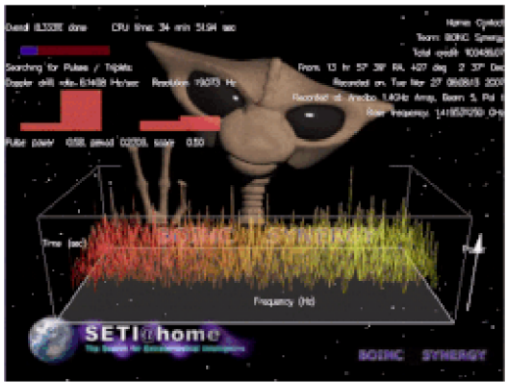
SETI@Home

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



✕ 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? 0/1

I would say that the most unique cyber security threat is a malicious data poisoning attack. Malicious data poisoning occurs when an attacker intentionally corrupts or manipulates data processed by a distributed computing system. In the case of SETI@Home, this could involve one or more volunteer computers from the attacker altering the radio signal data being analyzed.

What are zero-day attacks and why are they a threat? 1/1

This is a type of attack that mainly targets unknown vulnerabilities.
We call such vulnerabilities zero-day because they are exploited early or on day zero. When multiple vulnerabilities are discovered, it leaves no option for engineers and developers to stop the attack.
This type of attack is very dangerous because of the long time it takes to find and fix it.

What is port scanning and how is it a threat? 1/1

This is a technique for discovering open network ports. It performs penetration testing by sending dozens of requests (das or ddas) simultaneously and sequentially to determine which ports are open for connection.
While this is a legitimate way to manage a network, it can be used maliciously to gather information about vulnerabilities. That is why it can be a threat.

What are supercookies? Via what means do we most commonly obtain/receive them, and how do they create threats to our systems? 0/1

They are a type of tracking used in web browsers to store user data and browsing history. They are called super cookies because they are not deleted even after regular cookies are completely deleted and destroyed. They usually store a large amount of data, mainly in the browser's local memory. And if someone can eavesdrop on those cookies, they can impersonate you and access your history and data without your consent and abuse them. If you use HTTP instead of HTTPS, there is always someone else who can get hold of your information. Therefore, it can be a threat to us.

What makes a *worm* distinct from a *virus*? 1/1

1.worms Can operate independently, without the need for a host program but Viruses Typically require a host program to function and spread.
2. worms Often engage in network activity, such as scanning for vulnerable hosts, spreading to new systems, or communicating with command and control servers but Viruses Usually don't engage in network activity, focusing on local system infection.

✓ Provide a technological example of "security through obscurity". 1/1

We can use custom port numbers so that there is no known port in our system.

✓ Distinguish the concepts of SSH and VPN. 1/1

SSH is a protocol used for secure remote access to a computer or network. It provides a secure channel for data transfer, allowing users to access and manage remote systems, execute commands, and transfer files. SSH uses encryption and authentication to ensure the confidentiality and integrity of data.

A VPN is a network technology that creates a secure, encrypted connection between two endpoints, typically a user's device and a VPN server. This connection, often referred to as a tunnel, allows users to access a remote network as if they were directly connected to it.

✓ What purpose does the X.509 standard serve? 1/1

X.509 is a standard for Public Key Infrastructure (PKI) that serves various purposes in cryptography and secure communications. It defines the format and structure of digital certificates that are used to establish trust and verify the identity of entities and devices.

✗ Why might a company want to perform pen testing? 0/1

to perform penetration testing operations and receive company security violations in the form of a report from these people to improve their security.

✓ Of the below HTTP status codes, which most likely suggests that a distributed denial of service (DDoS) attack may be occurring? 1/1

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

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.

12