Identifying and Modeling

Unwanted Traffic on the Internet

by

Paul Soto

Submitted to the Department of Electrical Engineering and Computer Science

in Partial Fulfillment of the Requirements for the Degree of

Master of Engineering in Electrical Engineering and Computer Science

at the

MASSACHUSETTS INSTITUTE OF TECHNOLOGY

[February 2006]

November 2005

Author ____________________

Department of Electrical Engineering and Computer Science
November 4, 2005

Certified by ____________________

Dr. Richard Lippmann
Thesis Supervisor

Accepted by ____________________

Arthur C. Smith
Chairman, Department Committee on Graduate Theses

Identifying and Modeling
Unwanted Traffic on the Internet

by

Paul Soto

Submitted to the
Department of Electrical Engineering and Computer Science

Nov. 4, 2005

In Partial Fulfillment of the Requirements for the Degree of
Master of Engineering in Electrical Engineering and Computer Science

ABSTRACT

Accurate models of Internet traffic are important for successful testing of devices that provide network security. However, with the growth of the Internet, it has become increasingly difficult to develop and maintain accurate traffic models. While much Internet traffic is legitimate, productive communications between users and services, a significant portion of Internet traffic is the result of unwanted messages sent to IP addresses without regard as to whether there is an active host at that address. In an effort to analyze unwanted traffic, tools were developed that generate statistics and plots on captured unwanted traffic to unused IP addresses. These tools were used on a four-day period of traffic received on an inactive IPv4 class A network address space. Each class B subnet in this address space received an average of 7 million packets corresponding to 21 packets per second. Analyses were performed on a range of class B and C subnets with the intent of discovering the types of variability that are characteristic of unwanted traffic. Traffic volume over time, number of scans, destinations ports, and traffic sources varied substantially across class B and C subnets. The results of the analyses, along with tools to replay traffic, allow security tools to be analyzed on the LARIAT network testbed. LARIAT is a real-time adaptable network testbed developed at Lincoln Laboratory that provides an Internet-like environment in which to test network hardware and software.

Thesis Supervisor: Dr. Richard Lippmann
Title: Information Systems Technology Senior Staff, MIT Lincoln Laboratory

Acknowledgements

I would like to give my sincere thanks to Richard Lippmann. It was a privilege to have worked under his guidance. I valued his thought-provoking questions, which always had me wanting to go back to the dataset for further analysis.

I am deeply grateful to have worked with William Streilein. He has been an immense help on everything throughout the project.

Both Rich and Bill have provided me with many suggestions on avenues of approach for analyzing and understanding the dataset. They also offered useful comments and numerous corrections on the various drafts of this thesis, helping to make it clearer and more thorough.

I would like to thank Lee Rossey and Robert Cashman for their help. Among other things, they have provided me with ideas on the causes behind the traffic, how the traffic can be used in real-world systems, and what consumers would want to gather from analyzed traffic.

Many thanks go to Colleen Shannon at CAIDA for her insightful observations and remarks during the frequent reviews of the traffic result.

I would like to thank CAIDA for providing the dataset used in this research and Lincoln Laboratory for providing the resources to analyze the dataset.

Finally, my biggest thanks goes to my family for their never-ending support and encouragement.

I cannot stress enough how much I appreciated the help everyone had provided me.
Thank you.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Accurate models of Internet traffic are required to design and test devices that process, analyze, and act upon this traffic. Accurate estimates of traffic rates enable a manufacturer to design and build forwarding devices, such as routers and switches, which will keep up and not collapse under typical activity. Similarly, a commercial website designed in anticipation of a realistic number of requests per day stands a better chance delivering services to customers than one that has not been designed with these factors in mind. In addition to traffic rates, traffic complexity plays an important role in testing security devices. Firewalls, intrusion detection systems, and other security devices must be resilient to harmless traffic patterns that generate false alarms.

As the Internet has grown, the quantity and variety of Internet traffic has increased an enormous rate [1]. One might expect that such an increase in traffic is the result of productive communications between a growing number of users and new web pages and service applications now available on the Internet. While this is true to a large degree, it is also true that a significant amount of traffic seen on the Internet is destined to hosts that either did not request or do not expect the traffic. The increasing quantity and variety of this unrequested and unexpected traffic makes it difficult to develop realistic models of Internet traffic [1]. For the discussion and analysis that follows, unrequested and unexpected traffic is referred to as unwanted traffic (UT). UT is generally composed of malicious traffic sent from worms, viruses, probes, and spyware, but can also consist of traffic sent from misconfigured routers or applications, and traffic corrupted by noise or interference on network transmission lines [2,3]. While there has been a large amount of study on the volume and variety of productive traffic on the Internet, little work has been done to understand and classify UT on the Internet.

The goal of this project is to gain an understanding of key characteristics of UT through the use of exploratory data analysis. Toward this end, software tools were developed that describe UT through plots, tables, and short summaries. These representations of UT demonstrate that UT is complex and highly variable across subnets and time, and thus hard to model. Instead of modeling UT, I show how it can be replayed on a network testbed, for device testing. In addition, I attempt to classify a wide range of UT seen and catalog the attacks commonly seen in UT.

This project is motivated by the need to develop a testing environment that includes realistic UT. The analyses in this project will allow for the development of systems that model the Internet with greater accuracy. One system that models and generates Internet traffic is the Lincoln Adaptable Real-time Information Assurance Testbed (LARIAT) [4]. LARIAT generates Internet traffic that allows hardware and software security tools, such as, intrusion detection systems (IDS's) and firewalls, to be tested under reliable, repeatable real-world conditions without being exposed to real Internet traffic. This is accomplished using a network of computers that replicate Internet sites and model the various behaviors of users, such as browsing web pages, writing documents, and sending and receiving email. While this system does a good job at modeling typical user behavior and interaction with server machines, the generated traffic does not contain UT, as described above. The analyses performed here make it possible to select portions of UT to replay on LARIAT. This traffic replay will contain realistic UT traffic characteristics previously unavailable on LARIAT.

Another motivation of this project is to enhance the current understanding of Internet traffic. Organizations such as the Cooperative Association for Internet Data Analysis, CAIDA, strive to "provide enhanced insight into the function of Internet infrastructure worldwide" [5]. Developing tools that enable the identification and analysis of UT, now and in the future, will allow for the observation of trends in this area of traffic.

The rest of this thesis is laid out as follows. Chapter 2 explains the terminology used in the paper. Chapter 3 discusses previous work done in related areas and the traffic data used in the analysis. The methodology and analysis procedures are presented here. Chapter 4 presents the details of how the measurements, tables, and plots of the exploratory data analysis tools work and how their output should be interpreted. Chapter 5 discusses the results of the analyses and the various phenomena observed in UT. Chapter 6 presents a summary of the work and considers future directions.

Chapter 2

Network Terminology

This chapter defines terminology used to discuss and analyze unwanted traffic.

2.1 Classes of IPv4 Address Ranges

A *class A network* is a contiguous range of 2^{24} (16,777,216) IPv4 addresses, where the leading octet of the IP address is any constant between 1 and 126, inclusive. Each of the other three octets can range from 0 to 255, inclusive. The CIDR equivalent subnet mask for a class A network is /8. *Class B subnets* refer to an IP address range where the first two leading octets of the IP address are constant (ex. 1.2.0.0/16). There are 2^{16} (65,536) IP addresses within a class B subnet. Similarly, *class C subnets* refer to an IP address range where the first three leading octets of the IP address are constant (ex. 1.2.3.0/24). There are 2^{8} (256) IP addresses within a class C subnet.

2.2 Network Telescopes

A network telescope [6,7] is a routed but unused IP address space. An unused IP address space is a range of IP addresses that contains no active hosts generating or replying to traffic. Sources that send traffic to a network telescope have no reason to believe that there are active hosts to respond to the traffic, and so there is no legitimate purpose in sending traffic to a network telescope. A network telescope can be of any size, with larger network telescopes being more likely to observe packets sooner from Internet events, such as worms spreading. Network telescopes offer a convenient way of observing Internet-wide events, as there are no outbound packets, which would interfere with the composition of the traffic from these events.

2.3 Backscatter

Backscatter is defined as traffic received from victims that are responding to malicious denial-of-service (DOS) attacks. Since backscatter is response traffic, the packet types that backscatter can consist of are limited to TCP SYN/ACKs, TCP RST/ACKs, and certain ICMP types like Echo Reply and Destination Unreachable. Backscatter arrives at the unused address space because the source addresses of the attack traffic are spoofed. If the source address is spoofed randomly from the entire IPv4 address space, the probability of a backscatter packet reaching a network telescope is $n/2^{32}$, where n is the size of the network telescope.

Chapter 3

Unwanted Traffic Characterization

This chapter discusses some of the previous work performed in relation to unwanted traffic. The data used in the analyses and the methodology is also explained.

3.1 Previous Work

Only recently have researchers begun to analyze unwanted traffic. UT can be categorized into primary and secondary unwanted traffic. Primary UT is typically an initiating packet, such as a connection request originating from an attacker or misconfigured host. These packets are commonly TCP SYNs, UDP, or ICMP Echo Request packets. Secondary UT is response traffic solicited by primary traffic, where the source IP address is spoofed. These packets are commonly TCP SYN/ACKs, TCP RST/ACKs, or ICMP Destination Unreachable. Moore et al. [8] have looked at secondary unwanted traffic, referred to as backscatter, while Pang et al. [9] have looked at primary unwanted traffic.

The work of Moore et al. [8], presents an in-depth analysis of backscatter traffic as received by a network telescope. Through their analysis of three weeks worth of traffic from February 2001, on a class A network telescope, the authors derive an estimate of the composition of backscatter and the duration of denial-of-service attacks seen on the Internet. They observed approximately 71% of the backscatter packets to be ICMP packets (Destination Unreachable and TTL exceeded), 21% to be TCP RST/ACK packets, and 7% to be TCP SYN/ACK and TCP RST packets. They also observed that 90% of the attacks lasted less than an hour. Backscatter traffic represents a significant portion of unwanted traffic and will be a component of the data replayed through the current research. The work of Moore et al. did not look at primary unwanted traffic, which will be the other component of the replayed data.

Pang et al [9] present a second research effort related to the analysis of unwanted traffic. In a fashion similar to the work of Moore et al., the researchers capture and analyze traffic received at various unused IP address spaces. Denoting the unwanted traffic received as 'background radiation,' Pang et al. develop response agents that interact with primary traffic sources. By engaging the sources of the primary traffic in communication, the researchers are able to recognize specific attack types and develop detailed descriptions of the composition of this component of unwanted traffic. Before developing the responding agents to any packets, they collected a week of traffic on 10 contiguous class B subnets, from April 28 to May 5, 2004, and a week of traffic on a class A network with 1/10 sampling, from March 11 to March 18, 2004. On the 10 class B subnets, the traffic was composed of 56.5% TCP, 39.6% ICMP, and 3.8% UDP. The top 3 TCP ports targeted, based on packet count, were 135, 445, and 139. These three ports accounted for over 60% of the TCP SYN packets. On the class A network, the traffic was comprised of 88.5% TCP, 0.3% ICMP, and 11.3% UDP packets. In both of these datasets, 99% of the TCP packets were TCP SYNs. Except for the ICMP packets in the 10 class B subnets (99.9% of which were ICMP Echo Request), there were no temporal patterns observed in the packet rate.

3.2 Traffic Data Used for Analysis

One of the goals of this project was to analyze unwanted traffic, including both primary and backscatter UT. UT was defined as unrequested and unexpected traffic. Care was taken to ensure that the dataset selected for analysis did not contain Internet traffic that was not UT. For this reason, the dataset chosen was derived from a network telescope. Because these sources sent traffic to a network telescope, which, by definition, have no active hosts, this traffic was unrequested and unexpected, hence, unwanted traffic.

The dataset used was provided by CAIDA. It represents traffic destined for a class A network telescope. The dataset was collected over a period of 93 hours starting from 2:30 PM EST on Monday February 28, 2005 and ending at 11:30 AM EST on Friday, March 4, 2005. In total, there were 160GB of trace files.

There were certain filtering requirements on the traffic data. Although the address range of the network telescope was unused, it was not completely empty; there existed hosts on this network that were the source of data. While none of the machines in the network telescope communicated to the Internet, certain machines communicated to other machines within the class

A network. The class B subnets in the dataset that contained any machine either transmitting or receiving internal traffic within the class A subnet were filtered. This left 123 class B subnets free of any type of data contamination.

3.3 Methodology

The first analysis step was to break the data up into manageable segments and select the segments to analyze. The UT to be incorporated into LARIAT will be played back onto class B or C subnets, and so we analyzed the data as such. There were 123 class B and 31,488 class C subnets available for analysis. Unfortunately, performing a thorough analysis on this many subnets would have meant going through hundreds of thousands of plots and charts. As this would have be too time consuming, a quick analysis was performed on a measurement of interest to the users of LARIAT, namely, total traffic destined to a subnet. The class B and C subnets were divided into those at the top, middle, and bottom of a sorted total packet count list. Then 30 subnets were thoroughly analyzed from each group, 180 subnets in total.

The second step was to choose what information to extract from the chosen subnets. The set of measurements chosen are representative of some of the basic characteristics of network traffic. These measurements include traffic protocol composition, destinations addresses and ports hit, the number of source addresses sending traffic to the subnet, and the number of alerts and scans seen in the traffic. These measurements were analyzed with respect to all the traffic, the top 90% of traffic, and top 50% of traffic. The notion of 'top X% of traffic' is different with each measurement, and is explained in detail in chapter 4.2.

With all these measurements, one large table was created, where each row represented a different subnet and each column represented a measurement. The table was sorted according to different measurements, and groupings of subnets based on similar measurements were extrapolated.

The data revealed that class B subnets are hard to cluster based on their measurements. This is attributed to the relative low number of class B subnets available and the different combinations of variability found with 256 class C subnets composing a class B subnet. However, some patterns were identified as targeted specifically to a class B subnet.

The data revealed that class C subnets are easier to cluster based on their measurements. For example, many subnets have low traffic volume and share similar attributes in terms of number of sources sending traffic and number of unique ports destined. The ability to cluster these subnets will allow users to test security tools with a fraction of the class C subnets and yet achieve a wide coverage of the behaviors observed.

Chapter 4

Tools Developed

Software tools were developed that describe UT through measurements, tables, and plots. These tools were developed using the CoralReef [13] software suite, Dislin plotting library [14], and custom Perl scripts. This chapter describes traffic measurements used in the exploratory data analysis and how to interpret these measurements.

4.1 Measurements

The following is a description of each measurement taken on the subnets analyzed. In certain measurements, three values represent the measurement with respect to the top 100%, top 90%, and top 50% of traffic. The precise definition for 'top X% of traffic' differs depending on the measurement, and is defined explicitly in each of the applicable measurements.

1. Total packet and byte count

   The *total packet and byte count* is a measure of the volume of traffic seen on a subnet. This measurement is used as an initial classifier of subnets, where we sorted the subnets by the total packet count, and then analyzed the subnets from the top, middle, and bottom of this list.
2. Average packet and byte rate

   The *average packet and byte rate* for a subnet is *the total packet and byte count* divided by the duration, in seconds, of the dataset.
3. Peak packet and byte rate

The *peak packet and byte rate* is the highest count of packets and bytes received by the subnet in any one-second interval. This value represents the amount of traffic a replay system must be able to handle to avoid dropping packets.

4. Traffic composition in terms of percentage of TCP, UDP, and ICMP

   The traffic composition indicates the percentage of TCP, UDP, and ICMP traffic reaching the subnet. This is calculated by taking separate counts of TCP, UDP, and ICMP packets and dividing by the total packet count for the subnet. Occasionally, these three counts will not add up to 100%, since subnets can receive traffic protocols other than TCP, UDP, and ICMP. However, no other traffic protocol contributed more than 0.1% of the traffic, in any of the subnets analyzed.

5. TCP packet type breakdown

   TCP packets are further broken down into counts of TCP SYN, SYN/ACK, ACK, RST, RST/ACK, and OTHER types. TCP OTHER packets are any TCP packets where the TCP flags do not fall into any of the previously mentioned TCP types.

6. Number of unique Snort alerts

   The *number of unique Snort alerts* indicates how many different types of suspicious activities are hitting a subnet, based on the output from Snort [10]. Snort is a widely deployed intrusion detection system (IDS) that uses a rule-based language to detect potentially malicious packets. Snort was chosen as it represents a popular IDS used in industry.

7. Total number of Snort alerts

   The *total number of Snort alerts* is the sum of all the alerts, as seen by Snort, triggered by the packets received on the subnet.

8. Total number of scans and number of packets composing the scans

   This measurement indicates the total number of scans detected by Snort along with the sum of the packet count of each scan. In the analysis, a scan was defined as containing at least a 1/16 packet count in relation to the number of IP addresses of the subnet. In other words, a scan in a class C subnet, which contains 256 IP addresses, is comprised of at least 16 packets. A scan in a class B subnet, which contains 65,536 IP addresses, is comprised of at least 4,096 packets. Although somewhat arbitrary, 1/16 is the smallest fraction of packets pertaining to a scan that one can easily notice in the corresponding *destination IP address index versus time* plot.

9. Total number of unique destination ports

The *total number of unique destination ports* seen in the traffic help distinguish the level of focus of probes and attacks in the traffic. In the case of ICMP traffic, the ICMP type is treated as unique destination ports (ex. ICMP Destination Unreachable and ICMP TTL Exceeded would be two unique destination ports separate from any TCP or UDP port). The top X% in this measurement is calculated by sorting the total number of packets sent to each TCP port, UDP port, and ICMP type. The sum up the number of packets in this list, in descending order, is taken until the packet count is at least X% of the total packet count. A very low number of ports in the top X% mean that most of the traffic was focused on exploiting a small set of vulnerabilities. A high number in the top X% might mean that there was a lot of backscatter traffic destined for random ports.

10. Number of unique source IP hosts

    This measurement represents the number of unique IP hosts (IP addresses) sending traffic to the subnet. The maximum number of possible hosts in the IP address space is approximately 4 billion. The top X% is taken by sorting a list of source IP addresses, in descending order, by the total number of packets sent to this subnet. The packets sent by each IP address is added until the total contribution of packets sent by these source IP hosts is at least X% of the total number of packets sent. A high number of unique source IP hosts in the top X% means there is a relatively large number of IP addresses sending packets to this subnet. This signifies a distributed attack or random traffic. A low number of unique source IP hosts in the top X% can signify an attack from few sources, or backscatter arriving on the subnet due to a spoofed source IP address in the original attack packet.

11. Average packet and byte count per source

    The *average packet and byte count per source* is calculated by dividing the total packet and byte count by the number of unique source IP hosts sending traffic to the subnet. The top X% is calculated by dividing the total packet and byte count by the top X% value for the number of unique source IP hosts.

12. Number of unique destination IP hosts

    This measurement is similar to the *number of unique source IP hosts* measurement, except that the count is of the number of unique IP addresses inside the subnet that received traffic. The maximum number of possible destination hosts is 65,536 in a class B subnet and 256 in a class C subnet. Given enough time, every host in a class B or C subnet is expected to receive at least one packet. The top X% is calculated by sorting the list of destination IP addresses by total packets received. The packets received by each destination IP address is added, in descending order, until at least X% of the total traffic received on the subnet is accounted for. A high number of destination IP addresses in the top X% signifies that traffic is randomly distributed across the subnet. A low number of destination IP addresses in the top X% signifies that an attack is being directed to a specific machines, or that these machines are receiving backscatter.

13. Average packet and byte count per destination

    The *average packet and byte count per destination* is calculated by dividing the total packet and byte count by the number of unique destination IP addresses receiving traffic. The top X% is calculated by dividing the total packet and byte count by the top X% value for the number of unique destination IP addresses.

4.2 Tables

Several tables were developed as part of the analysis. Although only the top three values for each table per subnet are shown, the software tools developed create complete tables that account for all the traffic. The following is a description of the tables.

1. Protocol type and port destination, across TCP, UDP, and ICMP

   This table shows the total packet and byte counts and percentages destined to a unique protocol port. ICMP packets are included in this table but the ICMP type is used in place of the destination port. This table is sorted by packet count. Table A1-4 in Appendix A is an example of this table. In this example, ICMP does not show up because no ICMP type accounted for more than 12.9% of the packets.

2. Destination IP addresses

   This table contains the total count and percentage of traffic received by each IP address in the subnet, sorted by descending packet count. The first octet of each IP address in the table has been replaced by 'xx' to mask the class A network from which this dataset was collected. Table A1-5 in Appendix A is an example of this table.

3. Source IP addresses

Similar to the *destination IP addresses* table, this table shows the count and percentage of traffic each source IP address sent to the subnet. This table is sorted by packet count. Table A1-6 in Appendix A is an example of this table.

4. Snort alerts

   This table displays each Snort alert triggered by the traffic along with a count of the number of times the alert was triggered and a percentage of the total alert count. Table A1-7 in Appendix A is an example of this table.

4.3 Plots

There are six plots generated for each of the class B and C subnets analyzed. The following is a description of the types of plots generated for each subnet analyzed. Two of the plots have minor differences between the class B and C subnet versions, and are distinguished as different plot types in the list below.

1. Packets per hour versus time

   In the *packets per hour versus time* plots the X-axis represents time measured in hours from the start of the dataset. The Y-axis denotes the total packets received on the subnet per one-hour time interval. The horizontal line in the plot denotes the average packets per hour received on the subnet, measured over the course of the whole dataset. The Y-axis scale was fixed at 300,000 packets per hour for all class B subnet plots, and 14,000 packets per hour for all but one class C subnet plot. Figure A1-1 in Appendix A is an example of this plot.

2. Bytes per hour versus time

   The *bytes per hour versus time plot* is similar to the packet per hour versus time plot, except the data here is in terms of bytes. The Y-axis scale was fixed at 15,000,000 bytes per hour for all class B subnet plots, and 700,000 bytes per hour for all but one class C subnet plot. Figure A1-2 in Appendix A is an example of this plot.

3. Destination IP address index versus time for class C subnets

   In this plot, the X-axis shows time measured in hours. The Y-axis shows the decimal value of the rightmost IP address octet. In other words, all IP addresses in the class C subnet, 256 IP addresses, are represented on the Y-axis. Every point in the plot represents a packet sent at a specific time to a specific IP address. Solid horizontal lines form when one machine constantly received packets for a period of time. Vertical lines represent a range of IP addresses that received packets in a very small time interval. Although one can see horizontal and vertical lines in the plot, in reality the plot is solely composed of points. These points are close enough together that they form solid lines. All of the packets destined to the class C subnet were plotted. Figure B1-3 in Appendix B is an example of this plot. Although there are vertical bars that have the same thickness, such as the ones at +25 and +31, the amount of traffic within each bar cannot be assumed to be similar, as there can be a quick succession of packets which show up as a single point.

4. Destination IP address index versus time for class B subnets

   This plot is similar to the *destination IP address index versus time for class C subnets* plot, except that the Y-axis shows the decimal value of the two rightmost IP address octets. Every single IP address in the class B subnet, 65,536 IP addresses, is represented on the Y-axis. Since this plot contains a much greater range of IP addresses, there are diagonal lines, in addition to horizontal and vertical lines. The diagonal lines are similar to the vertical lines, denoting a range of IP addresses that received packets over the course of time. Another difference in this plot arises from the increased magnitude of packets destined to class B subnets. Although every packet was represented with a point in the class C plots, attempting to plot all the packets received by a class B subnet would yield an unreadable solid box in the plot window. To develop a readable plot for the class B subnet, every 100^{th} point (the title of the plot contains the phrase 'skip=100' to represent this) is plotted. While making the plot readable, plotting every 100^{th} point can lead to loss of significant events in the plot, such as scans. To provide some degree of confidence that there was no major loss of data, the same subnet was plotted various times, shifting the first point used each time. A shift in the first point causes a shift in all the points used that follow. I was able to confirm that the multiple plots of the same subnet were similar by visually observing that the same horizontal, vertical, and diagonal lines were visible in each plot. Figure A1-3 in Appendix A is an example of this plot.

5. Destination port versus time

   In the *destination port versus time* plot, the X-axis represents time, in hours. The Y-axis is a log scale of the port numbers a packet can be destined for, between 1 and 65,535. Each point is plotted as a unique color and symbol depending on the packet type. The packet types shown in this plot are UDP packets and TCP (SYN,

SYN/ACK, ACK, RST, RST/ACK, and OTHER) packets. ICMP packets are not shown, as these packets are not destined to ports. The *destination port versus time* plot allows one to discern which services are receiving packets and if multiple services are being attacked at the same time with similar duration and intensity. Figure A1-4 in Appendix A is an example of this plot. The points are plotted in descending order of packet type as based on the list in the legend. This means that packet types at the bottom of the list, such as RST/ACKs, will obscure packet types preceding them, such as UDP.

6. Total packets to each IP address for class C subnets

   In this plot, the X-axis represents each of the individual 256 IP addresses that compose the class C subnet. The Y-axis shows the total number of packets received over the course of the 93 hours in the dataset. This plot allows one to observe any bias towards a single IP address or a cluster of IP addresses, in terms of packet destination. Figure B1-5 in Appendix B is an example of this plot. This plot shows a bias towards the lower half of the IP range, and that certain IP addresses such as xx.55.145.202 received eight times as many packets as the average. Figure B2-5 in Appendix B is another example of this plot where xx.128.8.14 received so many packets that the quantities received by the other IP addresses do not show up because of the magnitude of the Y-axis scale.

7. Total packets in each class C subnet for class B subnets

   This plot is similar to the *total packets to each IP address for class C subnets* plot except that the X-axis represents each of the 256 class C subnets that compose the class B subnets. For example, on the xx.1.0.0/16 class B subnet plot, the Y-value corresponding to 98 on the X-axis would represent the total packets received by the class C subnet represented by xx.1.98.0/24. Figure A1-5 in Appendix A is an example of this plot.

8. Snort alerts versus time

   In the *Snort alerts versus time* plot, the X-axis represents time measured in hours. The Y-axis on this plot lists each of the Snort alerts seen over the course of the 93 hours, in ascending order, by alert count, where the alert count is shown in parenthesis. Each point on the plot marks a time when a single alert was triggered. Since some of the high-count alerts would show up as solid bars, the point is color-coded to signify the number of alerts seen in that one-hour period. Note that the plot will show a unique point for every single alert, so in a one-hour period, all the points will be the same color, and the number of alerts in that whole one-hour period is equivalent to the associated color in the legend. Figure B1-6 in Appendix B is an example of this plot.

Chapter 5

Characteristics of Unwanted Traffic

This chapter discusses the characteristics of the unwanted traffic arriving on the class A network. The first section explains the general results observed across the whole class A network. Sections 5.2 and 5.3 delve into the phenomena observed within the class B and C subnets. Section 5.4 describes high volume traffic patterns targeted to specific IP addresses.

5.1 General Results

The 123 class B subnets in the dataset received 842 million packets over the course of 93 hours. The composition of the traffic seen in the dataset is shown in Table 1. TCP SYNs, UDP, and ICMP Echo Request packets (comprising 90% of the ICMP packets), are considered types of primary UT and made up 82% of the traffic, while the backscatter is composed of the remaining 18% of the traffic.

Packet Type	% of Total Packets
TCP SYN	59
TCP SYN/ACK	9
TCP RST/ACK	8
TCP OTHER	1
UDP	20
ICMP	3

Table 1 - Breakdown of packet types in the dataset.

The traffic breakdown differs significantly from both Moore's and Pang's results, and hint at how much the distribution of traffic across protocols can differ. Moore's work, which looked at backscatter traffic in 2001, found a two-to-one ratio of ICMP destination unreachable packets to TCP RST/ACKs and TCP SYN/ACKs put together, whereas our dataset had a radically smaller ratio of nearly one-to-fifty. Pang's 2004 study found 11% of the packets in a class A network to be UDP and 88% of the packets to be TCP SYNs. Their class A network received traffic at a rate of 147 packets per destination IP address per day. In our class A network, 20% of the packets were UDP and 59% of the packets were TCP SYNs. The traffic rate was 27 packets per destination IP address per day.

On average, each class B subnet received 6.8 million packets, with 5.2 million packets on the low end, 9.8 million packets on the high end, and two outliers with 12.0 million packets. Figure 1 shows the amount of TCP, UDP, and ICMP packets received by each class B subnet. The amount of ICMP and UDP traffic received at each class B subnet was consistent; however, the amount of TCP traffic varied significantly between the lower and upper half of the class A network. The amount of TCP traffic decreased by approximately 20%, or 1.2 million packets, between the lower half of the class A network (from xx.0.0.0/16 to xx.127.0.0/16, there were 55 class B subnets analyzed) and the upper half of the class A network (from xx.128.0.0/16 to xx.255.0.0/16, there were 68 class B subnets analyzed). This decrease was caused by the unexpected distribution of backscatter traffic.

