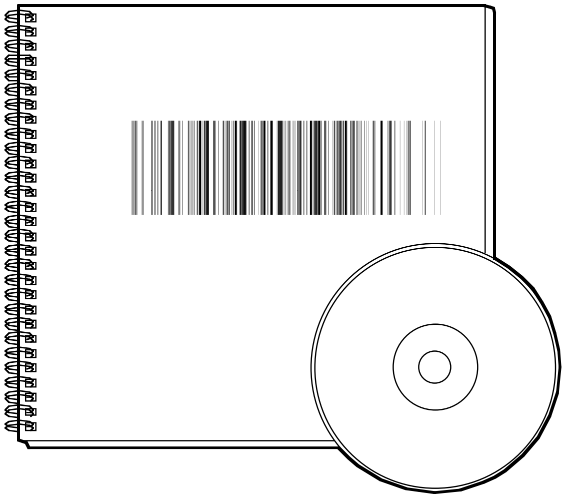
BLACK BOX®
NETWORK SERVICES

LanVue Traffic and Protocol Analyzer



Troubleshoot and debug your network now with this advanced security software.

Key Features

- *Pinpoints media abusers and instantly detects variances in specific protocol uses.*
- *Alerts you to security breaches and attacks as they occur.*
- *Hones your search for specific devices that may be responsible for weak spots in your security web.*
- *Tests device reactions to specific illegal or broken packet types.*
- *Available for both Ethernet and Token Ring applications. Or order the combo software package.*
- *Tracks internal traffic, overseeing the activity of all users.*

Reduce the threat of Internet intruders with the LanVue security tool from Black Box.

The software functions as a network traffic and protocol analyzer, making the complex tasks of troubleshooting and debugging networks easy. Working like a telephone tap, it captures all data packets of the network and provides you with the means to analyze patterns at the highest level and inspect packets—the building blocks of network communication—at the lowest level.

It's particularly valuable to security analysts who want to audit and redesign their networks around a secure model.

LanVue determines the composition of network traffic and identifies specific spots of vulnerability. In fact, it's the definitive security analysis tool and one of the few tools on the market that can actively test firewall and router configurations. LanVue tells you if your existing security measures are sophisticated enough to keep out today's highly skilled computer criminals.

LanVue is extremely useful when you install, test and verify security products in use on other networks, as well as when you investigate and gather evidence against hackers and other intruders.

Using the software's filter-writing capabilities, you can quickly determine the reason behind failed password connections or the source of random logic hacking. Furthermore, you can also use LanVue to filter connection-request messages. By looking for "what does not belong" on the network connections, you'll identify potential security issues before they become big problems. For instance, LanVue informs you of multiple connection attempts from a specific external address—activity that you may want to investigate before it results in serious consequences.

LanVue can also be used to reinforce your firewall as a separate undetectable intrusion-detection system, monitoring the firewall's effectiveness and the exact nature of the traffic getting through. Via a pager, LanVue can alert you to illegal traffic passing through the firewall.

You can also use the software to set up a monitoring station so you can observe traffic to and from certain servers. This is particularly useful if you're running a server farm with a great number of servers within one protected subnet. Studies show that nearly 90% of all successful attacks come from trusted users within networks.

(Continued on page 2.)

Typical Application

Use LanVue to verify that your network file servers, mail systems, and databases are secure. The software examines their logins, verifying that they are, in fact, correctly configured and contain the required password encryption.

(Continued from page 1.)

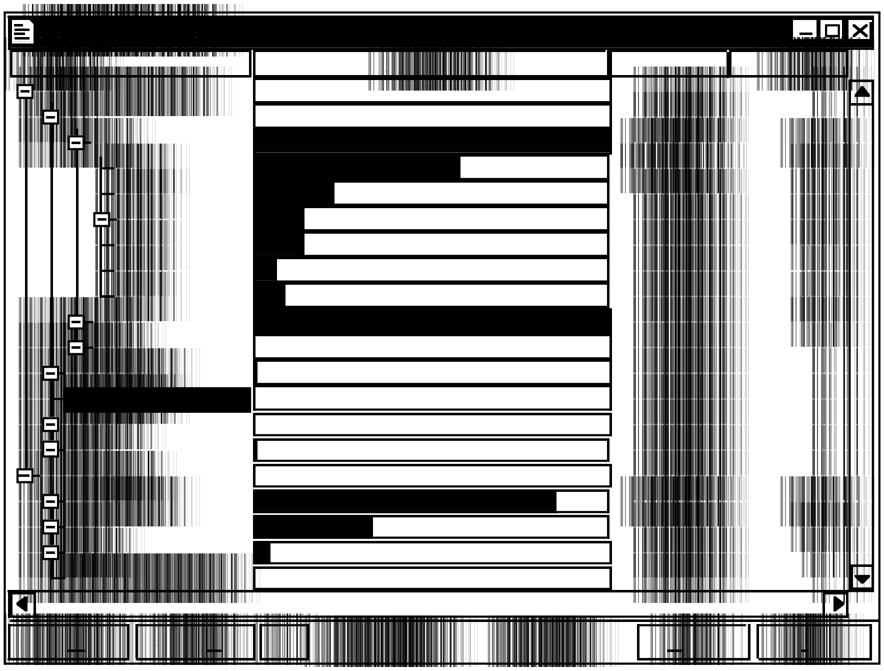
On the proactive side, you can use LanVue to inspect your firewall's installation and prevent security packet leaks from the firewall to the untrusted side.

