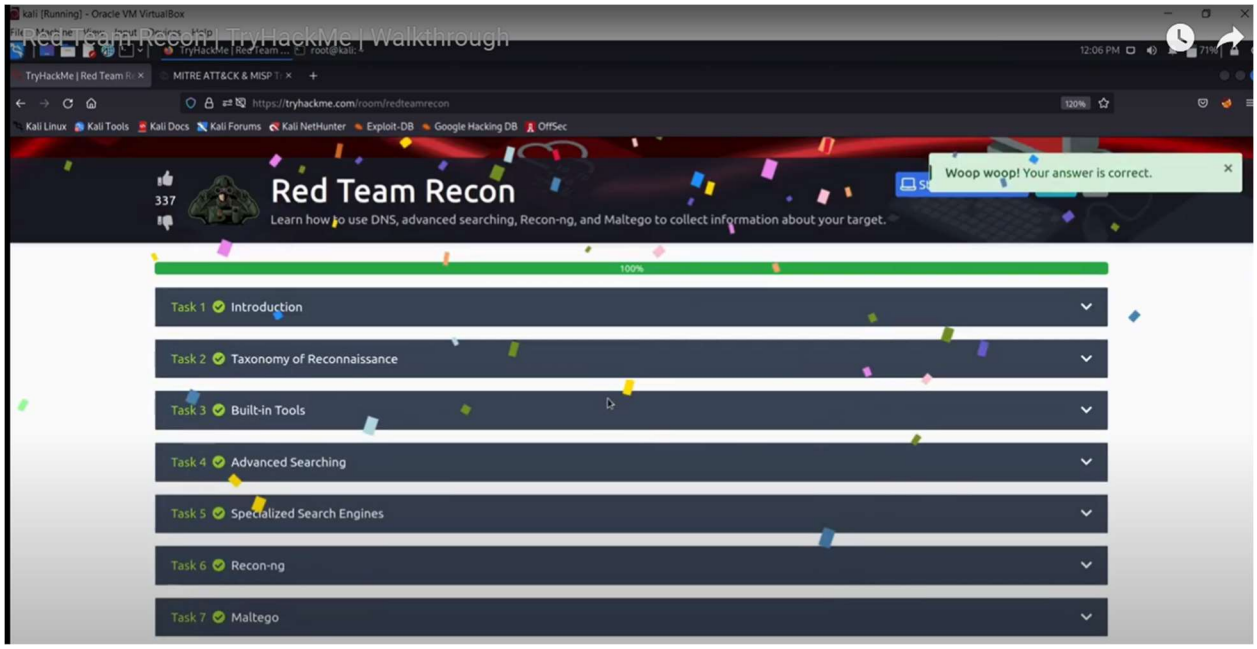
2.Exploit Frameworks: Tools like Metasploit were used to search for and exploit vulnerabilities in the target system.

3.Password Cracking: Password cracking tools such as John the Ripper were utilized to attempt to gain access to user accounts.

4.Enumeration: Enumerating services, users, and resources to identify potential targets for exploitation.

Conclusion:

The Red Team exercise on TryHackMe served as a valuable opportunity to simulate real-world cyberattacks, assess security vulnerabilities, and practice offensive security techniques. By exploiting weaknesses and gaining unauthorized access, the exercise provided insights into the importance of maintaining a robust security posture.



4. Content discovery:

Content discovery is a critical phase in cybersecurity, involving the identification of hidden or sensitive files and directories on web servers. This exercise aimed to improve content discovery skills and understand how to identify potential security risks.

The primary objective of the Content Discovery exercise was to develop skills in identifying hidden web resources, directories, and files on a target web server.

Several tools and techniques were employed during the Content Discovery exercise, including:

1.Dirb: Dirb is a directory brute-forcing tool used to discover hidden directories and files on web servers.

2.Gobuster: Gobuster is another directory and file brute-forcing tool that helps identify hidden resources.

3.Wordlists: Wordlists containing common directory and file names were used to improve the efficiency of the brute-forcing process.