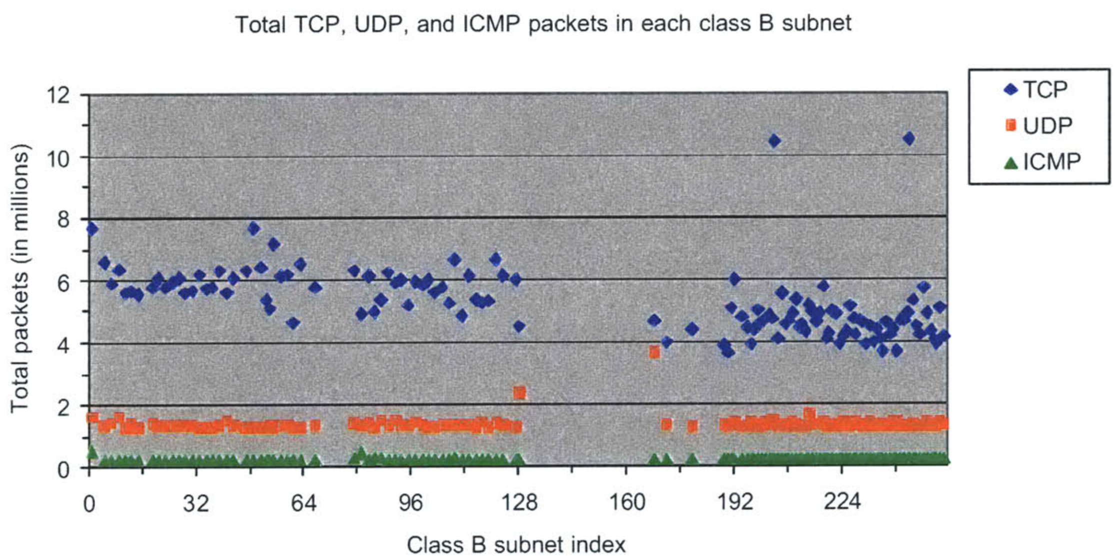

Figure 1 – The total amount of TCP, UDP, and ICMP packets received by each class B subnet.

5.1.1 The Nature of Backscatter

As explained in section 2.3, backscatter traffic is response traffic received from machines replying to spoofed source addresses. It is typically assumed that the source address for the packet causing backscatter is randomly spoofed, and chosen uniformly from the IPv4 address space. Assuming uniformity in spoofed addresses allows one to calculate the amount of backscatter on the Internet, based on the backscatter seen at a network telescope. Two well-known exceptions to the randomness and uniformity of spoofed source addresses are reflector attacks and broken pseudo-random number generators (PRNGs).

Reflector attacks are distributed denial-of-service (DDOS) attacks in which backscatter arrives from multiple machines to a single fixed spoofed source address [11]. The backscatter from this type of attack is meant to disrupt a single machine. This type of attack is recognizable since only a few hosts in a class A network would receive a large amount of backscatter traffic.

PRNGs are used to generate random numbers for IP addresses. A correctly implemented PRNG would generate a uniform distribution of random numbers. Broken PRNGs generate uneven distribution of random numbers. When a broken PRNG generates spoofed source or destination IP addresses, packets will arrive to certain addresses at a higher frequency than other addresses, and some addresses might never be generated.

Closer examination of the TCP traffic, as shown in Figure 2, illustrates that the drop in traffic was due to a decrease in TCP SYN/ACK and RST/ACK packets. The decrease in these two backscatter packet types at different regions of the class A network indicates that the spoofed addresses for backscatter was not selected uniformly from the IPv4 address space. The other types of TCP packets, which contributed to backscatter but comprised less than 1% of the TCP packets, are shown in Figure 3. It is interesting to note, in Figure 3, that the amount of TCP ACKs dropped precipitously in the upper half of the class A network.

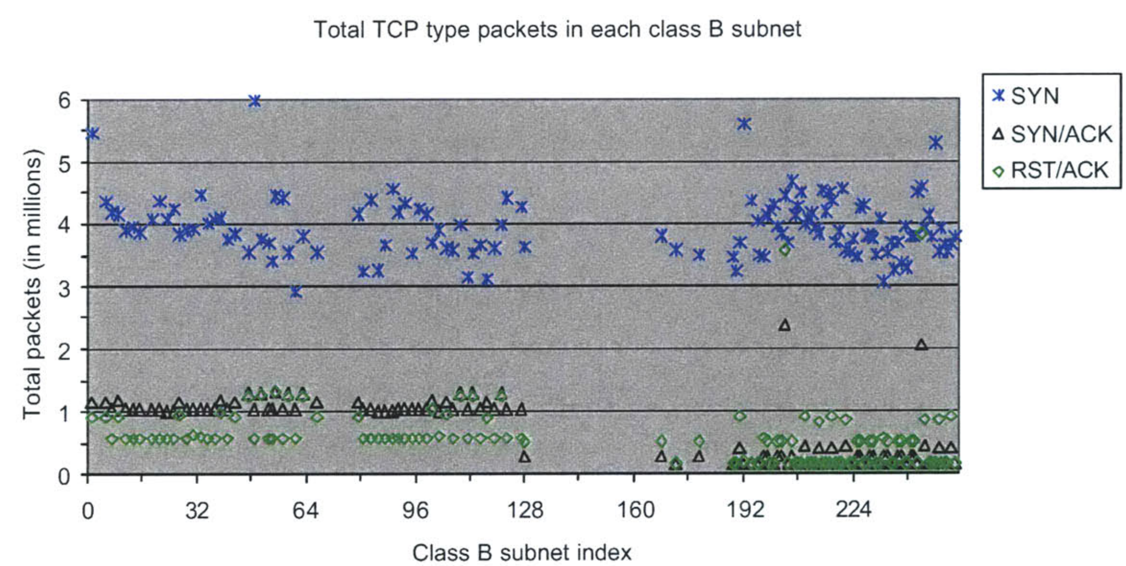

Figure 2 - The three significant TCP packet types received on each class B subnet.

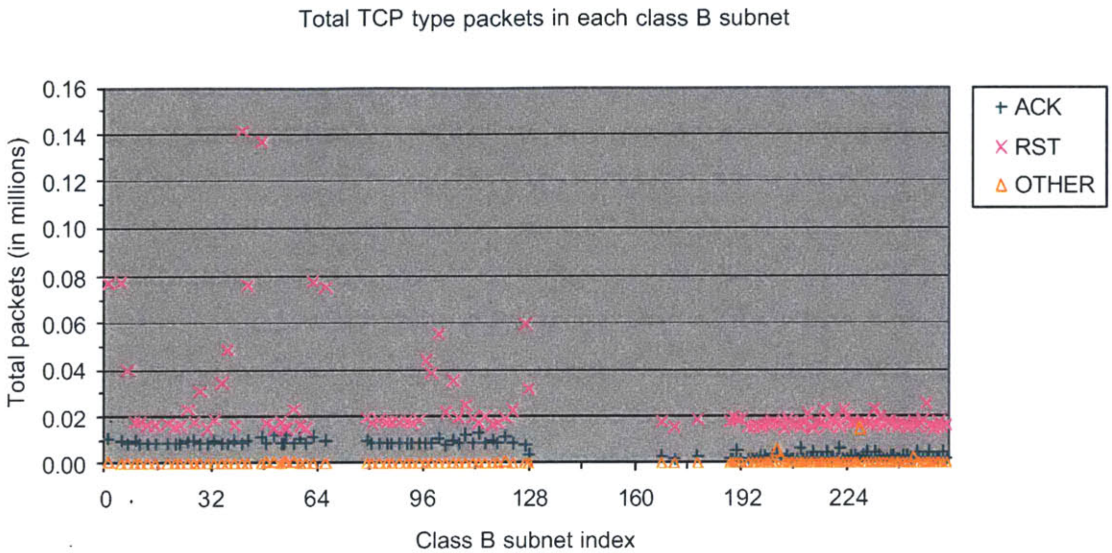

Figure 3 - The remaining TCP packet types received on each class B subnet.

The differences in backscatter between the two halves of the class A network suggest that the backscatter addresses within the class A network were not chosen uniformly. Figure 4, which shows the total amount of backscatter received on each of the class B subnets, reveals that even within the two halves of the class A network, backscatter was not destined uniformly. There were several 'fixed' quantities of backscatter received at different class B subnets throughout both halves of the class A network. Though not literally fixed, the amounts of backscatter received fall into identified clusters with very small standard deviations. From the 123 class B subnets analyzed, there were six clusters of total backscatter, shown in Figure 5 (ignoring 2 outliers at 6 million). Figure 5 was created by plotting the total backscatter on each of the class B subnets, where the subnets are sorted by ascending backscatter quantities. Similarly, the total primary traffic was sorted for all the class B subnets and plotted in Figure 5. Note that the X-axis values do not pertain to any specific class B subnet as the primary and backscatter packet totals were sorted independently and plotted on the same graph for easier comparison. The six clusters of backscatter in Figure 5 form at 620,000, 1.1 million, 1.6 million, 1.9 million, 2.4 million, and 2.9 million packets. These clusters represent a set of impulses in backscatter, concentrated at six values. Primary traffic, on the other hand, has a continuous nearly straight-line curve, which indicates the class B subnets received a uniform distribution of packets between 4.5 and 6 million.

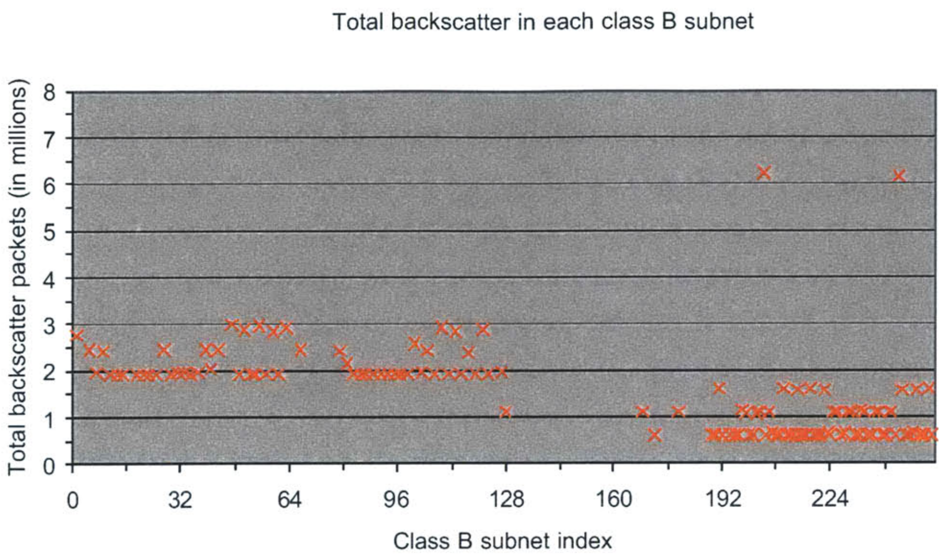

Figure 4 - Backscatter received on each class B subnet.

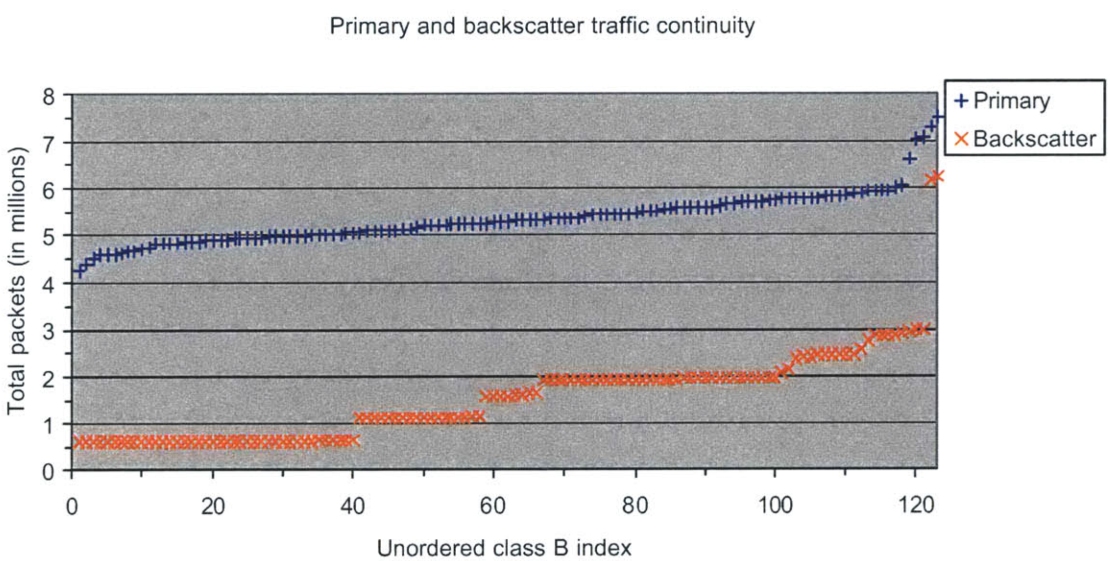

Figure 5 - Primary and backscatter traffic amounts destined to the class B subnets. Both plots sorted independently to illustrate differences in uniformity.

The two main contributors of backscatter were TCP SYN/ACK and TCP RST/ACK packets. SYN/ACK and RST/ACK each accounted for approximately half of the backscatter. SYN/ACKs are sent when a TCP connection attempt is successful. RST/ACKs are sent when the TCP connection is unsuccessful due to an active computer not receiving packets on a specified port. In effect, these two packet types compliment each other, and you would not expect to receive one if you have received the other. However, in the dataset, there was an extremely high correlation, shown in Figure 6, between the number of SYN/ACK packets and the number of RST/ACK packets each class B subnet received. The first three clusters on the left half of Figure 6 correspond to the upper half of the class A subnet and have a ratio of between one and two RST/ACK packets for every one SYN/ACK. The second three clusters, on the right half of Figure 6, correspond to the lower half of the class A subnet and have a ratio of between one and two SYN/ACK packets for every two RST/ACKs. Similarly, there is a very strong correlation between the number of SYN/ACK packets and the number or ACK packets, shown in Figure 7.

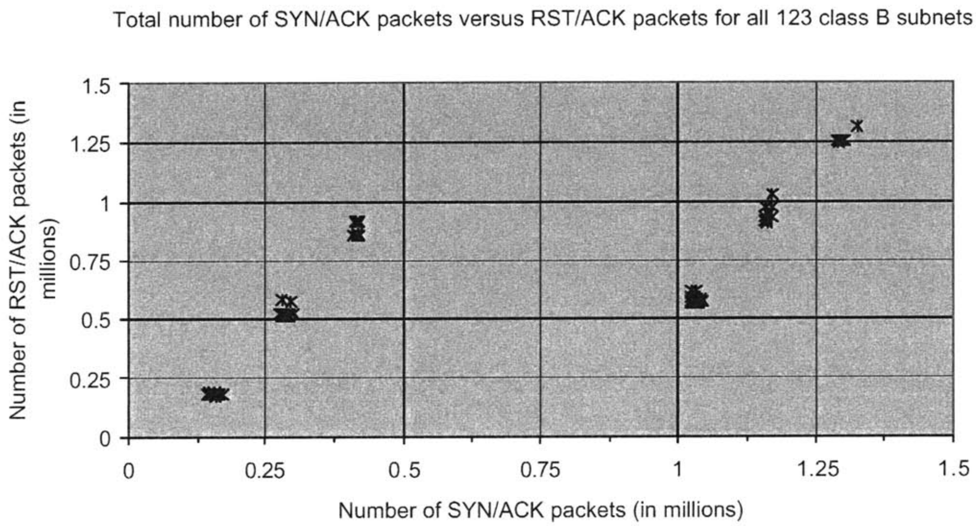

Figure 6 - The amount of RST/ACKs compared to SYN/ACKs that each class B subnet receive d (two high volume outliers not plotted). The number of class B subnet points in each cluster from left to right is 40, 18, 8, 36, 11, and 8.

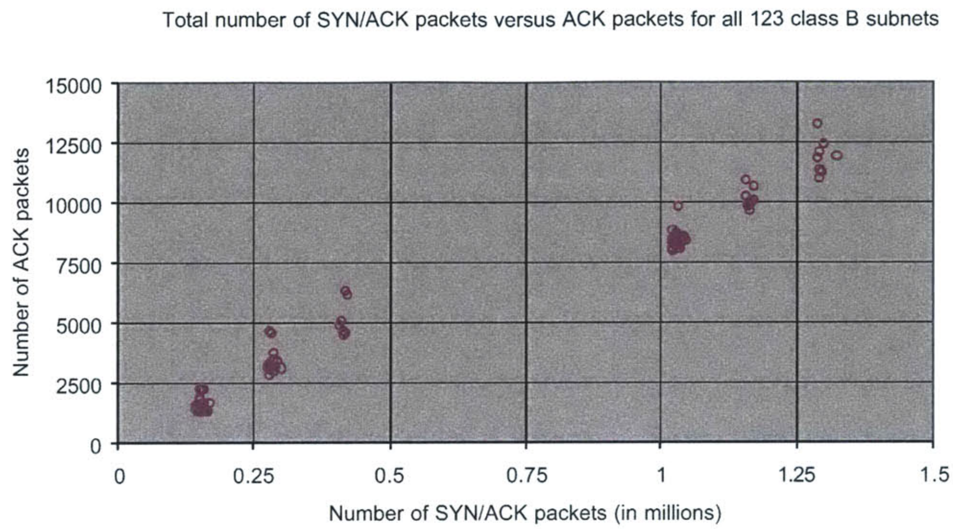

Figure 7 - The amount of ACKs compared to SYN/ACKs that each class B subnet receive d (two high volume outliers not plotted).

While the non-uniformity of backscatter was unexpected, there were other expected characteristics of backscatter confirmed in the dataset. One characteristic found in backscatter was that the more backscatter a subnet received, the more destination ports there were that received traffic. Since backscatter is a reply to a packet attempting to connect to a service on a fixed port, the destination port is typically a random high number application port. Figure 8 shows how the number of destination ports accounting for the top 90% of traffic increases as a class B subnet receives more backscatter. This behavior would be missed if one plots the backscatter amount against the number of unique destination ports in *all* the traffic received on a subnet, because each port is eventually expected to receive a random packet. On the same figure, for a consistent amount of backscatter, the number of unique destination ports in the top 90% increased as the total primary traffic decreased. This was caused by the *relative* increase in backscatter as primary traffic decreased (i.e. the ratio of backscatter to primary traffic increased).

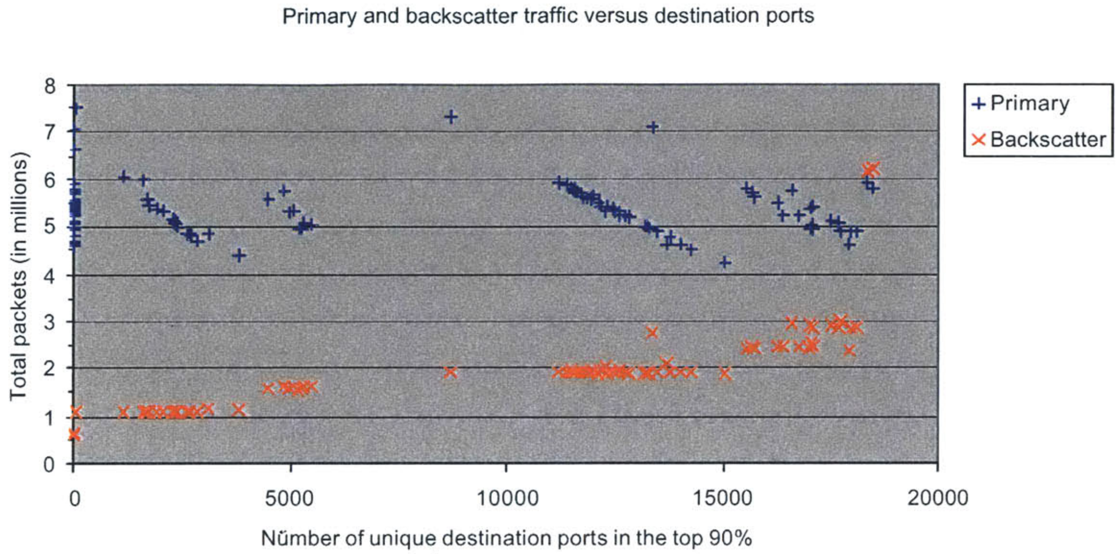

Figure 8 - Primary and backscatter amounts for each class B subnet as a function of destination ports.

Another observed characteristic of backscatter was that as the amount of backscatter decreases, the number of IP sources contributing to the top 50% of traffic increased (Figure 9). Since backscatter is the response traffic from specific sources, more backscatter translates to these specific sources contributing a greater percentage of the traffic. The amount of primary traffic remained independent of the number of unique IP sources.

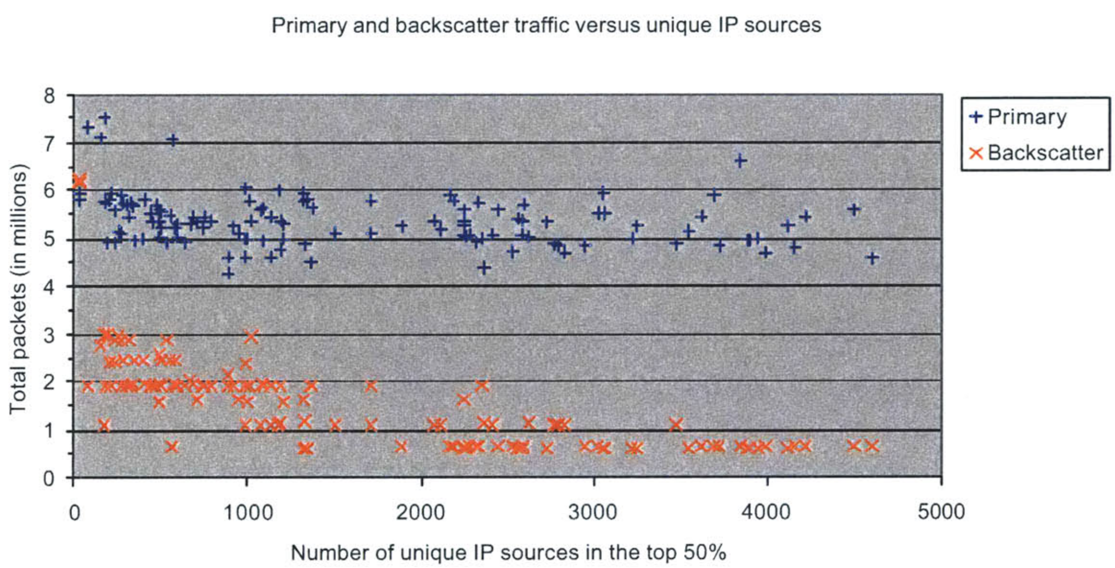

Figure 9 - Primary and backscatter amounts for each class B subnet as a function of IP sources.

5.1.2 Snort alerts

Overall, Snort generated few alerts. This was mainly because most of the packets in the dataset, which included TCP SYNs, SYN/ACKs, and RST/ACKS contained no data. Much of the malicious TCP traffic, which would have otherwise generated Snort alerts, was never sent to the network telescope because machines could not establish a TCP connection to the IP addresses in the class A network. The few alert types that Snort generated in high quantities were MS-SQL worm propagation attempts, ICMP ping nmaps, and ICMP destination unreachable. Figure 10 shows an example of a typical alert plot for the class B subnets; MS-SQL worm and ICMP ping nmap accounted for at least 90% of the alerts visible across all but one of the class B subnet alert plots. The high volume ICMP destination unreachable alert only occurs in one of the analyzed class B subnets, and is discussed in section 5.2.5.

The 'MS-SQL worm propagation attempt' alert is generated by Snort when the Slammer worm packet is detected. The Slammer worm, originally released in January 2003, is a single packet UDP (port 1434) worm that attempts to compromise a Microsoft SQL server [12]. Since the Slammer worm, which propagates without verifying that the target IP address is active, is contained within a single UDP packet, it is easily identified by Snort. The MS-SQL worm alerts were diurnal with double peak rates of ~2600 alerts/hour at around +4 and +10 hours.

The 'ICMP ping nmap' alert is generated when an ICMP ping packet that is likely caused by the nmap tool, is detected. ICMP pings are used to detect whether there is a computer operating at a specified IP address. ICMP pings generated by nmap are used to scan a subnet for active hosts and can be a precursor to future attacks targeted at the active hosts found by the tool. The ICMP ping nmap alerts were diurnal, with a peak rate of ~1700 alerts/hour at +18 hours.

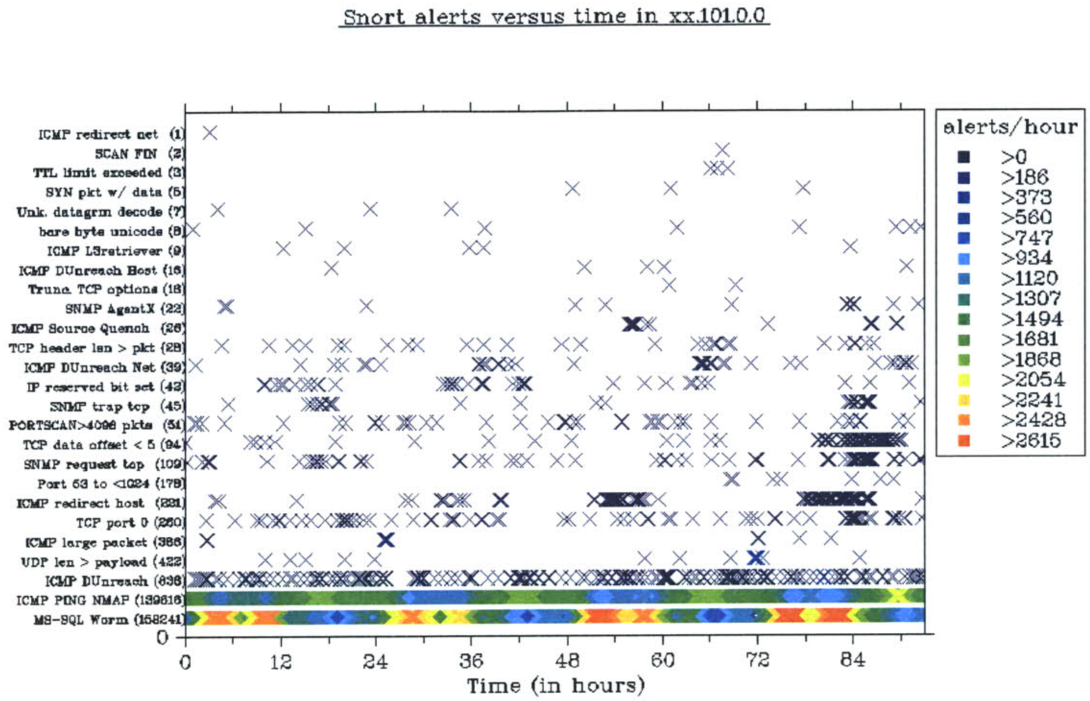

Figure 10 - Snort alerts in 101B.

5.2 Class B Results

There is a wide variety of phenomena to be observed within the class B subnets. As stated earlier, the lowest volume on a class B subnet was 5.2 million packets and the highest volume, ignoring the two outliers, was 9.8 million packets. Tables and plots for high volume class B subnets are presented in sections A.1, A.2, A.5, A.6, and A.9 of appendix A. Tables and plots for mid volume class B subnets are presented in sections A.3, A.4, A.7, A.8, and A.10 of appendix A. Tables and plots for mid volume class B subnets are presented in section A.11 of appendix A. While 30 class B subnets were chosen from the highest, middle, and lowest total packet count, there was no clear characteristic separating the three categories. Instead, the phenomena observed, including non-uniformity in traffic distribution, banded traffic, multi-port attacks, and sweeps, seemed to have been targeted at random class B subnets. In this section, each class B subnet is referred to by the class B subnet index followed by the letter B (ex. 244B refers to xx.244.0.0/16). The results concerning TCP traffic are discussed in sections 5.2.1 to

5.2.4, followed by the ICMP traffic results in sections 5.2.5 and 5.2.6, and the UDP traffic results in sections 5.2.7 and 5.2.8.

5.2.1 Non-Uniform Backscatter

The two subnets that received the most amount of traffic, 204B and 244B, exhibited non-uniform backscatter. Each subnet received 12 million packets, 20% more than the third highest volume subnet. The cause of this was a dramatic increase in backscatter. 204B received more than 2 million TCP SYN/ACKs and 244B received more than 3.5 million TCP RST/ACKs, 700 thousand and 2.2 million more packets, respectively, than the third highest SYN/ACK and RST/ACK volume in a single subnet. This backscatter had an unusual distribution; it was specifically targeted at the first 40 class C subnets within either class B subnets. Figure 11 shows a high amount of TCP traffic, which appear as 'bars' at the bottom of the plot, destined for the first 10,000 IP addresses within 204B. These destination IP bars correspond to the packets of SYN/ACKs and RST/ACKS destined for the ports between 8,000 and 40,000 in Figure 12. The connection between these two figures is easier to notice by observing the gap between +84 and +90 hours; there is a single vertical line in the middle of the gap in both figures. Figure 13 shows how the first 40 class C subnets received roughly five times the amount of traffic compared to the other class C subnets.

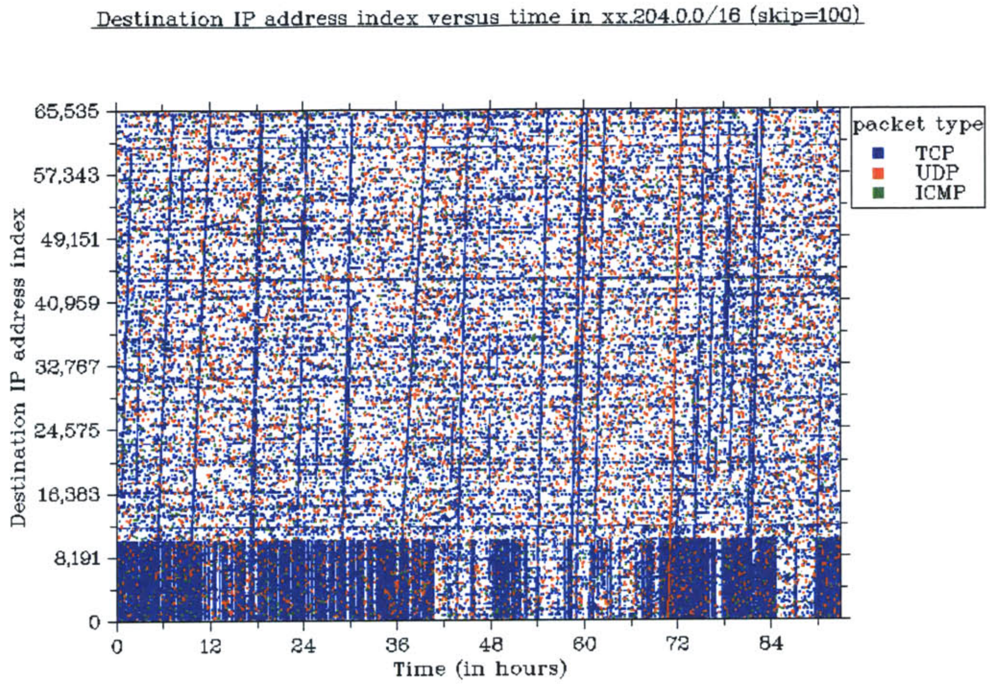

Figure 11 - Traffic destined to 204B, where TCP traffic is non-uniform.

