EtherPeek and Security: A definite match-up

By Dr. Bill Hancock, CISSP
Executive VP/CTO
Network-1 Software and Technology, Inc.
Web: http://www.network-1.com
E-mail: hancock@network-1.com

As a hard-core security and network geek, I can't do very much of a technical nature in what I do without a protocol analyzer and, of course, I use EtherPeek to do my work. In my case, I spend a lot of time designing and analyzing all types of networks and their problems. When I am not doing that, I am chasing computer hackers. EtherPeek is a major part of that effort and has proven its mettle many times as a valued tool in the fight against computer crime.

Computer hacking comes in as many different "flavors" as personalities that are involved in its incarnations. Sometimes its malicious, sometimes done for financial gain, sometimes just for revenge, sometimes for youthful misunderstanding that data has a soul and should be "set free" like some caged animal. The bulk of hacking and security problems I encounter are internal personnel who are involved in, at a minimum, immoral use of internal resources (for their own gain) or, at a maximum, may be involved in major industrial espionage or other felonious activities that are harmful to their companies or governments. Hacking knows no age limit, and most of the time it is somewhat social-status neutral.

Using EtherPeek as a data analyzer is essential for identifying specific hacker activities on a network. For instance, I use it regularly for identifying specific IP addresses seen on firewall logging facilities on trusted-to-untrusted IP traffic that is suspicious in nature. Using the firewall activity logs (especially on stateful & proxy combination firewalls like FireWall/Plus), suspicious activities are logged by IP address and event. Firewalls usually do not capture enough information for legal prosecution to be airtight, so identification of suspects and then collection of activities via EtherPeek is a decisive one-two punch combination that assures success in tracking someone down, exactly. Taking suspicious IP addresses and creating an address filter in EtherPeek, followed by data collection at the right place in the network, allows collection of activities and events that back up the logging in the firewall and other network devices for producing proper evidence that will result in either civil or criminal prosecution of a hacker.

One of the major types of attacks from external sources is a denial-of-service attack called a TCP SYN flag attack. Basically, a high connection count attack is launched against a router, web site, etc., by creating a TCP packet with the SYN flag set in the header that causes systems in the path to set-up a new session. In the classic attack, the source address or destination address may change from packet to packet to confuse the analyst of the attacker's location or originating system. Setting up EtherPeek with a SYN flag filter as a trigger and then connecting to the Ethernet/802.3 network external to the firewall to the Internet is a great way to detect this type of attack and trap useful information in the tracing of the event. While a lot of firewall products will detect this type of attack and stop it from filtering through the firewall, firewall products typically do not provide complete traceback of the events or specific packet information useful in tracking down the offender. Using EtherPeek's pager option also allows early warning for sites which may be attacked and not realize it until it is too late to do anything about it or collect enough information to track down the offender.

Sometimes, the ability to search for specific filtered events such as TCP's SYN flag can also help find specific problems. One of our very large customers with a very active web site called up with a TCP SYN attack problem that the firewall successfully detected and thwarted. It went away. Then, it came back. Then it went away. Then it came back. Over and over. They could not figure out what was going on and asked for help. EtherPeek was attached to the DMZ on the web site and, sure enough, 32,000 SYN messages were seen in a 2 minute period. This happened eight more times in a 30 minute period. Analysis of the messages soon showed that there was no hacker at all. This site, with over 75 web servers and load balancing of web server requests, had a flaky web server that sometimes would hang. When this happened, customers would get frustrated and re-connect with their web browsers via RELOAD of the connection and a new TCP connection would be established. Since the site may service as many as 50,000 customers per second, it's not uncommon for a lot of customers to reset their connections. EtherPeek was essential to collect the proper security data and then save the information in a spreadsheet so that it could be sorted and collated. Through the use of EtherPeek and Excel, the problem was quickly identified and the offending web server fixed.

Other uses of EtherPeek in the security business include the collection of messages looking for passwords. File Transfer Protocol (ftp) application in the TCP/IP suite has a PASSWORD embedded command in the command stream channel that is ideal for filter writing. By setting up EtherPeek with a filter for PASSWORD commands embedded in FTP, the security person can quickly examine why systems are failing password connections or where high connection count password attempts are coming from when trying to find the source of random login hacking. Another popular security use for EtherPeek is the filtering of connection-request messages to security-sensitive high transaction servers from unauthorized address groups in various protocols. By looking for what "does not belong" on the network connections as well as what does allows the security analyst to identify potential security issues before they become problems. For instance, if there are a lot of connection attempts from a specific address external to the authorized group, it's time to pay a visit to the offender and find out what's going on before it gets serious.

On the more pro-active side of security, EtherPeek is essential in the installation and testing of firewall installations. By using a small repeater hublet on the untrusted side of the firewall and wiring in EtherPeek on the untrusted side connection, I was able to monitor all message traffic from the trusted side to the untrusted side. This allows verification that proper security rules and policies implemented in the firewall are functioning properly. Such actions are also critical in monitoring for security packet "leaks" from the firewall to the untrusted side so that they can be cleaned up before they are used to compromise the network. Also, EtherPeek's performance analysis capabilities allow the network security analyst to watch traffic levels to/from the firewall so that the network can be adjusted for optimal security performance. For instance, larger packets improve security system efficiency by reducing the number of IP headers that must be examined by the firewall system for a given message. If a message can be reduced to 1000 packets instead of 10,000 packets, there are only 1000 IP headers to examine and this improves performance in the firewall dramatically. Using EtherPeek to perform normal network performance analysis also improves security processing when the systems are adjusted properly.

As an example, a customer recently was complaining about performance of the firewall installed on a high transaction count site. Use of EtherPeek on the untrusted side of the network showed that there was a high retransmission count, a high collision count and large packets (web servers responding with IP packets greater than 1000 octets most of the time). Discussion with the customer revealed that they did not know about the collision

problem (the rate was over 30% of the gross packet count and should never exceed 1% on a switched network, which this one is), that the customers were mostly dial-up customers at 28.8kbps or less and that the large packets were for internal LAN efficiency. The discussion showed that shipping large packets to dial-up customers is a NO-NO as any single-bit “hit” would cause the entire packet to be retransmitted and this was causing the high retransmission count. By reducing the web-based packet size from over 1000 octets to 256 octets or less, the retransmission count was reduced dramatically and the collision count was also dropped (turns out that part of the problem was congestion between the node buffers and bridge buffers with large packets). By using EtherPeek to analyze the performance issue, the network was properly adjusted and the customers on both ends much happier with the site’s performance. As a closing note on this, a higher packet count due to smaller packet sizes increased the firewall’s work requirement (they had a macho-enough processor to deal with it so things worked out). By making the adjustments, the inconsistency on performance was corrected and the additional traffic load was more than compensated for by better overall performance for the users.

EtherPeek is extremely useful when installing, testing and verifying security products in use on networks as well as essential in the trackdown and evidence gathering activities associated with prosecuting the evil vermin that infest networks from time to time (read: hackers, crackers, etc.).