Andrew McDonald, CD BA

CYBERSECURITY PROFESSIONAL

About Me

I am an IT professional currently studying cybersecurity at Nova Scotia Community College with 20 years of experience in communications, information security, and IT operations and extensive training and experience using military systems in secret environments.

In my previous role as a Naval Electronics Technician (Communications) with the Royal Canadian Navy (RCN) I was responsible for the function, fault diagnostic, repair, maintenance, and operation of electronic combat systems and communications equipment aboard RCN ships as well as the supervision of junior technicians technically and administratively. Additionally, I have worked extensively with Communication Security (COMSEC) and Information Technology Security (ITSEC) requirements and networks. During this time, I held a Level III (Top Secret) security clearance.

As a student in the field of cybersecurity, I have had experience working with malware, access control systems, intrusion monitoring techniques, auditing, encryption, system hardening, ethical hacking, penetration testing, and network security in line with confidentiality, availability, and integrity of information systems. In addition, I have significant experience working with virtualization technologies.

Cover Letter

Andrew McDonald, CD BA
Cybersecurity Professional
Dartmouth, NS

Phone
902-488-6262
Email
acmcdonald@gmail.com
LinkedIn
www.linkedin.com/in/andrewcmcdonald

To whom it may concern,

As an IT professional and current cyber security student at Nova Scotia Community College with 20 years of experience in communications, information security, and IT operations with extensive training and experience using military systems in secret environments, I am writing to express interest in the Intermediate Security Analyst (SecOps) position at your company.

In my previous role as a Naval Electronics Technician (Communications) with the Royal Canadian Navy (RCN) I was responsible for the function, fault diagnostic, repair, maintenance, and operation of electronic combat systems and communications equipment aboard RCN ships as well as the supervision of junior technicians technically and administratively. I have extensive experience working with technical documentation. Additionally, I have worked with Communication Security (COMSEC) and Information Technology Security (ITSEC) requirements and networks. During this time, I held a Level III (Top Secret) security clearance.

As a student in the field of cyber security, I have had experience working with SIEM and EDR, security incident response, network security zoning, security controls, system hardening, penetration testing, and scripting in addition to proficiency in the Microsoft Office suite of applications including, Word, PowerPoint, and Excel. I am currently working towards obtaining my Security+ certificate.

Due to my extensive experience in technology and national defence, I feel that I would be an excellent addition to your team.

Sincerely,

Andrew McDonald

Resume

Andrew McDonald, CD BA
Cyber Security Professional

Phone
902-488-6262
Email
acmcdonald@gmail.com
LinkedIn
www.linkedin.com/in/andrewcmcdonald

Profile

I am an IT professional with 20 years of experience in communications, information security, and IT operations with extensive training using military systems in secret environments. I am set to complete the Cyber Security Diploma from Nova Scotia Community College, class of 2024. I am seeking a role in the field of cybersecurity with a focus on digital forensics or security operations.

Education

Cyber Security Diploma, *Honours*
Nova Scotia Community College, Halifax, NS — Graduating June 2024

Journeyman Electronics Technician
Naval Engineering School, Halifax, NS — 2014

Defence and Security Certificate, *Honours*
Algonquin College, Ottawa, ON — 2014

Bachelor of Arts (Double Arts Concentration in Political Science and History)
Saint Mary's University, Halifax, NS — 2007

Professional Experience

Security Operations Centre - Tier I Analyst *(Work Term)*
rSolutions — April 2023 – May 2023

- Evaluated security events by triaging and determining severity through source identification, scope assessment, and impact analysis.
- Responsible for delivering initial response and containment measures as well as escalating incidents to higher tiers when necessary.

Naval Electronics Technician
Canadian Armed Forces — March 2010 – October 2022

- Achieved the rank of Master Sailor and was responsible for the supervision of junior technicians technically and administratively.
- Responsible for the function, fault diagnostic, repair, maintenance, and operation of electronic combat systems and communications equipment aboard RCN ships.
- Member of the first team to successfully implement LINK 22 communications between NATO nations.

- Served aboard HMC Ships in numerous multi-national operations at home and abroad.
- Qualified as a Workplace Harassment Advisor, Sentinel (peer mentor), and Security Representative.
- Awarded the Sacrifice Medal and selected to participate as Special Guest to the Chief of Defense Staff for the National Remembrance Day Ceremony in 2019, representing all injured veterans of the CAF.

