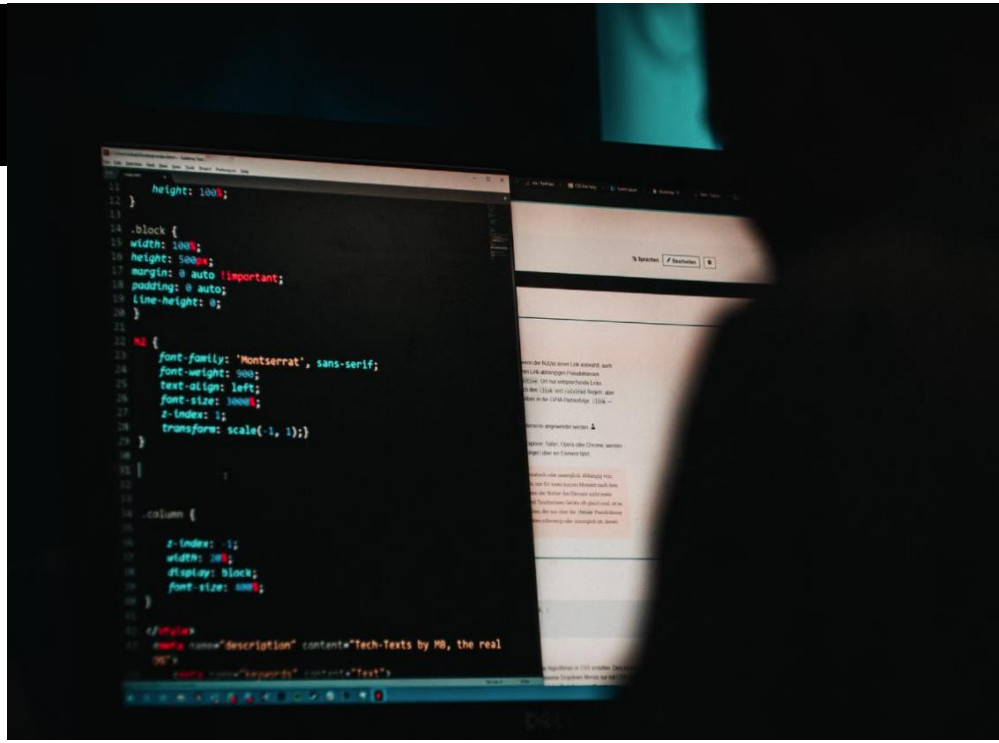
FANSHAWE

INFO-6065

Ethical Hacking & Exploits

Special Topics



FANSHAWE

Agenda

- Housekeeping notes
- Crypto Currencies
- Evolving attacks
- Overview of Lab 11

Housekeeping Notes

Housekeeping

Final Exam details:

- **Thursday April 20th @ 10am**
- **Requires Respondus lockdown browser**
- **Requires Respondus monitor**

- Similar format to test 01 and test 02
- You will have 90 minutes to complete the exam once you have logged in
- Password will be sent by email closer to the date

FANSHAWE

Crypto Currencies

FANSHAWE

Crypto Currencies

- There are numerous crypto currencies currently available on the market
- These are digital currencies that are managed without the use of a centralized body
- Transaction records are kept by numerous machines using cryptography

FANSHAWE

Crypto Currencies

Online Exchanges offer the ability for users to buy/sell crypto currencies

- Every user will have a “digital wallet” where their balance is kept
- If a user loses their *wallet* then the funds will not be available to that user
- Wallets use public/private keys
- Not all exchanges are regulated the same way

FANSHAWE

Crypto Currencies

A blockchain is used to validate crypto coins using a ledger

- This ledger is maintained by “miners”
- Miners are nodes in a cryptocurrency network that work together to validate, relay, or maintain a copy of the blockchain
- Miners are typically rewarded by getting a piece of the crypto currency they are supporting

FANSHAWE

Crypto Currencies

Since cryptocurrencies such as BitCoin are digital, it is difficult to track

- This makes it challenging for law enforcement
- These currencies are preferred by criminals when receiving ransom payments because they offer a level of anonymity
- There are a few countries (El Salvador, Cuba) who have adopted BitCoin as legal tender

FANSHAWE

Evolving Attacks

FANSHAWE

Evolving Attacks

- Attackers took notice that more users are working remotely and the increase in potential victims grew
- As the pandemic hit, companies were forced to adjust the way that employees work, mainly having them change to a work-from-home situation

FANSHAWE

Evolving Attacks

- Many businesses were not prepared as they did not have the infrastructure in place to allow remote users access to company network resources
- Implementation was not bullet proof as a lot of setup was done in a hurry