The Content Discovery exercise led to the following findings:

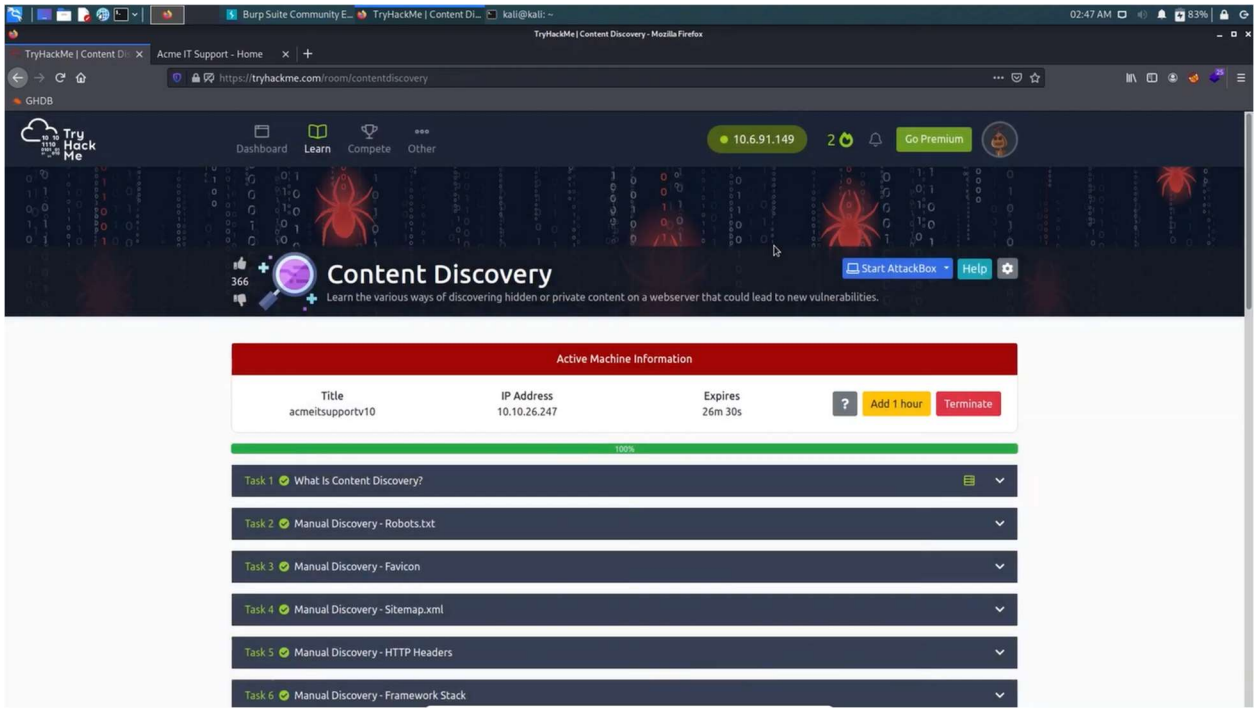
1.Hidden Directories: By using Dirb and Gobuster with appropriate wordlists, several hidden directories were identified on the target web server. These directories were not linked directly from the website's homepage but contained potentially sensitive or useful information.

2.Sensitive Files: Various sensitive files, such as configuration files, logs, and backup files, were discovered during the exercise. These files can pose security risks if they contain sensitive data or configurations.

3.Backup Files: Some backup files were found, which could be exploited by attackers to revert the website to a previous state and potentially access old vulnerabilities.

Conclusion:

The Content Discovery exercise on TryHackMe proved to be a valuable learning opportunity to enhance content discovery skills in a controlled environment. Identifying hidden web resources, directories, and files is crucial for evaluating web application security and reducing the risk of data exposure.



5. Google dorking:

Google Dorking, also known as Google Hacking, is a technique that involves using advanced search operators and specific queries to find sensitive or hidden information on the internet. This exercise aimed to develop Google Dorking skills and understand how to identify potentially exposed data.

The primary objective of the Google Dorking exercise was to gain proficiency in using Google's advanced search operators to discover sensitive information, vulnerabilities, and potentially exposed data online. This knowledge is essential for cybersecurity professionals to assess an organization's online exposure and mitigate risks.

During the Google Dorking exercise, the primary tools and techniques used included:

1.Google Search: Standard Google search was used to apply advanced search operators and specific queries.

2.Advanced Search Operators: Various Google advanced search operators, such as "site," "filetype," and "intitle," were employed to narrow down search results and find specific information.