Signal Operator
Canadian Armed Forces — November 2003 – March 2010

- Responsible for the control, configuration, and management of combat net radios and fiber optic links.
- Operated, administered, controlled, and managed Communication Security (COMSEC) and Information Technology Security (ITSEC) requirements and networks.
- Deployed on Operation ATHENA to Kandahar, Afghanistan as member of the National Support Element in 2008 providing communications in tactical and strategic operations.

Volunteer Experience

Vice President of Communications, Institute of Technology Campus
Nova Scotia Community College Student Association — October 2023 - April 2024

- Responsible for the development and execution of the Student Associations' marketing and communications strategy and overseeing general advertising and promotions.
- Accountable for the general recruitment and management of the Student Association Student's Council including the preparation of monthly Council agendas and minutes.

Work Samples

1. BadUSB
2. Pwnagotchi
3. BASH Scripting
4. Malware
5. Log_Scanning

BadUSB

A BadUSB is a device that resembles an ordinary USB stick but instead emulates a keyboard to send malicious commands to a PC. For this project I took a Raspberry Pi Pico and transformed it into a functional BadUSB though hardware and software modifications. This was a personal project that I took on in my free time to explore building my own tools for cybersecurity.

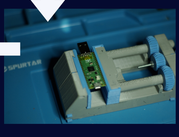
Hardware:

The Pico comes with a Micro USB Type B jack preinstalled, but I wanted a standard connector that would match a regular USB stick such as a male USB Type A plug. I found it best to run a USB A cable across the body of the Pico and have it sticking off the back end rather than have both connectors on the same end in order to shrink the form factor of the BadUSB.

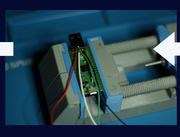
The Pico prepped

Using Kapton tape to prevent shorts

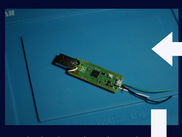
Attaching the USB A plug



Preparing to solder on the leads

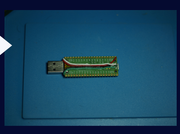


Leads attached to the USB A plug



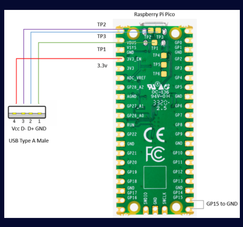
Running the leads to the other side of the PCB

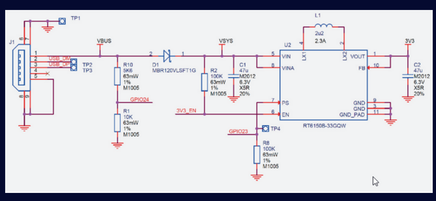
Cable management with some CA glue



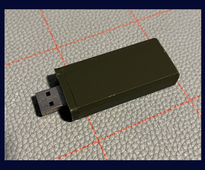
The finished product

The USB Type A plug was wired to the Raspberry Pi Pico as shown below:



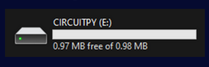


Next, I 3D Printed a case to contain the Raspberry Pi Pico and attempt to make it resemble a normal USB stick.



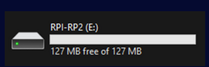
Software:

First, I connected the Raspberry Pi Pico to my PC while holding the BOOTSEL button.



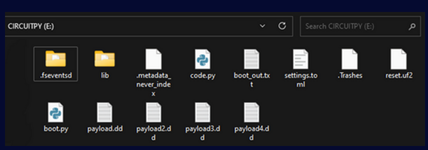
Next, I download MicroPython then transferred the file adafruit-circuitpython-raspberry_pi_pico-en_US-8.1.0.uf2 onto the Pico.

When complete, the Pi reconnected to the PC and looked like this:



Next, I download the files from here and unzipped them. You can use the configuration tool that is included (run.bat) to install the configuration files on the pi.

