

Hot Summary Statistics

Over the past several months, I have been presenting my Network Analysis, Troubleshooting, and Cyber Crime course in major cities in the United States and Canada. During this road show, I've had the opportunity to share many of my favorite tools, tricks, and techniques for network troubleshooting and cyber-crime detection and testing.

One particularly useful tool is EtherPeek's Summary Statistics window—it's hot! (EtherPeek is a protocol analyzer made by Wild Packets Inc. To open the Summary Statistics window in EtherPeek, click the Summary Statistics icon on the main toolbar.) Using the information provided in the Summary Statistics window, I can identify the following traffic behaviors on networks:

- Ping scans are looking for active systems on the entire network.
- OS fingerprinting is attempting to identify operating system types and versions.
- Port scans are looking for active services over TCP or User Datagram Protocol (UDP).
- Routing configurations are causing packet redirection or advertising new default gateway settings.
- Address Resolution Protocol (ARP) scans are looking for active systems on a subnet.
- Services are not configured properly, or services are not functioning properly.
- Traceroute is attempting to discover network paths.

EtherPeek's Summary Statistics window is organized into categories. During onsite analysis visits, I focus on the following two categories:

- Internet Control Message Protocol (ICMP) analysis
- IP analysis

ICMP ANALYSIS SUMMARY INFORMATION

During an onsite analysis visit, one of my first tasks is to baseline network performance and identify the "personality" of the network. To perform this baseline, I first look for ICMP packets.

One of the most informative protocols available in the TCP/IP protocol suite, ICMP is used for both good and bad. On one hand, some ICMP packets help you isolate network configuration and performance problems. On the other hand, ICMP is the protocol of choice for people who perform reconnaissance on networks, operating systems, and network services for the eventual purpose of hacking in.



EtherPeek's Summary Statistics window provides quite a bit of detail about the ICMP traffic on a network. (See Figure 1 on p. 24.) You should monitor the following types of ICMP packets:

Ping Packet Statistics (ICMP Echo Packets)

Three items in the Summary Statistics window deal with ping operations:

- Pings Unanswered
- Ping Requests
- Ping Responses

The Pings Unanswered value is equal to the ping requests minus the ping responses.

If I see a high number of ping requests (and even a counter that increments) but a low number of pings unanswered, I know that one device is successfully pinging another device.

Because pinging is typically used for a short connectivity test, a high number of pings is not normal on a network. Of course, a high number of pings may indicate that a user is playing with the PING command. My next step in this case would be to identify the devices that are sending continuous pings and get them to shut up!

If I see a high number of ping requests and a high number of pings unanswered, however, I will look for someone performing a ping scan on the network. A ping scan is used to identify all of the active systems on a network.

Is there any reason a system should perform such an operation? Watch out for your network management tools. They may use a ping scan to build one of those lovely network maps.

Whatever the reason, you need to check out which device or program is ping scanning and why. You definitely don't want ping scans coming from the Internet. In fact, you may want to block all outgoing ICMP communications to thwart these types of probes.

| Statistic | Current |
|--------------------------|---------|
| ICMP Analysis | |
| - Pings Unanswered | 0 |
| - ICMP Packets | 250 |
| - Ping Responses | 32 |
| - Ping Requests | 32 |
| - ICMP Router Advert | 0 |
| - ICMP Router Solicit | 3 |
| - ICMP Time Exceeded | 0 |
| - ICMP Param Problem | 0 |
| - ICMP Timestamp Req | 4 |
| - ICMP Timestamp Rep | 4 |
| - ICMP Obsolete (7) | 4 |
| - ICMP Addr Mask Req | 4 |
| - ICMP Addr Mask Rep | 4 |
| - ICMP Source Quench | 0 |
| - ICMP Net Redirect | 0 |
| - ICMP Host Redirect | 0 |
| - ICMP Net Srv Redirect | 0 |
| - ICMP Host Srv Redirect | 0 |
| - ICMP Dest Unreach | 163 |
| - ICMP Net Unreach | 0 |
| - ICMP Host Unreach | 0 |
| - ICMP Proto Unreach | 0 |
| - ICMP Port Unreach | 163 |
| - ICMP Frag Needed | 0 |
| - ICMP Route Failed | 0 |
| - ICMP Net Unknown | 0 |
| - ICMP Host Unknown | 0 |
| - ICMP Net Prohibit | 0 |
| - ICMP Host Prohibit | 0 |
| - ICMP Net Srv Block | 0 |
| - ICMP Host Srv Block | 0 |
| - ICMP Conn Prohibited | 0 |
| - ICMP Host Violation | 0 |
| - ICMP Precedence Cutoff | 0 |

Figure 1. The ICMP Analysis section can help identify configuration problems as well as OS fingerprinting and UDP-based port scans.