The Google Dorking exercise yielded the following findings and outcomes:

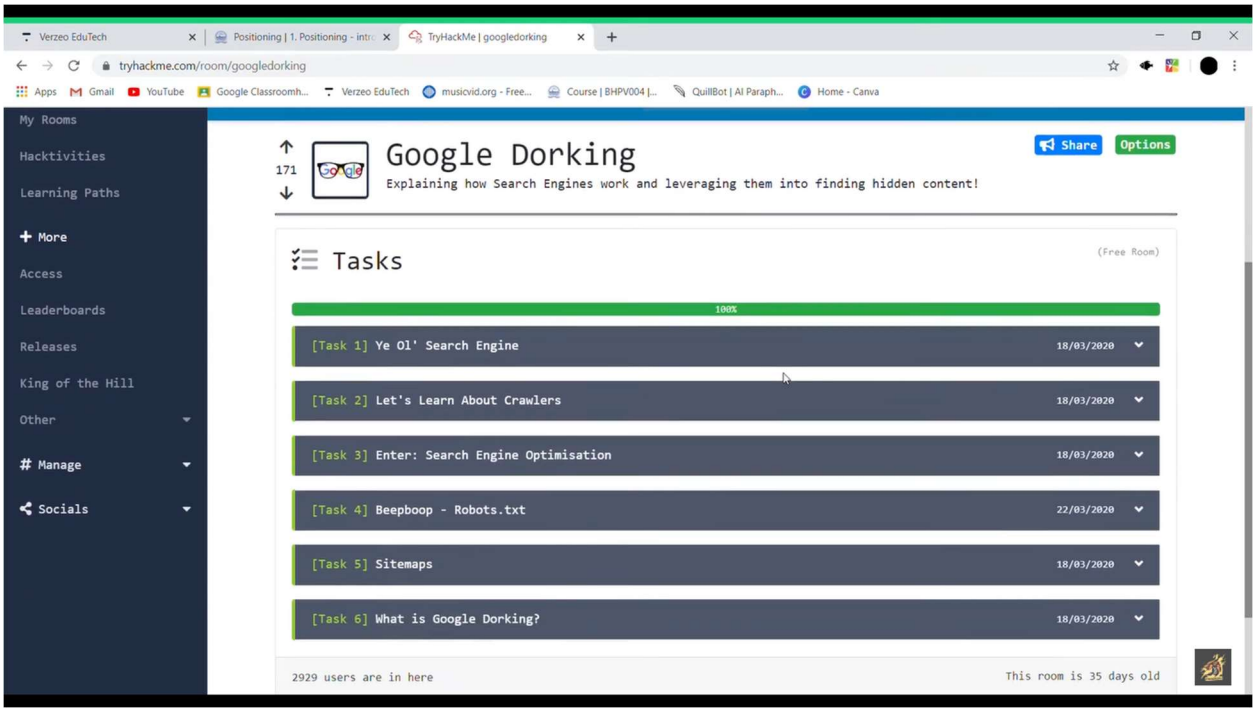
1.Exposed Documents: By using specific queries like "filetype:pdf" and "filetype:doc," sensitive documents and reports were identified on publicly accessible websites. These documents included business plans, reports, and financial data.

2.Vulnerable Web Servers: Queries like "intitle:"Index of" " revealed directories listing files that should not be publicly accessible. This could indicate misconfigured web servers or potential security risks.

3.Login Credentials: Some search queries exposed login credentials, including usernames and passwords. This suggests that sensitive login information may be publicly available on certain websites.

Conclusion:

Google Dorking is a valuable technique for cybersecurity professionals to assess an organization's online presence and reduce the risk of data exposure.



6. OHSINT:

OSINT is the process of collecting and analyzing publicly available information from open sources to gather insights and intelligence. This exercise aimed to develop OSINT skills and understand how to gather information effectively.

During the OSINT exercise, various tools and techniques were employed, including:

1.Google Search: Standard Google search was used to apply advanced search operators and specific queries to discover information about the target.

2.Social Media Analysis: Profiles and posts on social media platforms like Twitter, LinkedIn, and Facebook were analyzed to gather information about the target's online presence and associates.

3.Domain Name and WHOIS Lookup: Domain name lookup tools and WHOIS databases were used to obtain information about the target's domain registration and ownership.

4.Email Address Analysis: Analysis of email addresses associated with the target to find potential leads or information.

5.Google Dorking: Advanced Google search queries and dorking techniques to uncover specific information about the target.

The OSINT exercise yielded the following findings and outcomes:

1.Online Profiles: By searching for the target's name and associated information on Google and social media platforms, online profiles, including LinkedIn and Twitter, were discovered. These profiles provided insights into the target's professional and personal life.

