EyeQ Dot Net Pvt. Ltd.

LEARN FROM REAL HACKERS

TASK 1: CYBERSECURITY: RESEARCH REPORT

What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and data from digital attacks, unauthorized access, and damage orchestrated by threat actors. It involves implementing security measures to safeguard information (PII and SPII) and ensure privacy. Key components include detecting vulnerabilities, responding to threats, and preventing future attacks. Cybersecurity is essential for maintaining the integrity, confidentiality, and availability of sensitive information in today's digital world.

Who needs Cybersecurity?

Cybersecurity is essential for anyone using digital devices, from individuals to large organizations. Businesses need it to protect sensitive data, financial transactions, and customer information from cyber threats. Governments rely on cybersecurity to safeguard national security and critical infrastructure. Even individuals require cybersecurity to protect personal information and prevent identity theft or online fraud. As long as there is a cyber world there is cybersecurity.

How many categories are there in security?

Security is generally divided into several categories, each focusing on different aspects of protection. The main 6 categories include:

1. **Network Security:** Protects networks from unauthorized access, attacks, and breaches.

2. **Information Security:** Safeguards the integrity, confidentiality, and availability of data.

3. **Application Security:** Focuses on securing software and applications from vulnerabilities.

4. **IoT Security:** IoT Security involves protecting connected devices and networks in the Internet of Things from cyber threats.

5. **IAM:** IAM (Identity and Access Management) ensures that the right individuals access the appropriate resources securely.

6. **Cloud Security:** Secures data, applications, and services stored in cloud environments.

What is cybersecurity awareness, and what is cybercrime?

Cyber Awareness:

Cybersecurity awareness refers to educating individuals and organizations about the risks and best practices for staying secure online. It involves understanding common threats like phishing, malware, and social engineering, and how to prevent them. By promoting awareness, people can recognize potential cyberattacks and take steps to protect sensitive information (SPII). Building cybersecurity awareness is crucial for reducing vulnerabilities and enhancing overall security posture.

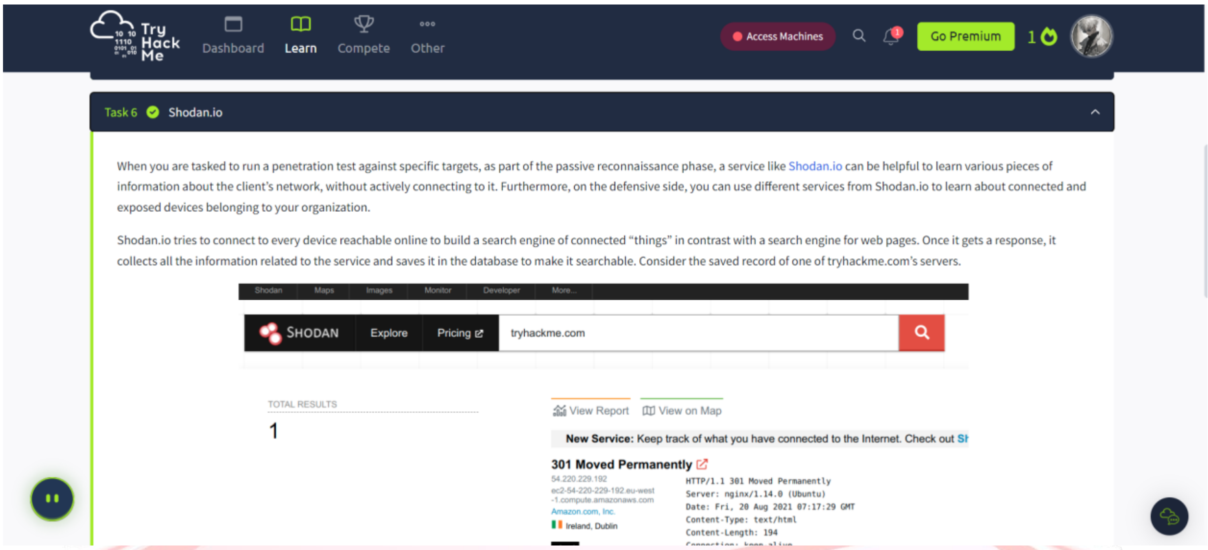
Cybercrime:

Cybercrime refers to illegal activities carried out using computers or the internet, targeting individuals, organizations, or governments. It includes actions like hacking, data theft, online fraud, and spreading malware. One example of cybercrime is phishing, where attackers trick users into revealing sensitive information, such as passwords or financial details, through deceptive emails or websites. Cybercrime poses a significant threat to global security and privacy, requiring constant vigilance and protective measures.