OS Fingerprinting

As the name suggests, OS fingerprinting is used to identify the operating system and version running on a computer. Several tools, such as the following, are used for OS fingerprinting:

- Xprobe (www.sys-security.com/html/projects/X.html)
- nmap (www.insecure.org/nmap/nmap-fingerprinting-article.html)
- LANguard Network Scanner (www.gfi.com)

In the early days of OS fingerprinting, tools used TCP connections and banner pages to determine which OS was running on a system. Banners are initial connection details that are displayed when you reach an open service such as FTP or telnet. Many times the operating system identifies itself when the initial connection is established.

In recent years, however, many FTP servers do not disclose their operating system by default. As a result, OS fingerprinting

with TCP is difficult or even impossible. This is where ICMP comes into play.

ICMP-based OS fingerprinting uses a technique documented by Ofir Arkin in "ICMP Usage in Scanning" (www.sys-security.com/html/projects/icmp.html). Tools using this technique send an assortment of ICMP packets that are well-formed or malformed and watch the replies. Operating systems respond in a variety of ways, enabling hackers to classify the operating systems and decide the next step based on the operating system's vulnerabilities.

The following ICMP packets are commonly used during OS fingerprinting:

- Echo requests (ICMP Type 8) and replies (ICMP Type 0)
- Host parameter problem (ICMP Type 12)
- Timestamp requests (ICMP Type 13) and replies (ICMP Type 14)
- Information requests (ICMP Type 15) and replies (ICMP Type 16)
- Address mask requests (ICMP Type 17) and replies (ICMP Type 18)
- Router Solicitation (ICMP Type 10) and replies (ICMP Type 9)

OS fingerprinting tools may not use all of these packet types, but they do typically use several of them.

By reviewing the EtherPeek Summary Statistics window, you can determine if these types of packets have been transmitted on your network. In Figure 1, for example, ICMP Router Solicitations, Timestamp Requests/Responses, and Address Mask Requests/Replies have been transmitted across the network.

Because these types of ICMP packets are rarely used for legitimate purposes, you must look closely to see if someone is running OS fingerprinting on the network. You may want to use a protocol analyzer to define special filters that capture these suspect packets.

Network/Host Redirection

When a host sends a packet to a router that knows it is not the best router to get to the destination, that receiving router sends an ICMP Network/Host Redirection packet back to the host. This redirection packet contains the IP address of the preferred router that the host should use.

Upon receiving an ICMP Network/Host redirection message, the host updates its routing tables with a dynamic entry for the destination network/host. By typing ROUTE PRINT in the command box, you can see the new entry in the routing table.

If a network shows a high number of these redirection packets, either the default gateway setting is not appropriate for the network hosts or someone may be trying to redirect packets for a malicious purpose. To determine the cause, you should capture the traffic for a while and watch the redirection packets.

By determining which device is sending the redirection packets and by examining the preferred router information within the packets, you can tell if the redirection is occurring because the router did not offer the best path or if the redirection points to a system that should not be offering routes. In the latter case, you may have a hacker. By redirecting the packets through his or her system, the hacker can read the traffic to identify information such as usernames, passwords, and unencrypted data.

Destination Unreachables and UDP Port Scans

EtherPeek's Summary Statistics window contains a list of ICMP Destination Unreachable packet types:

- Network unreachable
- Host unreachable
- Protocol unreachable
- Port unreachable

You should pay particular attention to the port unreachable statistics. If the network has a high number of Port Unreachable packets, either a host is misconfigured, or a UDP port scan may be underway.

If a host is misconfigured, the device sends a message to the desired destination device—such as a Domain Naming System (DNS) server. If the destination device doesn't support the services requested, it responds with an ICMP Destination Unreachable packet—specifically a Port Unreachable packet.

You should examine the ICMP communication to watch the systems sending the ICMP Port Unreachable packets. Because these are basically service refusals, you need to know what is causing them and create a solution to eradicate these packets from the network.

