

# You're Being Watched

## Cyber-Crime Scans

*Editor's Note: This article supplements Laura Chappell's session TUT233, "Cyber Crime at Packet-Level," at Novell BrainShare 2001 in Salt Lake City. (For more information about Novell BrainShare 2001, visit [www.novellbrainshare.com](http://www.novellbrainshare.com).)*

**A**s the following headlines show, last year was a busy year for hackers:

- "Hacker Pleads Guilty in New York City to Hacking Into Two NASA Jet Propulsion Lab Computers Located in Pasadena, California" (December 1, 2000)
- "Orange County Man Pleads Guilty to Hacking Into Government Computers" (November 7, 2000)
- "Nine Are Indicted for Unlawfully Accessing Computers of U.S. Postal Service, State of Texas, and Canadian Department of Defense" (October 12, 2000)
- "Three Kazak Men Arrested in London for Hacking Into Bloomberg L.P.'s Computer System" (August 14, 2000)
- "Darkside Hacker' Sentenced to 21 Months in Prison" (July 24, 2000)

Before launching these attacks, the hackers engaged in some reconnaissance, or information-gathering, processes such as the following:

- **Social Engineering.** By taking advantage of employees' unsuspecting nature, hackers can obtain important information about a company's network. For example, a hacker may pose as an executive's secretary and call the company's IS department, saying, "I'm Mr. Markson's secretary. Unfortunately, Mr. Markson left his presentation on his desktop computer. I need his password to retrieve the file and send it to him." Or a hacker may pose as an IS technician and ask individual users for permission to time their workstations' response times as they log in. Of course, the hacker then writes down these users' passwords if those passwords are passed in clear text form.
- **Security Leaks.** If you lock your front doors but leave your windows open, you are susceptible to a break-in. Likewise, employees who leave confidential information in plain view on their desk or on white boards make their company susceptible to hackers. Employees may also make their company



vulnerable by failing to secure sensitive information, such as passwords and access lists.

- **Scanning, Probing, and Listening.** Using standard querying techniques and relying on their understanding of network communications and configurations, hackers actively and passively gather information about a company's network activity.

This article (and the accompanying Novell BrainShare 2001 presentation) examines the types of scans hackers use to identify and characterize network devices. Specifically, this article focuses on the evidence that a scan has occurred—evidence that you can find by analyzing the packet-level communications that cross the wire. After you understand the types of scans hackers use, you can build filters for your protocol analyzer to detect scans before hackers can actually launch a cyber attack.

Scanning techniques fall into the following categories:

- Address Resolution Protocol (ARP) scans
- Internet Control Messaging Protocol (ICMP) scans
- User Datagram Protocol (UDP) Port scans
- Transmission Control Protocol (TCP) scans

### ARP SCAN

Before communicating with a host, an IP device must obtain the hardware address of the destination host or the next-hop router along the path to the host. The IP device sends ARP broadcasts to resolve the hardware address of the destination with the known IP address.

Hackers can discover active devices on the local network segment by sending a simple series of ARP broadcasts and in-

No.	Time	Source Address	Dest Address	Summary
1		00E016A11883	Broadcast	ARP: C PA=[10.0.0.68] PRO=IP
2		3C00F 43F76B	00E016A11883	ARP: B PA=[10.0.0.68] HA=3C00F 43F76B
3		00E016A11883	Broadcast	ARP: C PA=[10.0.0.106] PRO=IP
4		00E016A11883	Broadcast	ARP: C PA=[10.0.0.62] PRO=IP
5		00E016A11883	Broadcast	ARP: C PA=[10.0.0.52] PRO=IP
6		Intel A35A02	00E016A11883	ARP: B PA=[10.0.0.52] HA=Intel A35A02
7		00E016A11883	Broadcast	ARP: C PA=[10.0.0.65] PRO=IP
8		Intel A3644F	00E016A11883	ARP: B PA=[10.0.0.65] HA=Intel A3644F
9		00E016A11883	Broadcast	ARP: C PA=[10.0.0.56] PRO=IP
10		Intel 86E44A	00E016A11883	ARP: B PA=[10.0.0.56] HA=Intel 86E44A
11		00E016A11883	Broadcast	ARP: C PA=[10.0.0.29] PRO=IP
12		00E016A11883	Broadcast	ARP: C PA=[10.0.0.51] PRO=IP
13		Intel 86E452	00E016A11883	ARP: B PA=[10.0.0.51] HA=Intel 86E452
14		00E016A11883	Broadcast	ARP: C PA=[10.0.0.56] PRO=IP
15		Intel 86E44A	00E016A11883	ARP: B PA=[10.0.0.56] HA=Intel 86E44A
16		00E016A11883	Broadcast	ARP: C PA=[10.0.0.49] PRO=IP
17		Intel 872012	00E016A11883	ARP: B PA=[10.0.0.49] HA=Intel 872012
18		00E016A11883	Broadcast	ARP: C PA=[10.0.0.51] PRO=IP
19		Intel 86E452	00E016A11883	ARP: B PA=[10.0.0.51] HA=Intel 86E452
20		00E016A11883	Broadcast	ARP: C PA=[10.0.0.55] PRO=IP
21		Intel 872455	00E016A11883	ARP: B PA=[10.0.0.55] HA=Intel 872455
22		00E016A11883	Broadcast	ARP: C PA=[10.0.0.49] PRO=IP
23		Intel 872012	00E016A11883	ARP: B PA=[10.0.0.49] HA=Intel 872012
24		00E016A11883	Broadcast	ARP: C PA=[10.0.0.50] PRO=IP