What will happen if there is no cybersecurity?

Without cybersecurity, sensitive data would be vulnerable to theft and exploitation, leading to significant financial and reputational damage for individuals and organizations. For instance, a major hospital could experience a ransomware attack, paralyzing its operations and compromising patient details. This could result in loss of trust from patients and hefty costs for recovery and legal liabilities. Ultimately, the absence of cybersecurity measures would create an environment where cybercriminals could operate freely, jeopardizing safety and privacy across all sectors.

Cybersecurity Training on TryHackMe:



Task 6 Shodan.io

When you are tasked to run a penetration test against specific targets, as part of the passive reconnaissance phase, a service like Shodan.io can be helpful to learn various pieces of information about the client's network, without actively connecting to it. Furthermore, on the defensive side, you can use different services from Shodan.io to learn about connected and exposed devices belonging to your organization.

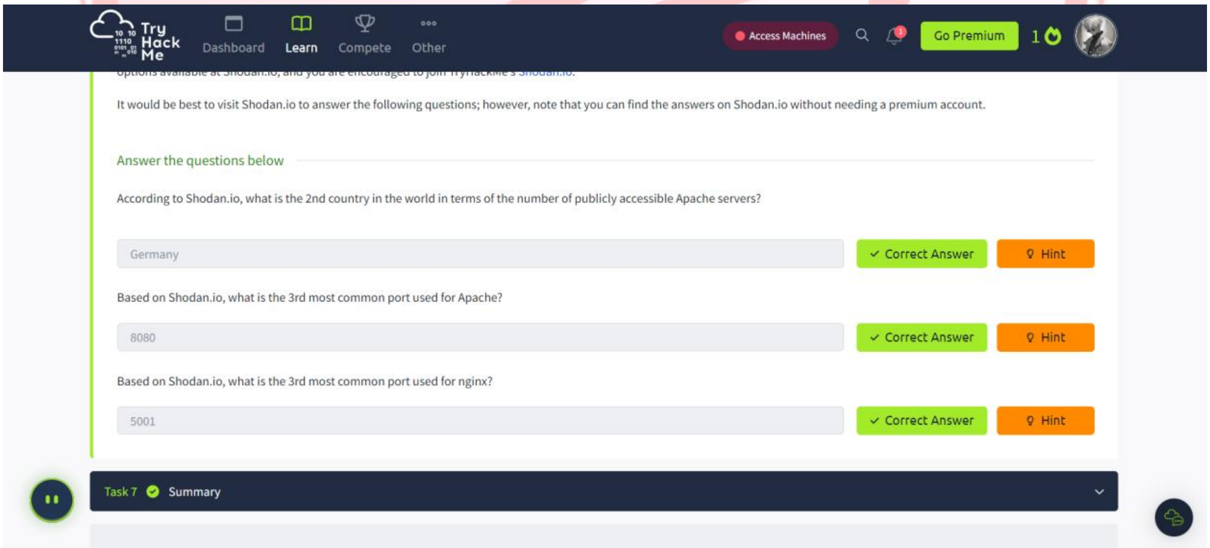
Shodan.io tries to connect to every device reachable online to build a search engine of connected "things" in contrast with a search engine for web pages. Once it gets a response, it collects all the information related to the service and saves it in the database to make it searchable. Consider the saved record of one of tryhackme.com's servers.

New Service: Keep track of what you have connected to the Internet. Check out Sh

301 Moved Permanently

54.220.229.192
ec2-54-220-229-192.eu-west-1.compute.amazonaws.com
Amazon.com, Inc.
Ireland, Dublin

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.14.0 (Ubuntu)
Date: Fri, 20 Aug 2021 07:17:29 GMT
Content-Type: text/html
Content-Length: 194
Connection: keep-alive
```



options available at Shodan.io, and you are encouraged to join TryHackMe's Shodan.io.

It would be best to visit Shodan.io to answer the following questions; however, note that you can find the answers on Shodan.io without needing a premium account.

Answer the questions below

According to Shodan.io, what is the 2nd country in the world in terms of the number of publicly accessible Apache servers?

Germany ✓ Correct Answer Hint

Based on Shodan.io, what is the 3rd most common port used for Apache?

8080 ✓ Correct Answer Hint

Based on Shodan.io, what is the 3rd most common port used for nginx?

5001 ✓ Correct Answer Hint

Task 7 Summary

References:

TryHackMe | Cyber Security Training