Blue Team

Cheat Sheets

Compiled by Chris Davis

TABLE OF CONTENTS

SECTION TITLE PAGE

Table of Contents - Networking/Blue Team Tools i

Table of Contents - IR / Linux / Windows / Misc i

Table of Contents - Incident Response / Notes i

NETWORKING / BLUE TEAM TOOLS

Common Ports........ 1

IPv4/TCP-UDP-ICMP Headers, Subnetting........ 2

IPv6/TCP Header 6

OSI Model,........ 9

HTTP, FTP, Decimal to Hex Conversion 12

20 Critical Security Controls 15

Cisco Networking All in One Reference........ 17

ARGUS/TCPDUMP/TSHARK/NGREP........ 21

Tcpdump 23

Berkeley Packet Filters and Bit Masking 24

Wireshark 27

NMAP 30

Python Quick Reference 34

Regular Expressions 36

SNORT........ 38

rwfilter 41