Figure 1. This ARP scan has identified 10 IP clients and their hardware addresses.

crementing the value for the target IP address field in each broadcast packet. For example, Figure 1 shows an ARP scan in progress. (The trace files shown in this article are available online at [www.packet-level.com/traces.htm](http://www.packet-level.com/traces.htm). The trace files are available in both Sniffer [.cap] format and EtherPeek [.pkt] format. Sniffer is a protocol analyzer available from Network Associates Inc. EtherPeek is a protocol analyzer available from Wild Packets Inc.)

The ARP scan is foolproof: Every IP device on a network segment must respond when its IP address is broadcast in an ARP request.

**ICMP SCAN**

ICMP provides error and information messages across the internetwork. In addition, hackers can use ICMP to discover information about active devices on the network. You should monitor the following ICMP scans on your company's network:

- ICMP Echo (ping) scans
- ICMP Router Solicitation scans
- ICMP Address Mask scans

**ICMP Echo (Ping) Scan**

The ICMP Echo scan is the most simplistic discovery method and the easiest to

detect. By sending a series of ICMP echo request (ICMP type 8) packets to various IP addresses, a hacker can determine which systems are active (or "alive"). Knowing that Intruder Detection Systems (IDSs) are designed to catch this type of discovery sequence, hackers vary the destination devices or delay the ping interval by minutes, hours, or even days.

The most efficient way to launch an ICMP Echo scan is to send pings to the broadcast address. Typically, TCP/IP stacks won't allow this type of packet to be sent, so hackers must use special utilities and packet generators to perform this type of scan.

**ICMP Router Solicitation Scan**

The ICMP Router Solicitation scan is used to actively find routers on a network. Of course, a hacker could set up a protocol analyzer to detect routers as they broadcast routing information on the network. In some instances, however, routers may not send updates. For example, if the local network does not have other routers, the router may be configured to not send routing information packets onto the local network.

ICMP offers a method for router discovery. Clients send ICMP router solicitation multicasts onto the network, and routers must respond (as defined in RFC 1122). (For more information about the process of ICMP router solicitation, see "Routing Sequences for ICMP" on p. 32.)

By sending ICMP Router Solicitation packets (ICMP type 9) on the network and listening for ICMP Router Discovery replies (ICMP type 10), hackers can build a list of all of the routers that exist on a network segment. Hackers often use this scan to locate routers that do not reply to ICMP echo requests.

**ICMP Address Mask Scan**

Hackers use the ICMP Address Mask scan to locate active devices on the network. During an ICMP Address Mask scan, a host sends out Address Mask requests (ICMP type 17) and listens for Address Mask replies (ICMP type 18).

Originally, ICMP Address Mask request packets were designed to obtain the local subnet mask for a client. Today, however, this functionality is not used because IP addresses and subnet masks are either assigned manually at the client or assigned automatically through Dynamic Host Configuration Protocol (DHCP).