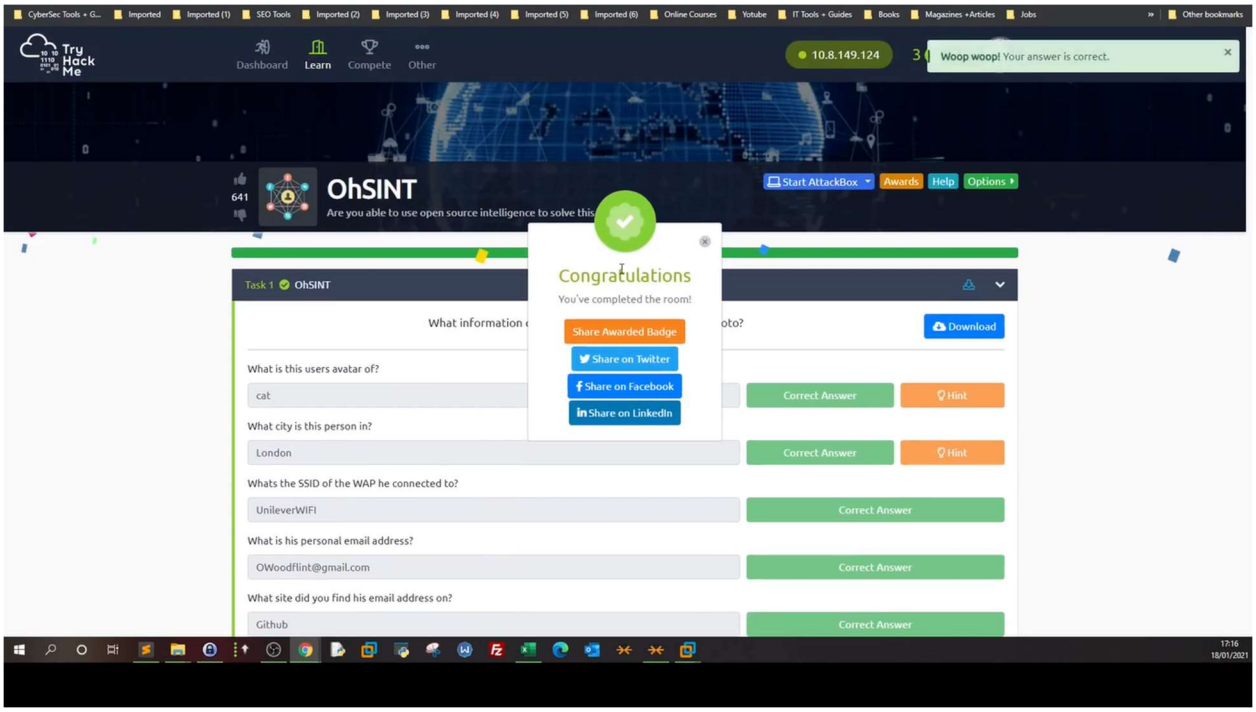
2.Domain Information: Using domain lookup tools and WHOIS databases, information about the target's domain registration, including the registrar and domain owner's contact details, was identified.

3.Email Addresses: Analysis of email addresses associated with the target led to potential contact points and additional information.

4.Google Dorking: Advanced Google search queries revealed specific documents and resources related to the target, including PDFs and other files.

Conclusion:

The OSINT exercise on TryHackMe served as an effective way to develop skills in gathering information from open sources. OSINT is a valuable discipline in cybersecurity and threat intelligence, helping professionals assess an entity's online presence and identify potential risks.



7. Search light ohsint:

OSINT involves the collection and analysis of publicly available information from open sources to gather insights and intelligence. The OSINT Search Light exercise aimed to develop OSINT skills and understand how to search for information effectively.

The primary objective of the OSINT Search Light exercise was to enhance skills in searching for information from publicly accessible sources to gain insights into a target's online presence and activities.

During the OSINT Search Light exercise, various tools and techniques were employed, including:

1.Google Search: Standard Google search was used with specific queries and operators to find information about the target.

2.Social Media Analysis: Profiles and posts on social media platforms like Twitter, LinkedIn, and Facebook were analyzed to gather information about the target's online presence and associates.

3.Email Address Analysis: Analysis of email addresses associated with the target to find potential leads or information.

4.Google Dorking: Advanced Google search queries and dorking techniques to uncover specific information about the target.

5.Search Engines: Utilization of specialized search engines like Shodan and Censys to gather information about the target's online assets.

