chadefry@gmail.com
(254) 316-1091

Chad Fry

GitHub: GlitchKraken
LinkedIn: Chad Fry

Portfolio

Employment

Info Security Sr Analyst AVP **Citibank** **Mar 2022 – Present**

- Performed deep packet analysis on network traffic for more than 6 of Citi's global accounts.
- Collaborated with 2 other security teams to escalate accounts involving malware and fraud.
- Developed 2 different Splunk dashboards used by team to expedite manual investigations into potential DOS events, as well as potential WAF attacks.
- Engineered scripts used by team to hasten non-investigative portions of processes, saving around 30 days of time a year.

Software Engineer **CGI** **Oct 2019 – May 2020**

- Debugged, Developed, and tested CGI "Advantage" software, using Java.
- Successfully patched longstanding logon issues for local users of Advantage-testing branch.

Oracle Database Administrator **Angelo State University** **Jan 2019 – May 2019**

- Created, updated, and managed user accounts / permissions for enterprise resource planning software (Banner) end-users.
- Crafted a bash-script to alert us when a database was down and not being backed up, saving the team around 10 minutes for each false-positive.
- Cleaned our databases of duplicate user data in Banner using SQL*Plus.

Languages and Technologies

Languages: C++; C; x86/64 Assembly; Java; C#.NET; SQL; JavaScript; Python; Bash; PowerShell

Tech: Windows; Linux; PwnDBG; Ghidra; Pwntools; x64Dbg; Cyber-Kill-Chain; Nmap; Metasploit; Virtualization; Firewalls; Networking; Akamai; Splunk ES / Core

Security Research and Projects

Pentesting **Mar 2021**

- Boot-To-Root style penetration testing for a Linux machine with the ShellShock vulnerability. *Linux; Nmap; Metasploit; Python.*

Network Monitoring **Jan 2021**

- Identified patterns for many threat actors in Wireshark- including DDOS, SQL injections, botnet/C2 activity, as well as CVA attacks and Logon Brute Forcing.
- Wrote Snort rules to accurately detect, prevent, and report on further events of the above types, with 99%+ accuracy.
- Constructed a Virtual Machine lab to replay captured network data, and ensure that only malicious activity was reported.

Advanced Binary Exploitation **Nov 2023**

- A CTF-style project where I wrote exploits/write-ups for advanced topics in Binary Exploitation: ROP chains, remote exploitation, format string vulns, heap exploits like use-after-free, double-free, heap overflows. Stack Canaries and techniques to bypass them, etc. *C/C++; Pwndbg/GDB; Pwntools; Python;*

Advanced Malware Analysis **Feb 2023**

- Constructed secure virtual machines as platforms for reverse engineering Windows/Android Malware.
- Faked network responses in order to reveal malware C2 servers, and discover additional behaviors.
- Worked with Intel PIN tool suite to automate behavior-detection/finding.
- Statically reverse-engineered behavior with Ghidra. *Ghidra; Intel PIN; AndroidStudio; WireShark; DNS; Virtualization.* Project-Github

Education

Georgia Institute of Technology

- M.S. in Cybersecurity

Angelo State University

- B.S. in Computer Science.