No.	Source Address	Dest Address	Summary	Time
152	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
153	[10.0.0.1]	[10.0.0.9]	LEP: S=73 S=1104 LEN=8	0:00:03
154	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
155	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
156	[10.0.0.1]	[10.0.0.9]	LEP: S=74 S=1105 LEN=8	0:00:03
157	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
158	[10.0.0.1]	[10.0.0.9]	LEP: S=75 S=1106 LEN=8	0:00:03
159	[10.0.0.1]	[10.0.0.9]	LEP: S=76 S=1107 LEN=8	0:00:03
160	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
161	[10.0.0.1]	[10.0.0.9]	LEP: S=77 S=1108 LEN=8	0:00:03
162	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
163	[10.0.0.1]	[10.0.0.9]	LEP: S=78 S=1109 LEN=8	0:00:03
164	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
165	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
166	[10.0.0.1]	[10.0.0.9]	LEP: S=79 S=1110 LEN=8	0:00:03
167	[10.0.0.1]	[10.0.0.9]	LEP: S=80 S=1111 LEN=8	0:00:03
168	[10.0.0.9]	[10.0.0.1]	Expert: ICMP Port Unreachable ICMP: Destination unreachable (Port unreachable)	0:00:03
169	[10.0.0.1]	[10.0.0.9]	LEP: S=81 S=1112 LEN=8	0:00:03

Figure 2. This UDP scan indicates that UDP port 75 and 79 are open.

## Creating Filters to Detect Cyber Attacks

SCAN TYPE	DESCRIPTION OF FILTER	THRESHOLD
ARP scans	Filter on 0x0806 in the Type field of the Ethernet II header.	ARPs are common. If a network experiences a high number of ARPs at one time or sequential ARP destinations, however, examine the source.
ICMP Echo (Ping) scans	Filter on the value 1 in the IP protocol field (indicating ICMP) and the values 8 (Echo) and 0 (Echo Reply) in the ICMP type field.	Pings should be limited on the network. Consider setting an alarm threshold at 50 ping packets per second. Be alert to the source of ping packets, and consider restricting incoming pings from the Internet.
ICMP Router Solicitation scans	Filter on the value 1 in the IP protocol field (indicating ICMP) and the values 9 (Router Solicitation) and 10 (Router Advertisement) in the ICMP type field.	Examine the network design to determine whether or not these packets are normal: Do hosts obtain their router information using this protocol? If not, consider disabling ICMP router advertisement responses and filtering on these packets.
ICMP Address Mask scans	Filter on the value 1 in the IP protocol field (indicating ICMP) and the values 17 (Address Mask request) and 18 (Address Mask reply) in the ICMP type field.	Examine the network to determine if this protocol is used intentionally. If not, consider filtering on these packets and examining the source of the request packets.
UDP Port scans	Filter on the value 11 in the IP header (indicating UDP) and a minimal packet size (value 28 in the IP total length field).	These packets should never occur on the network. They serve no purpose except as port scans. These scans can throw meaningless data after the UDP header, so you may need to adjust the total length value.
Vanilla TCP Connect scans	Filter on the value 6 in the IP header protocol field (indicating TCP) and the TCP flag field values 2 (SYN flag bit) or 12 (SYN and ACK flag bits).	Since TCP handshakes are a normal part of TCP network operations, you should not be alarmed by these packets unless they become excessive. Watch the number of these packets that occur on the network.
TCP Half-Open scans	Filter on the value 6 in the IP header protocol field (indicating TCP) and the TCP flag field value 2 (SYN flag bit).	TCP handshakes are a normal part of TCP network operations. Do not be alarmed by these packets unless you have a much greater number of SYN packets than SYN ACK packets. This situation indicates half-open connections.
TCP FIN scans	Filter on the value 6 in the IP header protocol field (indicating TCP) and the value 11 in the TCP flags field (the FIN and ACK bits).	The FIN and ACK flags are used to close TCP connections. However, an excessive number of these packets indicate a possible problem. Set an alarm threshold for 50 FIN ACKs per second, and monitor this threshold closely.
TCP XMAS scans	Filter on the value 6 in the IP header protocol field (indicating TCP) and the value 29 in the TCP flags field (the URG, PSH, and FIN).	These packets should never occur on the network. They serve no purpose except as a scan.

*continued on p. 28*

continued from p. 24

**SCAN TYPE**

TCP NULL scans

**DESCRIPTION OF FILTER**

Filter on the value 6 in the IP header protocol field (indicating TCP) and the value 0 in the TCP flags field (no flag bits set).

**THRESHOLD**

These packets should never occur on the network. They serve no purpose except as a scan.