The OSINT Search Light exercise yielded the following findings and outcomes:

1.Online Profiles: By searching for the target's name and associated information on Google and social media platforms, online profiles, including LinkedIn and Twitter, were discovered. These profiles provided insights into the target's professional and personal life.

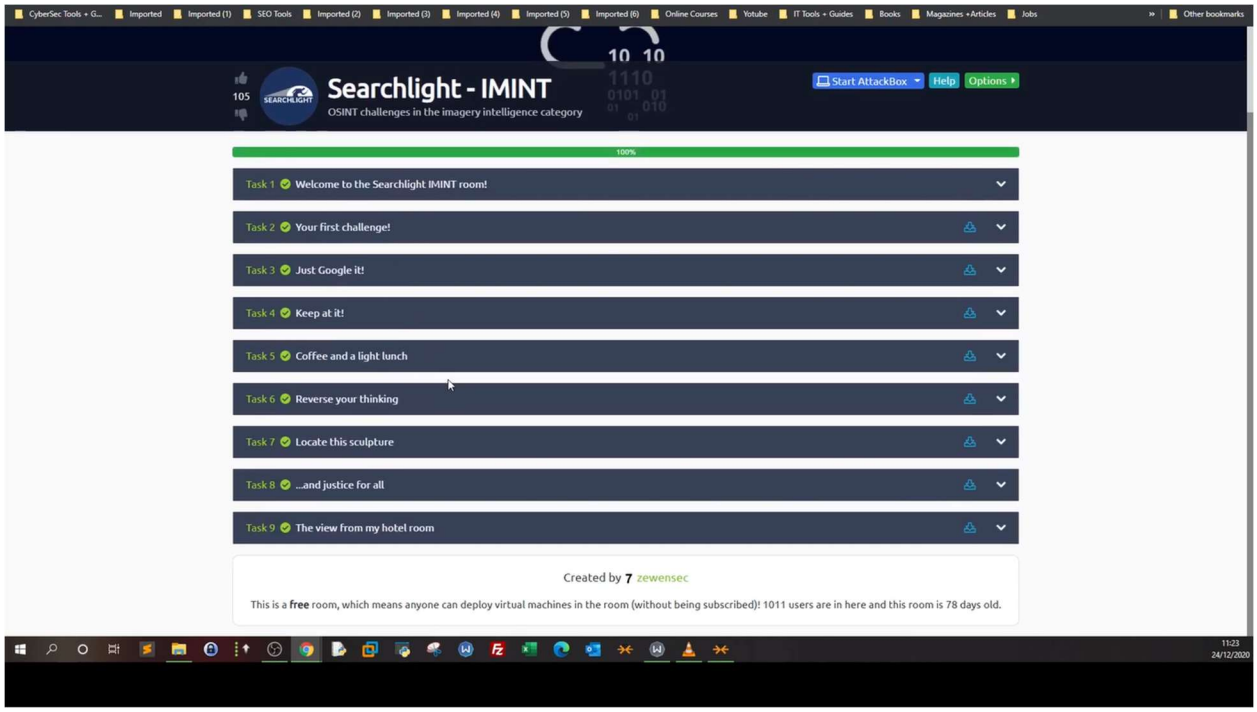
2.Email Addresses: Analysis of email addresses associated with the target led to potential contact points and additional information.

3.Google Dorking: Advanced Google search queries revealed specific documents and resources related to the target, including PDFs and other files.

4.Internet-Facing Assets: Through the use of specialized search engines like Shodan and Censys, information about the target's internet-facing assets, such as exposed web servers and devices, was identified.

Conclusion:

The OSINT Search Light exercise on TryHackMe served as an effective way to develop skills in searching for information from open sources. OSINT is a valuable discipline in cybersecurity and threat intelligence, helping professionals assess an entity's online presence and identify potential risks.



8. Shodan:

Shodan is a powerful search engine that allows users to find specific types of internet-connected devices and gather information about them. The Shodan exercise aimed to develop skills in using Shodan effectively to discover and analyze internet-connected devices.

The primary objective of the Shodan exercise was to enhance skills in searching for and analyzing internet-connected devices using the Shodan search engine. Shodan is a valuable tool for cybersecurity professionals to assess the exposure of devices and services on the internet.

During the Shodan exercise, the primary tool used was the Shodan search engine. Key techniques included:

1.Shodan Search Queries: The use of specific search queries to find internet-connected devices, services, and vulnerabilities.

