CHRISTOPHER SCHMID

FAWN GROVE PA, 17321
CHRISCHMID32@GMAIL.COM
(717) 209-1229

OBJECTIVE

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.

SECURITY CLEARANCE

Active Top Secret / SCI

EDUCATION

Bachelors of Computer Networking and Cyber Security

University of Maryland Global Campus, Columbia, Maryland
Expected Graduation: December 2022
Current GPA: 3.88

Specialized Training

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

2020-11 Chiron CNO Attack & Defend
2020-10 Chiron Adversarial Threat Modeling and Emulation
2020-08 Focal Point Malware Reverse Engineering
2020-07 Focal Point Assembly for Reverse Engineers
2020-04 Offensive Security Certified Professional
2020-02 FireEye Hunt Methodology and Practices
2019-12 MITRE Joint Cyber Analytics Development Workshop
2019-05 *Naval Information Operations Command Cyber Threat Emulation
2019-01 *Naval Information Operations Command Intermediate Cyber Corp
2017-04 *Marine Corps Cyber Security Technician School
2016-08 *Marine Corps Information Technology and Cyber Network Systems School
2012-03 *Marine Corps Telecommunication Systems School

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 led members of the community 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 redirector infrastructure in Cobalt Strike.

Certifications

CISSP
A+ IT Technician
Network+
Security+
CCENT
CCNA
CCNA Voice
OSCP (Trained)

Hard Skills

Active Directory Hunting
Bash Scripting
Cisco Networking
Cobalt Strike
Cyber Threat Emulation
Incident Response
McAfee ePolicy Orchestrator
Network Engineering
Network Information Security
OSCP Trained
PowerShell Scripting
Python Scripting
Security Center
Sleep (Cobalt Strike Automation)
UNIX/Linux OS
VMWare Administration / ESXI
Vulnerability Assessment
Windows Engineering
Windows Server 2003-2019
Windows XP-10

Soft Skills

Coaching/Teaching
Critical Thinking
Detail Oriented
Problem Solving
Leadership via Example

Availability

April 2021

GitHub

https://github.com/CoolHandSquid

EXPERIENCE

Cyber Threat Emulation Specialist
October 2017 to Present

Department of Defense, Columbia, Maryland

-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 capabilities of the internal cyber range 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
March 2015 to October 2017

Department of Defense, Jacksonville, North Carolina

-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 sights and over 1200 endpoints to be used for training and operational engagements.
-Built and maintained secure Windows 10 and Server 2016 baseline images that were 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
March 2013 to March 2015

Department of Defense, Ft. Urasoe, Okinawa Japan

-Consistently by-name requested to perform technical classes between missions, and aid in troubleshooting during missions, for a multitude of 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.

Special Skills

-Captain of High School Football team and currently holds records for most rushing yards attained in a single season and a career (1324, 2348).
-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).