In the end it should look similar to this:

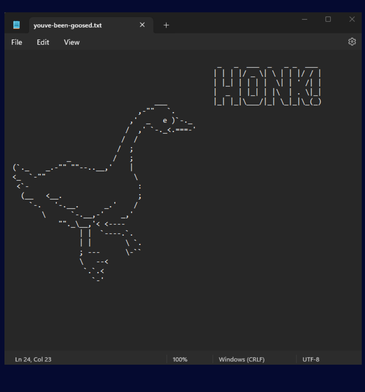


Scripting:

The BadUSB uses DuckyScript to code the malicious payload. The file is then saved on the BadUSB as payload.dd. For this example I created a benign script that opens Notepad, types a document, then saves it to the users machine.

The example script I used can be found here

The output of the script:



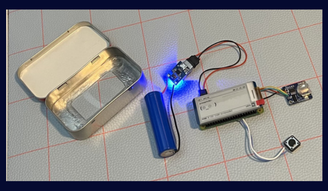
Pwnagotchi

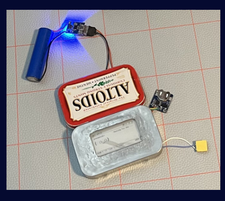
A Pwnagotchi is a mobile device that captures WPA handshakes via passive sniffing or de-authentication attacks. The files are collected as PCAP files and contain handshakes that are supported by hashcat. The name Pwnagotchi is derived from the 90's toy Tamagotchi which was a digital pet that you would feed and take care of. The Pwnagotchi works similarly as you interact with it by feeding the device Wi-Fi handshakes. This was another personal project of mine which again allowed me to work with hardware and software to build my own tools for use in cybersecurity.

Hardware:

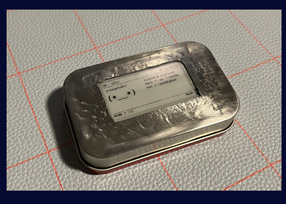
For this project I used a Raspberry Pi Zero W as the base with a 2.13inch E-Ink Display. I wanted the Pwnagotchi to be as stealth as possible so I decided I would install it inside an Altoids tin with the screen on the rear side so that when it is sitting on a desk it is completely incognito. I was concerned that the tin would block the Wi-Fi signals but this turned out to not be a problem.

Next I added a Real Time Clock (RTC) and a power switch to the Raspberry Pi Zero W and installed it inside the Altoids tin with some hot glue. I have yet to successfully get the RTC to work correctly with the Pi and will have to continue to work on it.





I wanted to extend the power and USB inputs out to the side of the tin so i soldered a Micro USB Type B plug to a USB Type B jack on a daughterboard which was attached to the side of the tin.



Software:

Using Balena Etcher, I wrote the pwnagotchi v1.5.5 image to a micro SD card. I then inserted the micro SD Card into the Raspberry Pi Zero W and connected the Pi to my computer using the Pi's data port.

The first boot of the pwnagotchi will take some time as it is generating RSA keys.

When the pwnagotchi is fully booted, the next step is to find out which COM port the pwnagotchi is using as it needs to be changed to an RNDIS device. Using Device Manager, right click on the device listed as 'BCM2708 Boot' --> Properties --> Driver --> Update Driver --> 'Browse my computer for drivers.'

At this point you will need to download the driver here

Once the driver is installed you need to open 'Network Connections' and find the Raspberry Pi Zero W. If you rename the adaptor it will make it easier to find in the future. From here you will have to open the adaptor's properties and then select 'Internet Protocol Version 4 (TCP/IPv4)' and click on properties. Then you will need to assign an IP address of 10.0.0.1, a Subnet Mask of 255.255.255.0, and a Default Gateway of 10.0.0.1.

To test that you have configured the device correctly, open the command prompt and ping the Raspberry Pi Zero W.

In order to use the display you need to create a config.toml file. The config file needs to be pasted into the pwnagotchi's directory.The code for this file can be found here.

At this point, if you boot the pwnagotchi with a power source you should have a working pwnagotchi.

This was a fun project that involved a lot of troubleshooting and exploring documentation to get it to function as intended. There are still configurations that need to be modified and/or adjusted to tune the device so that It works as best as possible but getting it to this point was a huge success.

Bash Scripting - Google Dorks

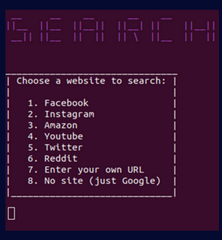
For my final assignment in OSYS2022 - Linux Scripting I wrote a script called 'Dorks' which allows a user to choose from a variety of websites and types of searches to be completed using Google Dorks without the user having to know any of the search commands. This script is written in the BASH command language and can be used to aid in conducting OSINT activities.

The script and how it functions:

Dorks opens with a menu page which prompts you for an input of 1-4:

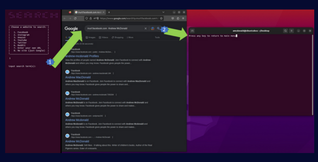
Main Menu

The bulk of the script takes place within the search submenu. When beginning a search, the user is prompted to choose a URL from the list which consists of six of the top 10 most visited sites in Canada (Facebook, Instagram, Amazon, YouTube, and Reddit) as well as an option for using your own URL or simply searching Google directly. If the user chooses options 1-6 they are asked for their search terms, if they choose 7 they are first prompted for a URL and then search terms. Option 8 contains additional options such as Searching for a filetype, searching in the title, searching for related materials, or a simple text search before being prompted for their search terms.

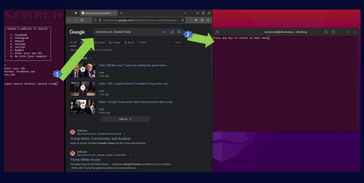


Search Menu

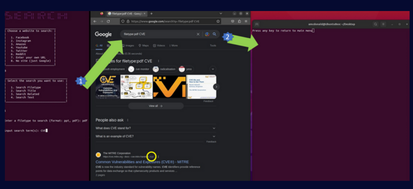
Once all of the data has been collected the script opens a Firefox browser as it is the default browser that comes installed with Ubuntu and completes the requested search with all of the additional search parameters added.



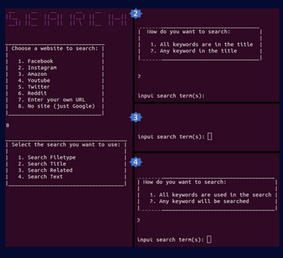
Search Options 1-6



Search Option 7

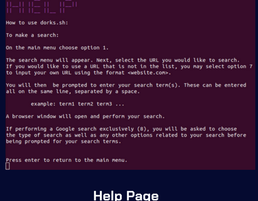


Search Option 8

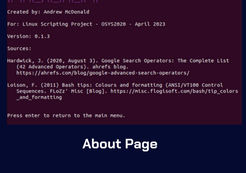


Search Option 8 – Additional Searches

Other main menu options include Help; which explains the user how to conduct a search using the script as well as About; which is an information page.



Help Page



About Page

The code for this script can be found here.

This project was a fun way to get used to making more complex Linux scripts but it could certainly use more development to make it work with more search terms and dorks for other websites.

Malware Development

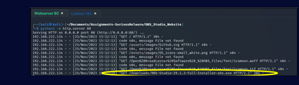
As part of my ISEC2079 - Evolving Technologies and Threats course we learned many ways that threat actors gain access and persistence to machines.

For the assignment that follows I walked through all of the steps that a malicious actor could gain access to a users machine and establish persistence which is important for understanding how to defend against such attacks.

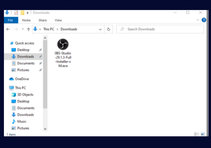
The assignment:

To simulate purchasing a domain in order to trick the user into downloading my fake version of OBS Studio I first made a copy of the real OBS Studio homepage. I then edited the html file and changed the downloads link to point to my own malicious installer file, then ran a python webserver to serve up the fake site:

When the user clicks on the Download button, a request is made to my webserver and the fake OBS Studio that is acting as my malicious installer file is downloaded to the user's downloads directory. The fake OBS file is named "OBS-Studio-30.0-Full-Installer-x64.exe" where I have swapped the first O with a 0 to keep the illusion of legitimacy of the executable without being noticed by the user. I have additionally modified the icon to resemble to real OBS Studio. The code for the malicious installer can be found at https://github.com/ACMCDONALD/Malware-Development-Example/blob/main/Annex%20A:%20OBS-Studio-30.0-Full-Installer-x64.py.

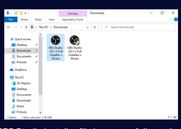


The webserver showing the malicious OBS Studio being downloaded



The malicious installer file is successfully on the users PC

The user then runs OBS-Studio-30.0-Full-Installer-x64.exe which downloads the legitimate OBS Studio installer and begins to install it as they expect.

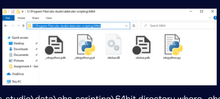


The real OBS Studio installer file is successfully on the users PC

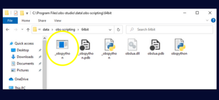
The installation begins

Once the installation is finished, the malicious installer then proceeds to download the payload named "_obspython.exe" from my webserver to the directory C:\Program Files\obs-studio\data\obs-scripting\64bit where it is hidden amongst similarly named files. The code for the payload can be found at https://github.com/ACMCDONALD/Malware-Development-Example/blob/main/Annex%20B:%20_obspython.cpp "Note" I have deleted the malicious portions of the program due to ethical reasons.

The GET request to the webserver for the payload _obspython.exe

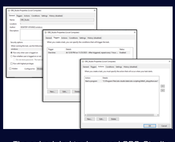


C:\Program Files\obs-studio\data\obs-scripting\64bit directory where _obspython.exe will be housed. Note the similarity in the file names.

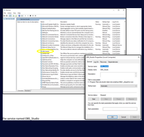


The directory with the payload

Once the payload has been downloaded, the malicious installer then runs commands to establish persistence on the user's machine via both a scheduled task and a service. The scheduled task is named OBS_Studio and it runs every hour. The service is also named OBS_Studio and it is started right after it is created and again every time the machine starts. Both instances run the payload, _obspython.exe, every time they are initiated. The choice to name them both after the software is meant to not raise suspicion if the user is looking at their services or scheduled tasks. With these two instances of persistence in place, if we are to lose the reverse shell, we can get another one within the hour or whenever the system is restarted, ensuring that we can always get our reverse shell back if we lose it for any reason.



The scheduled task named OBS_Studio

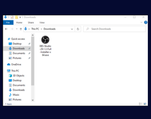


The service named OBS_Studio

Once the service has started via a command in the malicious installer, we have a system level reverse shell on the user's machine.

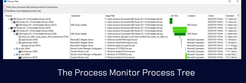
System level reverse shell

Once all of the commands have finished running from the malicious installer on the user's machine, the malicious installer then deletes the copy of the legitimate OBS Studio installer from the downloads directory leaving only the illegitimate OBS Studio installer file.



The user then deletes the fake installer file as they would the legitimate installer, but we still have a reverse shell into their machine.

If we look at Process Monitor while this entire process occurs, we can see that the process tree doesn't look too far off from what a normal program installation looks like.



The Process Monitor Process Tree

When the hash of the payload file is scanned by Virus Total, we come up with a result that 19 of 72 security vendors have flagged the file as malicious; suggesting it will bypass many anti virus programs on the market as of the day the hash was scanned.

The Virus Total score of the payload.

Log Scanning - Anomaly Detection

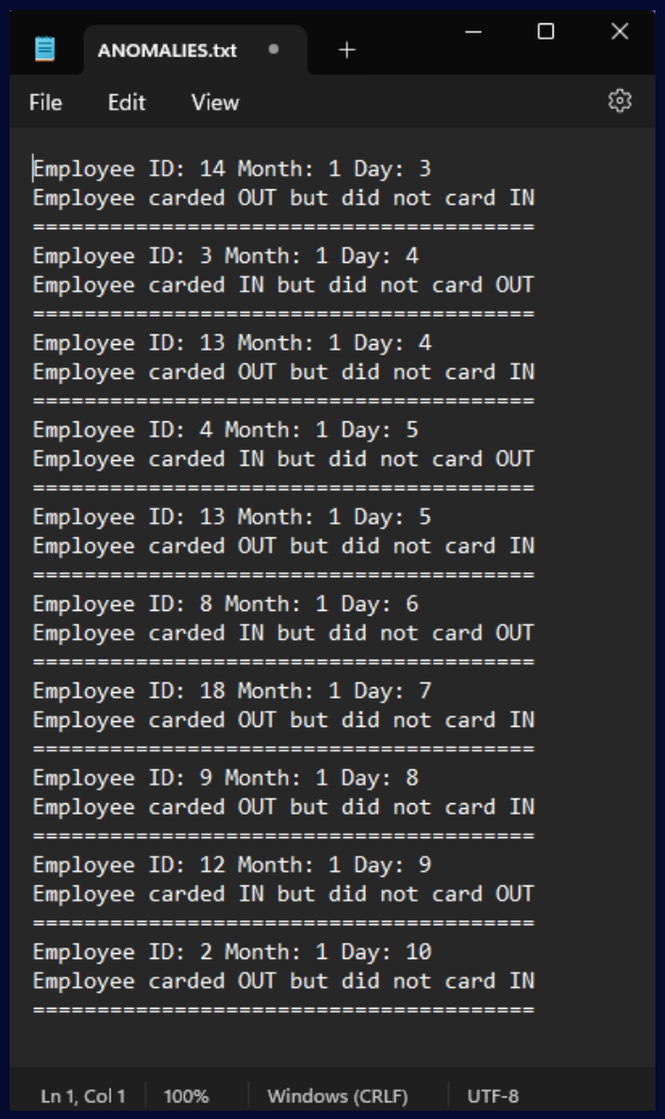
For the final assignment in ISEC2077 - Security Auditing and Control Systems I was given a fictitious log from a card key access system that covered a period of two weeks. The task was to write a program to parse the log and output the anomalies that were present. For example, if an employee carded in but not out or vice versa. The program then had to write these anomalies to a file named ANOMALIES.txt. I wrote the code for this assignment in Python to demonstrate my knowledge in this langauge.

The log is a CSV file where each line records the employee number (20 employees), the day, the month, the hour and minutes carded IN and the day, the month, and the hour and minutes carded OUT. All data is in integer format using a 24-hour clock. Employees are required to card IN and card OUT each day. If a value for any time has not been recorded it will be shown as 0.

The log file can be found here: https://github.com/ACMCDONALD/Anomaly-Detection/blob/main/cardKeyLog.csv

The code can be found here: https://github.com/ACMCDONALD/Anomaly-Detection/blob/main/Anomaly-Detection.py

My code worked as intended and found all of the anomalies and the output file looked like this:



Certificates

Nova Scotia Community College

certifies that

Andrew McDonald

successfully completed

SAFE1000: Introduction to
Workplace Hazardous Materials Information Systems

on Sunday, August 14, 2022

nscc

OHS Specialist

Nova Scotia Community College

certifies that

Andrew McDonald

successfully completed

SAFE1001: Introduction to the Nova Scotia
Occupational Health and Safety Act

on Monday, August 29, 2022

nscc

OHS Specialist

ALGONQUIN COLLEGE

has awarded this
Ontario College Certificate to

Andrew Cameron McDonald

upon the successful completion of the following
prescribed program, with concentration in
Defence and Security

General Arts and Science - One Year

THE BOARD OF GOVERNORS

HONOURS

President

Registrar

Signed and sealed at Ottawa, Ontario this 26th day of August 2014

CERTIFICATE OF APPRECIATION

CERTIFICAT D'APPRÉCIATION

Master Sailor

Andrew McDonald, CD

Upon your retirement, in recognition of your 18 years of devoted service to the Royal Canadian Navy and the Canadian Armed Forces

À l'occasion de votre retraite, et en reconnaissance des 18 années de service dévoué à la Marine royale canadienne et au sein des Forces armées canadiennes

Commandant de la Marine royale canadienne
Vice-amiral

Angus Topshee OMM, MSM, CD
Vice-Admiral
Commander Royal Canadian Navy

Certificate of Appreciation

Presented to

Master Seaman Andrew McDonald, CD

Fleet Maintenance Facility Cape Scott
Halifax, NS

In recognition of your selection from the nominees across Canada to be the special guest of the Chief of the Defence Staff at the 2019 Remembrance Day Ceremony at the National War Memorial and for your contribution to the Sentry Ceremony and Program.

General J.H. Vance,
Général
Chief of the Defence Staff
Chef d'état-major de la Défense

Chief Warrant Officer A. Guimond,
Adjudant-chef
Canadian Armed Forces Chief Warrant Officer
Adjudant-chef des Forces armées canadiennes