2.Analysis of Device Information: Analyzing the information provided by Shodan, including open ports, banners, and potential vulnerabilities.

The Shodan exercise yielded the following findings and outcomes:

1.Exposed Internet-Connected Devices: Through Shodan search queries, various internet-connected devices were discovered, including web servers, routers, IP cameras, and more.

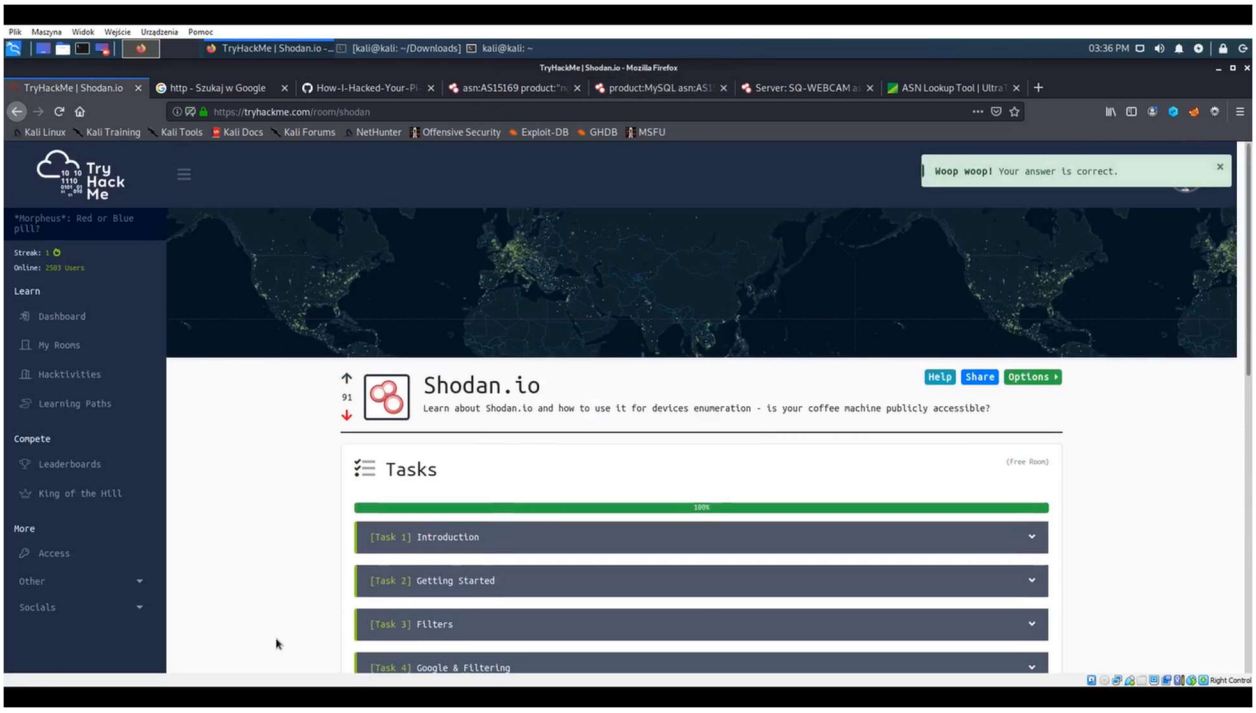
2.Open Ports: Analysis of device information revealed open ports, providing insights into the services and protocols running on these devices.

3.Banner Information: Banner information from open ports helped identify specific software and versions in use, which is crucial for assessing potential vulnerabilities.

4.Vulnerability Assessment: Based on the information gathered from Shodan, potential vulnerabilities in internet-connected devices were identified. These vulnerabilities could pose security risks if not properly addressed.

Conclusion:

The Shodan exercise on TryHackMe served as an effective way to develop skills in using the Shodan search engine to discover and analyze internet-connected devices. Shodan is a valuable tool for cybersecurity professionals to assess the exposure of devices and services on the internet and identify potential security risks.



9. Vulnversity:

Vulnversity is a vulnerable virtual machine designed for educational purposes, allowing users to practice penetration testing and ethical hacking techniques on a controlled environment. This exercise aimed to enhance skills in identifying and exploiting vulnerabilities.

The primary objective of the Vulnversity room exercise was to develop skills in identifying and exploiting common security vulnerabilities found in web applications and services. The exercise provided an opportunity to practice penetration testing techniques in a controlled and ethical environment.