During a UDP port scan, a hacker sends a series of UDP packets to a range of ports. The hacker usually focuses on the ports that offer vulnerable or interesting services over UDP, such as Dynamic Host Configuration Protocol (DHCP), DNS, and Simple Network Management Protocol (SNMP). If the service is not available on the target device, this device sends back an ICMP Port Unreachable packet.

If a network has a rapidly increasing number of ICMP Port Unreachable packets, you should carefully examine the traffic to determine if a device is sending a series of packets to a range of destination port numbers. Such behavior is not normal or acceptable on the network.

IP ANALYSIS SUMMARY INFORMATION

In the IP analysis category, EtherPeek lists the number of ARP requests, ARP responses, TCP SYNs (synchronize sequence number requests), FINs (notifications that a task is completed), RST (resetting or refusing a connection), and RARP (Reverse ARP) operations. (See Figure 2.) These statistics can indicate that a network configuration problem exists or that someone is scanning your network.

Excessive Unanswered ARPs

A high number of unanswered ARPs indicates that a device is looking up the hardware address of a local device that is not responding. This lack of response may be caused by one of the following:

- A network mask is misconfigured. (The sending device thinks the target device is on the same network when it is not.)
- The target device is not functioning.

A high number of unanswered ARPs may also indicate that an ARP scan is underway. ARP scanning is used to discover all of the hardware addresses of the systems running on the local network. Of course, some management systems may use ARP scanning to build those beautiful network maps, but you need to

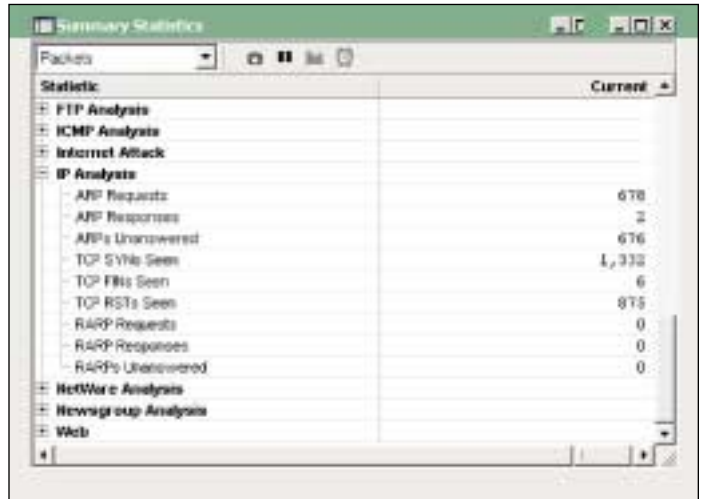


Figure 2. The IP Analysis section can be used to identify misconfigurations, ARP scans, and TCP scans.

capture the traffic to determine if that is actually the case.

TCP-Based Port Scanning

Just as UDP-based port scanning looks for systems supporting UDP-based services, TCP-based port scanning looks for services running over TCP. Because most of the really interesting services (such as FTP, telnet, or HTTP) run over TCP, you must watch out for these TCP scans on the network.

TCP scans generate an unusually high number of RST packets. During a TCP scan, a host sends a series of packets to the desired port (such as the FTP port 21) on a target device. If the device supports the service, it sends a TCP SYN ACK (synchronize with acknowledgment) response. If the device does not support the service, it sends a TCP Reset in response.

Although many people believe resets are sent at the end of every TCP communication to close the connection, in actuality, FIN packets are typically used. For example, when you close a web browser, the web client and the web server send FIN packets to indicate that the client is done with the tasks it was performing. When you see a high number of RST packets (greater than 30 percent of the number of SYN packets), check out the traffic to see if a TCP port scan is underway on your network.

CONCLUSION

WildPackets has done a great job of collecting key information in one location. You should regularly check the ICMP Analysis and IP Analysis categories in the Summary Statistics windows to look for unusual traffic patterns. You can identify possible problems—from client misconfigurations to hackers performing reconnaissance on your network—without capturing a single packet! (For more information about EtherPeek, visit www.wildpackets.com.)

You may also want to download the ICMP protocol poster from the Protocol Analysis Institute at www.packet-level.net/pdfs/icmp.pdf.

Laura Chappell performs onsite network analysis sessions for troubleshooting, optimization, and security checks. She also teaches hands-on courses on protocol analysis. For more information about how she can help your company's network run more efficiently and more securely, visit www.packet-level.com. ●