

Assignment on Securing Systems for CS50 Cybersecurity

1 message

Google Forms <forms-receipts-noreply@google.com>
To: ekrishnachaitanya2004@gmail.com

13 June 2024 at 18:42

Google Forms

Thanks for filling in [Assignment on Securing Systems for CS50 Cybersecurity](#)

Here's what was received.

Assignment on Securing Systems for CS50 Cybersecurity

All assignments in CS50 Cybersecurity are out of 10 points. A score of 7 points or better (70%) is required to be considered to have "passed" an assignment in this course. **Please do not resubmit an assignment if you have already obtained a passing score**--we consider that spam, and if detected, the submission will be deleted, meaning you will not receive the score back anyway. You don't receive a final grade at the end of the course, so it will have no bearing on your certificate, and it will only slow down our graders!

Unlike CS50x, assignments in this course are graded on a set schedule, and depending on when you submitted, it may take up to three weeks for your work to be graded. Do be patient! Project scores and assignment status on cs50.me/cs50cy (e.g. "Your submission has been received...") will likely change over time and are not final until the scores have been released.

Email *

ekrishnachaitanya2004@gmail.com

Name *

KRISHNA CHAITANYA

edX Username *

eKRISHNA2004

What is your GitHub username? *

If you do not already have a GitHub account, you can sign up for one at <https://github.com/join>. You can then use this account to log in to cs50.me/cs50cy to track your progress in the course (your progress will only show up after you have received at least one score release email from CS50 Bot, so do be patient!). Don't worry about seeing a 'No Submissions' message on submit.cs50.io, if you find that. The course collects submissions using Google Forms, and only the gradebook on cs50.me/cs50cy is important!

- **Be certain the username you provide is correct!** If you provide the wrong username, you will not be able to see your scores.
- **Your GitHub username should not be changed while you are taking this course.** The current gradebook system is not designed to accommodate name changes.
- **Be sure to remove extraneous characters,** such as an @ prefix. Do not input a URL or email address, just your username.

ekrishnachaitanya2004

City, State, Country *

Srikalahasthi,Andhra Pradesh,India.

This course is graded by human graders, and has a ZERO TOLERANCE plagiarism and collaboration policy. If *any* of your answers are copied and pasted from, or obviously based on (a) an online source, including non-course-sanctioned generative AI tools or (b) another student's work in the course, in *any* of the course's five assignments or the final project, you will be reported to edX and removed from the course immediately. There is no opportunity for appeal. There are no warnings or second chances. *

It is far better, we assure you, to leave an answer blank rather than risk it. This may be an online course, but it is offered by Harvard, and we're going to hold you to that standard. **The full essence of all work you submit to this course should be your own.**

I understand this policy and agree to its terms; I hereby affirm that I will not plagiarize any



answers in this course.

SETI@Home

[SETI@Home](#) was a distributed-research computing project that largely ran from 1999–2020.

Distributed computing is a network-driven tactic to leverage the processing power of many computers at once to, in this case, analyze radio signals captured from deep space in the hopes that those signals might reveal information about the presence of extraterrestrial life in the universe.

SETI@Home Wallpaper

Captionless Image

What type of cybersecurity threat is perhaps most uniquely, given the nature of it, a risk in a research project like SETI@Home, and how might that threat materialize?

In a research project like SETI@Home, the most uniquely relevant cybersecurity threat is the risk of data tampering or falsification by malicious volunteers. This threat could materialize through various methods, such as altering the software to submit falsified data mimicking potential extraterrestrial signals, intentionally corrupting work units, or exploiting vulnerabilities in the BOINC platform to gain unauthorized access to central servers or other volunteers' computers. These actions could undermine the integrity of the research, lead to false conclusions, and cause scientists to waste time and resources on invalid data.

What are zero-day attacks and why are they a threat?

Zero-day attacks exploit software vulnerabilities that developers haven't yet addressed, leaving systems vulnerable without any available fixes. Attackers can strike swiftly, affecting numerous users and systems with minimal defenses in place. This unpredictability makes zero-day attacks particularly dangerous, capable of causing widespread disruption and compromising sensitive information.

What is port scanning and how is it a threat?

Port scanning probes networks to find open ports, crucial for data exchange. Attackers exploit it to map networks, pinpoint vulnerabilities, and gather application data, posing threats like unauthorized access, data theft, and service disruption. Port scans can bypass security

measures, so organizations use firewalls, audits, segmentation, and monitoring to prevent breaches effectively.

What are supercookies? Via what means do we most commonly obtain/receive them, and how do they create threats to our systems?

Supercookies are advanced tracking tools that gather user data across websites without consent. They use methods like embedding identifiers in HTTP headers and Flash cookies. They threaten privacy by tracking browsing history, pose security risks with stored sensitive data, and persistently reinstall themselves. Mitigation involves browser data clearing and using privacy tools.

What makes a *worm* distinct from a *virus*?

A worm spreads autonomously across networks, replicating without requiring host files, which leads to fast and widespread infections. In contrast, viruses rely on user actions to spread by infecting files, affecting individual systems at a slower pace. Detection and removal methods vary, with worms typically monitored via network traffic analysis and viruses detected through file scanning and signature recognition processes.

Provide a technological example of "security through obscurity".

Non-Standard Ports for Services, Utilizing private, Customized ports for services

Distinguish the concepts of SSH and VPN.

SSH is focused on securing remote access and file transfers specifically, encrypting individual sessions or transfers. In contrast, VPNs provide broader security by encrypting all internet traffic, ensuring privacy, and enabling secure remote access to networks. SSH is primarily utilized in administrative and development contexts, whereas VPNs are employed for safeguarding internet activities, enhancing privacy, and bypassing geo-restrictions to access restricted content.

What purpose does the X.509 standard serve?

The digital certificate standard X.509 is used for secure network encryption and identification.

Why might a company want to perform pen testing?

A company might perform penetration testing to find and fix security weaknesses before hackers can exploit them. This helps improve security, protect sensitive data, prevent financial losses, and build customer trust. By addressing these vulnerabilities, pen testing helps keep the company's systems and information safe from cyberattacks.

Of the below [HTTP status codes](#), which most likely suggests that a distributed denial of service (DDoS) attack may be occurring?

- ☐ 200 OK
- ☐ 304 Not Modified
- ☐ 307 Temporary Redirect
- ☐ 403 Forbidden
- ☐ 404 Not Found
- ☐ 429 Too Many Requests
- ☒ 503 Service Unavailable

Feedback

How did you find the difficulty of this assignment?

*

1 2 3 4 5

Too easy



Too hard

About how many MINUTES would you say you spent on this assignment?

*

Just to set expectations for future students.

Create your own Google Form
Report Abuse