During the Vulnversity exercise, various tools and techniques were employed, including:

1.Nmap: Used for network reconnaissance to identify open ports and services.

2.Gobuster: Utilized for directory and file brute-forcing to discover hidden resources.

3.Exploitation Frameworks: Tools like Metasploit were used to exploit identified vulnerabilities.

4.Manual Exploitation: Techniques such as SQL injection and command injection were applied manually to exploit vulnerabilities.

The Vulnversity exercise led to the following findings and outcomes:

1.Open Ports: An Nmap scan identified open ports on the target, including port 22 (SSH) and port 80 (HTTP).

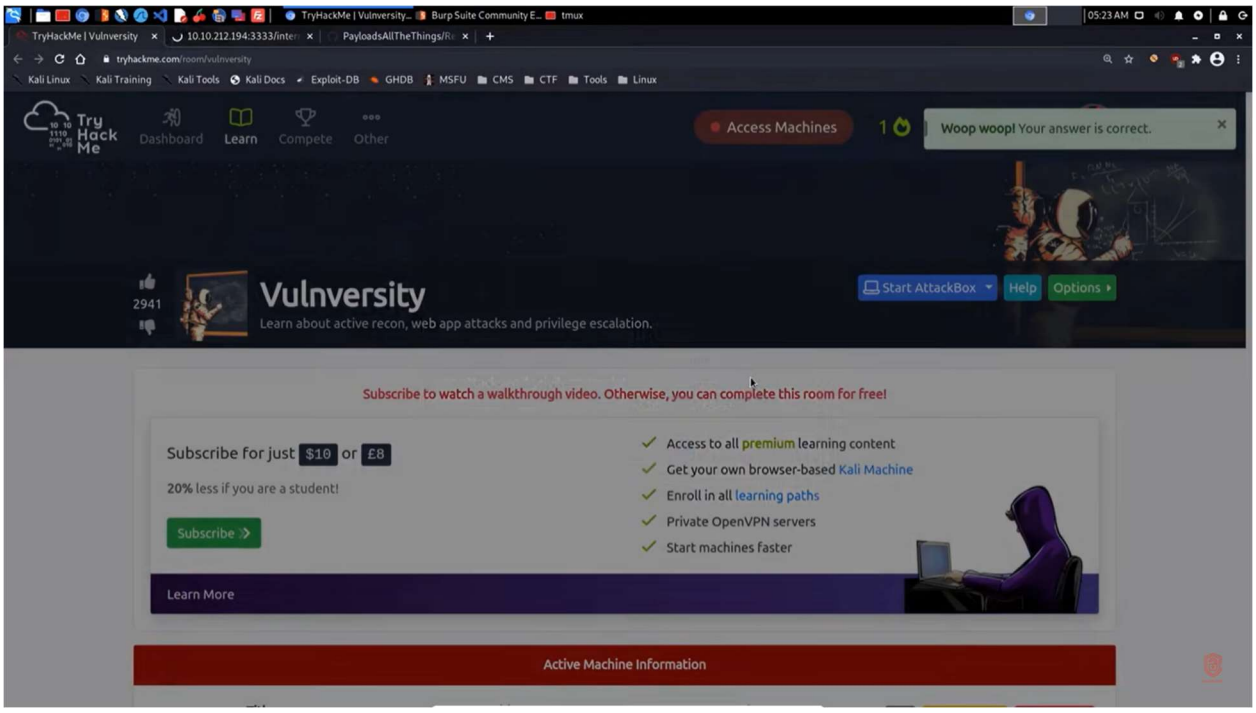
2.Web Application Vulnerabilities: The web application hosted on port 80 was found to be vulnerable to common web application vulnerabilities, including SQL injection and command injection.

3.Exploitation: Exploitation of the identified vulnerabilities was successfully performed, gaining unauthorized access to the target system and its files.

4.Privilege Escalation: Techniques for privilege escalation were applied to gain higher-level access within the compromised system.

Conclusion:

The Vulnversity room exercise on TryHackMe provided a valuable opportunity to practice penetration testing and ethical hacking techniques in a controlled environment. By identifying and exploiting common security vulnerabilities, participants gained insights into the importance of secure coding and vulnerability management.



10. Webohsint:

Web OSINT involves gathering publicly available information from web sources to gain insights and intelligence. This exercise aimed to develop skills in using OSINT techniques to extract information from web-based resources effectively.