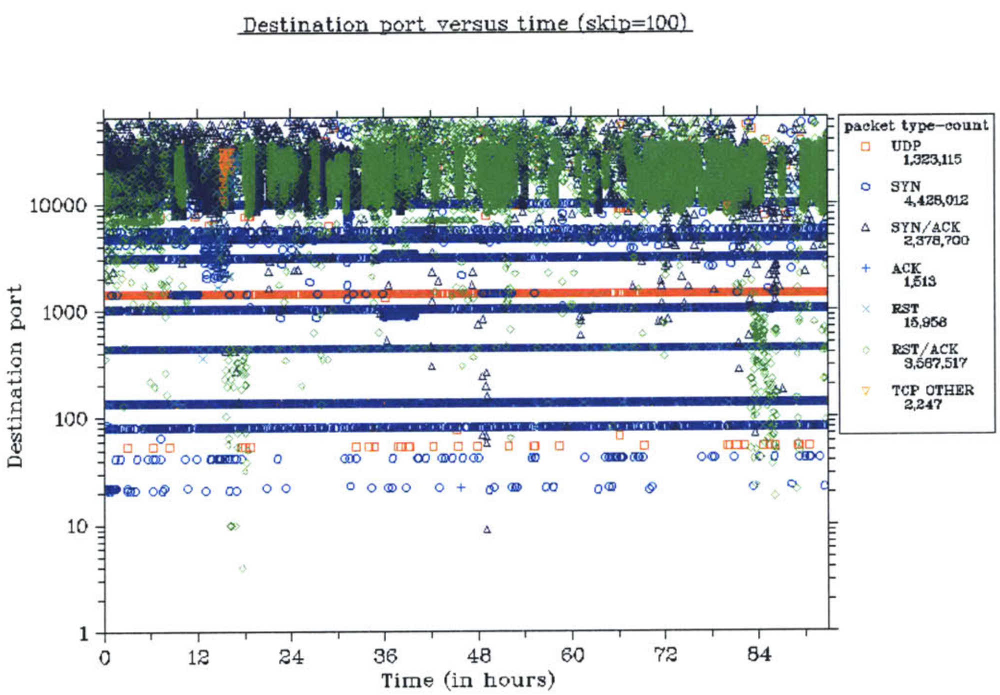

Figure 12 - Destination ports for 204B, where high ports receive a distinct pattern of traffic.

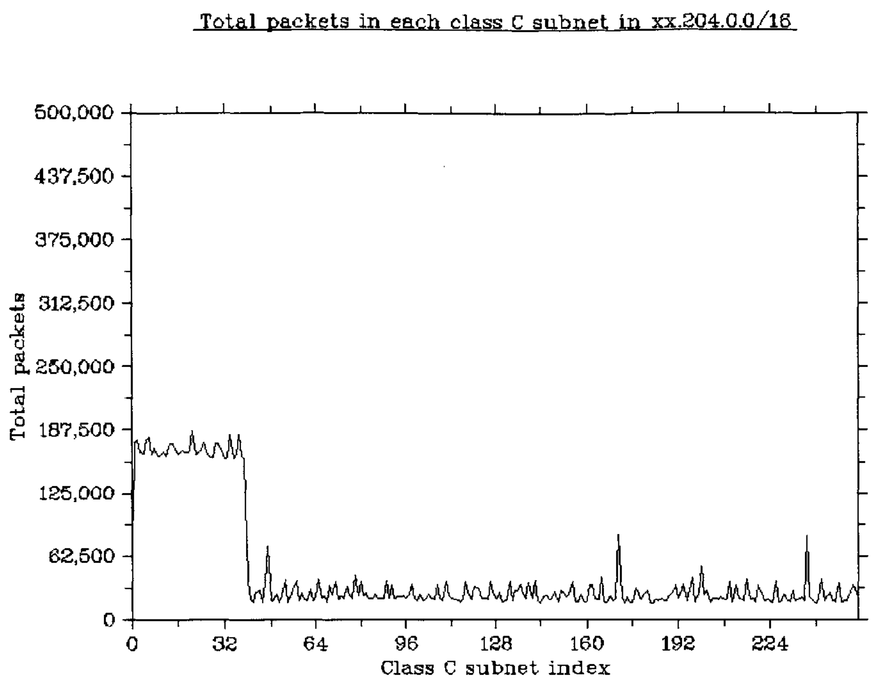

Figure 13 – A non-uniform distribution of packets received by each class C subnet in 204B.

Both 204B and 244B received at least 20% of their traffic from two sources, 61.177.64.171 and 61.152.91.151. These two IP addresses belong to class B networks owned by a Chinese telecom. Using Google to search for more information on the 61.177.64.171 IP address, cached results revealed forum posts, where people mentioned this IP address, dating back to within two weeks of the traffic dataset. These posts referred to links of peer-to-peer (P2P) torrent files for illegal movie and software downloads found at 61.177.64.171, a torrent server. It is difficult to explain the pattern of spoofed addresses used in the traffic directed towards the torrent servers, but this serves as an example of unusual UT that would be difficult to emulate.

5.2.2 Non-Uniform Primary Traffic

Similar to the non-uniform backscatter traffic, a few subnets received a non-uniform distribution of primary traffic across the class C subnets within. The clearest example of this was observed on 192B, shown in Figure 14. TCP SYNs to port 135 caused the increase in traffic, starting at the 18th class C subnet, and gradually decreasing again. This port received 2.7 million packets of approximately 48 bytes (1.8 million was the second highest amount of TCP port 135 packets destined to one class B subnet). Unlike the non-uniform backscatter traffic, no single source contributed more than 1.2% of the traffic on this subnet, the likely reason being that the source IP addresses were spoofed.

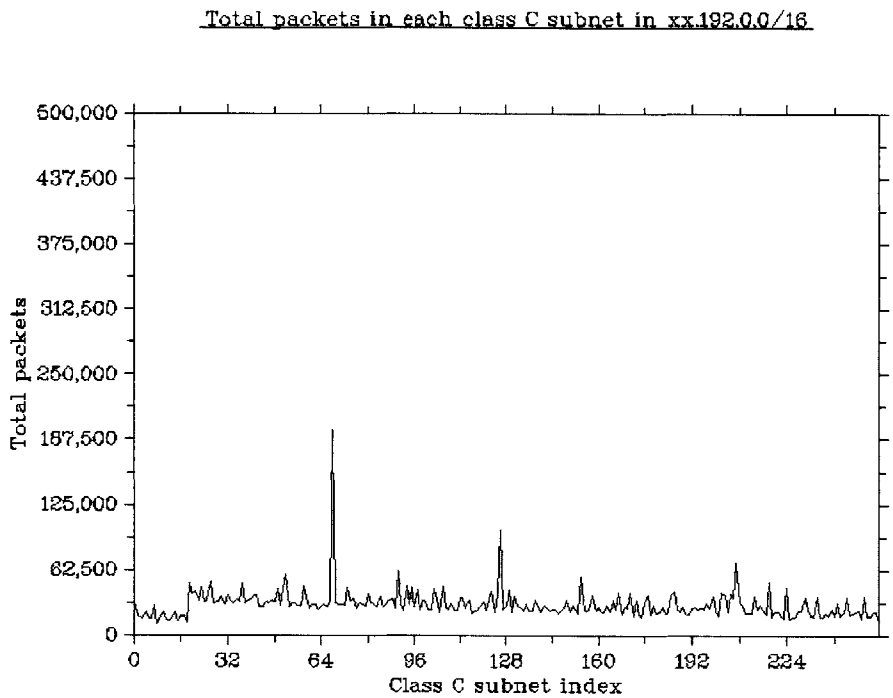

Figure 14 - A non-uniform distribution of packets received by each class C subnet in 192B.

5.2.3 Banded Traffic

One peculiar phenomenon that only appeared on one of the analyzed class B subnets, 49B, was horizontal and vertical bands of TCP traffic, shown in Figure 15. The three vertical bands indicate increased packet activity destined to all IP addresses within the class B subnet. Each vertical band lasted approximately 6 hours. The horizontal band lasted throughout the 93-hour dataset and affected 12 class C subnets within 49B. 49B received 20% of its traffic from a single source sending TCP SYN packets to port 445. There were 3.7 million TCP SYN port 445 packets sent to this subnet (1.8 million more than any other subnet). The bands are not simple sweeps across an IP range, as these would appear as thin lines. Instead, the bands indicate that for all IP addresses in the range, each IP address constantly received a TCP SYN port 445 packet for 6 hours.

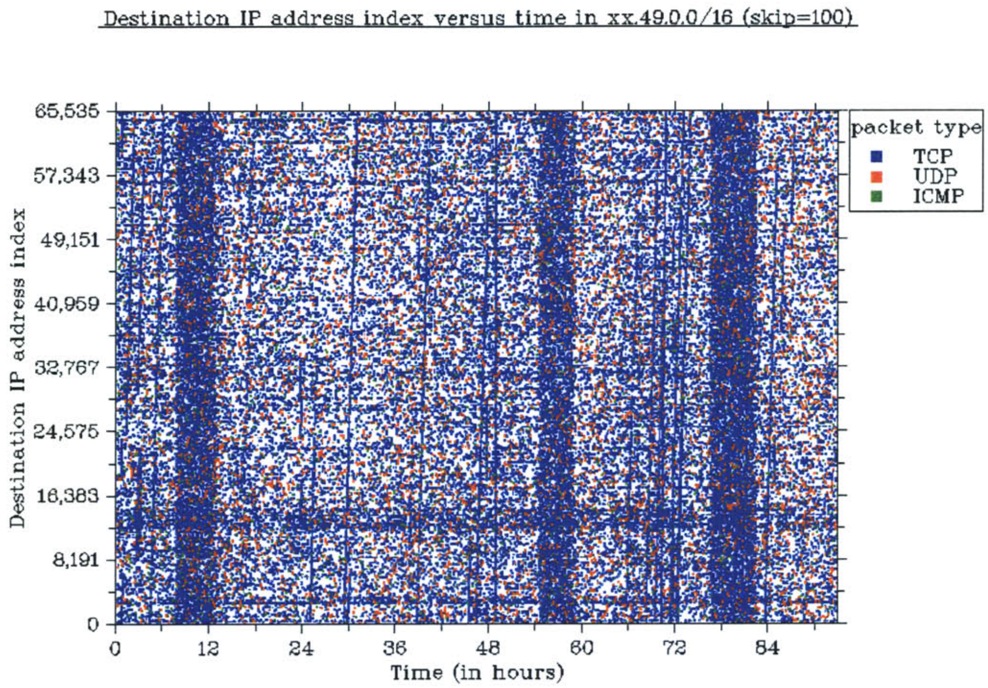

Figure 15 - Vertical bands of traffic in the 49B destination IP address plot.

5.2.4 Multi-port TCP attacks

Many class B subnets received short bursts of TCP packets destined to multiple ports. Figure 16 shows an example of this behavior, seen on 243B. Between +68 and +76 hours, 243B received TCP SYN packets destined to ports 901, 3410, 12345, and 27374. Each port received between 1% and 2% of the total traffic. While it can be assumed that the short multi-port TCP attacks were caused by a single event, the same cannot be said for the multiple TCP ports that received traffic throughout the whole 93 hours. These ports (ex. 80, 135, 139, 445, 1023, 1025, 3127, 5554, and 9898) do not share *unusual* temporal characteristics like the four TCP ports hit simultaneously for a short duration, and may have been caused by different events.

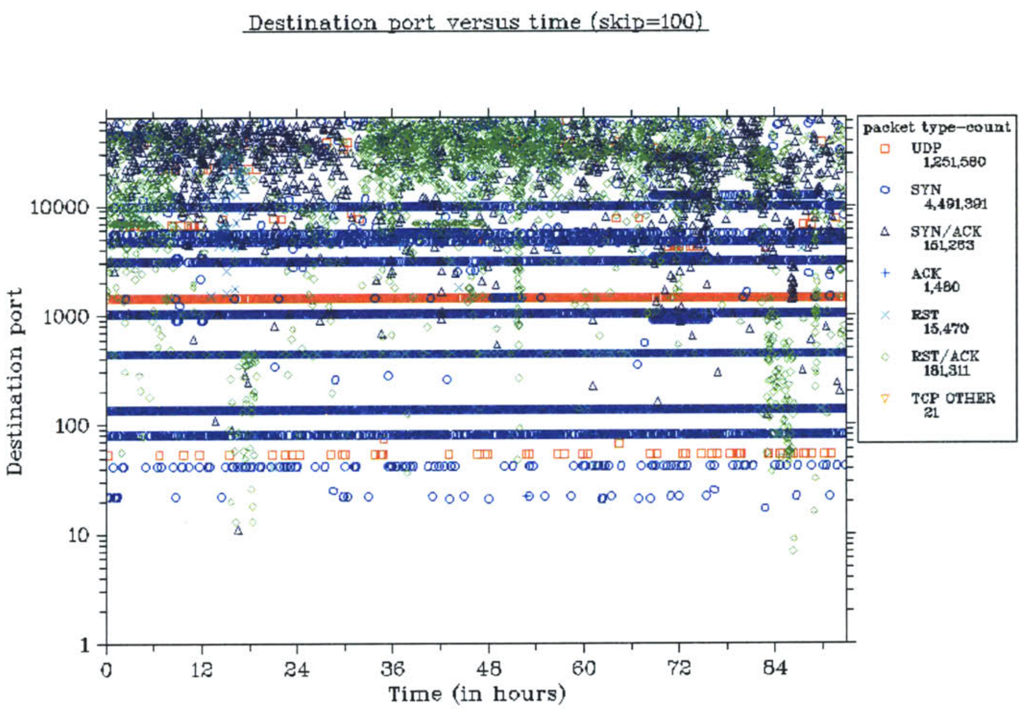

Figure 16 - Four ports on 243B received packets at the same time and with the same duration.

5.2.5 High Volume ICMP Destination Unreachable

On the 1B subnet, there was a high volume of ICMP destination unreachable packets. This subnet stood out as having more than twice as many ICMP packets compared with the other class B subnets. The majority of these ICMP packets were destined to a single IP address, xx.1.128.12. This was the only class B subnet where the MS-SQL worm and the ICMP ping nmap alerts were not the top two alerts. The bottom of Figure 17 shows how the ICMP destination unreachable packet volume peaks at +18, +42, and +90 hours.

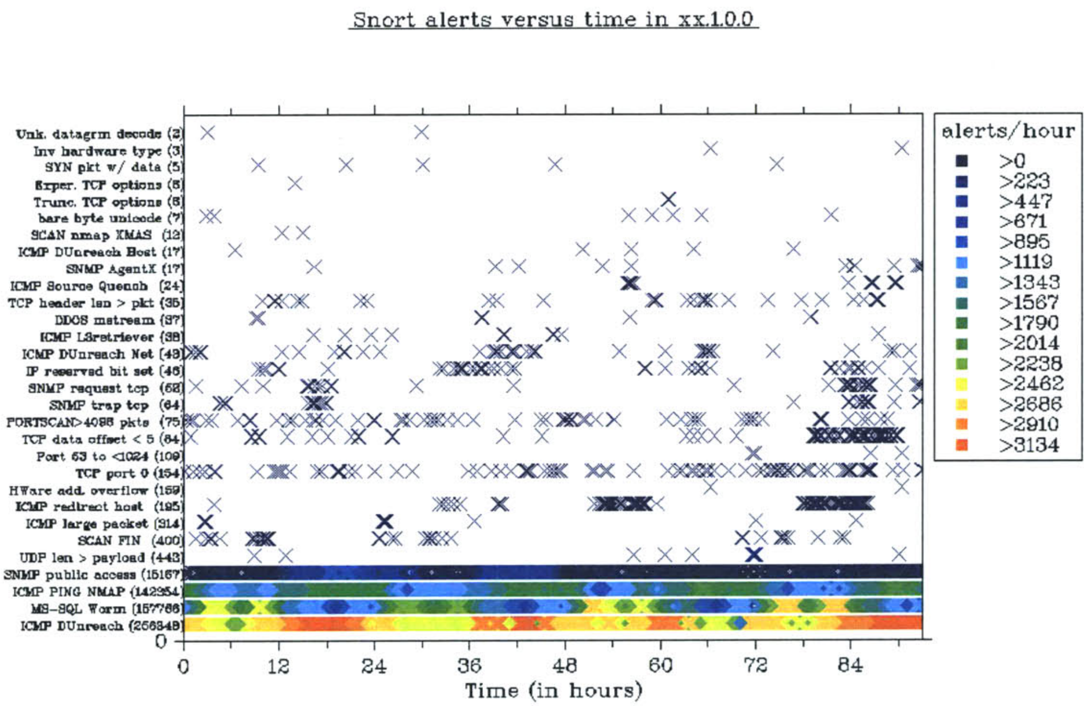

Figure 17 - Snort alerts for 1B, where ICMP destination unreachable is the highest volume alert.

5.2.6 ICMP Echo Request Sweep

Sweeps of any ICMP type were rarely seen in the analyzed class B subnets. However, on the 81B subnet, there was a visible ICMP echo request sweep across the whole subnet (Figure 18). The sweep started from +72 hours at the 0 IP address index and continues until +84 hours, where it reaches the 65,535 IP address index (note: the TCP and UDP packets have been filtered from the original plot, since the ICMP sweep cannot be seen when the plot is not in color). Figure A3-3 in appendix A shows the same plot as Figure 18, but without the TCP and UDP packet types filtered out from the plot. There were over 400,000 ICMP echo request packets, approximately 6% of the traffic, directed to this subnet. Because most of the other class B subnets received no more than 200,000 ICMP echo request packets, this sweep is likely composed of the additional 200,000 packets. Neither 79B nor 83B, the two spatially closest class B subnets analyzed, exhibited any ICMP sweep activity.

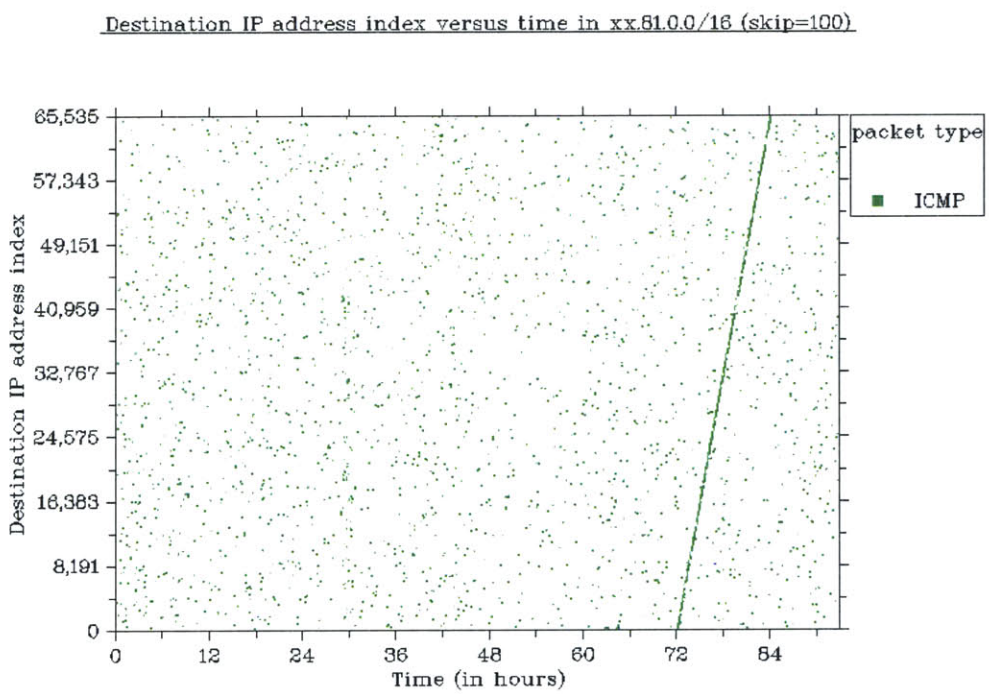

Figure 18 - An ICMP sweep going across 81B starting at +72 hours and ending at +84 hours.

5.2.7 Class B UDP Sweep

The 168B subnet received the most amount of UDP traffic, 3.6 million packets. 40% of the UDP traffic was 78-byte port 137 packets targeted to all machines. Port 137 UDP traffic is typically associated with NetBIOS name queries. No other class B subnet had nearly as many UDP sweeps visible in the *destination IP address index versus time* plot type, shown in Figure 19. The source IP addresses of the UDP sweeps were likely spoofed as no source contributed more than 2% of the traffic.

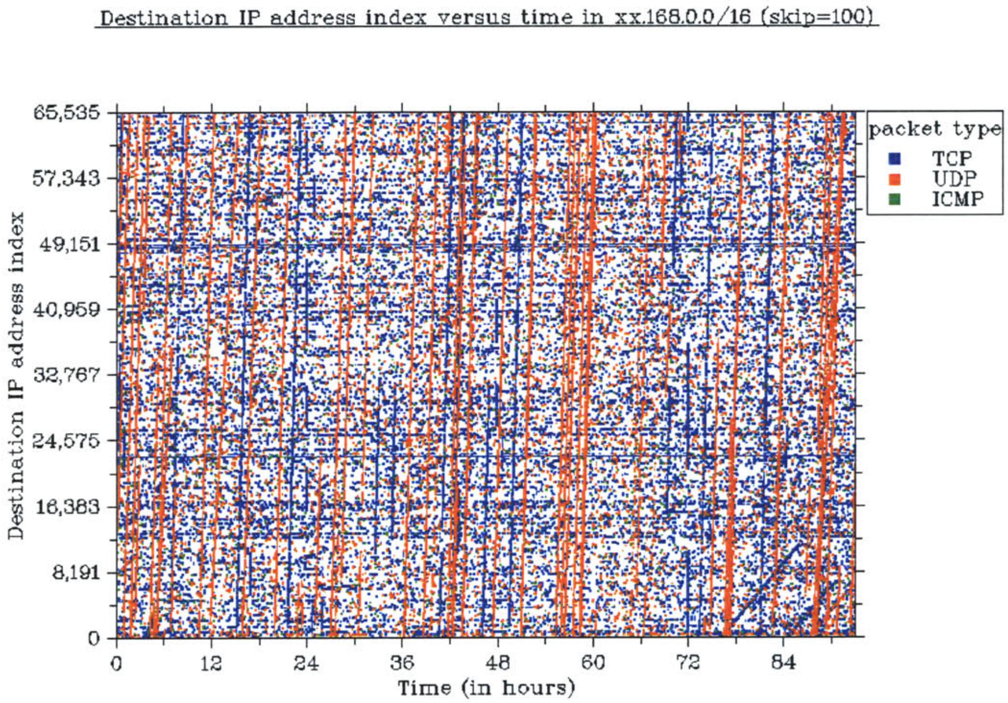

Figure 19 - Traffic destined to 168B, where vertical UDP sweeps visually outnumber the TCP sweeps.

5.2.8 Select Target High Volume UDP Traffic

The 128B subnet received the second highest total UDP packets, 2.4 million packets (third highest was 1.7 million UDP packets). All of the UDP traffic was destined to a single IP address xx.128.8.14. xx.128.8.14 received 840,000 160-byte packets to UDP port 1037. The fact that UDP packets are primary traffic, and that no source contributed more than 2.6% of the traffic, indicate that this activity was a DDOS attack.

5.3 Class C Results

The class C subnets plots allow us to discern the traffic behavior that composes a class B subnet. The low packet count class C subnets received around 10,000 packets. Tables and plots for these subnets are presented in sections B.6, B.7, and B.8 of appendix B. The mid packet count class C subnets (i.e. ranking 15,000 out of a sorted list of ~30,000 class C subnet packet counts) had around 20,000 packets. Tables and plots for mid volume class C subnets are presented in sections B.1 and B.4 of appendix B. Both the low and mid packet count subnets had a fairly even distribution of traffic, with 90% of the traffic going to an average of 216 IP addresses amongst the 256 IP addresses within each subnet. The high packet count class C subnets received over 500,000 packets and displayed phenomena targeted at specific IP addresses. Each of the 30 high volume class C subnets had at least 90% of the traffic destined to a single IP address within the class C subnet. Tables and plots for high volume class C subnets are presented in sections B.2, B.3, B.5, and B.9 of appendix B.

In this section, each class C subnet is referred to by the second and third IP address octet followed by the letter C (ex. 255.145C refers to xx.255.145.0/24). Only low and mid packet count class C subnets are discussed in this section, as they have characteristics pertaining to the subnet as a whole. Section 5.3.1 discusses an observed phenomenon where packet noise was contained in specific IP address ranges. Phenomena found in the high volume class C subnets, which in fact pertain to specific destination IP addresses within the subnet, are discussed in section 5.4.

5.3.1 Packet Noise

In the low and mid volume class C plots, there is behavior that helps explain the differences in total backscatter between the lower and upper half of the class A network. Figure 20 is a plot of the backscatter in the low and mid volume class C subnets analyzed. The class C index is computed by multiplying the second IP octet (from the left) by 256 and adding that to the third IP octet (ex. the class C index for X.Y.Z.0/24 is 256*Y+Z). Figure 20 shows that the low and mid volume class C subnets pertaining to the class B network below 128 received on average 5,000 more backscatter packets than those above that range. This is not surprising as the difference of 5,000 for each class C subnet, matches the 1.2 million packet difference (5,000*256 is approximately 1.3 million) between the class B subnets, explained in section 5.1. It turns out that the packets destined to each of the class C subnets below the 128-class B octet is not distributed evenly. The lower half of the IP range within each *class C subnet* received approximately 20% more traffic than the upper half.

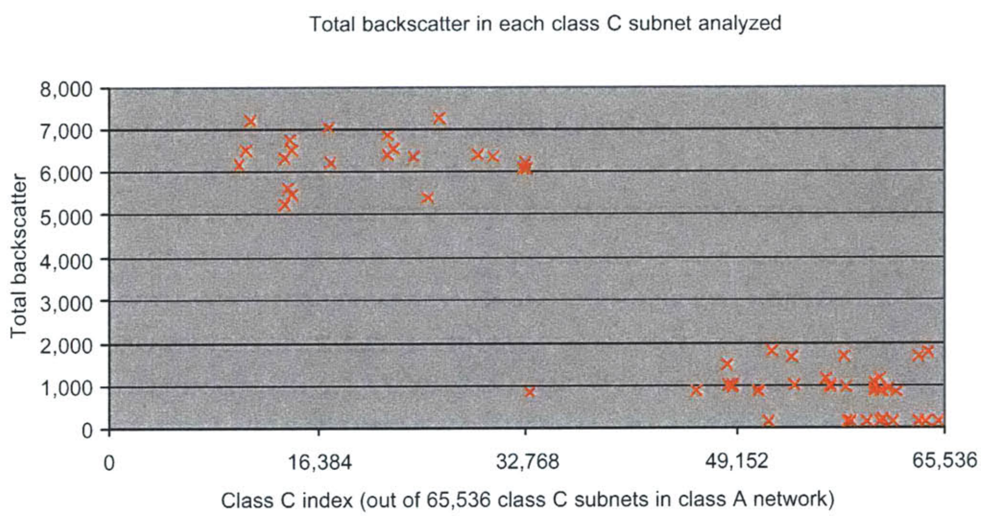

Figure 20 - Total backscatter in the low and mid volume class C subnets.

Figure 21 is an example of a class C subnet, 55.145C, below the 128-class B octet. The plot shows the total amount of traffic each of the 256 IP addresses, within the 55.145C subnet, received. There was a 20% drop in 'noise' after the xx.55.145.128 IP address index. The *destination IP address versus time* plot for 55.145C (Figure 22) reveals the cause of the drop in noise. The lower half of the graph has 'specks' of random TCP packets distributed throughout the whole time period. All of the class C subnets below 128 look similar in terms of the specks of

TCP packets seen below the 128 IP address, while those above the 128-class B octet, such as 198.188C (shown in Figure 23), were clear of those specks.

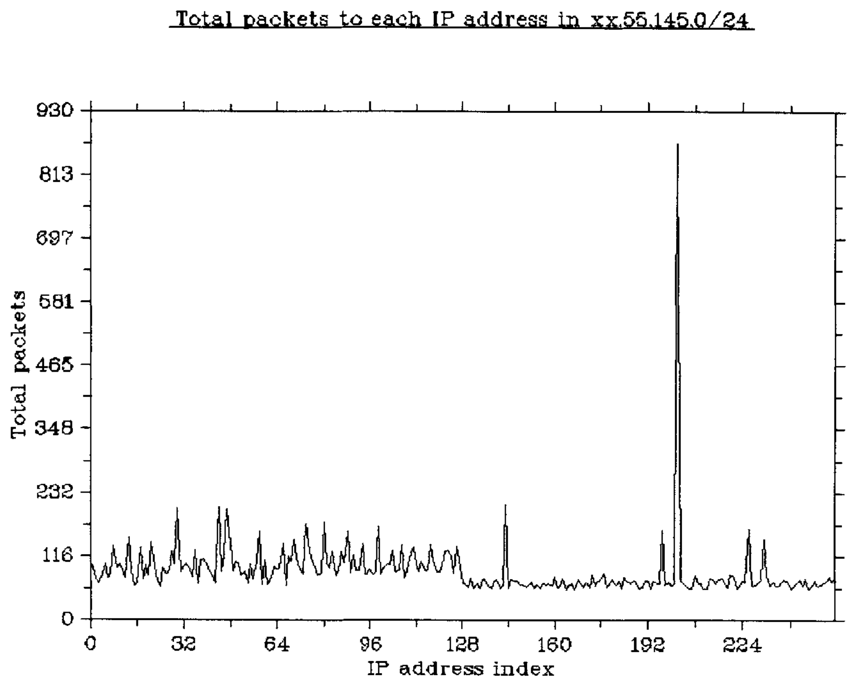

Figure 21 - Total amount of traffic received by each IP address within 55.145C.