TCP ACK scans

Filter on the value 6 in the IP header protocol field (indicating TCP) and the value 10 in the TCP flags field (the ACK bit).

These packets are used to acknowledge receipt of data. A high number of these packets, however, may signal a possible scan underway.

TCP SYN/FIN with Fragments scan

Filter on the value 6 in the IP header protocol field (indicating TCP) and the value 1 in the More to Come bit in the IP header.

If these packets are minimum size (fragmented within 20 bytes after the IP header), they should never occur on the network. They serve no purpose except as a scan. ●

**UDP PORT SCAN**

Hackers use UDP Port scans to identify listening UDP ports on a target host. These port numbers identify the UDP-based application-layer protocols, such as Trivial File Transfer Protocol (TFTP), which are running on a target device.

UDP scan packets include the data-link header, an IP header, and a UDP header. That's all. By varying the destination port number value in the UDP header and watching the responses, a hacker can determine which UDP ports are listening on the target device. If a target device does not listen on a port, the device replies with an ICMP: Destination unreachable (Port unreachable) packet. (See Figure 2 on p. 22.)

As you can see in Figure 2, the target host 10.0.0.9 does not send an ICMP response for ports 75 (dial-out service) or 79 (finger). This indicates that those ports are probably listening. As you can see by the source and destination port numbers, the UDP Port scan shown in Figure 2 is being performed in sequential order. A sophisticated hacker would most certainly vary the port numbers to avoid detection.

**TCP SCAN**

Hackers use TCP scans to identify active devices and their TCP-based application-layer protocols. TCP scans exploit either the TCP handshake process or the TCP connection maintenance process.

Seven types of TCP scans are commonly used:

- Vanilla TCP Connect scans
- TCP Half-Open scans

- TCP FIN scans
- TCP XMAS scans
- TCP NULL scans
- TCP ACK scans
- TCP SYN/FIN with Fragments scans

**Vanilla TCP Connect Scan**

Hackers use the Vanilla TCP Connect scan to identify listening TCP ports on a target device. These port numbers identify the TCP-based application-layer protocols (such as HTTP or FTP) that are running on the target device.

Most of the more important application-layer protocols use TCP as their transport method. TCP relies on a connection sequence that starts with a TCP handshake. (For more information about the TCP handshake process, see "Inside the TCP Handshake," *Novell Connection*, Mar. 2000, pp. 34–35.

You can download this article from [www.ncmag.com/past](http://www.ncmag.com/past).) This TCP connection sequence can be used to determine which listening ports are available on a target device.

During the Vanilla TCP Connect scan, a hacker sends the first packet of the handshake sequence with the Synchronize flag (SYN) set to the intended target device. If the target port is closed, the target device sends a TCP reply with the Reset (RST) flag set. If the target

port is open, the target device sends a TCP reply with the SYN and Acknowledgment (ACK) flag set. Finally, the hacker sends an ACK response to complete the three-way TCP handshake. (See Figure 3 on p. 30.)

Some IDS devices won't log this process as a hacking attempt because the connection was completed successfully. If the hacker does not send the final ACK packet, however, the connection will be left in a half-open state. This may trigger an IDS alarm.



**TCP Half-Open Scan**

Hackers use the TCP Half-Open scan to detect the listening ports on a target device. Unlike the Vanilla TCP Connect Scan, TCP Half-Open scans do not include the final ACK packet, the third packet of the TCP three-way handshake.

**Note.** You can use the Windows NETSTAT utility to identify the half-open connections on your company's network.

**TCP FIN Scan**

Hackers use the TCP FIN scan to identify listening TCP port numbers based on how the target device reacts to a transaction close request for a TCP port (even though no connection may exist before these close requests are made). This type of scan can get through basic firewalls and boundary

