

Security Logging via the Windows Firewall for Investigative Purposes

Useful on a local host when you need to monitor ingress/egress traffic...

One often overlooked opportunity to log potentially malicious traffic, on Windows hosts in particular, comes courtesy of the Windows Firewall. Included in its feature set is the ability to enable security logging to capture all ingress/egress network traffic.

Do so as follows:

Start...Settings...Network Connections...right click Local Area Connection, choose Properties...Choose Advanced....Select Settings...Choose Advanced again...Select Settings in Security Logging...check Log Successful Connections and set the size limit to 16512kb.

The pfirewall.log file will then be written to C:\WINDOWS.

This allows instant review of all inbound and outbound connections by IP, port, and timestamp. Very useful forensically if you're curious as to what external IP addresses malware on the local host may be communicating with or what address an attacker may be attempting to exploit from. As a whole, Security Logging is no replacement for IDS or a SEM, but it's great in a pinch.