FANSHAWE

Waterhole Attacks

- Attackers avoid having the end user initiate the attack by being tricked into clicking on links or running infected files
- A popular website used by a certain group of individuals is infected with malware
- Targets certain types of individuals who often visit a site that is deemed safe/legitimate by its user group

FANSHAWE

Waterhole Attacks

- In the end, these attacks target the users through a website they visit
- The malicious code the user downloads from the website is just the beginning of the attack
- Further instructions (malware) can be downloaded once the victim is infected
- Initial malware can do a vulnerability scan of the user's machine and report back to the attacker

FANSHAWE

Waterhole Attacks

There have been various popular websites and major organizations that were successfully attacked

Fake Flash updates? Sound familiar? (BeEF)

https://securelist.com/holy-water-ongoing-targeted-water-holing-attack-in-asia/96311/

Waterhole Attacks

These can target specific organizations…

Important Message on New Circulating Spam\Phishing E-mail

ITSD Communication
To

Reply | Reply All | Forward

Tue 2023-03-28 1:47 PM

This message was sent with High importance.

This is a reminder that the **negative impacts to College services when receiving malicious e-mails are caused by Fanshawe Employees clicking on unsolicited e-mail links** claiming to be from any "Fanshawe Service" and filling out their login information. This does include hurting the College's worldwide e-mail reputation status and creating e-mail delays\blockages when Fanshawe accounts attempt to e-mail outside providers.

Please **DO NOT CLICK** on any unsolicited e-mail links that ask you to update your login information or **from sources or people you do not recognize**.

If you do click on a suspicious link requesting your account information, **please let the IT Service Desk know immediately**. It will be much easier to reset your password now, rather than waiting until your account has been used in malicious activity.

In addition, some phishing e-mails will not offer malicious links, **but will masquerade as a Fanshawe Employee asking for help**. Generally, that help will be a **request to purchase gift cards** and to send the card information back via e-mail but can be in the form of **joining other dubious money schemes**.

Here is an example of a malicious spam message that has been circulating and originated from a compromised Fanshawe employee account and providing a job offer:

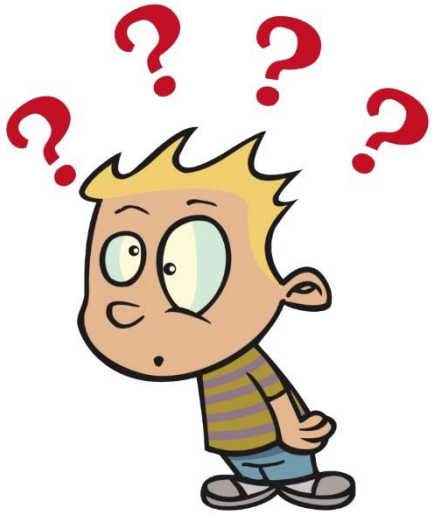
FANSHAWE

Gift Cards

- Involves an attacker phoning someone and pretending to be a person of authority
- Most of the time, the attacker claims to be with the government or a police officer
- Victims are told to purchase gift cards (Google play, etc.) and provide the caller with the PIN of the card
- Victims think they are doing this for legitimate reasons

Gift Cards

- The attacker will use the gift cards to make purchases or sell them online for a portion of the gift card's value
- These gift cards cannot be traced to the attacker as they had someone else do the purchase
- You can avoid this by not buying gift cards for the Police…



FANSHAWE

Gift Cards

- More sophisticated versions of this attack include an attacker discovering the PIN on a gift card but not using it until it is purchased legitimately
- Once the victim activates the card, the balance is updated, and the attacker can now use the funds available on the card before the user has a chance

FANSHAWE

Gift Cards

- This requires the attacker to monitor the card's balance
- The victim will activate the card and the full balance will show up, so it doesn't spook the victim

FANSHAWE

SIM Swapping

- Two-factor authentication is being used more widely
- One-time passwords or PINs are sent through SMS to a person's phone
- These are used in combination with a username and password for various applications
  - Gmail
  - Banking
  - Etc.

FANSHAWE

SIM Swapping

- The problem occurs when an attacker has the ability to retrieve or intercept these SMS messages
- SIM Swapping happens when an attacker is able to convince a mobile provider to port over the victim's phone number to a phone that the attacker controls

FANSHAWE

SIM Swapping

- The attacker is able to reset the victim's accounts
- If access to the victim's primary email account is obtained, that in combination with a compromised phone number may allow the attacker to gain access to most of the victim's accounts
- Social media accounts could be defaced, etc.