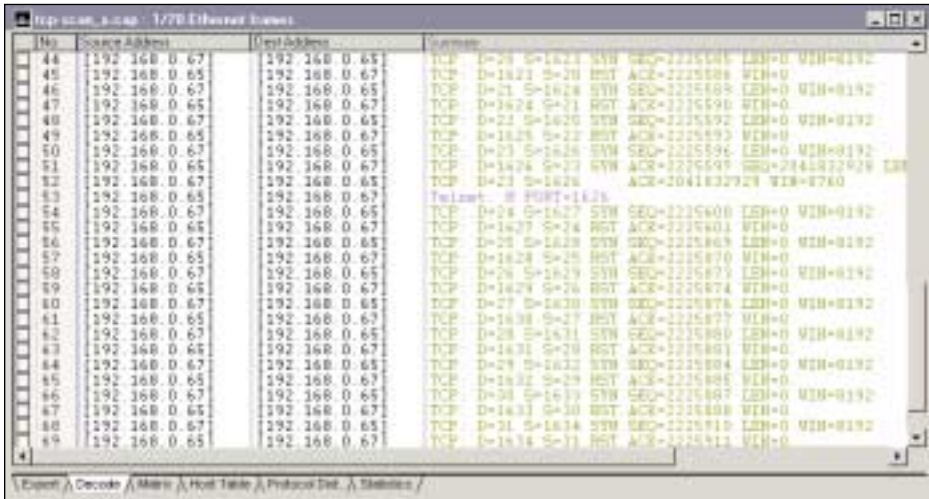


Figure 3. The TCP Port scan indicates that the destination device supports telnet.

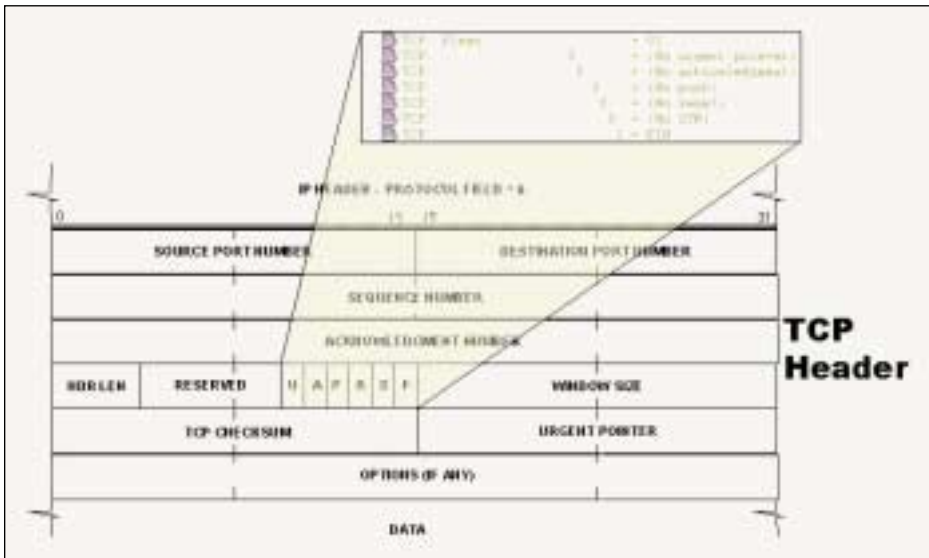


Figure 4. The breakdown of the TCP FIN flag setting in the TCP header.

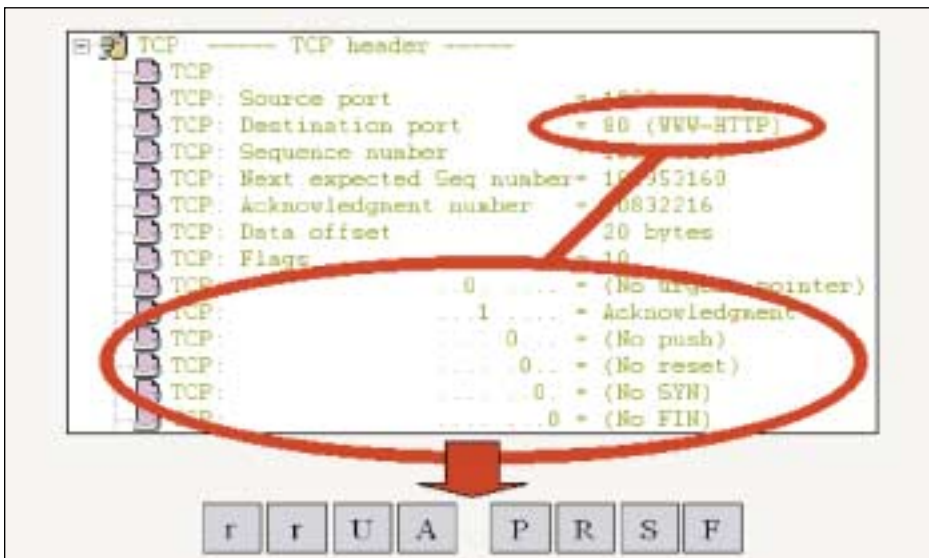


Figure 5. The TCP ACK scan packet can go through firewalls to test for active systems.

routers that filter on incoming TCP packets with the Finish (FIN) and ACK flag combination. The TCP packets used in this scan include only the TCP FIN flag setting.

