CommView® Helps Connetic Secure the Customer's Network

Case Study

Illegal LAN Usage by Insiders

As an outsourced IT firm that specializes in security, Connetic often takes on difficult and demanding security related jobs for its clients. In a recent case, a publicly-traded customer in a real estate related industry was forced to release more than 75% of its IT staff when it was discovered that the IT director and others were stealing bandwidth and server assets to operate an illegal web-based business (actually illegal—not just against company policy). The only people who survived the dismissal were lower-level IT staff who had no knowledge of the scheme.

Connetic was called in on three days' notice to secretly survey the network and prepare to take control of it. "We would not even know in advance whether we would be able to retrieve administrative passwords for the Windows-based domain or for network layer devices," says Matthew Strebe, CIO at Connetic.

At the point staff were notified, Connetic was on-site to take control of the network, shut down any portions of the network that could allow remote access, survey the entire network, scan for vulnerabilities and secret back doors, remediate any high-risk vulnerabilities or vectors for attack, restore services that had to be taken off-line, and provide recommendations to improve security and control of IT in the future.

The Takeover

Securing a completely unknown network against the very individuals who set it up is the most difficult possible security task. The individuals involved would be highly motivated to remotely access the network because the assets of their illegal business were on the customer's network. It was imperative that they not regain access to the network and destroy evidence. Fortunately, Connetic staff managed to retrieve passwords secretly prior to the event using a surreptitiously installed hardware key logger. This obviated the need to take all Internet-related services offline to crack administrative passwords or wipe and refresh network devices such as the firewall. Once in possession of these passwords, the team was ready to come on site and assert control of the network.

During the exit interview process, Connetic was escorted to the server room and began the process of changing passwords on all devices to lock existing staff out. Because Connetic did not have complete documentation as to the structure of the network, it was imperative that Connetic knew about all information flowing to and from the Internet during the takeover process.

CommView Provides Network Visibility

To accomplish this, a monitoring point was established by using a hub to breakout the connection between the primary switches and the LAN port on the primary firewall. All traffic to or from the Internet would flow through this hub, but being behind the firewall would mean that false positives or the "background radiation" of hacking attempts that normally occur on the Internet would be filtered out.

With the monitoring point established, a laptop running CommView was attached and began monitoring traffic. According to Matthew Strebe, "Because of CommView's ability to show TCP connections in real time, we were easily able to keep track of "normal" networking activity, and established filters to block traffic that we had cleared as legitimate. The ability to reconstruct TCP streams by right-clicking on a connection was priceless in this situation--it made understanding a connection much faster and allowed us to truly monitor the situation in real time without being bogged down in the details of chaining packets together at the network layer."

At the end of the contract, Connetic was able to safely secure the network and guarantee to the client that no unauthorized access had taken place, so the chain of custody of their evidence was intact. That level of certainty couldn't be provided without CommView's ability to efficiently and effectively provide visibility into network traffic in real time.

About CommView

CommView is a powerful network monitor and analyzer for Ethernet networks. Loaded with many user-friendly features, CommView combines performance and flexibility with an ease of use unmatched in the industry.

About TamoSoft

TamoSoft develops cutting-edge security and network monitoring software for the Internet and Local Area Networks, providing clients with the ability and confidence to meet the challenges of tomorrow's technology. Keeping pace with industry trends, TamoSoft offers professional tools that support the latest standards, protocols, software, and hardware in both wired and wireless networks.

TamoSoft
PO Box 1385
Christchurch 8140
New Zealand

Phone (USA): +1 866 582 6675
Phone (UK): +44 (0) 2070 602 806
Fax: +64 3 310 2413

sales@tamos.com
WWW.TAMOS.COM