The primary objective of the Web OSINT exercise was to enhance skills in conducting OSINT investigations on web sources. It focused on identifying and gathering information from publicly accessible web pages, websites, and online platforms to gain insights into a target's online presence and activities.

During the Web OSINT exercise, various tools and techniques were employed, including:

1.Google Search: Standard Google search was used with specific queries and operators to find information about the target.

2.Social Media Analysis: Profiles and posts on social media platforms like Twitter, LinkedIn, and Facebook were analyzed to gather information about the target's online presence and associates.

3.Email Address Analysis: Analysis of email addresses associated with the target to find potential leads or information.

4.Domain Name Lookup: Domain name lookup tools and WHOIS databases were used to obtain information about the target's domain registration and ownership.

The Web OSINT exercise yielded the following findings and outcomes:

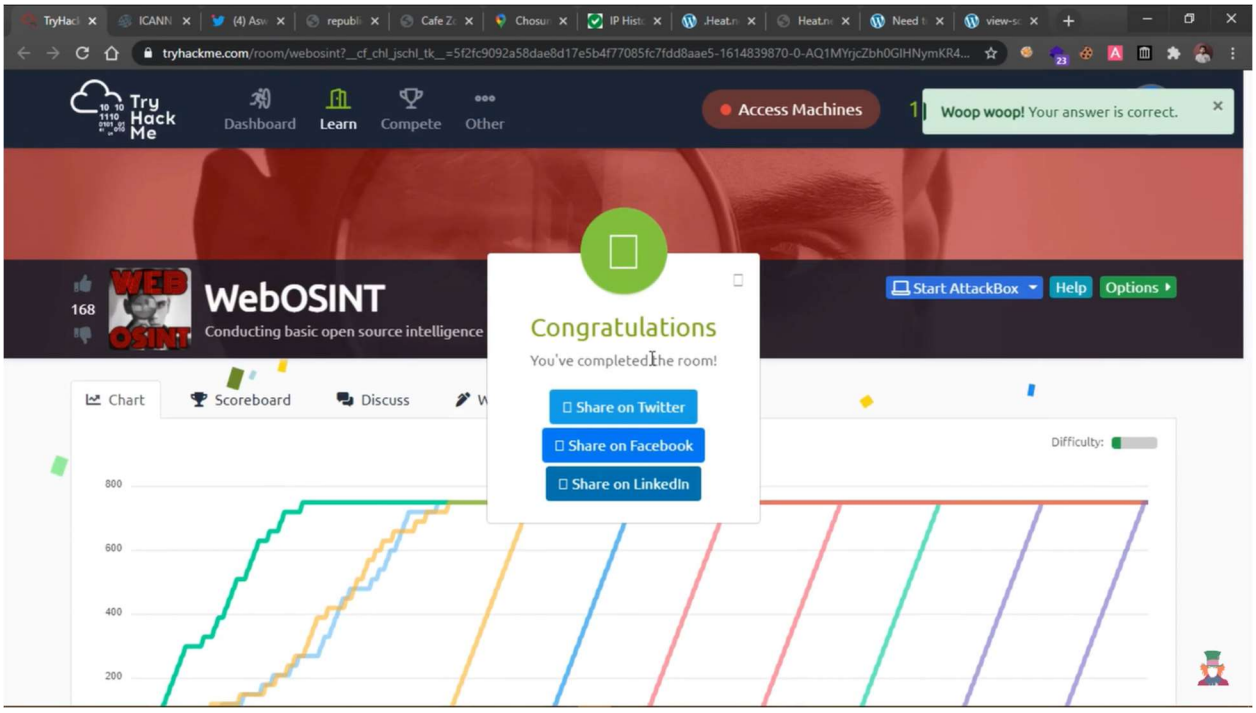
1.Online Profiles: By searching for the target's name and associated information on Google and social media platforms, online profiles, including LinkedIn and Twitter, were discovered. These profiles provided insights into the target's professional and personal life.

2.Email Addresses: Analysis of email addresses associated with the target led to potential contact points and additional information.

3.Domain Information: Using domain lookup tools and WHOIS databases, information about the target's domain registration, including the registrar and domain owner's contact details, was identified.

Conclusion:

The Web OSINT exercise on TryHackMe served as an effective way to develop skills in gathering information from web-based sources. Web OSINT is a valuable discipline for cybersecurity professionals to assess an entity's online presence and identify potential risks.



Note:

I can’t complete Sakura room because of some critical medical conditions and I honestly don’t understand that room.