If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target device discards the FIN and sends no reply. Figure 4 shows the TCP flags field when the FIN scan is used.

### TCP XMAS Scan

Hackers use the TCP XMAS scan to identify listening TCP ports. This scan uses a series of strangely configured TCP packets, which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags. Again, this type of scan can get through some basic firewalls and boundary routers that filter on incoming TCP packets with standard flag settings.

If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP XMAS scan, sending no reply.

### TCP NULL Scan

Hackers use the TCP NULL scan to identify listening TCP ports. This scan also uses a series of strangely configured TCP packets, which contain a sequence number of 0 and no flags. Again, this type of scan can get through some firewalls and boundary routers that filter on incoming TCP packets with standard flag settings.

If the target device's TCP port is closed, the target device sends a TCP RST packet in reply. If the target device's TCP port is open, the target discards the TCP NULL scan, sending no reply.

### TCP ACK Scan

Hackers use the TCP ACK scan to identify active web sites that may not respond to standard ICMP pings because these web sites have been configured not to respond to these pings. The TCP ACK scan uses TCP packets with the ACK flag set to a probable port number—a port number that is most likely open on the destination. For example, port 80 is the standard port used for HTTP communications. (Figure 5

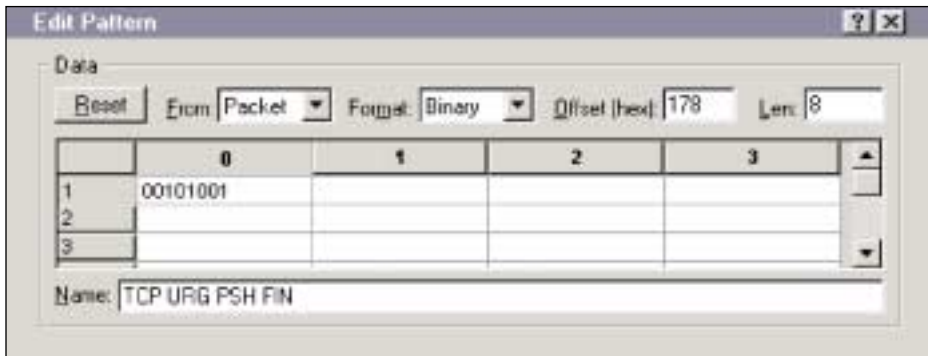


Figure 6. The TCP XMAS filter

shows the flag setting used in TCP ACK scan packets.)

The purpose of the TCP ACK packet is to simply determine if the host is active. Also, hackers do not then need to use the ping packet.

If the target device is available and the HTTP port is open, the target device sends a TCP RST packet in reply.

#### TCP SYN/FIN With Fragments Scan

Hackers often use the TCP SYN/FIN With Fragments scan to bypass a filter-

ing device. To perform this scan, hackers fragment a packet inside the TCP header. Unless the filtering device reassembles the packet, this device will not know that the incoming packet is a TCP SYN/FIN packet.

#### CATCHING SCANS WITH A PROTOCOL ANALYZER

Using a protocol analyzer, you can easily set up a series of filters that can identify the flag patterns used in scan packets. For example, in Figure 6, I

created a filter to catch all TCP XMAS scan packets. These packets contain the value 0x29 at the flags' offset in the TCP header.

"Creating Filters to Detect Cyber Attacks" on page 24 will help you identify the most common types of scans and the filters you can use to detect these attacks. In some cases, a single packet signals a problem on the network. In other cases, a low threshold should trigger an alarm.

Since performing a scan is the first step to launching a cyber attack, detecting scans as quickly as possible is important. For more information about building advanced filters for your protocol analyzer, see the "Advanced Packet Filtering" article, which is posted online at [www.packet-level.com](http://www.packet-level.com). You can also attend the "Advanced Network Analysis" session TUT231 at BrainShare 2001 in Salt Lake City.

Laura Chappell has just released *Advanced Network Analysis Techniques*, which is available online at [www.podbooks.com](http://www.podbooks.com). ●

Please visit our advertiser  
**Castelle**  
 at [www.castelle.com](http://www.castelle.com).