ROBERT GRAHAM

Penetration Tester / Cyber Applications Developer

San Antonio, 78254

☎ 210-473-7789

robert.graham.dev@gmail.com

Websites

https://github.com/Krieglied

https://Krieglied.github.io

www.linkedin.com/in/robert-graham-gxpn

Skills

Languages

- Python, Powershell, C, Assembly, C#, Java, PL/SQL

Platforms

- Git, Visual Studio, Vim, Windows, Kali Linux

Techniques

- Reverse-Engineering, Purple Teaming, Threat Emulation, Vulnerability Research, Cyber Network Operations Development, Protocol Exploitation

Certifications

Active TS/SCI Clearance + CI Polygraph (2016)

CompTIA Security+ - Renewed Dec 2020

Apprentice Cyber Network Operations Developer - Oct 2018

Certified Penetration Testing Engineer - Dec 2018

GIAC Certified Incident Handler - Renewed Jul 2019

Certified Advanced Cyber Programmer - Aug 2019

GIAC Exploit Researcher and Advanced Penetration Tester - Sep 2019

Professional Summary

Experienced Cyber Subject Matter Expert with over 5 years in Cyber Adversary Tactics and 9 years of experience in Cyber Development. Excellent reputation for resolving problems, improving mission partner capabilities, and meeting operational requirements. Striving to constantly update skills and knowledge in the domain of cyber.

Education

2005 - 2009 Bachelor of Science: Computer Science

Texas A&M University, College Station, TX

Minor in Mathematics

2011 - 2012 Associate of Science: Computer Science Technology

Community College of The Air Force, Montgomery, AL

2015 - 2016 Associate of Science: Cyber Security

Community College of The Air Force, Montgomery, AL

Work Experience

2017 - Present Team Chief, Air Force Malware Laboratory

United States Air Force

- Held position of Agile Product Owner for 10 member development team/ developer responsible for designing and implementing a generic control platform that ties over 7 samples of malware together and automating adversary actions, for use by Red Team members to train Blue Team operators. Integrated to work with MITRE's CALDERA system.
- Served as Red Team exercise support for 7 US Cyber Command exercises to train over 300 defense cyber operators, both to meet Congressional mandates and maintain operational readiness of cyber forces.
- Selected as advisor to a threat emulation team for a Headquarter's directed cyber operation. Trained and guided 6 member team on proper tactics and techniques leading to successful validation of defense operators tactics.
- Assisted a Cyber Protection Team of 15 members as a Malicious Process/Malware Subject Matter Expert to offer on-mission support.
- Received training for cyber development, in the realm of reverse-engineering, vulnerability research, and exploitation development, with an emphasis on the Windows Operating Systems, using C, Python, Assembly, and Git.

2015 - 2017 Offensive Cyber Operation Student

United States Air Force

- Learned Red Team, Penetration Testing Tactics and Techniques, using Python, Linux, Windows, and Networking Skills, as training to become a US Cyber Command operator.

2011 - 2014 Electronic Warfare Applications Programmer

United States Air Force

- Developed an intelligence processing application used to facilitate mission planning by the Department of Defense war fighting communities, using PL/SQL, C# and Java.
- Maintained several web portals for intelligence reporting, accessed by all member of North Atlantic Treaty Organization, with Oracle APEX, PL/SQL, PHP, and HTML.