



Blue Team Notes

A collection of one-liners, small scripts, and some useful tips for blue team work.

I've included screenshots where possible so you know what you're getting.

Did the Notes help?

I hope the Blue Team Notes help you catch an adversary, thwart an attack, or even just helps you learn. If you've benefited from the Blue Team Notes, would you kindly consider making a donation to one or two charities.

Donate as much or little money as you like, of course. I have some UK charities you could donate to: [Great Ormond Street - Children's hospital](#), [Cancer Research](#), and [Feeding Britain - food charity](#)

Table of Contents

- [Shell Style](#)

- Windows
 - OS Queries
 - Account Queries
 - Service Queries
 - Network Queries
 - Remoting Queries
 - Firewall Queries
 - SMB Queries
 - Process Queries
 - Recurring Task Queries
 - File Queries
 - Registry Queries
 - Driver Queries
 - DLL Queries
 - AV Queries
 - Log Queries
 - Powershell Tips
- Linux
 - Bash History
 - Grep and Ack
 - Processes and Networks
 - Files
 - Bash Tips
- MacOS
 - Reading .plist files
 - Quarantine Events
 - Install History
 - Most Recently Used (MRU)
 - Audit Logs
 - Command line history
 - WHOMST is in the Admin group
 - Persistence locations
 - Transparency, Consent, and Control (TCC)
 - Built-In Security Mechanisms
- Malware

- [Rapid Malware Analysis](#)
- [Unquarantine Malware](#)
- [Process Monitor](#)
- [Hash Check Malware](#)
- [Decoding Powershell](#)
- [SOC](#)
 - [Sigma Converter](#)
 - [SOC Prime](#)
- [Honeypots](#)
 - [Basic Honeypots](#)
- [Network Traffic](#)
 - [Capture Traffic](#)
 - [TShark](#)
 - [Extracting Stuff](#)
 - [PCAP Analysis IRL](#)
- [Digital Forensics](#)
 - [Volatility](#)
 - [Quick Forensics](#)
 - [Chainsaw](#)
 - [Browser History](#)
 - [Which logs to pull in an incident](#)
 - [USBs](#)
 - [Reg Ripper](#)

As you scroll along, it's easy to lose orientation. Wherever you are in the Blue Team Notes, if you look to the top-left of the readme you'll see a little icon. This is a small table of contents, and it will help you figure out where you are, where you've been, and where you're going