1.reconnaisance

2.owasp10,NIST framework,sans25

3. Today your teams have to work on some programming.

Details:

1. Write a program to scrape the web page urls on google.com and open individual urls and scrape the data.

And store everything in document format as results.

2. Write a small script to scan the target given input by user and perform the information gathering like subdomains, technical information, port scanning, other details. Etc. then conduct security audit like finding the vulnerabilities show in results.

Use any programming language try to develop.

Hello Team Leads, today there might be a meeting of Batch 1 all Teams.

This is for everyone today Research:

1. Start working on writing 2 research articles.

Details: Take any topics which are related to cybersecurity. Articles should be unique. Our team will evaluate and best articles going to be published on our company blog.

Note: Try to research and write articles. No Ai is going be use in any case.

2. Prepare the attack lab scenario for any type of attack with detailed report.

Example injection attack scenarios including attacking tools and damages. You can choose any type of attack on any target(Web, Network, Cloud, Mobile, API, IoT,)

3. Prepare the security controls and measures for the previous attacks with detailed Roadmap.

Reports Submission:

Share the zip files along with your full name and IMAGE of you. If any articles are selected your details will

Posted on our Blog.

Q: All Team leads share the information with your teammates. Research and prepare the road map to conduct security audit on Cloud and API.

Which security configurations are mainly causing the damage to the targeted infrastructure and its impact. Any licensed tools or open source repos to use for security audit.

Along with this daily article submission