Moreover, the software tests various denial of service attacks and determines why specific network services fail, isolating good packets from broken packets. LanVue's triggers can be set up to capture specific packets when you suspect a particular network service contains a vulnerable port.

LanVue is also essential for identifying specific hacker activities on a network. What's more, it can be used to easily pinpoint IP addresses in suspicious IP traffic. Along with the activity information logged by your firewall, you just may have enough evidence to pursue successful legal action against the culprit.

The software can also be used to secure your Web server from outside intruders and ensure proper use of Internet services by your authorized users.

LanVue is available for either Ethernet (TD200) or Token Ring (TD201), or you can purchase a kit containing both software packages TDD202).



You can customize the main capture window to specify relevant network information for troubleshooting your security setup. Protocol-hierarchical breakouts provide you with an instant analysis of media use.

Technically speaking

A Firewall's Best Friend

Your firewall may not be enough security. But with LanVue installed, you'll be able to monitor traffic flow to and from the firewall so you can adjust you network for optimal security.

For example, 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 1,000 packets instead of 10,000, then your firewall only needs to examine 1,000 IP headers. This dramatically improves the firewall's performance. LanVue provides you with this network analysis. In turn, you can adjust your systems to improve your security processing.

LanVue can also troubleshoot your firewall. A firewall is often extremely difficult to properly configure, particularly if it's used with filters on routers. But you can use your LanVue to probe firewalls, hosts, and routers and directly observe the results of the probing via the Tools menu. In addition, you can inject various queries and observe the results of those queries on one or both sides of the firewall or router.

When you employ LanVue as a separate intrusion-detection device, it is installed on the outside of the firewall, set to record all attack information to a log file. This way, you can have an additional record of attacks to supplement the log file from the firewall itself.

Note: Firewalls vary greatly in their ability to actively log information; some flood the log file with arcane information, while others have no logging capability at all. Adding LanVue to your overall security plan can supplement logging activities or customize them for enhanced readability.

Guarding vs. Attacks

Set up to trap external attacks, LanVue is a highly effective against TCP SYN flag, a denial-of-service attack.

Although many firewall products detect this type of attack and stop it from filtering through, they typically don't provide you with a complete traceback of the events or specific packet information that may help you identify the offender. Setting up LanVue with a SYN flag filter as a trigger is a great way to detect this kind of attack and, more importantly, garner enough information to trace the attack.

And having the ability to search for specified filtered events (such as SYN flag) can also help you uncover other problems. For example, many Web sites have SYN attack problems that are random and recurring but don't have anything to do with an intruder attack. LanVue can detect, capture, and analyze SYN messages and, in many cases, prove that the problems can simply be attributed to a flaky server, not a hacker.

Added Features:

- A main capture window, which you can customize to specify relevant network information for overall network and security auditing.

(Continued on page 3.)

(Continued from page 2.)

- An extensive array of protocol and sub-protocol decoders. Use these to detect password abuse by interpreting data packets from IP and all major protocol suites.
- Automatic name-to-address mapping with the building of Name Table from Lookup, which enables you to work with familiar names for easy packet and device analysis.
- ProtoSpecs™ protocol-layer hierarchical breakouts with definitions. These provide you with an instant analysis of media use broken out by protocol and subprotocol contributors.
- SmartDecoders threading technology. With this, you can easily identify conversational threads buried in overall traffic for intelligent analysis or suspect communications.

In the Bundle…

With the LanVue, you get two additional software packages: AG NetTools and EtherHelp.

The **NetTools** feature:

- Ping, which pings Internet devices with a specified number of packets, timeout, and time interval. Minimum, maximum, and average response times are reported back.
- NameLookup: uses DNS to resolve names to addresses and addresses to names.
- Finger: uses the finger protocol to obtain user information on a given server.
- WhoIs: obtains whois information about the owner of a domain name.
- Throughput: tests for the availability of resources (via FTP or HTTP) on the Internet and calculates the time, size, and speed of a download.
- PortScan: searches ports to find supported services, such as HTTP/telnet/FTP.
- PingScan: pings a range of IP addresses to find out those currently in use.
- ServiceScan: scans a range of IP addresses for services.
- NetworkInfo: provides basic network information, such as AppleTalk, IP and hardware addresses.

EtherHelp, a remote packet-capturing utility, allows LanVue users to obtain information from a remote network without having to be on site.

It captures network traffic in the form of packet trace files to be imported into LanVue for decoding and analysis.

Des questions supplémentaires ?

Appelez notre support technique gratuit au 01.45.60.
Nos techniciens vous aideront à trouver les produits
conviennent à votre application.

Ordering Information

This information will help you place your order quickly.

PRODUCT NAME	ORDER CODE
LanVue (EN)	TD200
LanVue (TR)	TD201
LanVue +	TD202