FANSHAWE

Smart Homes

- More and more devices have the option of connecting to your home network
- A lot of these will also have an internet connection
  - Security cameras
  - Baby monitors
  - Lights
  - Etc.

FANSHAWE

Smart Homes

Who produces these devices?

- If these devices are manufactured by companies that do not use best practice when it comes to security, they may be inherently vulnerable

How often are firmware upgrades available?

- If there are no updates available, the device cannot be updated if vulnerabilities are discovered

FANSHAWE

Smart Homes

- If an attacker can compromise a smart device through an internet connection, they could potentially move on to other targets on the internal network
- The more connected devices, the more of a chance of exposure and potential vulnerabilities to exploit

FANSHAWE

Smart?

- Sometimes technology enables crime
- This usually begins as a convenience or benefit for legitimate users but attackers will exploit these

Stealing new cars may be easier than old ones…

https://www.youtube.com/watch?v=bR8RrmEizVg

TikTok

You will see grumbling in the news about governments moving to ban TikTok from “government issued” devices

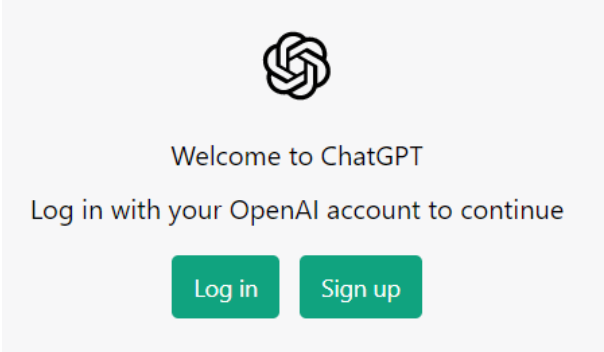
- Does this prevent external access?

FANSHAWE

ChatGPT

ChatGPT took the world by storm when it was introduced in late November 2022 by OpenAI

- ChatGPT 4 was released on March 14, 2023
- Based on Large Language Models (LLMs)



FANSHAWE

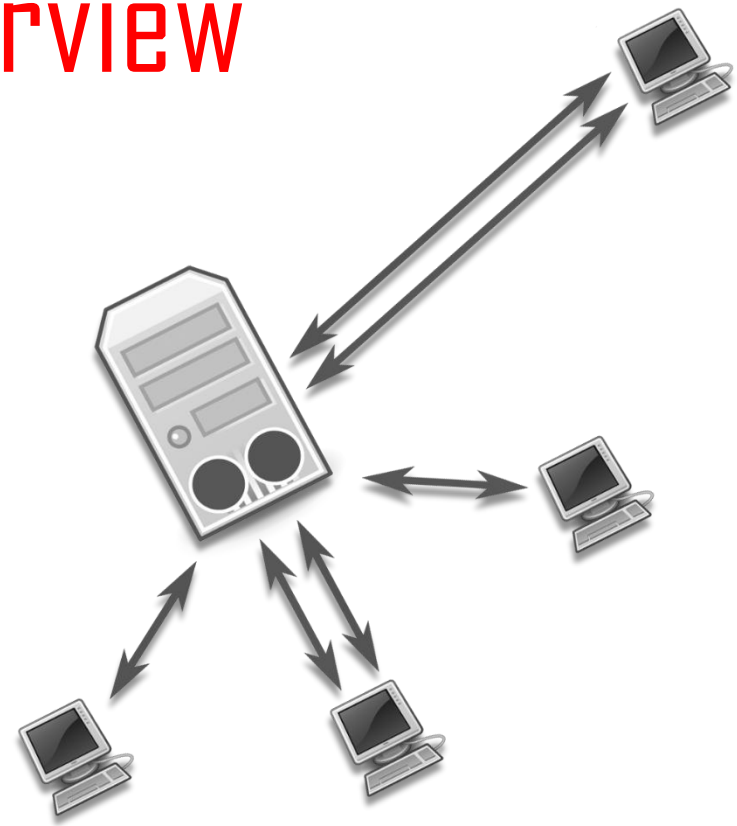
ChatGPT

Institutions are still trying to figure out how to "manage" the use of AI chat bots

- It can be great for certain tasks like updating your Python Code from 2 to 3
- Also has the ability to "hallucinate" and provide answers that are incorrect

FANSHAWE

Lab 11 Overview



FANSHAWE

Lab 11 Overview

- Part 01: Create shellcode for a ProFTPD Exploit on MS2
- Part 02: Inject an image with Jhead
- Part 03: Using exploit-db.com
- Part 04: Using Proxy Chains