# Christopher C. Schmid

## Cyber Security Technician

Fawn Grove, PA 17321 | (717) 209-1229 | chrischmid32@gmail.com

Driven Cyber Security Technician with a breadth of security experience built on a strong information technology foundation. Eager to acquire a challenging position in the cyber field, which can be engaged to make the world a better place via research, study, and implementation of offensive security techniques, tactics, and procedures. Anticipated availability of April 26, 2021.

## Clearances & Certifications

| | | |
|---|---|---|
| Top Secret/SCI Security Clearance | | Current |
| Counterintelligence (CI) Polygraph | | Current |
| IAT Level III | DoDI 8570.01-M | Current |
| Certified Information Systems Security Professional (CISSP) | CompTIA | 2019 |
| Security+ | CompTIA | 2013 |
| Network+ | CompTIA | 2013 |
| A+ IT Technician | CompTIA | 2013 |
| Cisco Certified Network Associate Voice (CCNA Voice) | Cisco Systems | 2014 |
| Cisco Certified Network Associate (CCNA) | Cisco Systems | 2014 |
| Cisco Certified Entry-Level Network Technician (CCENT) | Cisco Systems | 2014 |
| Offensive Security Certified Professional (OSCP) | Offensive Security | Trained |

## Contributions

- Added Berkley Packet Filter support to SnappyCap of PacketTotal Labs.
- Presented research of "User Access Control" bypass techniques at the December 2019 MITRE Joint Cyber Analytics Development Workshop and offered a potential analytic that could be used for detection. The analytic has since been published to their analytics database.
- Coached, trained, and community members from more than 20 nations, universities, and governmental departments during a legion of Red vs. Blue exercises.
- Research conducted during a named operation led to the discovery and confirmation of adversary activity upon high-value target systems.
- Led the development of an automated attack vector identification tool used to prioritize 81 CPT hunt efforts (can be found on GitHub as TireFire).
- Wrote Aggressor scripts in sleep (language) to automate on-net actions and python scripts to generate

## Professional Experience

### Threat Emulation Specialist

United States Marine Corps (USMC), Fort Meade, MD
81 Cyber Protection Team (81 CPT)
October 2017 - Present
Supervisor: Ryan McHale, (717) 578-2339
Average Work Week: 45 hours (Equivalent GS-2210-13)

- Currently tasked to conduct network navigation, tactical forensic analysis, and collection of operational data in support of squad and team missions. Identify and mitigate operating system vulnerabilities and embedded persistent threats, as well as Research emerging threat actor tactics, techniques, and procedures with an emphasis on threat emulation techniques to guide overall mission development.
- Cleared for TOP SECRET//SCI information and granted access to sensitive compartmented information based on a single scope background investigation completed in August 2018.
- Discovered an original technique to bypass Windows Defender by utilizing Shell7er, PowerCat, and ZoomRooms.exe. This exploit is currently being used to train new members of the team on analytics creation.
- Developed a series of PowerShell and Python scripts to query object architecture information from the ntds.dit file of a domain controller, which filled a time-sensitive, engagement-specific requirement of a forward-deployed cyber hunt team.
- Added to the internal cyber range capabilities by building intentionally vulnerable machines of various operating systems and exploiting them to train analysts.
- Created a course with labs to summarize the essentials of what an analyst must know about how active directory functions, what some of the most common misconfigurations oriented vulnerabilities are, and what they look like when conducted.
- Supported a forward-deployed hunt-forward team via research and Python automation to identify each possible Tor Browser Ja3 Signature from 2007 to 2020.
- Supported a forward-deployed hunt-forward team via analysis and contribution of scalable identification techniques of modern Russian malware ComRat v4.

### Cybersecurity Technician

USMC, Camp Lejeune, NC
8th Communications Battalion
March 2015 – October 2017
Supervisor: Tyrell Anderson, Cyber Security Chief, (910) 265-1890
Average Work Week: 45 hours (Equivalent GS-2210-12)

- Served as the battalion's subject matter expert for the implementation of network security and technologies.
- Planned, configured, deployed, secured, and maintained network assets in a production network, including hardware replacement, software patches, and antivirus updates.
- Maintained adequate backups, configuration management, and documentation of network architecture.
- Designed, constructed, and maintained the forest root domain and logical ISP for the Marine Corps North Carolina tactical networks enabling a secure, resilient, and scalable system for units performing operations or training to connect.

