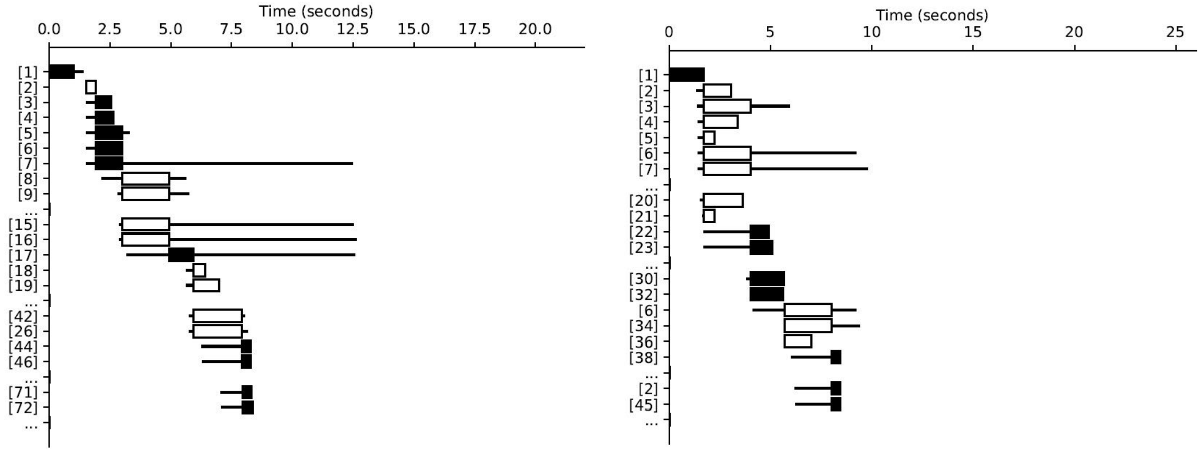
SCENARIO #4: Website Fingerprinting

Scenario:

The foundational principles of the Internet, such as universality of access and transparency, have been steadily diminishing. While individuals are not explicitly denied their right to full internet access, the prevalence of Internet censorship is escalating [1,2]. This censorship empowers state agencies to impede the flow of information to and from blacklisted websites. Even when content is encrypted or a proxy is utilized, these agencies can still discern access to targeted websites. One such method is the Website Fingerprinting Attack [3], employing machine learning techniques to recognize unique traffic patterns, as exemplified by accessing the CNN and New York Times website below. Upon detecting a similar traffic pattern, the attacker can obstruct access. However, given the inherent uncertainty in accurately identifying such connections, there is a possibility that censors may compromise service quality through tactics such as randomly dropping packets or throttling traffic [4].



Website fingerprinting attack exploits the differences in traffic pattern when accessing websites, e.g., CNN website (left) and New York Times (right). Note that to access a website is to request and obtain necessary resources such as text, image, video, etc. and the figure shows the resource-by-resource timing information during webpage loading. (https://ieeexplore.ieee.org/document/9693373)

In this laboratory experiment, students will delve into a well-known machine learning attack approach known as k-Nearest Neighbors (kNN). They will collect and analyze traffic patterns from several websites, employ machine learning tools to identify unique traffic characteristics (packet lengths, packet length frequency, packet ordering, and inter-packet timing that are irrelevant to the content itself) [3]. Specifically, students will be provided with a list of well-known websites (assuming black-listed) and will access their main pages using the HTTP protocol to initiate browsing sessions for those websites. They will visit each website 15 times. The objective of the attack is to determine whether the tested traces are from one of the blacklisted websites.

It's worth noting that defenses against website fingerprint attacks are to reschedule the packets or to insert padding units to confuse the attacker [3], which is beyond the scope of this lab experiment.

Additionally, students will explore laws related to digital surveillance from a comparative perspective. They will examine legal issues faced by multinational corporations like Google and Facebook in complying with internet censorship laws in jurisdictions outside the U.S. [5,6].

NICE Workforce Framework for Cybersecurity:

Scenario #3 & #4 will cover the following Knowledge areas.

K0001 Knowledge of computer networking concepts and protocols, and network security methodologies.
K0005 Knowledge of cyber threats and vulnerabilities.
K0007 Knowledge of authentication, authorization, and access control methods.
K0013 Knowledge of cyber defense and vulnerability assessment tools and their capabilities.
K0046 Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
K0049 Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).
K0104 Knowledge of Virtual Private Network (VPN) security.
K0135 Knowledge of web filtering technologies.
K0202 Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).
K0205 Knowledge of basic system, network, and OS hardening techniques.
K0336 Knowledge of access authentication methods.

References:

[1] R. Deibert, J. Palfrey, R. Rohozinski, J. Zittrain, and J. G. Stein, Measuring Global Internet Filtering. MIT Press, 2008.

[2] P. Winter and S. Lindskog, How the Great Firewall of China is blocking Tor. USENIX-The Advanced Computing Systems Association, 2012.

[3] T. Wang and I. Goldberg, Walkie-talkie: An efficient defense against passive website fingerprinting attacks, in 26th USENIX Security Symposium (USENIX Security 17), 2017, pp. 1375-1390.

[4] R. Ensafi, J. Knockel, G. Alexander, and J. R. Crandall, Detecting intentional packet drops on the internet via tcp/ip side channels, in International Conference on Passive and Active Network Measurement. Springer, 2014, pp. 109-118.

[5] Content regulation - what's the (online) harm?, https://edri.org/content-regulation-whats-the-online-harm/

[6] Illegal and harmful content, https://www.esafety.gov.au/key-issues/Illegal-harmful-content