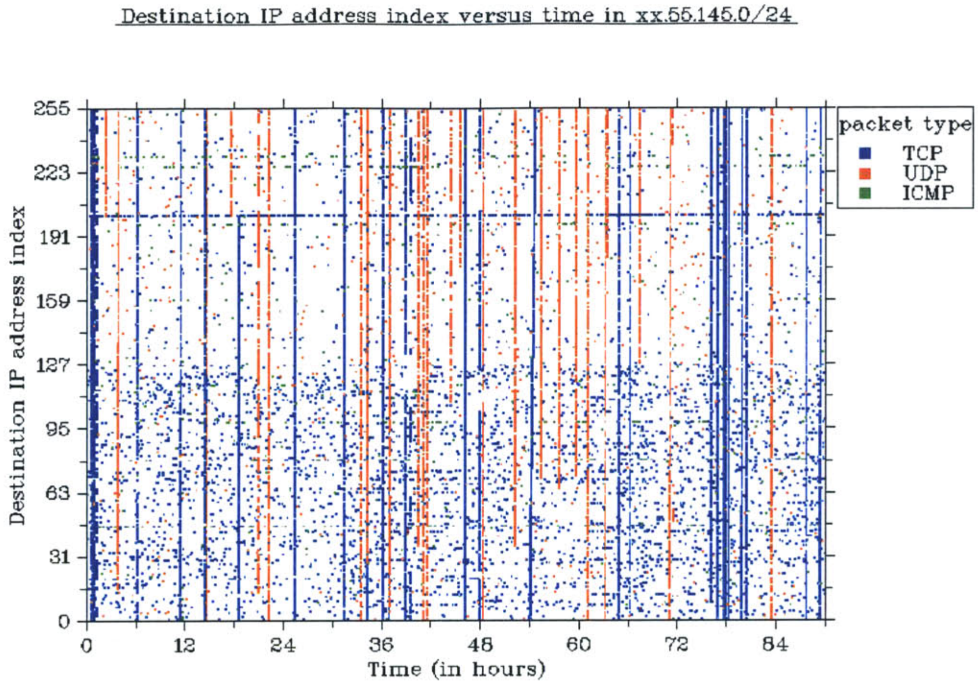

Figure 22 - A plot of every packet received by each IP address in 55.145C.

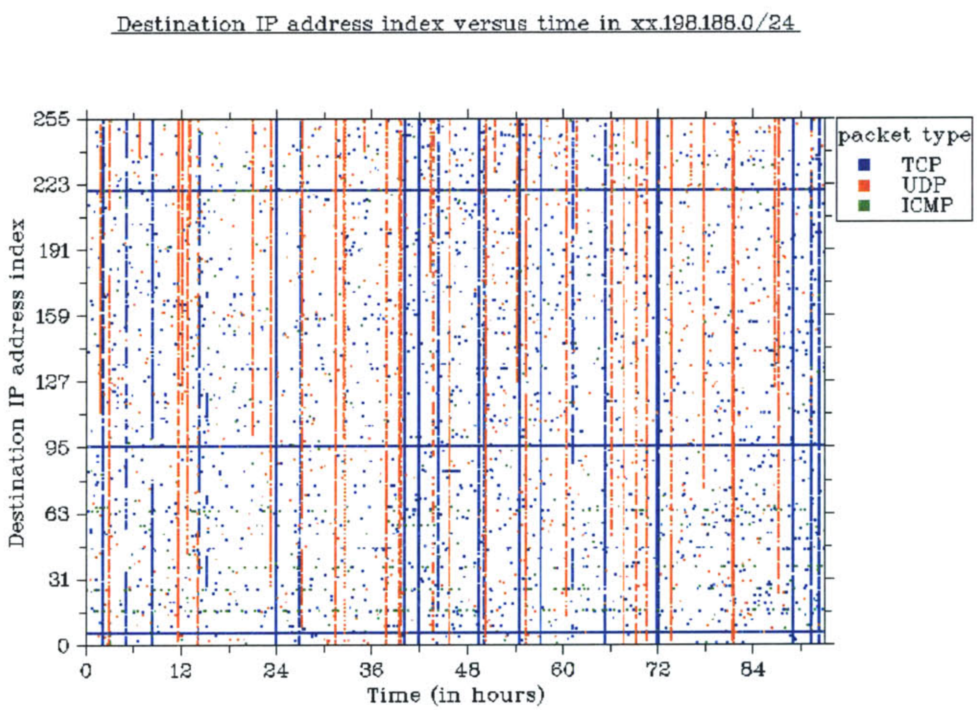

Figure 23 - A plot of every packet received by each IP address in 198.188C.

5.4 Targeted IP Address Results

The high volume targeted IP address results are all based on the high volume class C results. All 30 of the high volume class C subnets, which received over 500,000 packets, had at least 91% of the packets directed to a single IP address within their class C subnet. It should be noted that the average volume of packets received by each class C subnet across the class A network was 27,000.

There were four phenomena observed in the 30 high volume targeted IP addresses. The phenomena include 5 IP addresses with a diurnal packet per hour pattern, 23 IP addresses which all had a similar temporal packet pattern, 1 IP address which received a large amount of P2P traffic targeted at port 4662, and 1 IP address which received a lot of UDP port 1037 traffic (discussed in section 5.2.8).

5.4.1 Diurnal Packet Pattern

A diurnal pattern was observed in the *packet versus time* plots of five class C subnets. All of these IP addresses received between 480,000 and 700,000 packets. The diurnal pattern targeted at the 5 IP addresses were all similar; an example of the 109.116C pattern is shown in Figure 24. The diurnal pattern appears to be a scan for particular port vulnerabilities, since 6 ports accounted for a large percentage of the traffic. Table 2 shows that six destination ports accounted for over 95% of the packets in these subnets.

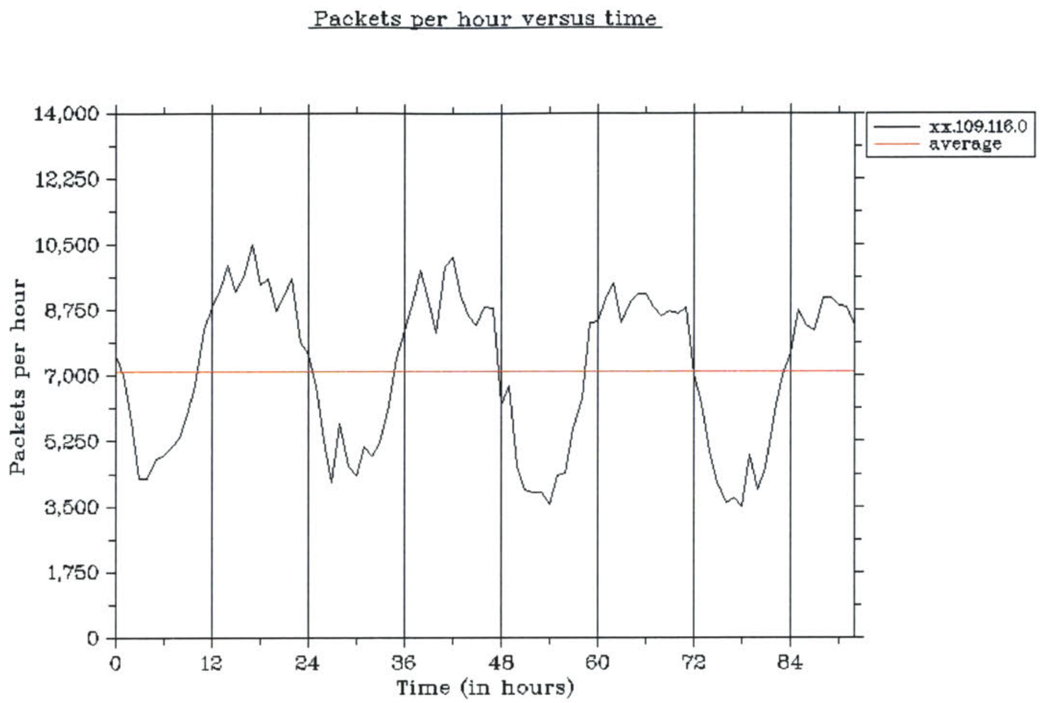

Figure 24 - Diurnal packet per hour versus time plot for 109.116C.

		IP Address				
		x.25.161.40	**x.109.116.137**	**x.217.229.249**	**x.232.94.123**	**x.248.246.112**
% of Total Traffic per Port	**TCP 1025**	21.0	21.1	21.2	21.3	21.3
	TCP 42	20.9	21.2	21.4	21.2	21.1
	TCP 80	19.4	18.9	19.0	19.2	19.2
	TCP 139	17.0	17.9	18.0	17.8	17.8
	TCP 445	10.8	11.5	11.8	11.6	11.5
	TCP 135	6.6	6.7	7.0	6.9	7.3
Total %		**95.7**	**97.3**	**98.4**	**98.0**	**98.2**

Table 2 - The traffic breakdown, by port, for the 5 IP addresses that had a diurnal packet pattern.

5.4.2 Similar Temporal Traffic Pattern across Class B Subnets

One interesting phenomenon observed was that 23 IP addresses, which spanned distant class B and C subnets, received a similar temporal traffic pattern. This traffic pattern is divided into two groups, where the difference between the groups was caused by a single IP source. One group consisted of 10 IP addresses where the IP source, 210.245.191.90, sent 5,500 packets; the other group consisted of the remaining 13 IP addresses where the same IP source sent 60,000 packets. The packet per hour versus time pattern of the former group is shown in Figure 25; the pattern of the latter group is shown in Figure 26. The difference to observe between these two figures is the increase in traffic between +22 and +38 hours, which accounts for approximately 50,000 packets. Figure 27 shows an example of the total number of packets sent by the top 18 IP sources, to 4 of the 23 IP address destinations. The IP source on the far right of the plot can be seen to have sent a significantly greater amount of traffic to two of the four IP destinations. In fact, all 23 IP addresses shared the same top 18 IP sources, with the same relative amounts except for the traffic received from IP source 210.245.191.90 (the 23 IP addresses share more than 18 IP sources, but there was a 20% drop in total packets after the 18th IP source). Considering that the same IP sources are involved in the form of backscatter seen on these 23 IP addresses, a single event is likely to have caused this phenomenon, where a distinct set of IP addresses were targeted.

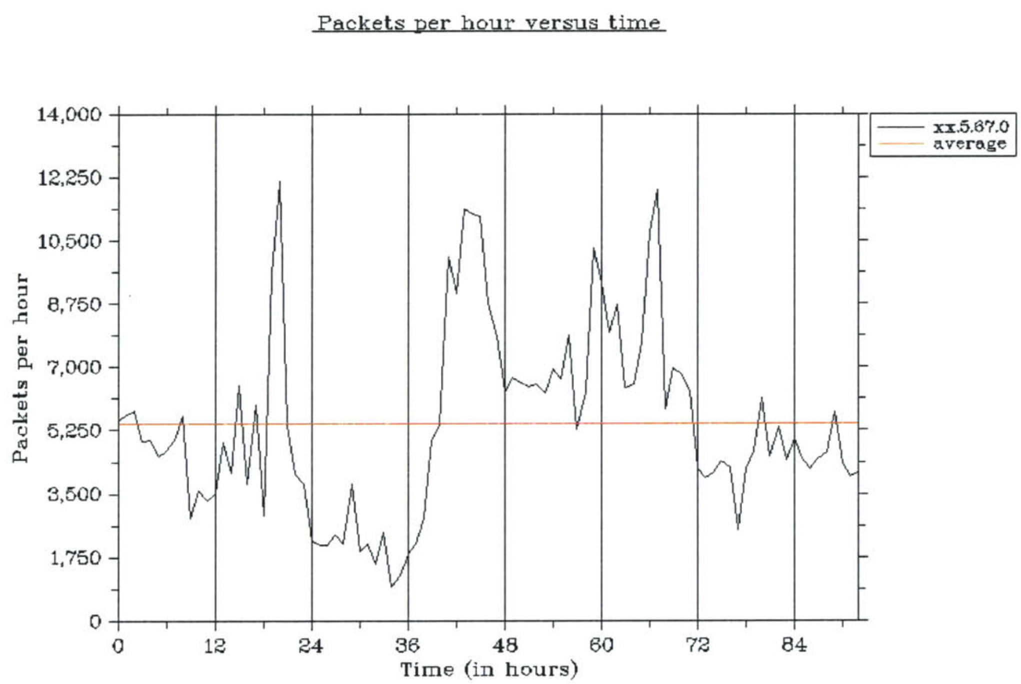

Figure 25 - Packet per hour plot for 5.67C in which 210.245.191.90 sent little traffic.

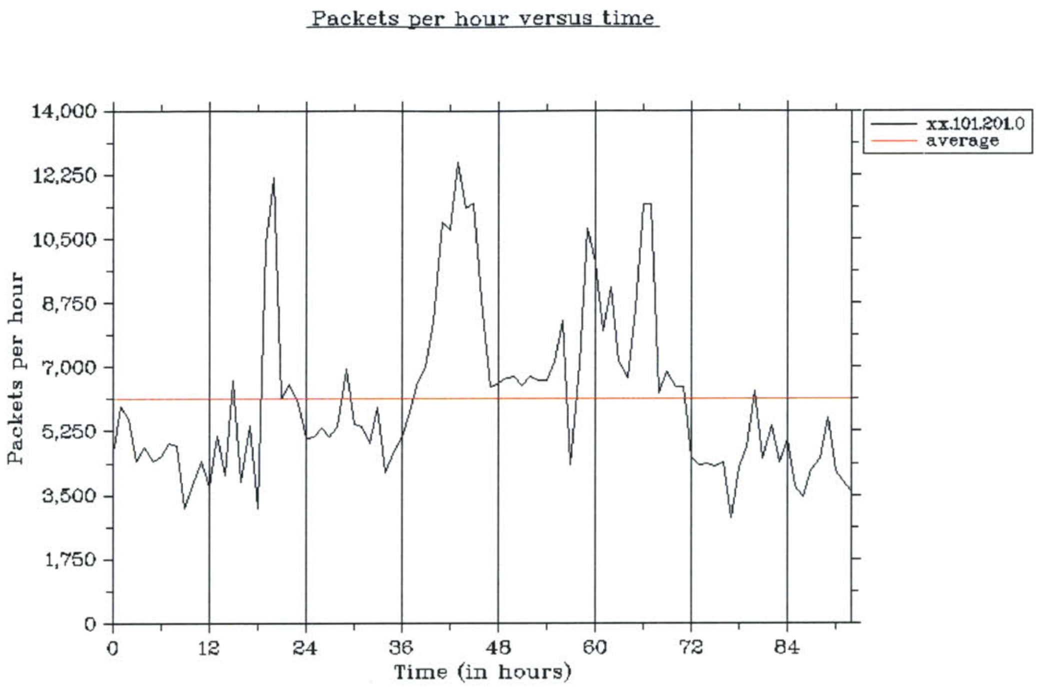

Figure 26 - Packet per hour plot for 101.204C in which 210.245.191.90 sent a high volume of traffic.

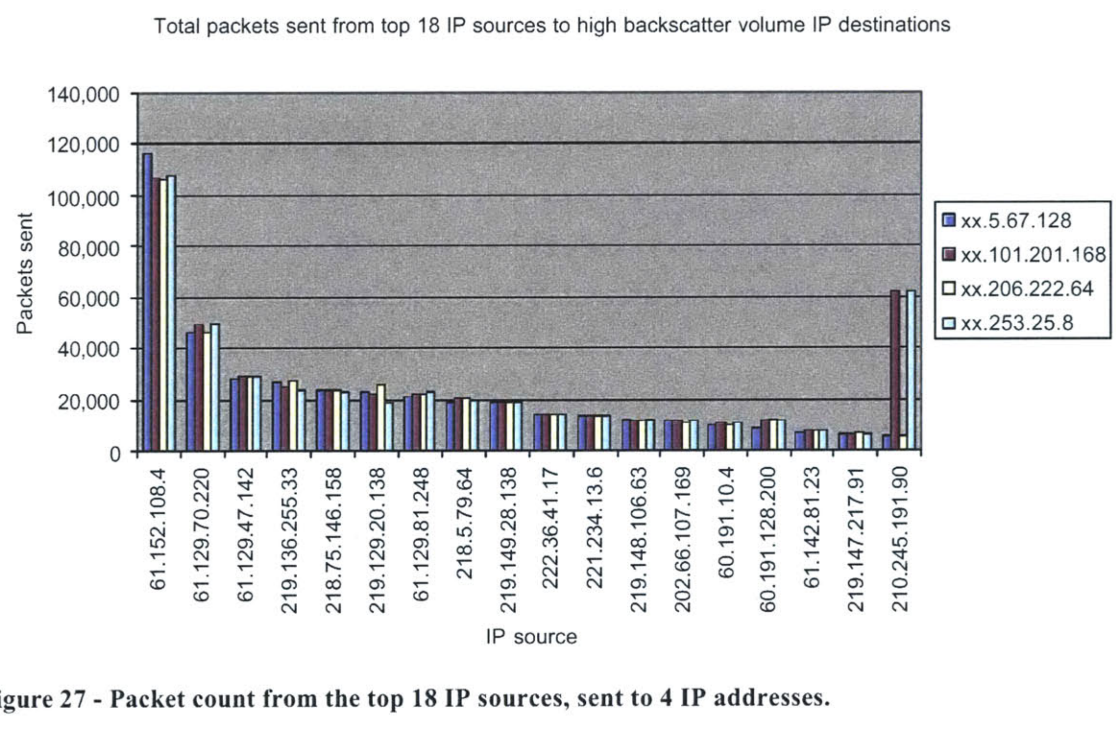

Figure 27 - Packet count from the top 18 IP sources, sent to 4 IP addresses.

The only pattern distinguishing whether 210.245.191.90 sent traffic was that only those destination IP addresses where their rightmost octet was a multiple of 16, did not receive traffic from this source, shown in Figure 28. The other octets did not seem to bias the distribution of traffic from this IP source. The traffic from this source, 210.245.191.90, is what separates the 23 IP addresses into those that received 532,000 backscatter packets versus those that received on average 482,000 backscatter packets. This 50,000-packet difference was solely a difference in the volume of TCP RST/ACKs. This distinct separation of backscatter quantity may explain why there were clusters of backscatter found in the section 5.1.1 backscatter analysis.

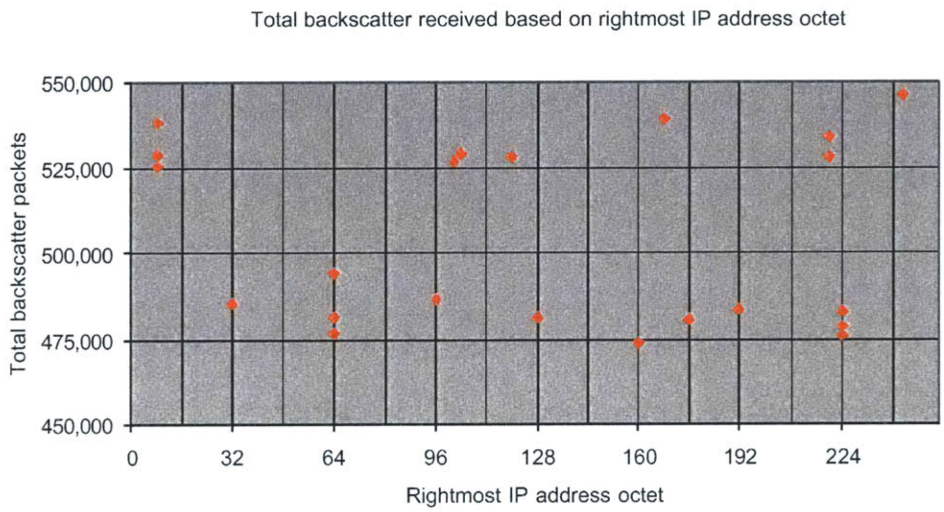

Figure 28 - Total backscatter received on the 23 IP addresses, based on the rightmost octet

These 23 IP addresses all received over 470,000 packets of backscatter. This translates to each IP address representing approximately 10% of the backscatter observed within their class B subnet. 2 of the 23 IP addresses analyzed actually pertained to the same class B subnet. This suggests that the backscatter received on each of the class B subnets might have been the aggregate of the backscatter received by 10 IP addresses within the subnets.

5.4.3 Single Target P2P Primary Traffic

One IP address, xx.218.68.212, received 486,000 packets, of which at least 92% were TCP SYN packets to port 4662. EDonkey P2P client commonly uses this port. The attack did not appear to start until +20 hours, shown in Figure 29; it continued throughout the rest of the dataset period, with two large bursts of traffic lasting approximately 24 hours each. No source contributed more than 0.1% of the packets. Unlike the P2P activity, which caused a large amount of backscatter, discussed in section 5.2.1, this P2P activity consists of primary traffic. The likely cause of the activity seen on xx.218.68.212 is that the IP address was incorrectly listed as a P2P server.

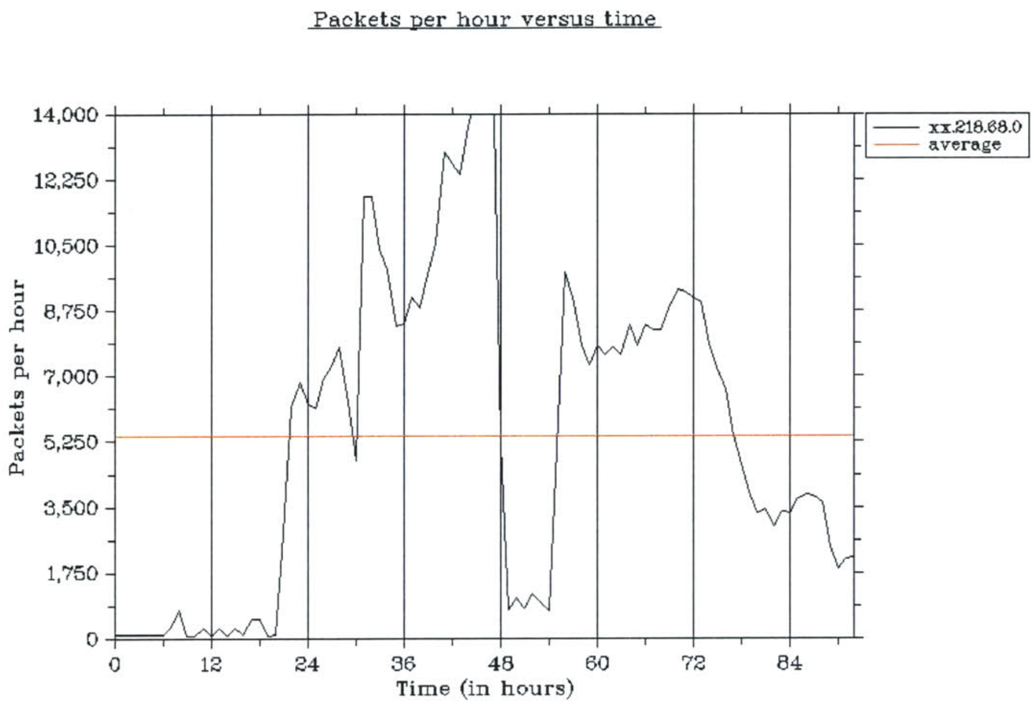

Figure 29 - Packet per hour plot of P2P traffic sent to xx.218.68.212.

Chapter 6

Conclusion

This thesis presents the results of analyses performed on unwanted traffic received on a class A network telescope. The results show the various types of traffic phenomena that were observed including a variety of sweeps, diurnal and irregular traffic patterns, non-uniform traffic distributions, and high volume attacks. These phenomena were targeted at different class B subnets, class C subnets, and IP addresses across the whole class A network and were difficult to predict. While one subnet would receive a certain pattern of traffic, an adjacent subnet would be devoid of such a pattern. A large portion of the dataset could not be analyzed at the class C or individual IP address level, and so it cannot be assumed that the list of phenomena presented is comprehensive. In addition, many of the phenomena lasted longer than the 93-hour period of the dataset, and so the temporal aspects of these phenomena could not be ascertained. The unusual nature of the traffic, the inability to analyze all of the class C and individual IP address activity, and the short duration of the dataset make it difficult to create artificial models of unwanted traffic. Future work towards improving the understanding of UT includes automating the statistical analysis of traffic measurements using clustering techniques, analyzing longer datasets and classes within those datasets more efficiently, and looking at the root causes behind these phenomena.

The results also show that the backscatter in this dataset was not uniform. When the class B subnets were observed at the class A network level, a large disparity was seen between two regions of the network. Assuming uniformity in backscatter, especially since uniformity can be observed in clusters of class B subnets, can lead to gross miscalculations of backscatter characteristics on the Internet.

References

[1] Sally Floyd and Vern Paxson, "Difficulties in Simulating the Internet," IEEE/ACM Transactions on Networking, Vol. 9, Issue 4, pp. 392-403, Aug. 2001.

[2] Steven M. Bellovin, "Packets Found on an Internet," ACM SIGCOMM Computer Communication Review, Vol. 23, Issue 3, pp. 26-31, Jul. 1993.

[3] Stuart Staniford, Vern Paxson, and Nicholas Weaver, "How to 0wn the Internet in Your Spare Time," In Proceedings of the 11th USENIX Security Symposium, pp. 149-167, Aug. 2002.

[4] Lee M. Rossey, Robert K. Cunningham, David J. Fried, Jesse C. Rabek, Richard P. Lippmann, Joshua W. Haines, and Marc A. Zissman, "LARIAT: Lincoln Adaptable Real-time Information Assurance Testbed," IEEE Aerospace Conference Proceedings, Mar. 2002.

[5] CAIDA mission statement, 2005. http://www.caida.org/projects/progplan/progplan03.xml

[6] David Moore, "Network Telescopes: Observing Small or Distant Security Events," In Presentation at the 11th USENIX Security Symposium, 2002.

[7] David Moore, Colleen Shannon, Geoffrey M. Voelker, and Stefan Savage, "Network Telescopes: Technical Report," Technical Report, Cooperative Association for Internet Data Analysis - CAIDA, Apr. 2004.

[8] David Moore, Geoffrey M. Voelker, and Stefan Savage, "Inferring Internet Denial-of-Service Activity," In Proceedings of the 10th USENIX Security Symposium, pp. 9-22, Aug. 2001.

[9] Ruoming Pang, Vinod Yegneswaran, Paul Barford, Vern Paxson, and Larry Peterson, "Characteristics of Internet Background Radiation," In Proceedings of the 4th ACM SIGCOMM Conference on Internet Measurement, pp. 27-40, 2004.

[10] Martin Roesch, Snort network intrusion prevention and detection system, 2005. http://www.snort.org/.

[11] Rocky K. C. Chang, "Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial," IEEE Communications Magazine, Vol. 40, Issue 10, pp. 42-51, Oct. 2002.

[12] David Moore, Vern Paxson, Stefan Savage, Colleen Shannon, Stuart Staniford, and Nicholas Weaver, "The Spread of the Sapphire/Slammer Worm," Technical Report, Cooperative Association for Internet Data Analysis - CAIDA, Jan. 2003.

[13] CoralReef software suite, 2005. http://www.caida.org/tools/measurement/coralreef/.

[14] Helmut Michels, Dislin plotting library, 2005. http://www.dislin.de/.

Appendix A:

Tables and Plots for Class B Subnets

A.1 - XX.1.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	9,804,326	29	1,140	78.3	16.2	5.5
Bytes	563,168,457	1,168	54,420	64.0	31.4	4.6

Table A1-1 – Packet and byte statistics for 1B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	5,450,198	1,158,305	10,845	76,868	923,111	735

Table A1-2 – TCP packet types in 1B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	31	574K	1.1M (75)	59,691	400,657	25	1.4K	65,536	150	8.6K
90	X	X	X	13,360	80,178	110	6.4K	52,261	169	9.6K
50	X	X	X	4	153	32.1K	1.8M	12,140	404	21.2K

Table A1-3 – Statistics for all, the top 90%, and the top 50% of traffic in 1B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 135	1,829,158	18.7	87,414,378	15.5
TCP – 445	1,801,637	18.4	86,758,899	15.4
UDP – 137	1,260,528	12.9	98,328,687	17.5

Table A1-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 1B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.1.50.192	471,531	4.8	19,437,178	3.5
xx.1.128.12	256,446	2.6	14,396,629	2.6
xx.1.199.75	139,617	1.4	6,732,568	1.2

Table A1-5 – Top 3 destination IPs across all packet types by packet count, in 1B.

IP Source	Packets	Packet %	Bytes	Byte %
61.152.241.175	263,933	2.7	11,617,276	2.0
194.200.29.110	255,934	2.6	14,332,304	2.5
61.234.250.206	236,036	2.4	10,243,668	1.8

Table A1-6 – Top 3 source IPs across all packet types by packet count, in 1B.

Alert Name	Alert Count	Alert %
ICMP Destination Unreachable Communication Administratively Prohibited	256,348	44.6
MS-SQL Worm Propagation Attempt	157,766	27.5
ICMP Ping NMAP	142,355	24.8

Table A1-7 – Top 3 alerts by alert count, in 1B.

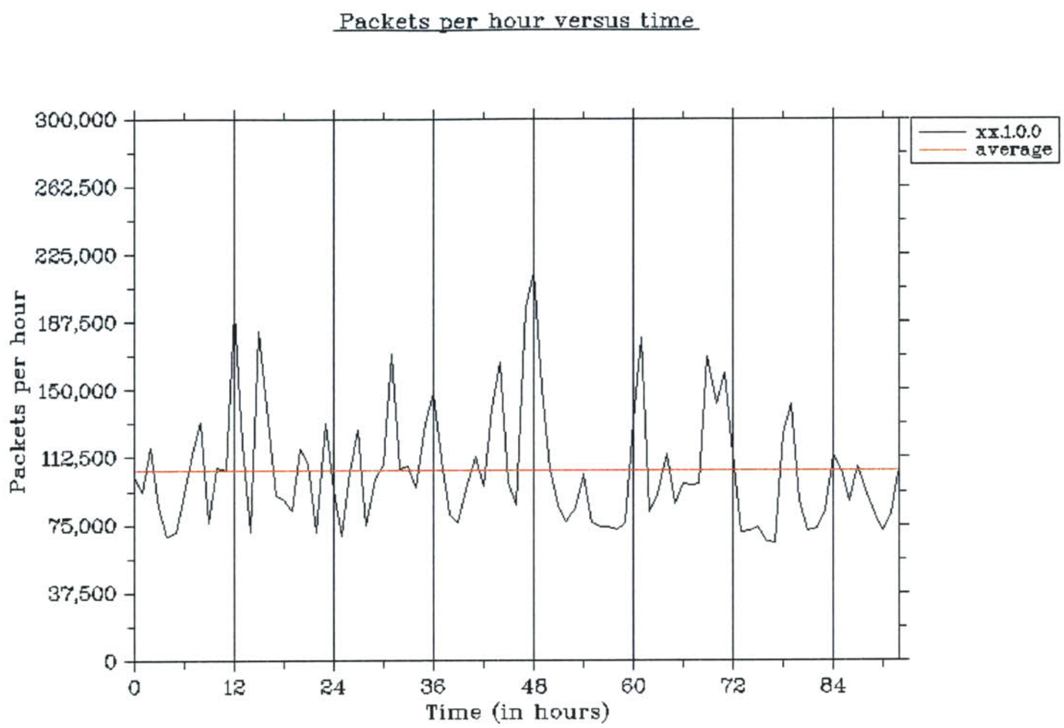

Figure A1-1 - Packets per hour versus time in 1B.

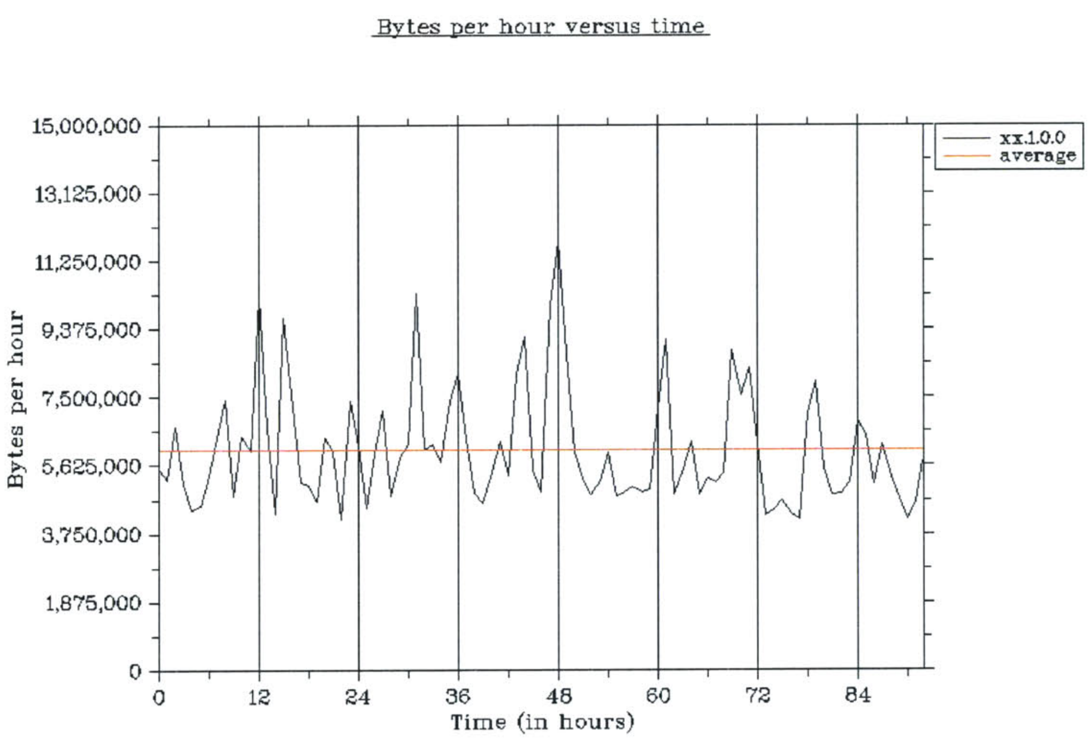

Figure A1-2 - Bytes per hour versus time in 1B.

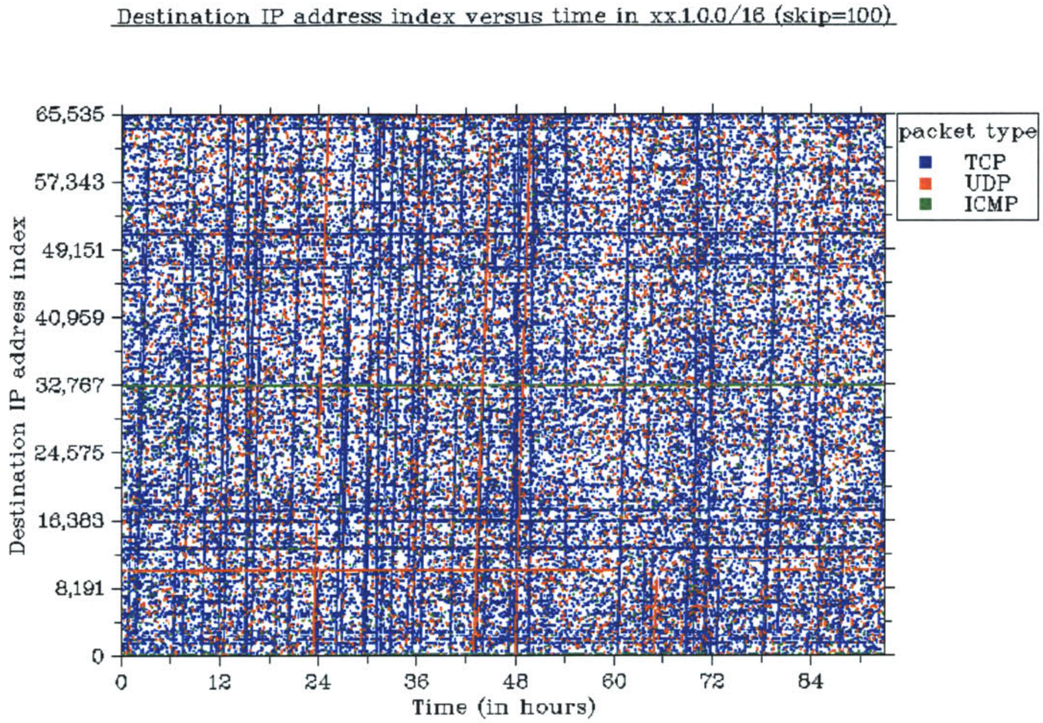

Figure A1-3 - Destination IP address index versus time in 1B.

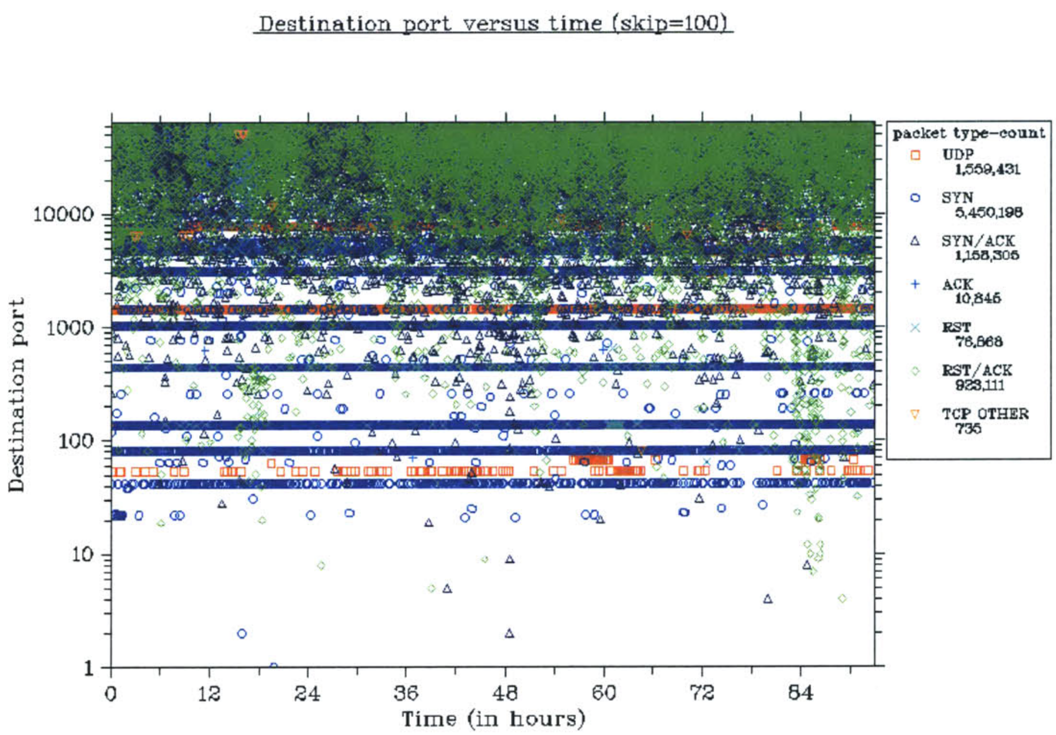

Figure A1-4 - Destination port versus time in 1B.

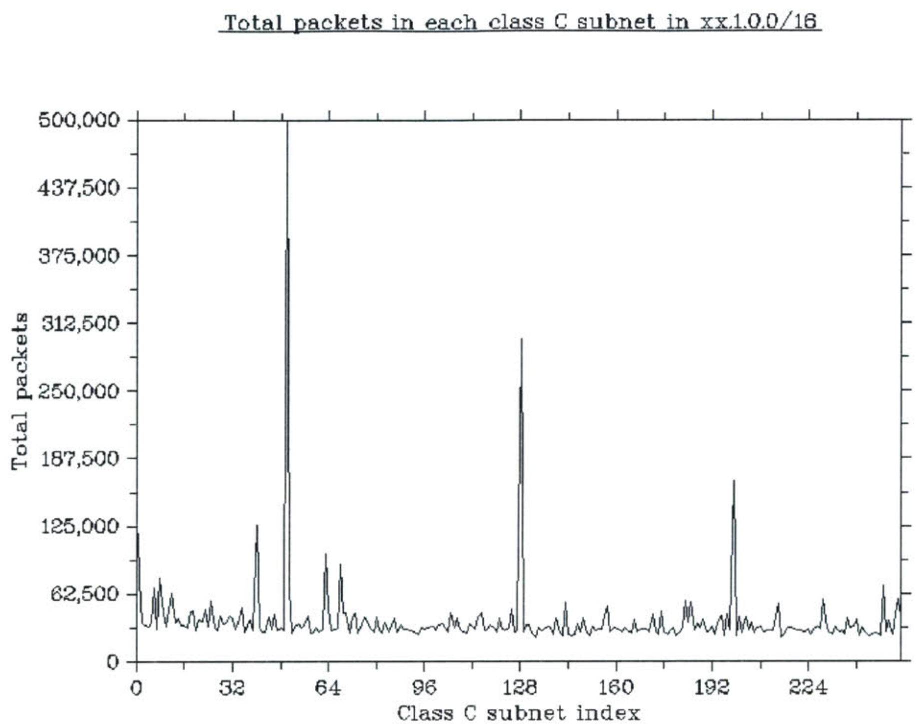

Figure A1-5 - Total packets in each class C subnet in 1B.

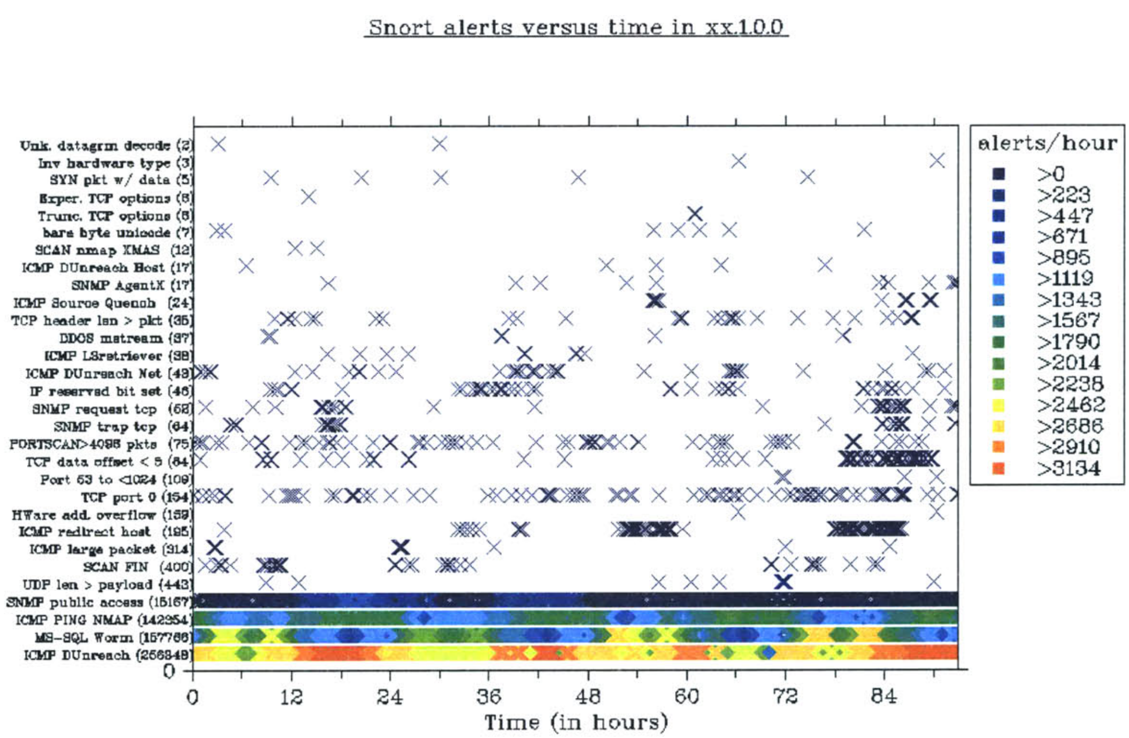

Figure A1-6 - Snort alerts versus time in 1B.

A.2 - XX.49.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	9,178,836	27	2,440	83.4	14.1	2.5
Bytes	522,324,712	1,560	107,536	69.3	29.1	1.6

Table A2-1 – Packet and byte statistics for 49B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	5,964,026	1,028,269	8,639	17,030	586,557	449

Table A2-2 – TCP packet types in 49B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	28	298K	670K (43)	57,837	381,097	24	1.4K	65,536	140	8.0K
90	X	X	X	8,733	75,904	109	6.3K	53,822	154	8.7K
50	X	X	X	2	86	53.4K	2.9M	17,537	262	13.9K

Table A2-3 – Statistics for all, the top 90%, and the top 50% of traffic in 49B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	3,715,752	40.5	178,623,634	34.2
UDP – 137	1,109,883	12.1	86,572,392	16.6
TCP – 135	894,402	9.7	42,835,582	8.2

Table A2-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 49B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.49.10.69	44,592	0.5	2,154,271	0.4
xx.49.251.163	32,551	0.4	1,577,568	0.3
xx.49.251.82	29,114	0.3	1,414,612	0.3

Table A2-5 – Top 3 destination IPs across all packet types by packet count, in 49B.

IP Source	Packets	Packet %	Bytes	Byte %
61.180.41.196	2,052,122	22.4	98,501,856	18.9
61.152.241.175	265,155	2.9	11,671,016	2.2
61.234.250.206	235,071	2.6	10,204,596	2.0

Table A2-6 – Top 3 source IPs across all packet types by packet count, in 49B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,173	53.0
ICMP Ping NMAP	137,280	46.0
SNMP Public Access UDP	576	0.2

Table A2-7 – Top 3 alerts by alert count, in 49B.

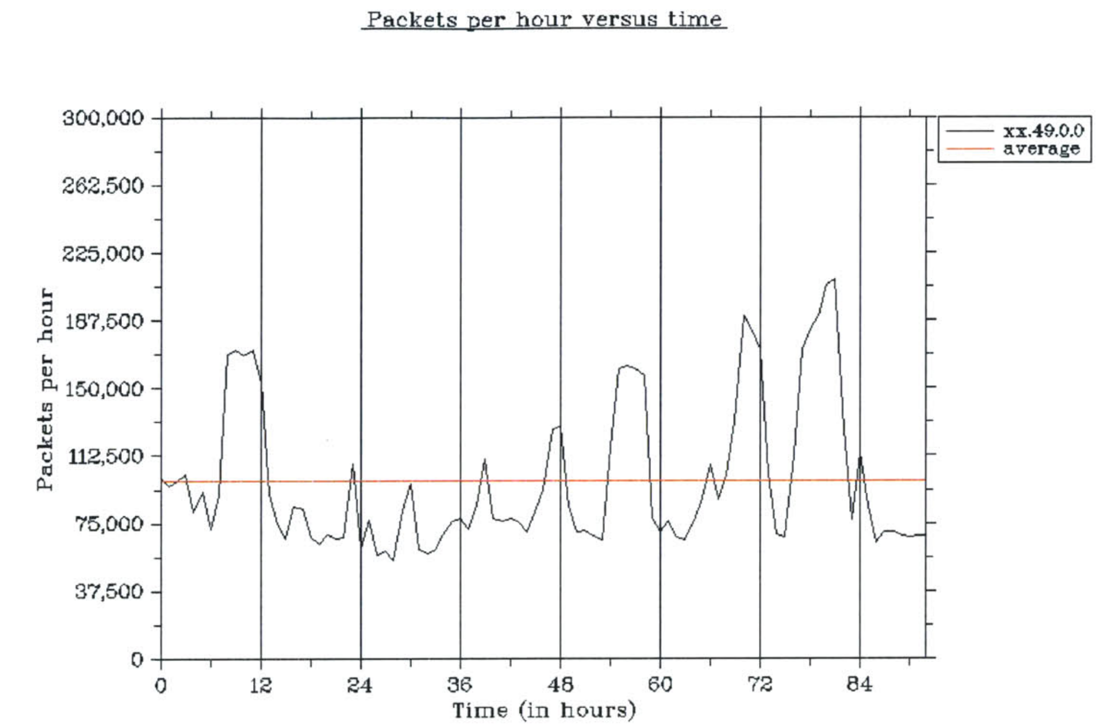

Figure A2-1 - Packets per hour versus time in 49B.

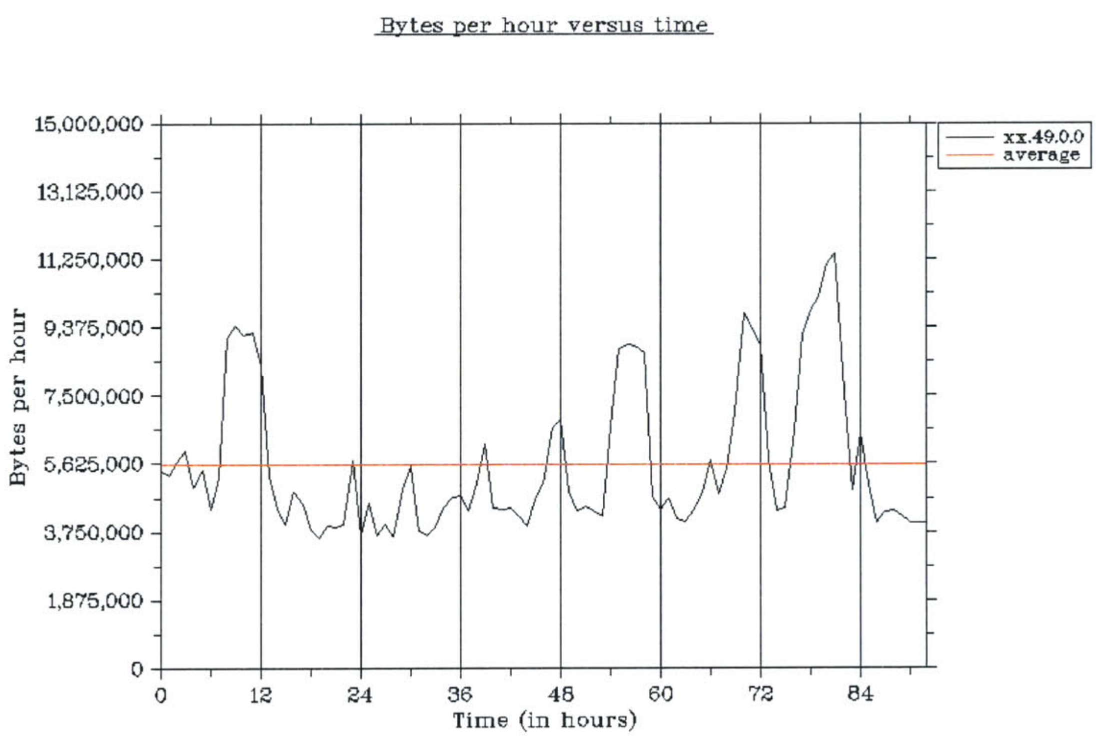

Figure A2-2 - Bytes per hour versus time in 49B.

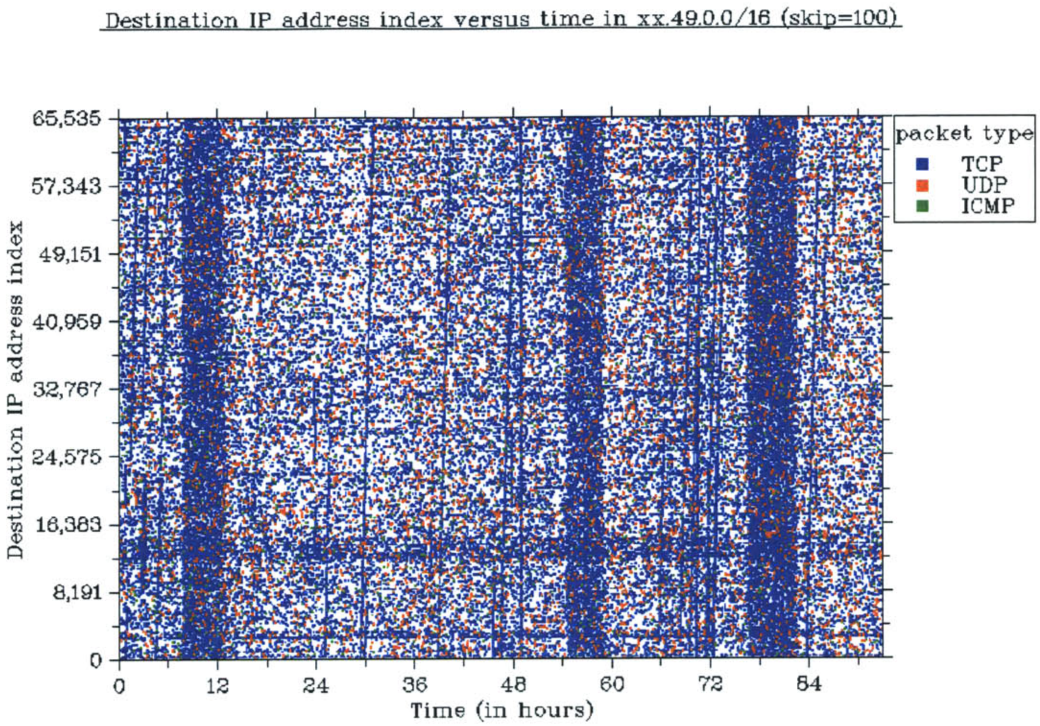

Figure A2-3 - Destination IP address index versus time in 49B.

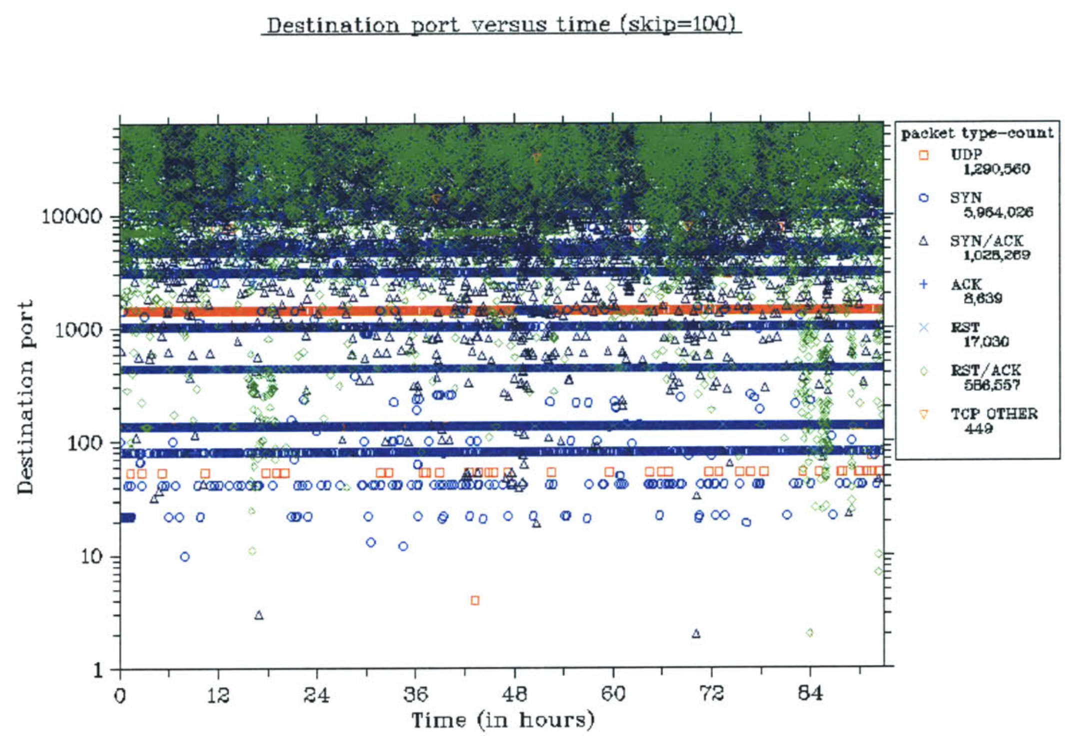

Figure A2-4 - Destination port versus time in 49B.

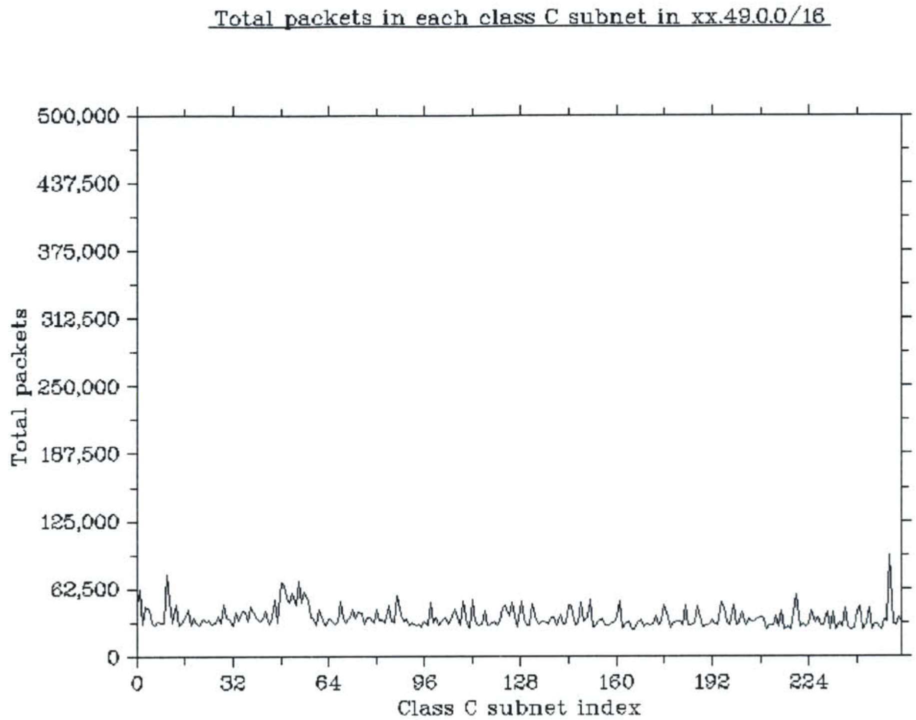

Figure A2-5 - Total packets in each class C subnet in 49B.

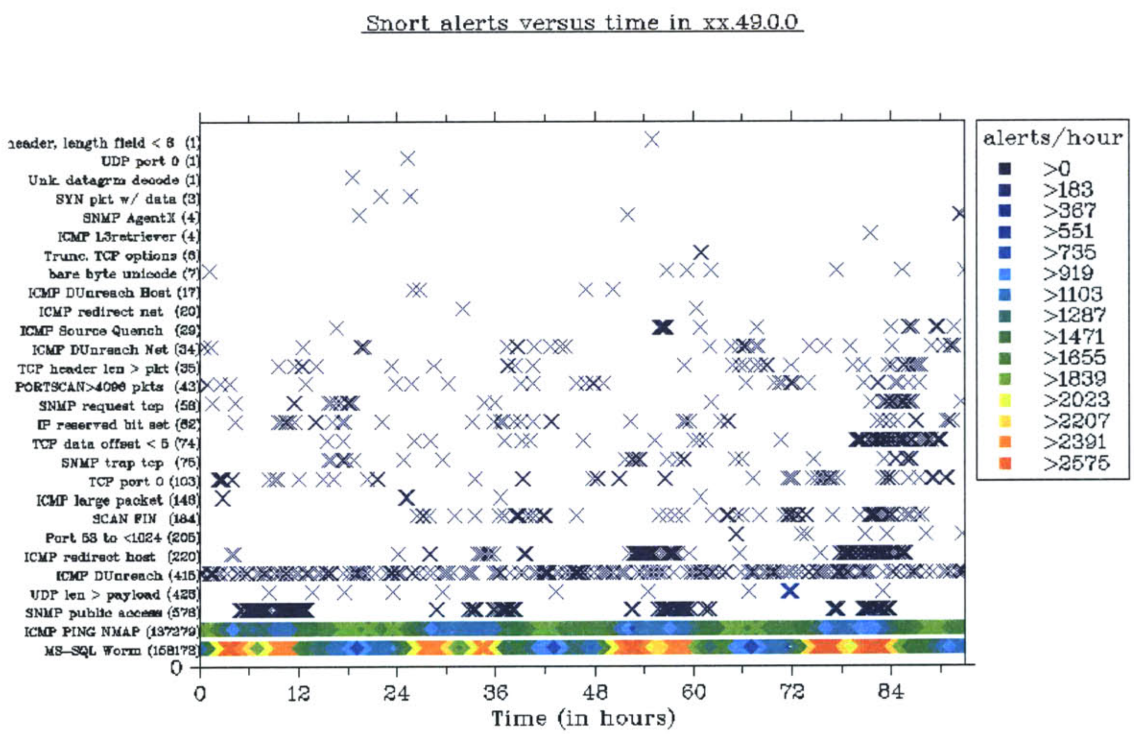

Figure A2-6 - Snort alerts versus time in 49B.

A.3 - XX.81.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	6,699,348	20	2,970	73.3	20.1	6.6
Bytes	405,173,024	1,210	131,250	56.7	38.1	5.2

Table A3-1 – Packet and byte statistics for 81B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	3,217,758	1,041,876	8,409	16,993	574,614	230

Table A3-2 – TCP packet types in 81B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	24	301K	536K (43)	58,006	372,169	18	1.1K	65,536	102	6.2K
90	X	X	X	13,695	106,321	57	3.5K	51,920	116	6.9K
50	X	X	X	4	893	3.8K	232K	13,910	241	12.8K

Table A3-3 – Statistics for all, the top 90%, and the top 50% of traffic in 81B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,550,119	23.1	74,665,687	18.4
UDP – 137	1,115,871	16.7	87,037,938	21.5
TCP – 135	660,758	9.9	31,727,655	7.8

Table A3-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 81B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.81.254.184	77,003	1.2	3,721,069	0.9
xx.81.220.175	43,880	0.7	2,120,147	0.5
xx.81.220.27	30,681	0.5	1,478,834	0.4

Table A3-5 – Top 3 destination IPs across all packet types by packet count, in 81B.

IP Source	Packets	Packet %	Bytes	Byte %
61.152.241.175	265,547	4.0	11,687,964	2.9
61.234.250.206	235,940	3.5	10,239,928	2.5
213.96.162.222	194,397	2.9	11,663,820	2.9

Table A3-6 – Top 3 source IPs across all packet types by packet count, in 81B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,564	52.8
ICMP Ping NMAP	139,164	46.3
ICMP Destination Unreachable Communication Administratively Prohibited	824	0.3

Table A3-7 – Top 3 alerts by alert count, in 81B.

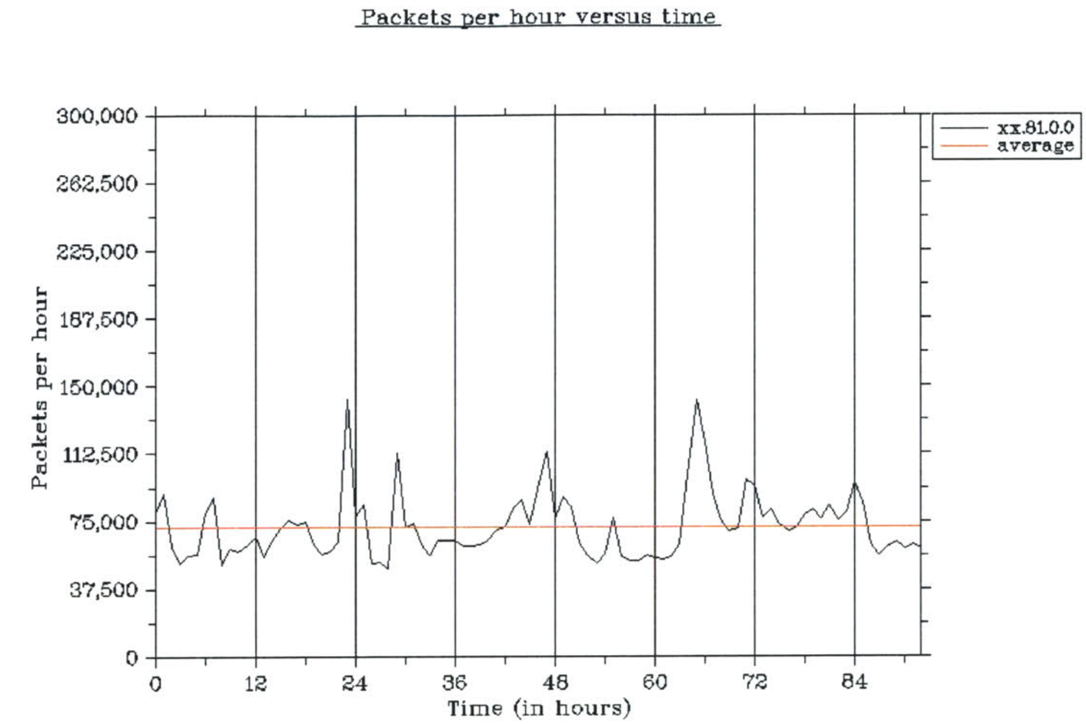

Figure A3-1 - Packets per hour versus time in 81B.

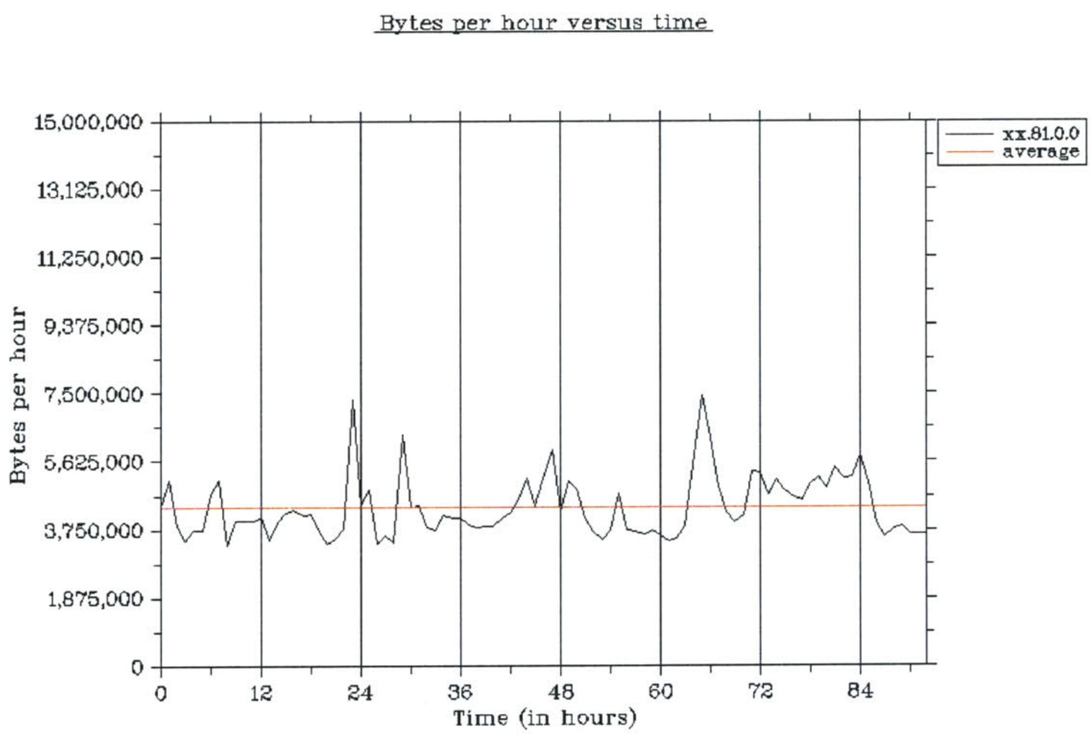

Figure A3-2 - Bytes per hour versus time in 81B.

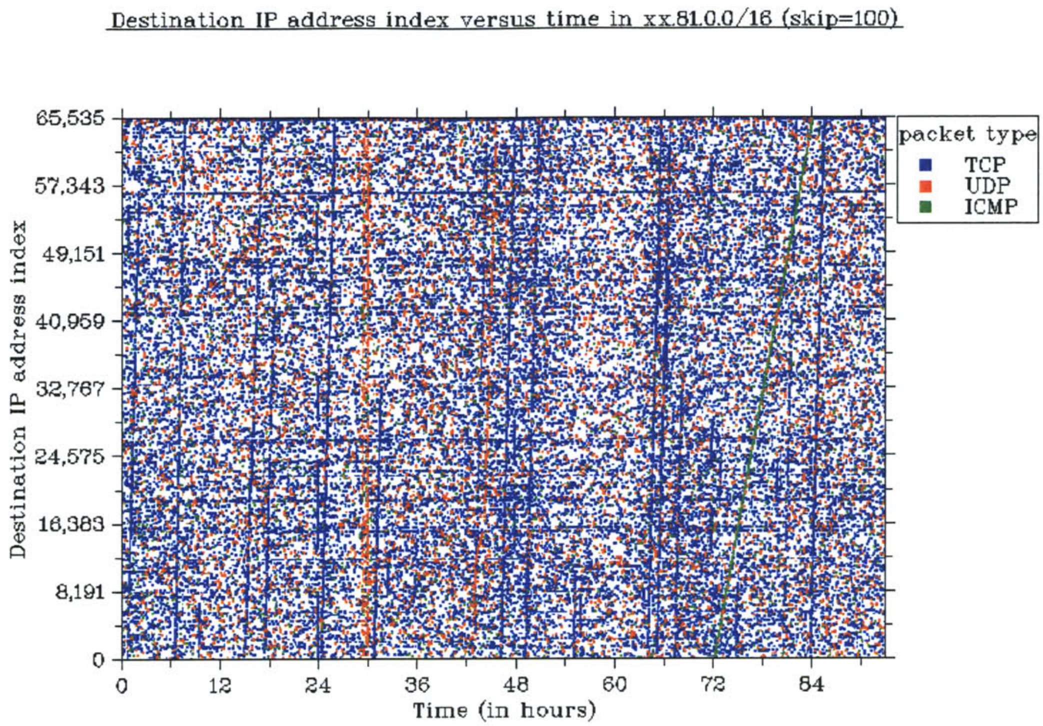

Figure A3-3 - Destination IP address index versus time in 81B.

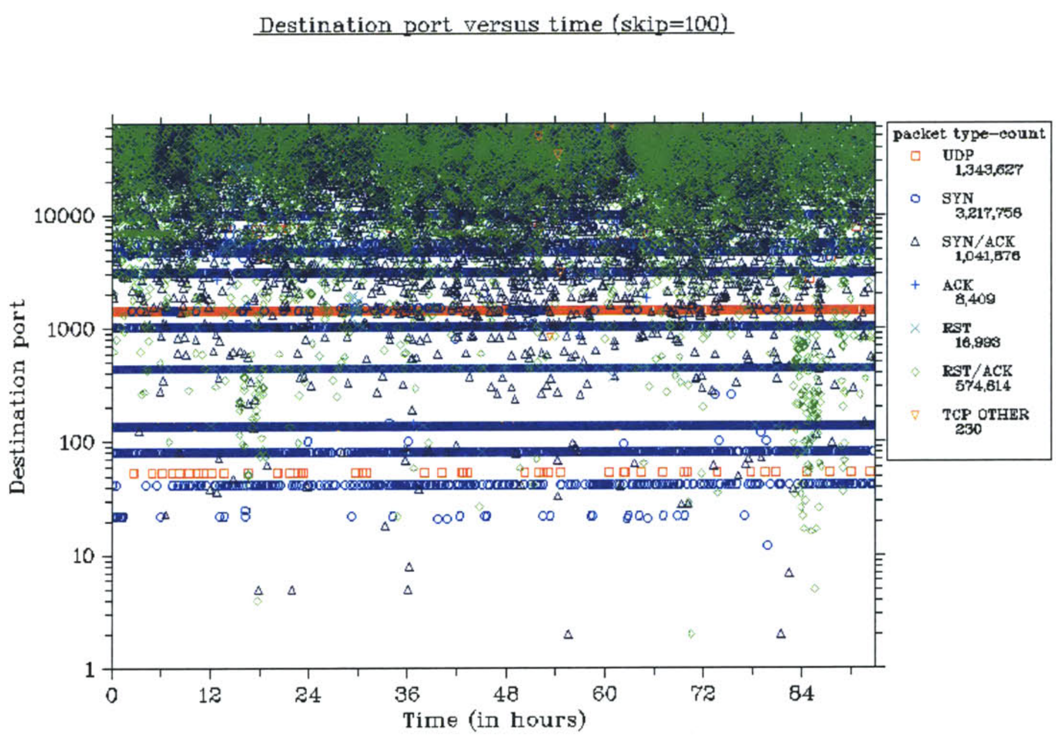

Figure A3-4 - Destination port versus time in 81B.

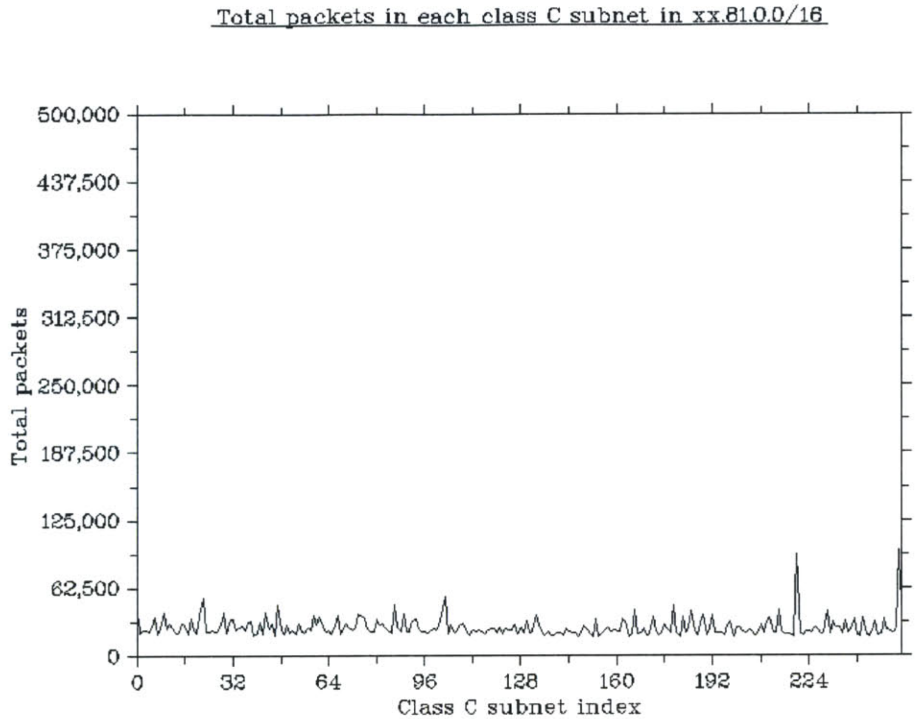

Figure A3-5 - Total packets in each class C subnet in 81B.

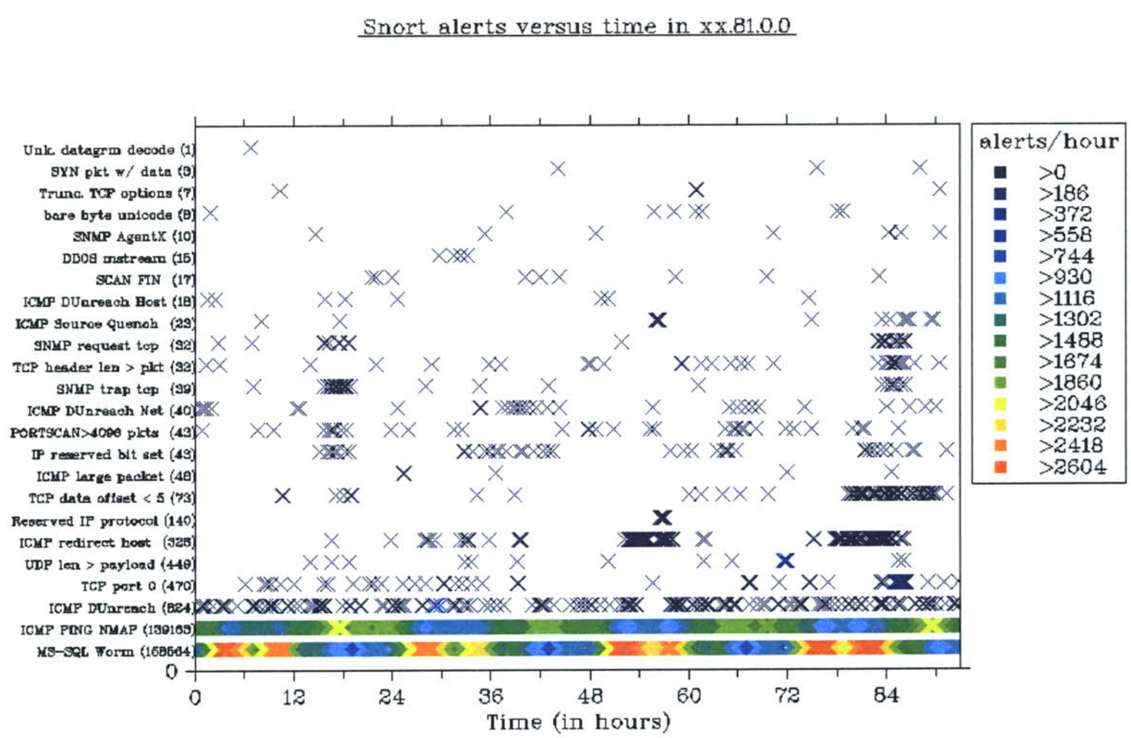

Figure A3-6 - Snort alerts versus time in 81B.

A.4 - XX.128.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	7,080,623	21	3,930	63.2	33.3	3.5
Bytes	536,255,022	1,622	278,750	39.4	58.9	1.7

Table A4-1 – Packet and byte statistics for 128B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	3,620,414	289,605	3,456	31,086	515,151	61

Table A4-2 – TCP packet types in 128B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	30	308K	441K (35)	54,024	384,173	18	1.4K	65,536	108	8.2K
90	X	X	X	1,615	110,515	58	4.6K	48,421	132	10.1K
50	X	X	X	3	1,179	3.0K	282K	1,377	2.6K	206K

Table A4-3 – Statistics for all, the top 90%, and the top 50% of traffic in 128B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,664,061	23.5	80,138,061	14.9
UDP – 137	1,098,741	15.5	85,862,957	16.0
TCP – 135	832,482	11.8	39,879,165	7.4

Table A4-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 128B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.128.8.14	830,425	11.7	132,503,739	24.7
xx.128.247.192	469,569	6.6	19,373,962	3.6
xx.128.110.120	60,694	0.9	7,773,099	1.5

Table A4-5 – Top 3 destination IPs across all packet types by packet count, in 128B.

IP Source	Packets	Packet %	Bytes	Byte %
212.64.161.175	181,920	2.6	23,308,759	4.4
213.146.105.136	118,420	1.7	5,684,160	1.1
61.152.108.4	108,174	1.5	4,328,724	0.8

Table A4-6 – Top 3 source IPs across all packet types by packet count, in 128B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,105	51.3
ICMP Ping NMAP	136,317	44.2
SNMP Public Access UDP	7,718	2.5

Table A4-7 – Top 3 alerts by alert count, in 128B.

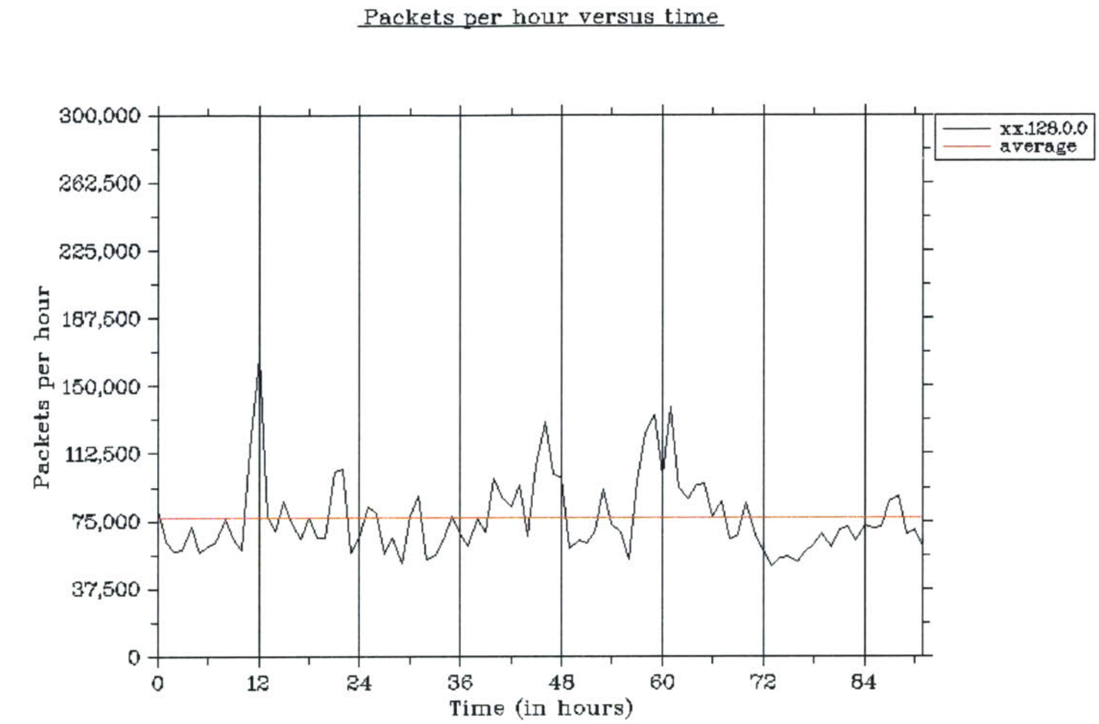

Figure A4-1 - Packets per hour versus time in 128B.

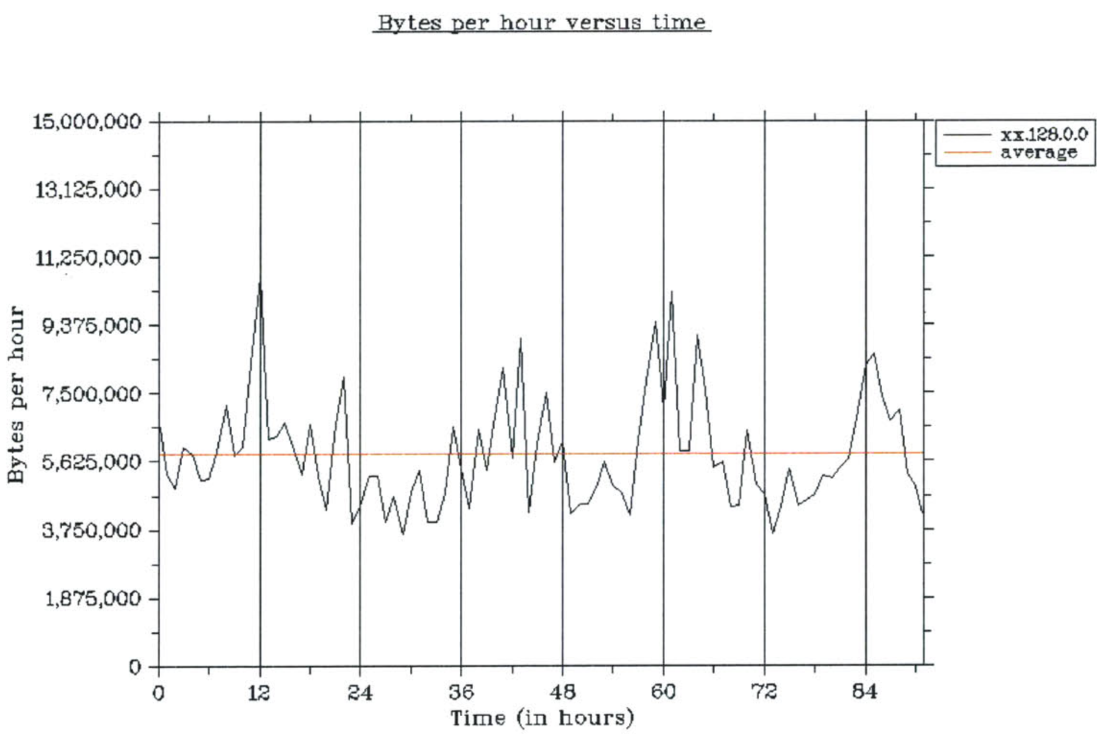

Figure A4-2 - Bytes per hour versus time in 128B.

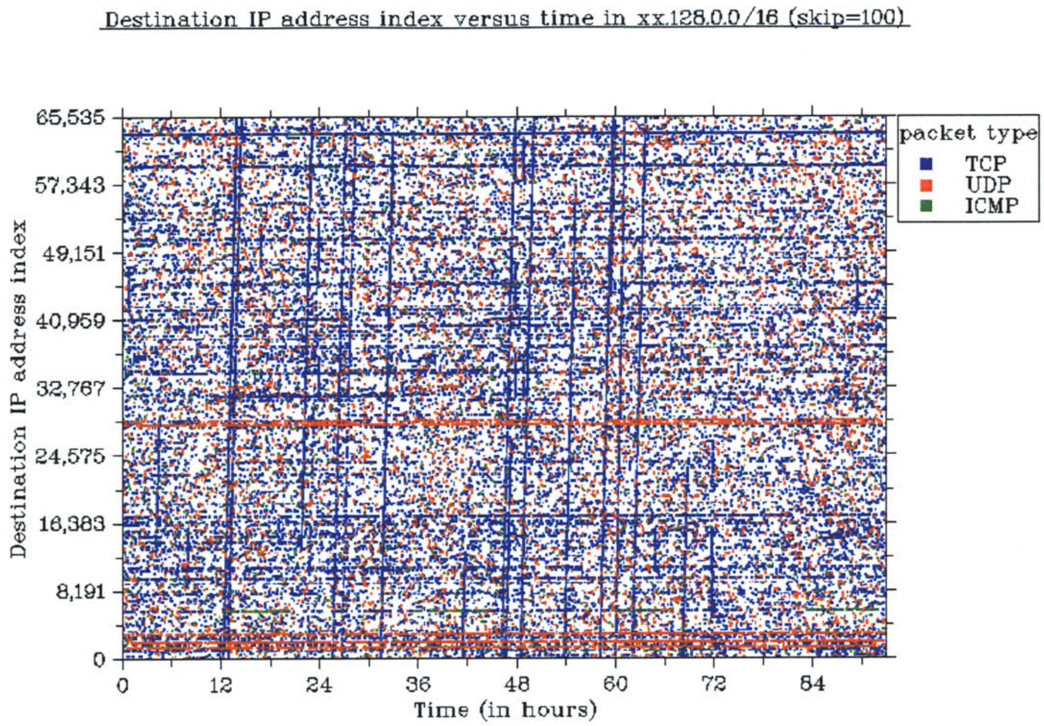

Figure A4-3 - Destination IP address index versus time in 128B.

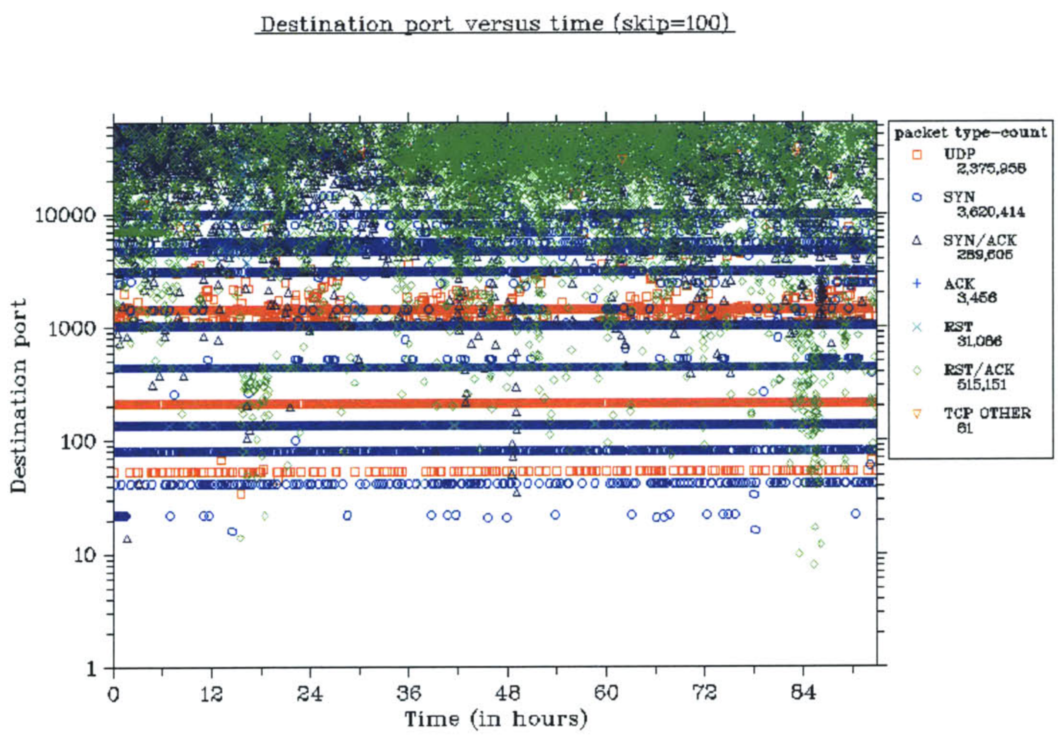

Figure A4-4 - Destination port versus time in 128B.

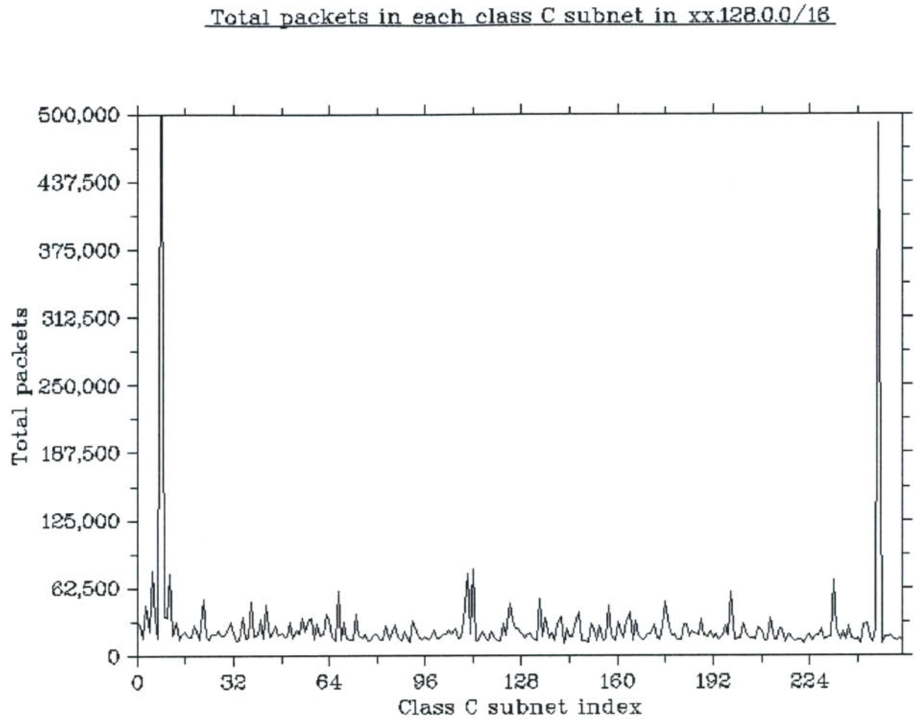

Figure A4-5 - Total packets in each class C subnet in 128B.

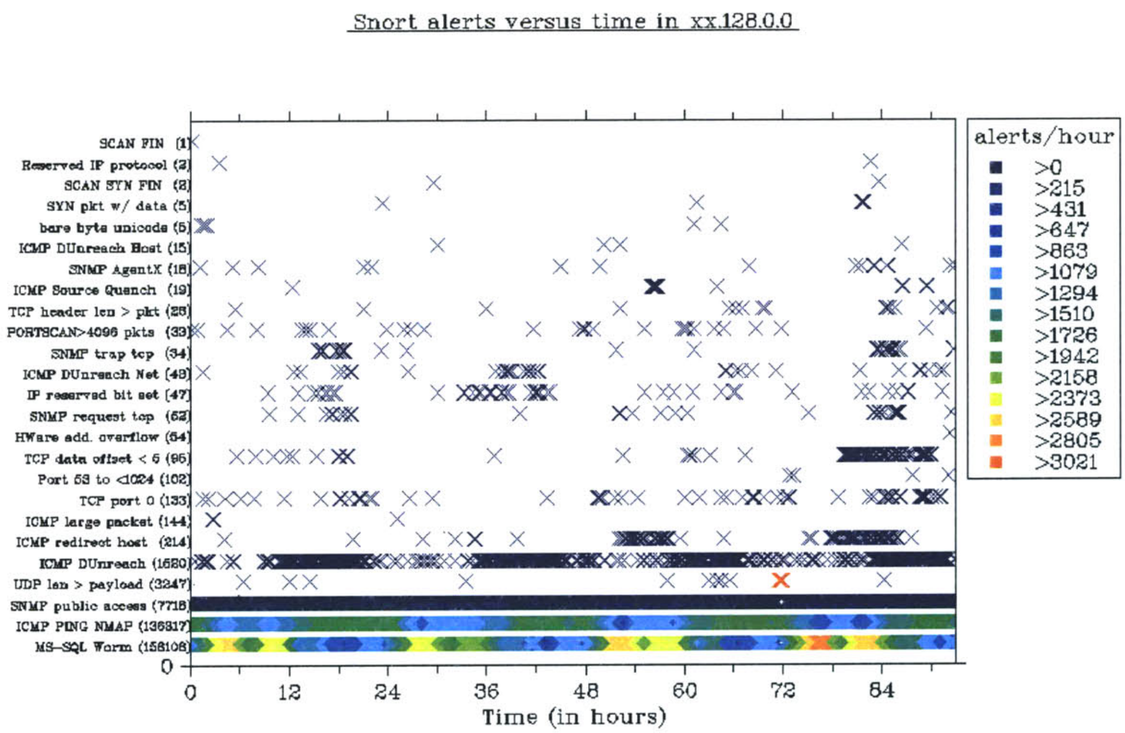

Figure A4-6 - Snort alerts versus time in 128B.

A.5 - XX.168.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	8,544,791	26	2,650	55.0	42.4	2.6
Bytes	563,926,084	1,684	117,206	39.4	59.2	1.4

Table A5-1 – Packet and byte statistics for 168B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	3,821,079	282,380	3,057	17,452	519,781	341

Table A5-2 – TCP packet types in 168B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 4K pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	24	304K	521K (46)	52,512	379,794	23	1.5K	65,536	130	8.6K
90	X	X	X	58	80,961	95	6.5K	53,769	143	9.3K
50	X	X	X	2	176	24.3K	1.8M	15,411	277	15.8K

Table A5-3 – Statistics for all, the top 90%, and the top 50% of traffic in 168B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
UDP – 137	3,437,748	40.2	268,147,878	47.6
TCP – 445	1,688,090	19.8	81,324,677	14.4
TCP – 135	787,759	9.2	38,162,440	6.8

Table A5-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 168B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.168.88.0	471,637	5.5	19,445,706	3.5
xx.168.171.94	72,452	0.9	3,498,028	0.6
xx.168.190.53	43,929	0.5	2,123,544	0.4

Table A5-5 – Top 3 destination IPs across all packet types by packet count, in 168B.

IP Source	Packets	Packet %	Bytes	Byte %
65.93.159.190	169,930	2.0	13,254,540	2.4
138.89.152.173	116,279	1.4	9,069,762	1.6
129.44.61.42	110,295	1.3	8,603,010	1.5

Table A5-6 – Top 3 source IPs across all packet types by packet count, in 168B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,928	52.3
ICMP Ping NMAP	142,832	47.0
Short UDP Packet, Length Field > Payload Length	432	0.1

Table A5-7 – Top 3 alerts by alert count, in 168B.

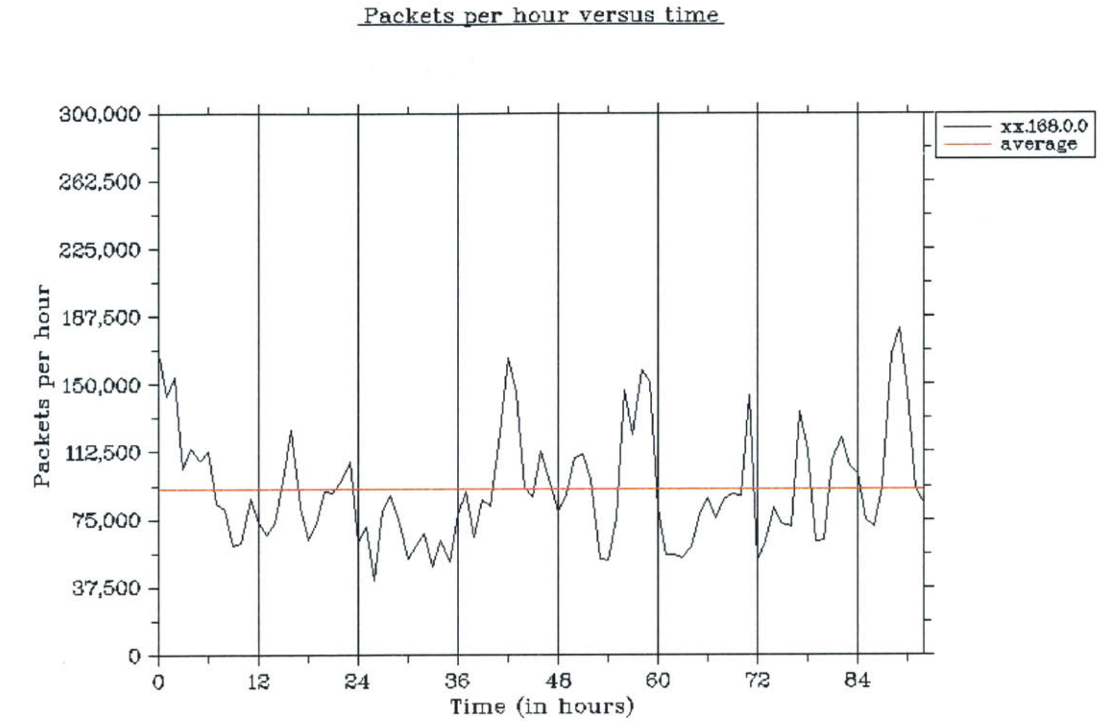

Figure A5-1 - Packets per hour versus time in 168B.

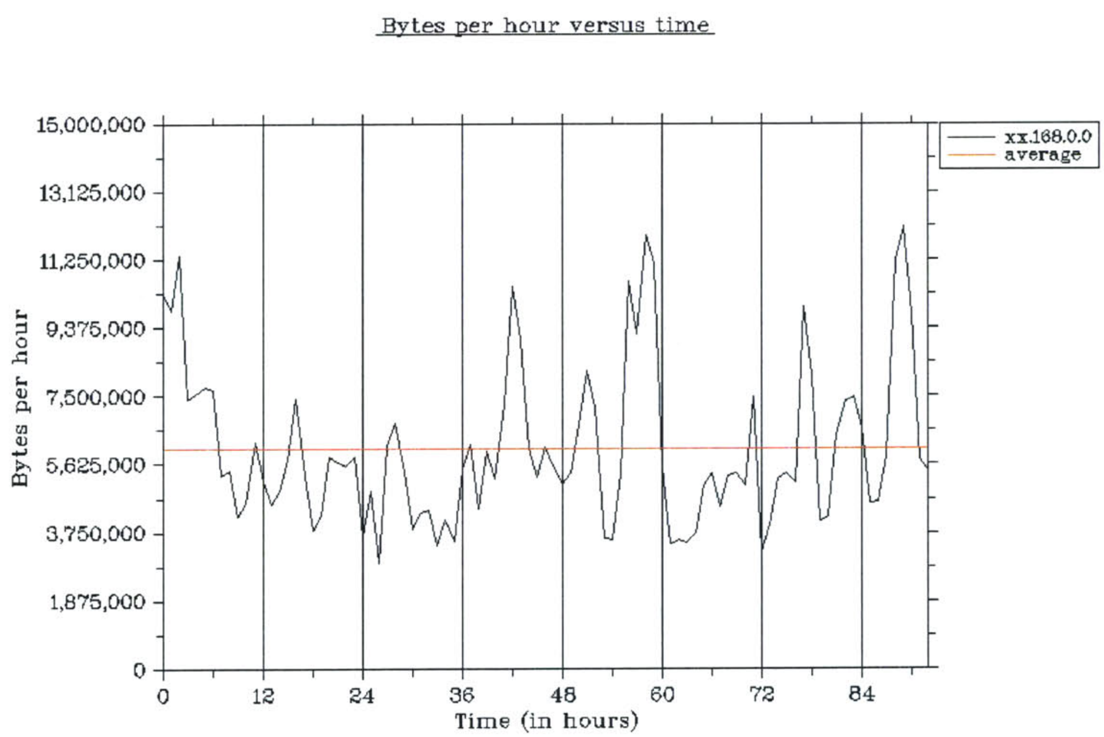

Figure A5-2 - Bytes per hour versus time in 168B.

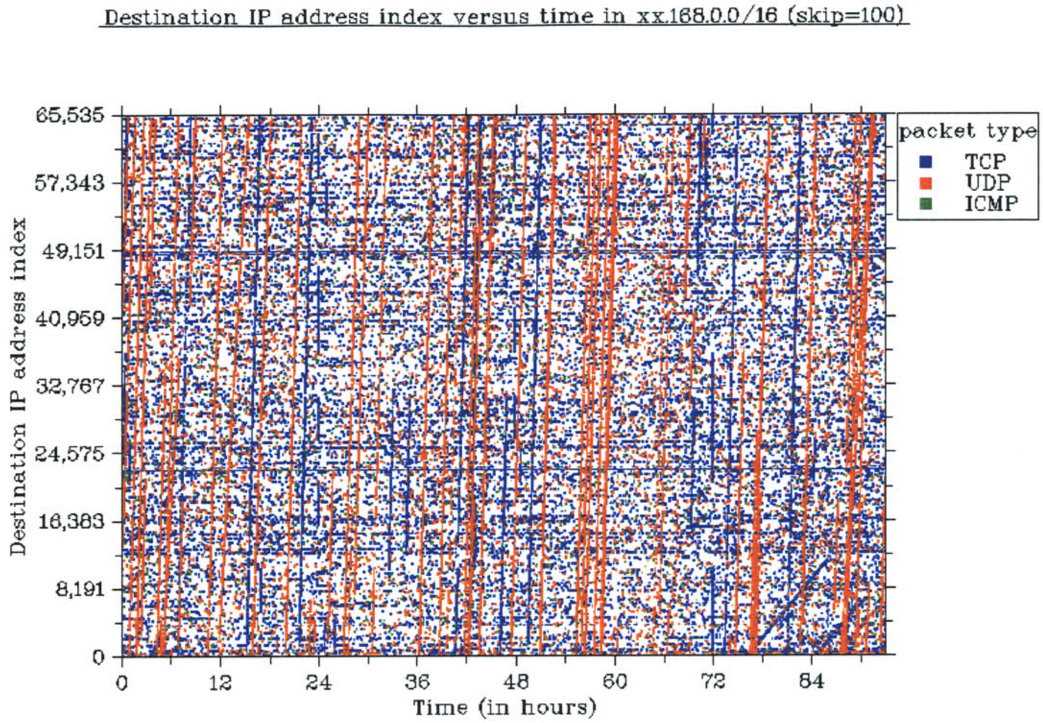

Figure A5-3 - Destination IP address index versus time in 168B.

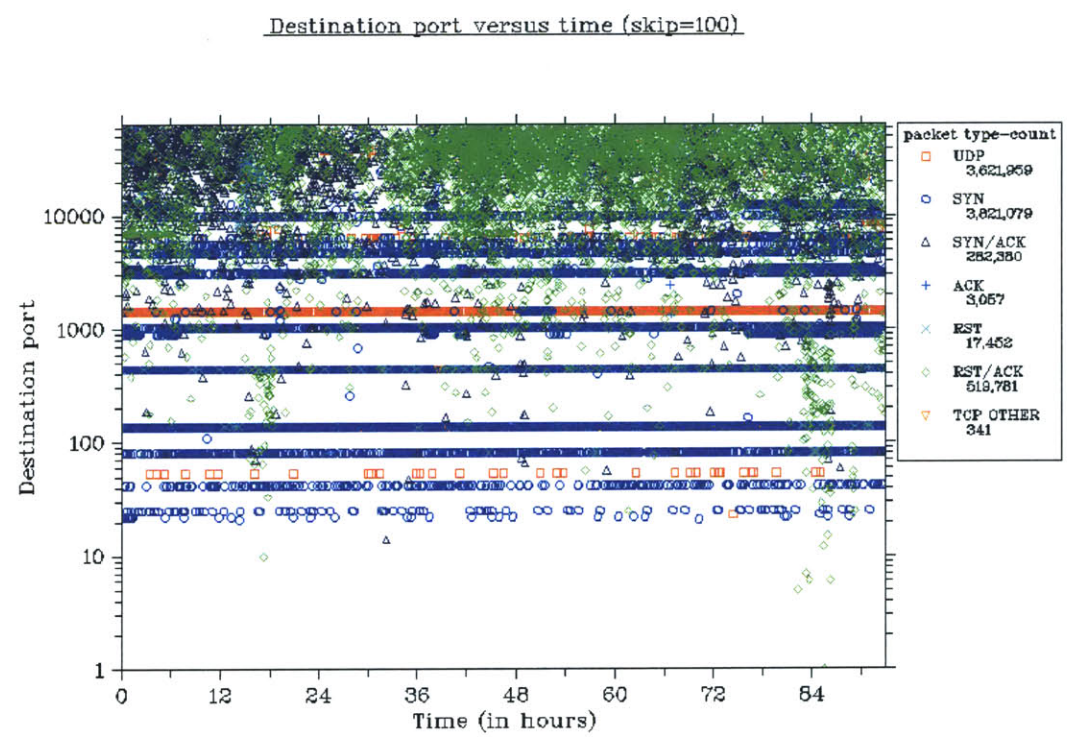

Figure A5-4 - Destination port versus time in 168B.

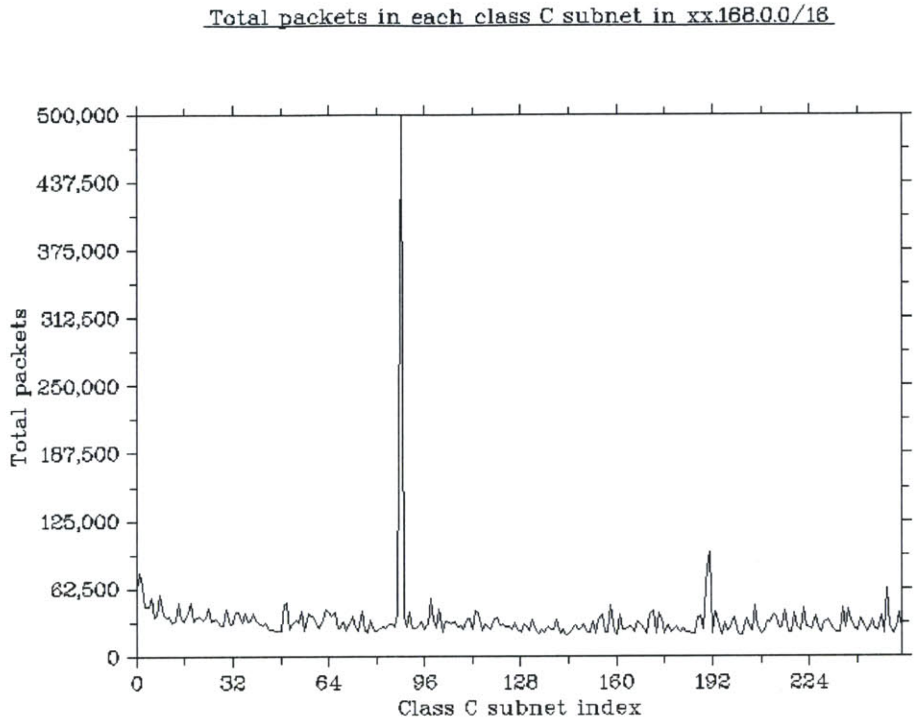

Figure A5-5 - Total packets in each class C subnet in 168B.

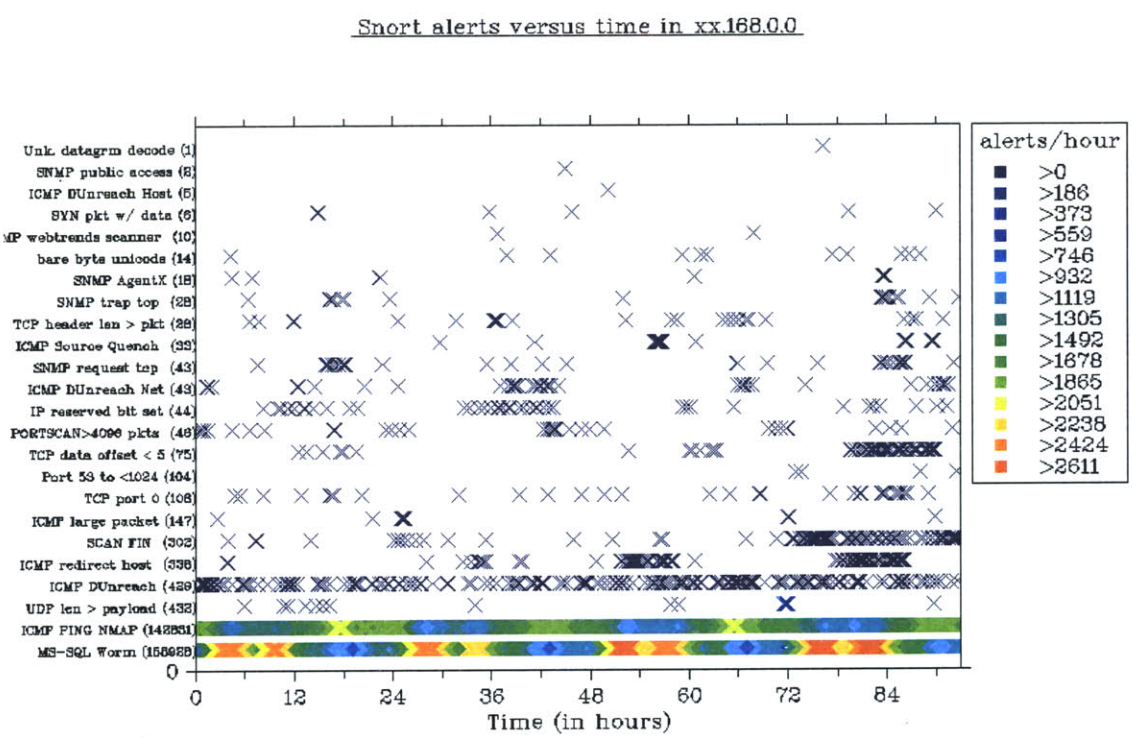

Figure A5-6 - Snort alerts versus time in 168B.

A.6 - XX.204.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	11,987,846	36	18,220	87.1	11.1	1.8
Bytes	626,254,640	1,871	728,750	74.1	24.7	1.2

Table A6-1 – Packet and byte statistics for 204B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	4,428,012	2,378,700	1,513	15,958	3,567,517	2,247

Table A6-2 – TCP packet types in 204B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 4K pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	26	302K	760K (53)	53,030	378,074	32	1.7K	65,536	183	9.6K
90	X	X	X	18,470	38,679	279	14.7K	45,198	239	12.2K
50	X	X	X	97	31	194K	8.8M	7,034	852	39.0K

Table A6-3 – Statistics for all, the top 90%, and the top 50% of traffic in 204B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,643,270	13.7	79,141,390	12.6
TCP – 135	1,159,156	9.7	55,645,126	8.9
UDP – 137	1,147,945	9.6	89,539,710	14.3

Table A6-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 204B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.204.171.140	64,601	0.5	3,121,276	0.5
xx.204.237.82	54,053	0.5	2,634,288	0.4
xx.204.47.46	53,884	0.5	2,603,037	0.4

Table A6-5 – Top 3 destination IPs across all packet types by packet count, in 204B.

IP Source	Packets	Packet %	Bytes	Byte %
61.177.64.171	1,676,994	14.0	73,787,736	11.8
61.152.91.151	1,096,223	9.1	43,849,916	7.0
211.204.30.94	520,458	4.3	24,981,984	4.0

Table A6-6 – Top 3 source IPs across all packet types by packet count, in 204B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,308	52.4
ICMP Ping NMAP	141,336	46.8
ICMP Destination Unreachable Communication Administratively Prohibited	458	0.2

Table A6-7 – Top 3 alerts by alert count, in 204B.

Packets per hour versus time

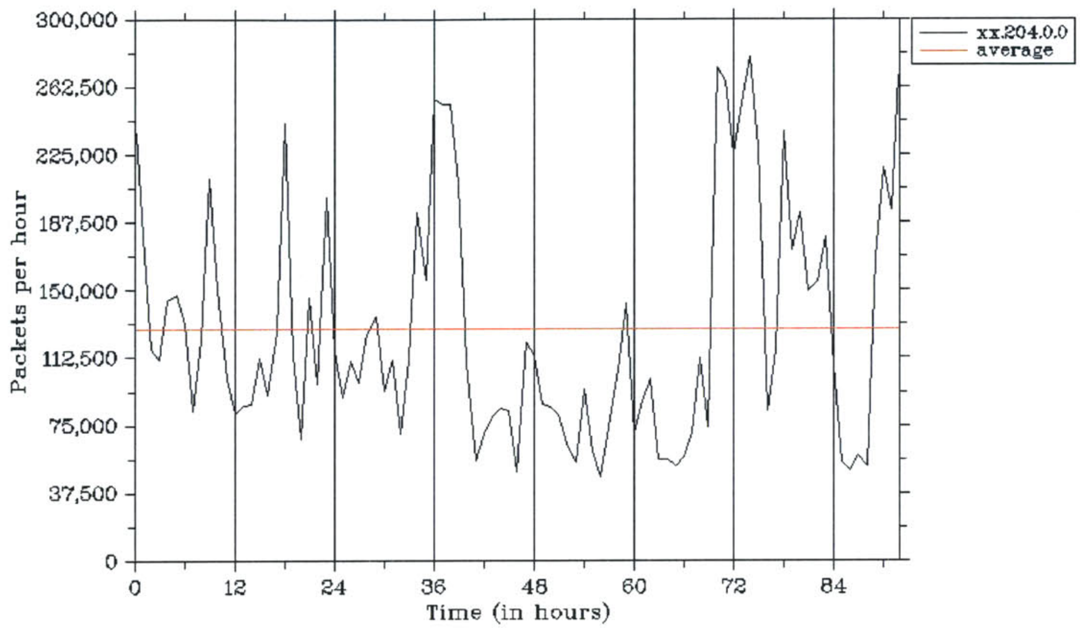

Figure A6-1 - Packets per hour versus time in 204B.

Bytes per hour versus time

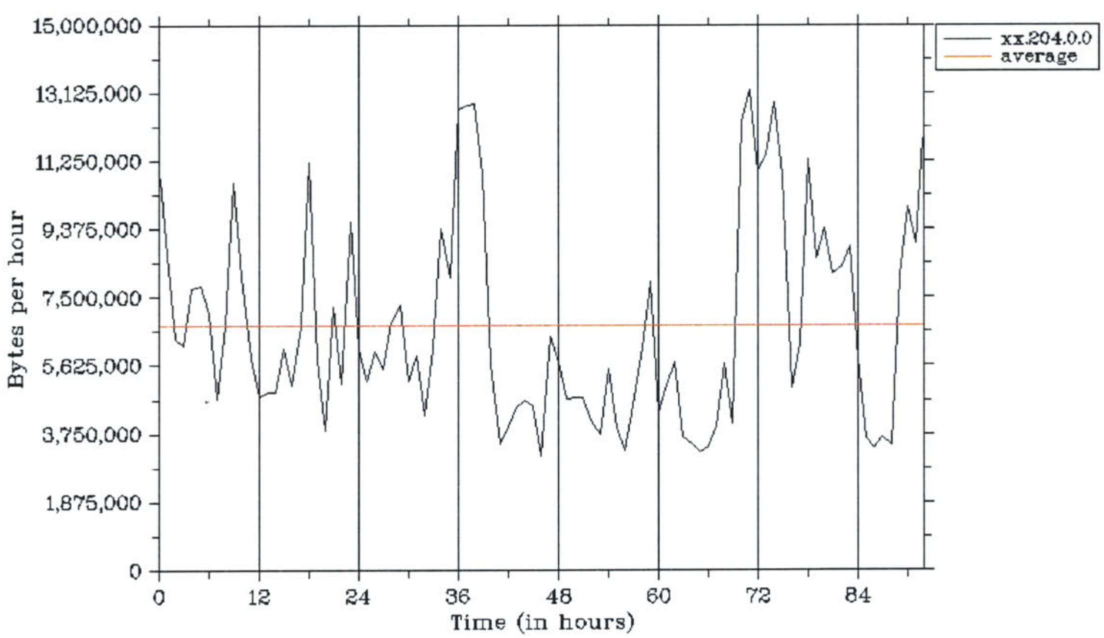

Figure A6-2 - Bytes per hour versus time in 204B.