- Engineered networks often involving four or more physical sites, and over 1200 endpoints used for training and operational engagements.
- Built and maintained secure Windows 10 and Server 2016 baseline images distributed to all tactical Marine Corps units in North Carolina.
- Ensured compliance by conducting regular assessments at remote sites and continually performed security monitoring, incident response, and affable coaching
- Formal and informal classes were persistently given over a vast array of technical disciplines to increase the proficiency of the network operators, domain administrators, and the voice team in addition to the organization's overall increase of effectiveness
- The combined knowledge of VOIP and firewall functionalities led to the first successful implementation of tactical VoSIP in the Marine Corps, which increased the security posture of not just the unit, but the entire of the Marine Corps.

## Voice Systems and Network Administrator

USMC, Camp Kinser, Okinawa Japan
March 2013 – March 2015
Communication Company, Combat Logistics Regiment 37 (CLR 37)
Supervisor: Tyrell Anderson, Network and Data Systems Lead, (910) 265-1890
Average Word Week: 48 hours (Equivalent GS-2210-12)

- Consistently by-name requested to perform technical classes between missions, and aid in troubleshooting during missions, for many VOIP and network technologies, including Cisco Unified Communications Manager, Cisco Call Manager Express, and the Marine Corps Deployable End Office Suite for the communications teams throughout the island of Okinawa.
- Made an executive engineering decision during an operation to temporarily stand up a Call Manager Express to service over 150 endpoints immediately after the hardware failure of two physical servers hosting a cluster of Cisco Unified Call Managers. The actions maintained the service for the mission with minimal downtime until the hosts could be replaced.

## Education

Computer Networks and Cybersecurity, University of Maryland Global Campus
January 2018-Present
Scheduled to complete a Bachelor's Degree in 2022

## Specialized Training

*Denotes graduation with a standing of either 1st or 2nd.

| | | |
|---|---|---|
| Advanced SSH Usage | Udemy | 2021 |
| Windows Privilege Escalation (Heath Adams) | Udemy | 2021 |
| Windows Privilege Escalation (Tib3rius) | Udemy | 2021 |
| Splunk Fundamentals 2 | Splunk | 2021 |
| Splunk Fundamentals 1 | Splunk | 2021 |
| SQLite Integration to Python | Udemy | 2021 |
| Git Crash Course | Udemy | 2021 |
| Vim Masterclass | Udemy | 2020 |
| Build Chrome Extensions | Udemy | 2020 |
| Cyber Network Operator Attack & Defend | Chiron | 2020 |
| Adversarial Threat Modeling and Emulation | Chiron | 2020 |
| Malware Reverse Engineering | Focal Point | 2020 |
| Assembly for Reverse Engineers | Focal Point | 2020 |
| Offensive Security Certified Professional | Offensive Security | 2020 |
| FireEye Hunt Methodology and Practices | FireEye | 2020 |
| Joint Cyber Analytics Development Workshop | MITRE | 2019 |
| *Cyber Threat Emulation | NIOC | 2019 |
| *Intermediate Cyber Core | NIOC | 2019 |
| *Cyber Security Technician Course | United States Marine Corps | 2017 |
| *Information Technology and Cyber Networks | United States Marine Corps | 2016 |
| ESXI Virtualization Implementation | United States Marine Corps | 2015 |
| Deployed Security Interdiction Device | United States Marine Corps | 2014 |
| *Telecommunications Systems | United States Marine Corps | 2013 |

## Hard Skills

Active Directory Hunting, Cisco Networking, Cobalt Strike, Cyber Threat Emulation, Incident Response, McAfee ePolicy Orchestrator, Network Engineering, Network Information Security, OSCP Trained, Security Center, VMWare Administration (Workstation and ESXI), Vulnerability Assessment.
**Languages:** Bash, Powershell, Python, Sleep.
**Operating Systems:** Windows XP-10, Windows Server 2003-2019, Unix/Linux OS, Cisco IOS.

## Soft Skills

Coaching/Teaching, Critical Thinking, Detail Oriented, Problem Solving, Leadership Via Example.

## Special Skills

-Captain of High School Football team and currently holds records for most rushing yards attained in a single season and a career (1162, 2187).
-Captain of High School Wrestling team and is tied for the mark of fifth-most wins in the school's history (104).
-Recipient of 2012 Lancaster County PA "Distinguished Athlete" award.
-Meritorious graduate from Marine Corps boot camp.

-2nd place finish at 2019 AvengerCon Hacking Contest.
-Hack The Box level, Hacker (CoolHandSquid).

## GitHub

https://github.com/CoolHandSquid