Homework 13: Examining an Open-Source Honeypot

1. Start a Web browser, if necessary, and go to opencanary.org.
2. Read through the OpenCanary homepage.

A screenshot of a computer

Description automatically generated

1. Under the Services section, click the Linux Web Sever link and review the configuration file presented to the screen.

A screenshot of a computer

Description automatically generated

1. What ports does the configuration file enable, and what software is served from these ports?

In the Linux Web Server configuration, OpenCanary enables several ports for emulating services. It enables FTP on port 21, with the banner set to "FTP server ready." The HTTP service is enabled on port 80 with the banner "Apache/2.2.22 (Ubuntu)" and offers optional login skins, such as "basicLogin" or "nasLogin" designed to mimic a Synology NAS login page. Additionally, SSH is enabled on port 8022 with the SSH version banner "SSH-2.0-OpenSSH\_5.1p1 Debian-4," making it appear like a legitimate SSH service.

1. Go back to the homepage and click the following links and review the configurations for each: Windows Server, MySQL Server, MSSQL Server.
2. Navigate around the other sections.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

1. What are all the services that OpenCanary currently supports faking natively?

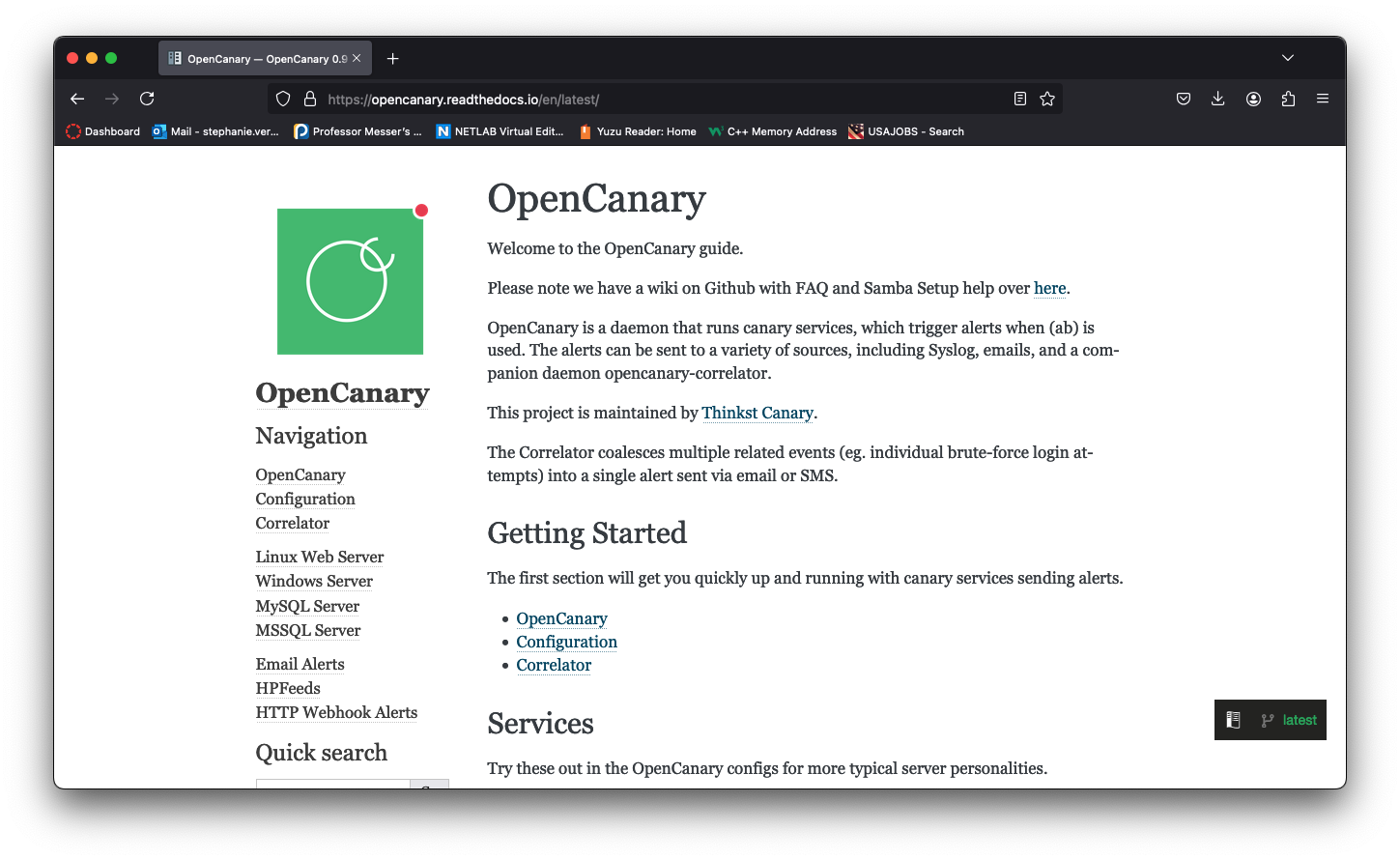
OpenCanary can natively emulate several common server types, including Linux Web Server, Windows Server, MySQL Server, and MSSQL Server. Each of these services can be customized to look realistic, with specific banners, ports, and login screens that enhance the illusion of genuine services, increasing the chances that attackers will interact with them.

1. Summarize what OpenCanary is, where you would set it up, how you would go about setting it up, and how you would be alerted upon intrusion.

OpenCanary is an open-source honeypot tool designed to detect unauthorized access by emulating common services attackers target. It works by setting up these fake services such as FTP, HTTP, SSH, and server databases and triggering alerts whenever someone tries to access them. The goal is to make attackers think they are interacting with real services, which allows administrators to detect suspicious activity early.

Setting up OpenCanary is straightforward. You install it on a server one that’s not critical and then adjust the .opencanary.conf file to choose which services to simulate and on which ports. Once it’s set up, OpenCanary runs in the background, monitoring for any interactions with these fake services.

If an attacker tries to access one of these services, OpenCanary can send alerts in several ways. It can log events, send emails, trigger webhooks, and even send text alerts with the Correlator tool, which links separate security events to find patterns that might signal an attack.



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated