DREW YOUNG
STUDENT

✉ dmy625@comcast.net
📞 5085308771
⌂ drew-young

A computing security student focused on penetration testing/red teaming.

Skills

LANGUAGES

Python
Java
KQL
Bash
Powershell
Rust
C

TOOLS

Wireshark
Nmap
Sentinel
Tanium
Sumo Logic
ADX
Mimecast
Cribbl
Crowdstrike
MS Defender
CylanceOPTICS
Azure AD
Ansible
Terraform
Burp Suite
AWS
Cobalt Strike
Mythic
C3
Mailgun
BloodHound

OPERATING SYSTEMS

Windows 10
MacOS
Kali
Ubuntu
pfSense

CERTIFICATIONS

GCP Digital Leader

COMPETITIONS

Incident Response Security Competition (IRSeC) - 2021 (Blue Team)
University of Buffalo Lockdown (UB Lockdown) - 2022 (Blue Team)
Information Security Talent Search Competition (ISTS) - 2022 (Purple Team)
University of Buffalo Lockdown (UB Lockdown) - 2022 (Red Team)
Incident Response Security Competition (IRSeC) - 2022 (RedTeam)
Information Security Talent Search Competition (ISTS) - 2023 (BlackTeam)
Collegiate Cyber Defense Competition (CCDC) - 2023 (Blue Team)
Incident Response Security Competition (IRSeC) - 2023 (Black Team)

Education

Rochester Institute of Technology — Aug. 2021 to Current
B.S. Computing Security 2025
Current GPA: 3.85
Dean's List (Fall 2021, Spring 2022, Spring 2023)

Employment

Security Risk Advisors — Rochester, NY
Advisory Red Consultant (Co-op) — May 2023 to Current
- Perform external/internal penetration tests and other offensive security engagements for various companies across multiple industries
- Generate reports with specified observations and recommendations for clients
- Created script to automatically stand up infrastructure using Ansible and Terraform for Purple Team engagements

CSOC Consultant (Co-op) — Rochester, NY / May 2022 to May 2023
- Monitor SCALR XDR and enterprise clients to ensure security posture is maintained
- Investigate and analyze users actions to determine legitimacy
- Perform alert triage, notification and response, along with tuning and engineering
- Develop new workflows involving scripting to increase SOAR capabilities and investigation efficiency

RIT Cyber Range — Rochester, NY
Support Materials Developer (Part-Time) — Feb. 2022 to June 2022
- Work with team to develop support materials (encryption smart card, glossary of cyber terms, training labs, etc.) to enhance training for Standard and Poor's Global Cyber Risk Rating System

RIT Tech Crew — Rochester, NY
Junior Technician (Part-Time) — Sept. 2021 to Current
- Collaborate with team to provide sound, lighting, and power services to all departments across RIT's campus

Supercharged Entertainment — Wrentham, MA
Guest Services (Seasonal) — July 2019 to Jan. 2022
- Collaborated with a team of over 150 employees to deliver a unique experience to over 10,000 customers/week
- Trained new staff members in all departments
- Assisted customers with setting up reservations for various entertainment activities

USA Hockey — Massachusetts, New York
Referee (Seasonal) — Sept. 2017 to Current
- Officiate youth, adult, and high school ice hockey games
- Enforce the rules of the game and assess penalties for violations while maintaining order with coaches, players, and parents during the game
- Mentored new/young officials
- Refereed over 1000 games and obtained highest level in USA Hockey (level 4)

Projects

Command and Control Server and Implant (Constant Control) — Jan. 2022 to Current
- Developed a socket server and implant to establish a reverse shell to control multiple clients by using python subprocesses and threading
- Rewrote client code in Rust for faster execution
- Furthered knowledge of connections and python modules

Vulnerability Assessment — Oct. 2021 to Dec. 2021
- Reviewed company's infrastructure and topology to determine vulnerabilities within the network
- Provided solutions on ways to improve security

Web Request Shell (Requestor) — Sept. 2022 to Current
- Developed a tool with an implant that makes HTTPS requests to a web server and executes queued commands
- Implemented HTTPS for covert communication
- Added support for OS and host specific commands

Open Door Policy — Mar. 2023 to Current
- Created a tool that utilizes three different binaries to establish communication through firewalls for competitions
- Researched raw socket communication

Activities/Clubs

RITSEC · Club Member — July 2021 to Current
- Attend weekly education and research presentations to further my knowledge of computing security
- Past member of a mentorship group focused on Logging/SIEM (created ELK stack to consolidate logs from multiple clients)
- Attend weekly workshops to develop penetration testing tools for use during competitions as a red team member

RIT Red Team · Red Team Member — Aug. 2022 to Current
- Participate in red vs. blue security competitions as part of the red team
- Collaborate with other team members to create malware for competition use
- Coordinate with teammates to organize service interruption for all teams

Collegiate Cyber Defense Competition (CCDC) · Blue Team Member — Jan. 2023 to Current
- Participate in qualifier, regional, and national cyber defense competitions
- Work with teammates to keep services up and complete injects
- Attend weekly practices to learn common linux services