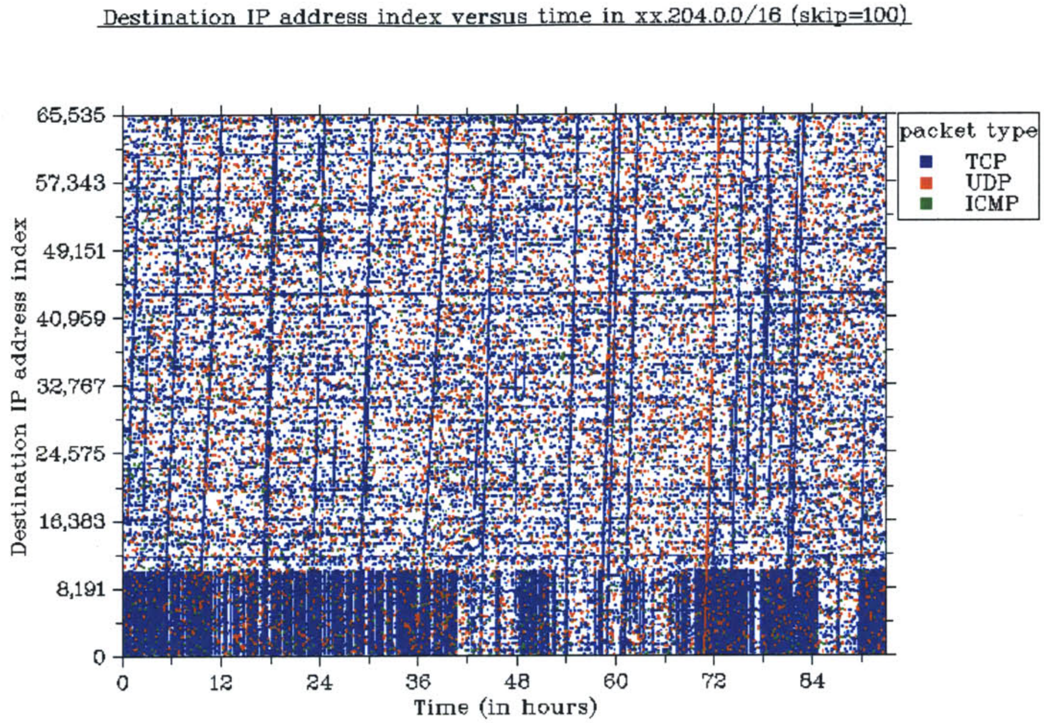

Figure A6-3 - Destination IP address index versus time in 204B.

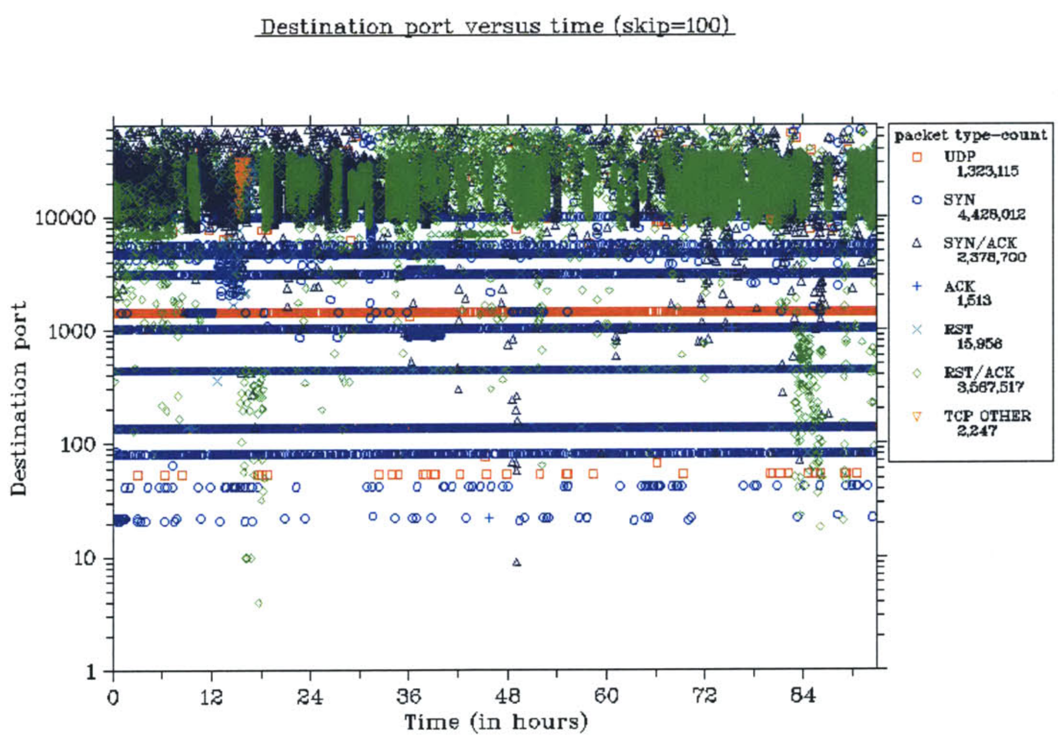

Figure A6-4 - Destination port versus time in 204B.

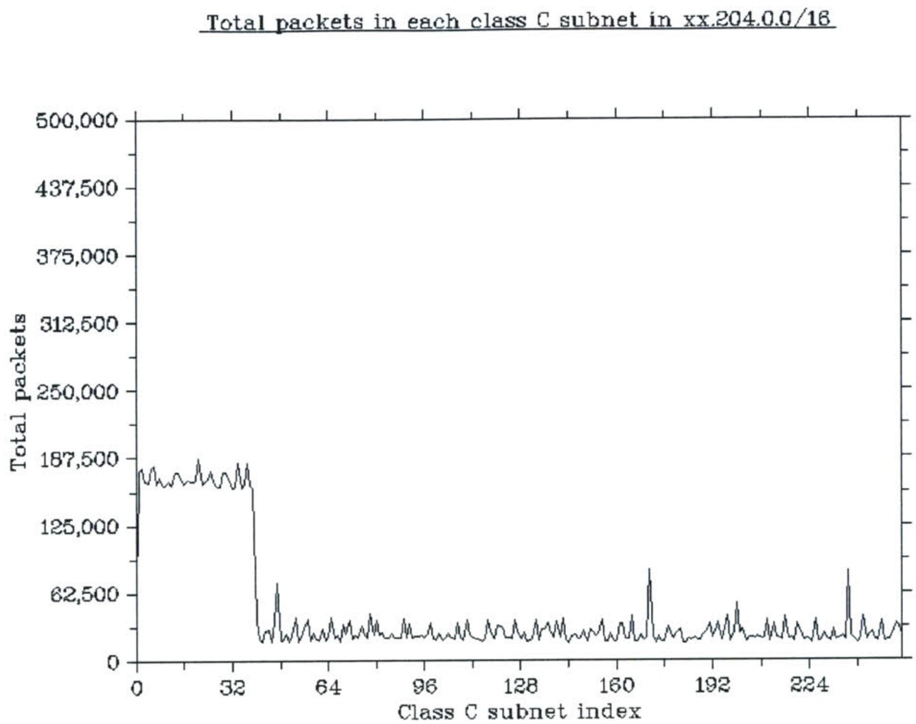

Figure A6-5 - Total packets in each class C subnet in 204B.

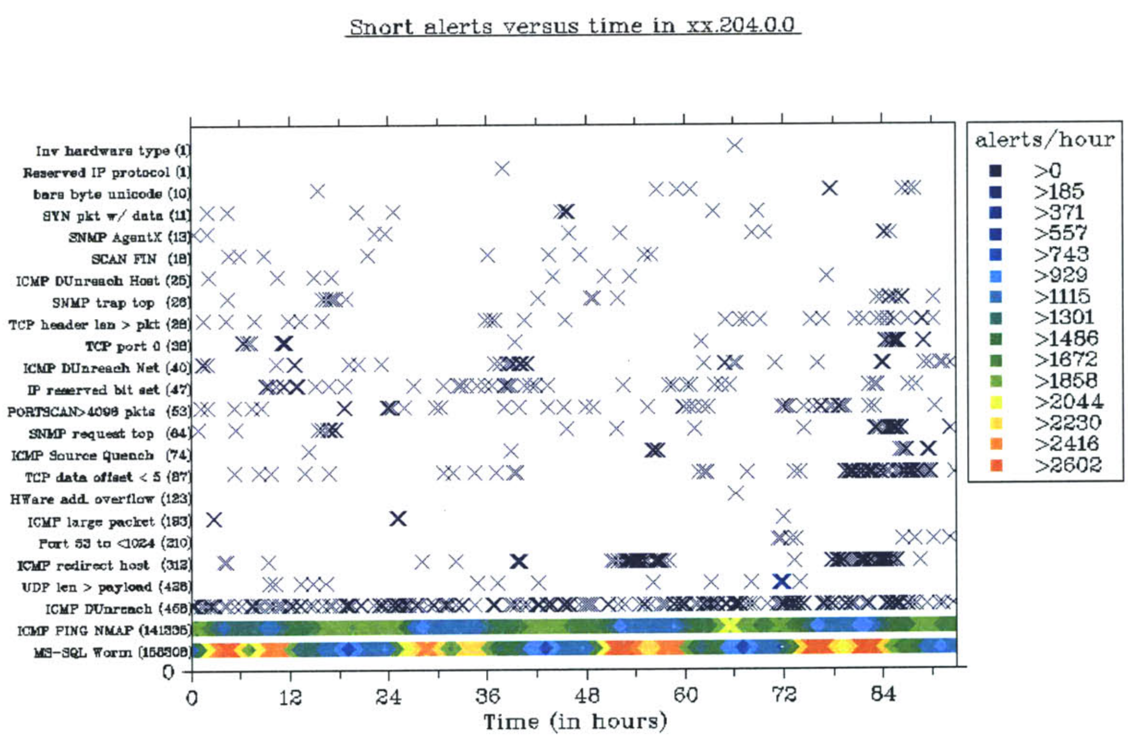

Figure A6-6 - Snort alerts versus time in 204B.

A.7 - XX.229.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	6,209,234	19	1,540	75.1	21.2	3.7
Bytes	382,977,523	1,144	76,713	57.7	40.2	2.1

Table A7-1 – Packet and byte statistics for 229B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	3,785,241	283,895	3,102	17,826	523,502	43

Table A7-2 – TCP packet types in 229B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	23	300K	635K (50)	52,384	373,498	17	1.0K	65,536	95	5.8K
90	X	X	X	2,275	118,494	47	3.0K	51,528	109	6.6K
50	X	X	X	3	2,113	1.5K	96.6K	9,107	341	17.8K

Table A7-3 – Statistics for all, the top 90%, and the top 50% of traffic in 229B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,583,517	25.5	76,278,180	19.9
UDP – 137	1,135,286	18.3	88,552,308	23.1
TCP – 135	969,172	15.6	47,099,093	12.3

Table A7-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 229B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.229.251.176	484,057	7.8	19,973,460	5.2
xx.229.80.19	193,626	3.1	9,331,825	2.4
xx.229.140.73	102,853	1.7	4,968,571	1.3

Table A7-5 – Top 3 destination IPs across all packet types by packet count, in 229B.

IP Source	Packets	Packet %	Bytes	Byte %
61.109.112.63	127,344	2.1	6,112,512	1.6
83.129.81.10	118,905	1.9	6,183,060	1.6
61.152.108.4	118,194	1.9	4,729,532	1.2

Table A7-6 – Top 3 source IPs across all packet types by packet count, in 229B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,061	52.7
ICMP Ping NMAP	139,182	46.4
Short UDP Packet, Length Field > Payload Length	445	0.2

Table A7-7 – Top 3 alerts by alert count, in 229B.

Packets per hour versus time

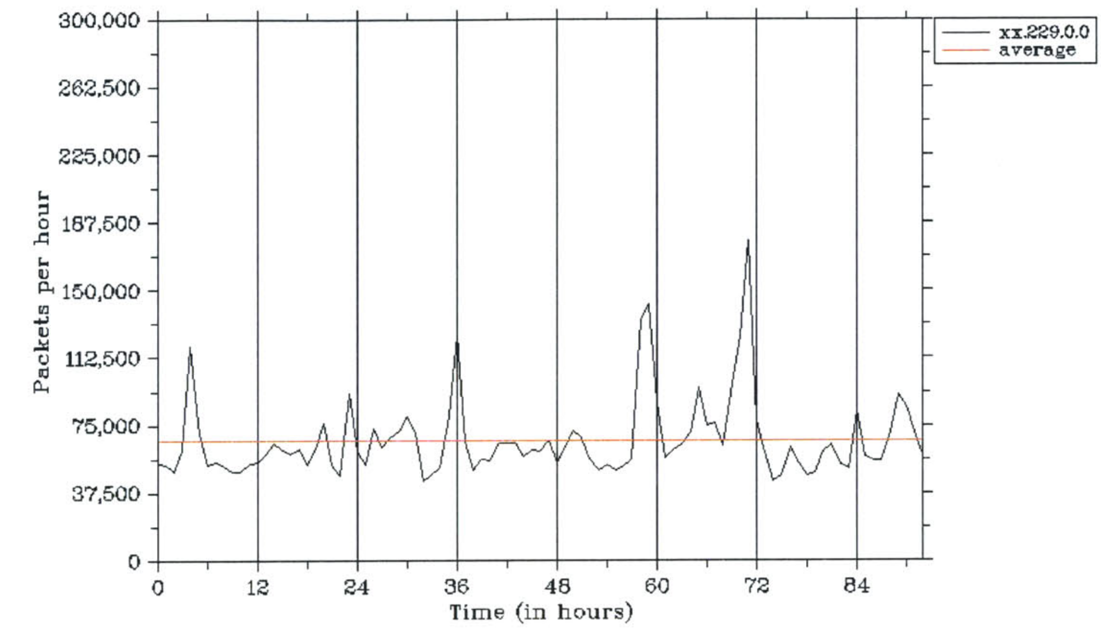

Figure A7-1 - Packets per hour versus time in 229B.

Bytes per hour versus time

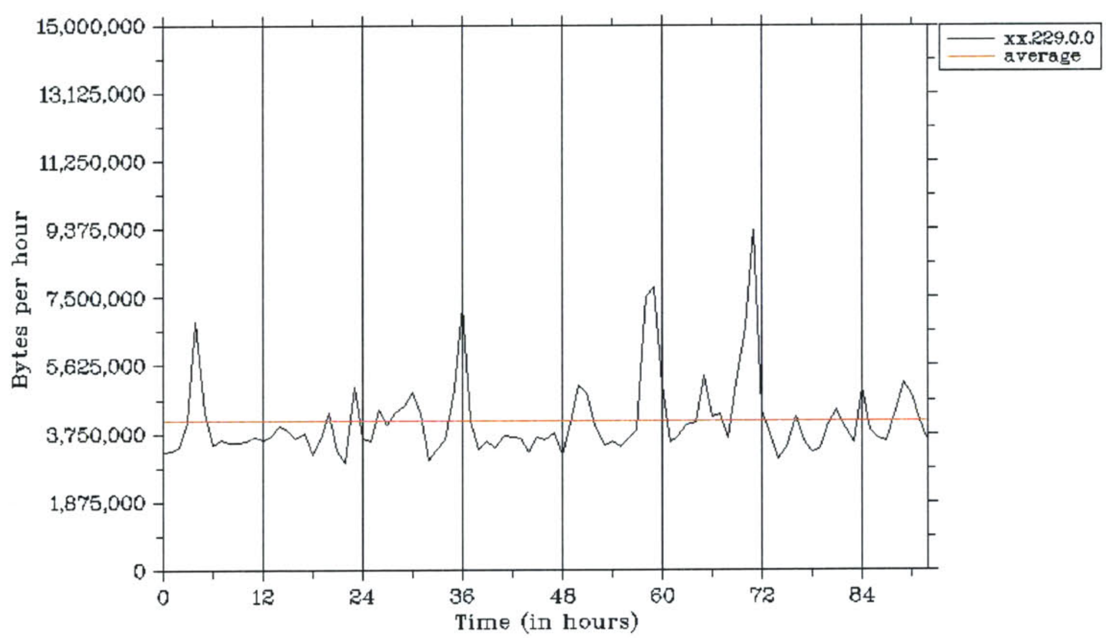

Figure A7-2 - Bytes per hour versus time in 229B.

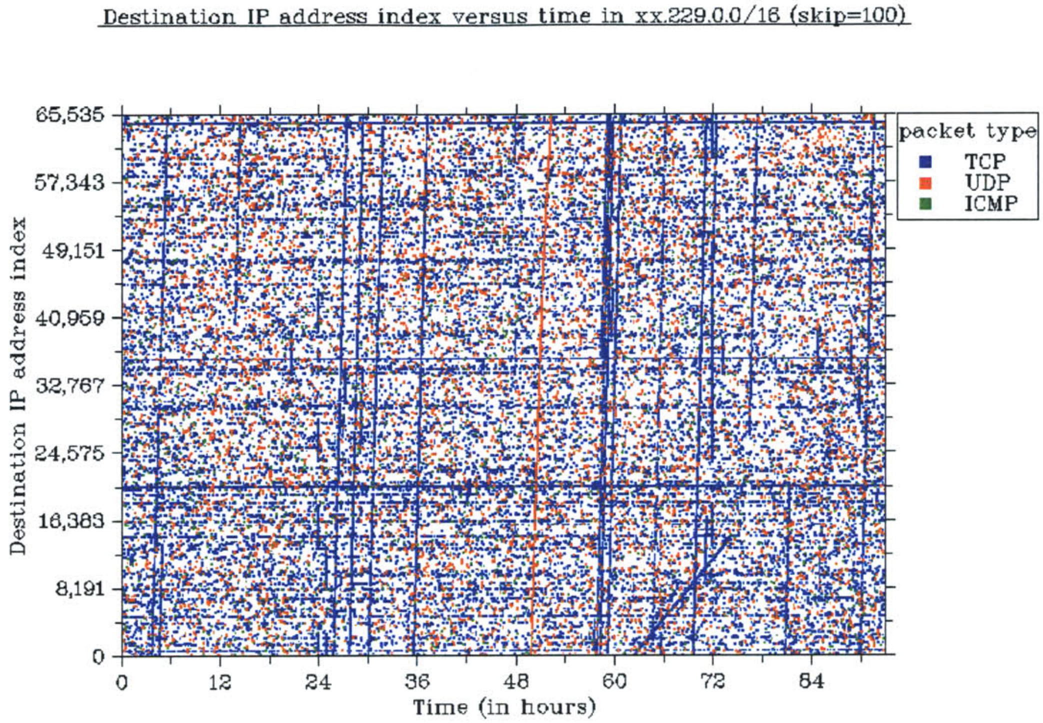

Figure A7-3 - Destination IP address index versus time in 229B.

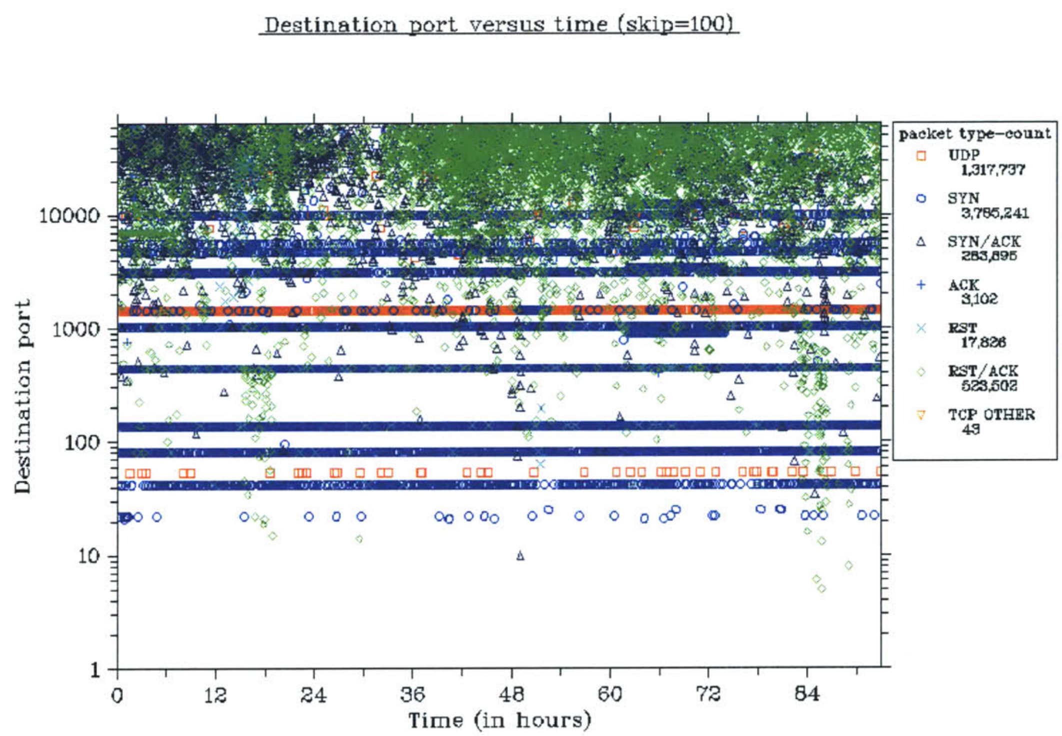

Figure A7-4 - Destination port versus time in 229B.

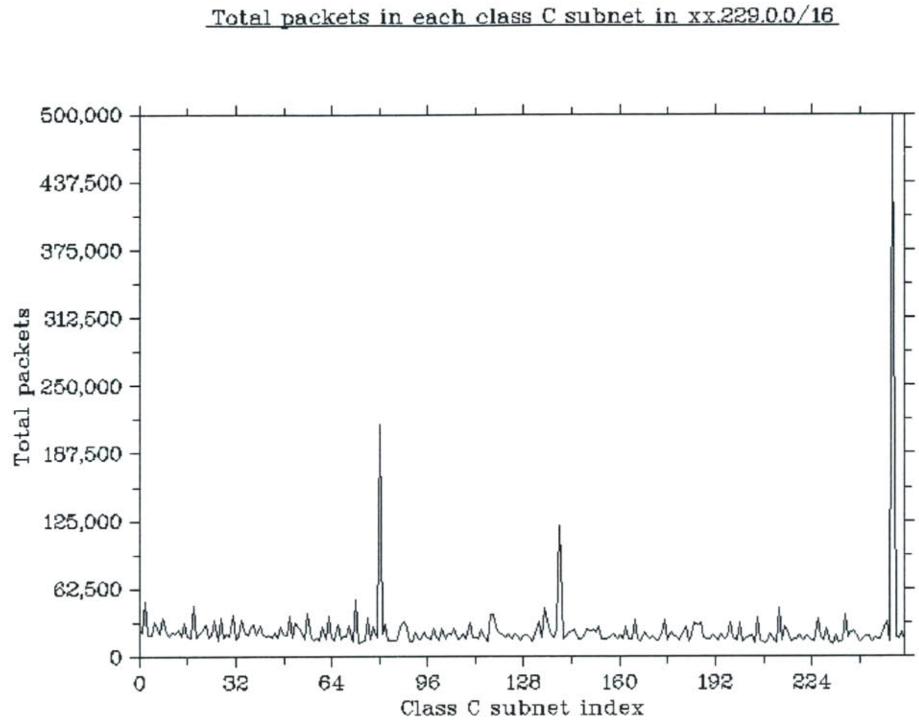

Figure A7-5 - Total packets in each class C subnet in 229B.

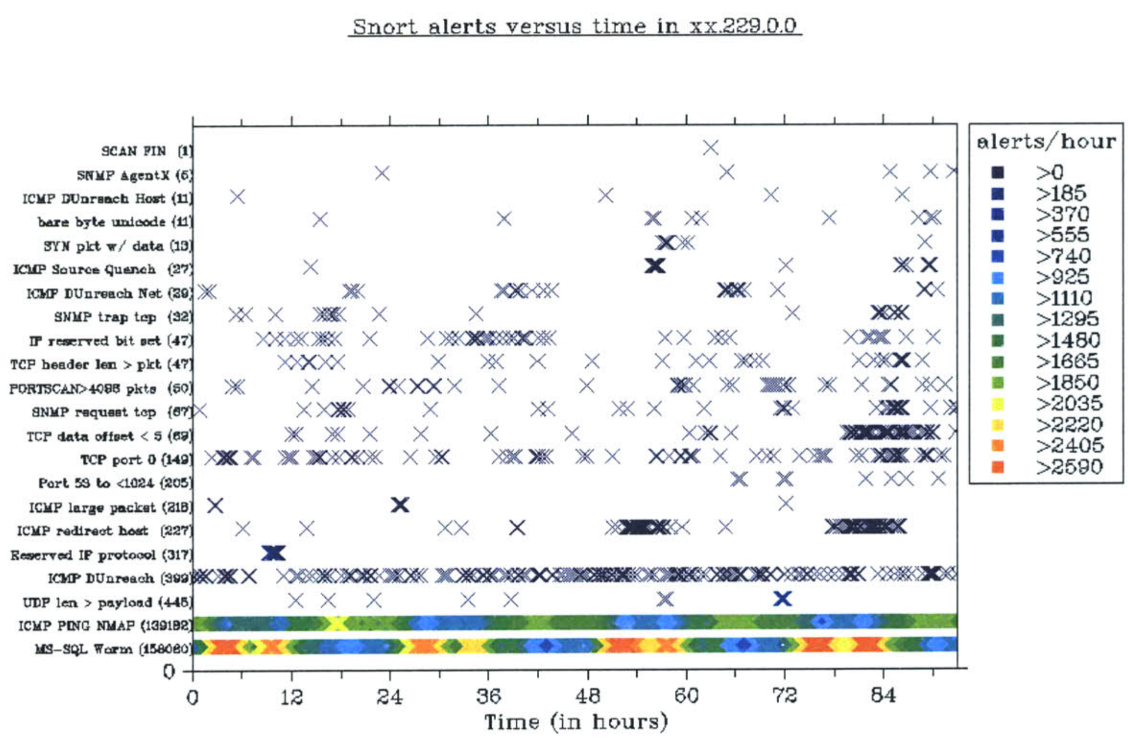

Figure A7-6 - Snort alerts versus time in 229B.

A.8 - XX.243.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	6,368,592	19	738	76.8	19.7	3.5
Bytes	391,935,243	1,171	40,888	60.0	38.1	1.9

Table A8-1 – Packet and byte statistics for 243B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	4,491,391	151,263	1,480	15,470	181,311	21

Table A8-2 – TCP packet types in 243B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	25	301K	752K (56)	48,984	383,538	17	1.0K	65,536	97	6.0K
90	X	X	X	16	120,112	48	3.0K	53,977	106	6.5K
50	X	X	X	3	1,343	2.4K	153K	16,329	195	11.1K

Table A8-3 – Statistics for all, the top90%, and the top 50% of traffic in 243B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,647,118	25.9	79,324,868	20.2
UDP – 137	1,077,621	16.9	84,054,438	21.5
TCP – 135	1,061,316	16.7	51,427,972	13.1

Table A8-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 243B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.243.174.77	93,871	1.5	4,535,629	1.2
xx.243.172.166	27,435	0.4	1,322,235	0.3
xx.243.246.65	27,422	0.4	1,321,513	0.3

Table A8-5 – Top 3 destination IPs across all packet types by packet count, in 243B.

IP Source	Packets	Packet %	Bytes	Byte %
211.243.194.82	689,308	10.8	33,086,784	8.4
83.129.66.115	119,435	1.9	6,210,620	1.6
61.35.241.4	66,429	1.0	3,188,592	0.8

Table A8-6 – Top 3 source IPs across all packet types by packet count, in 243B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	158,555	52.6
ICMP Ping NMAP	141,024	46.8
Short UDP Packet, Length Field > Payload Length	462	0.2

Table A8-7 – Top 3 alerts by alert count, in 243B.

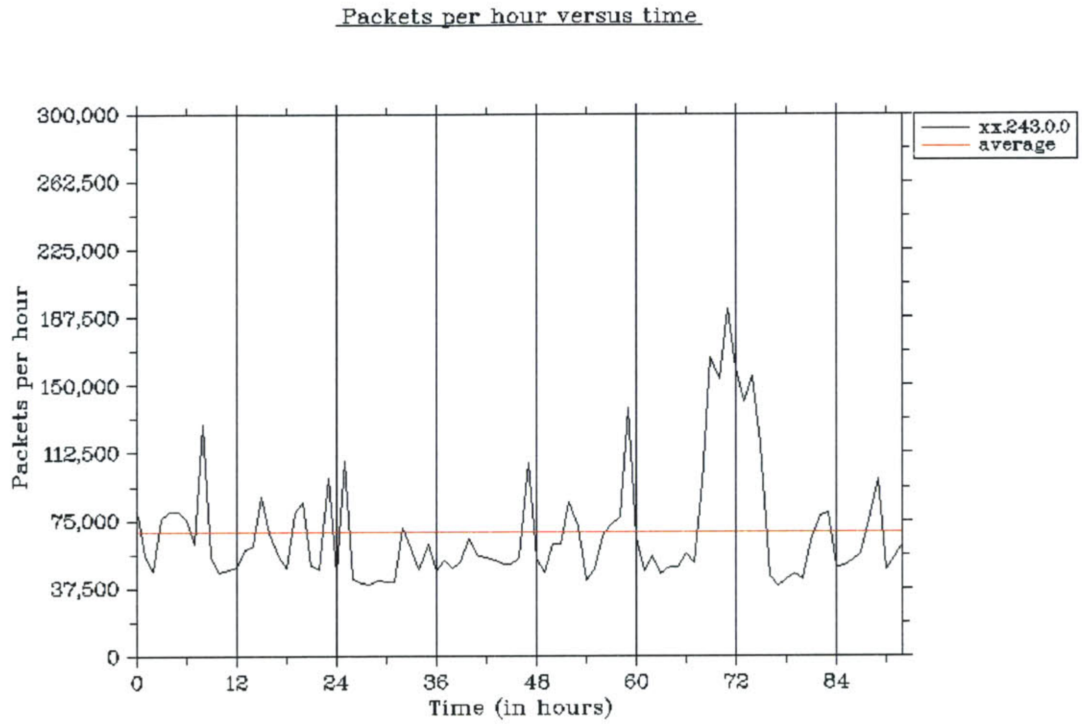

Figure A8-1 - Packets per hour versus time in 243B.

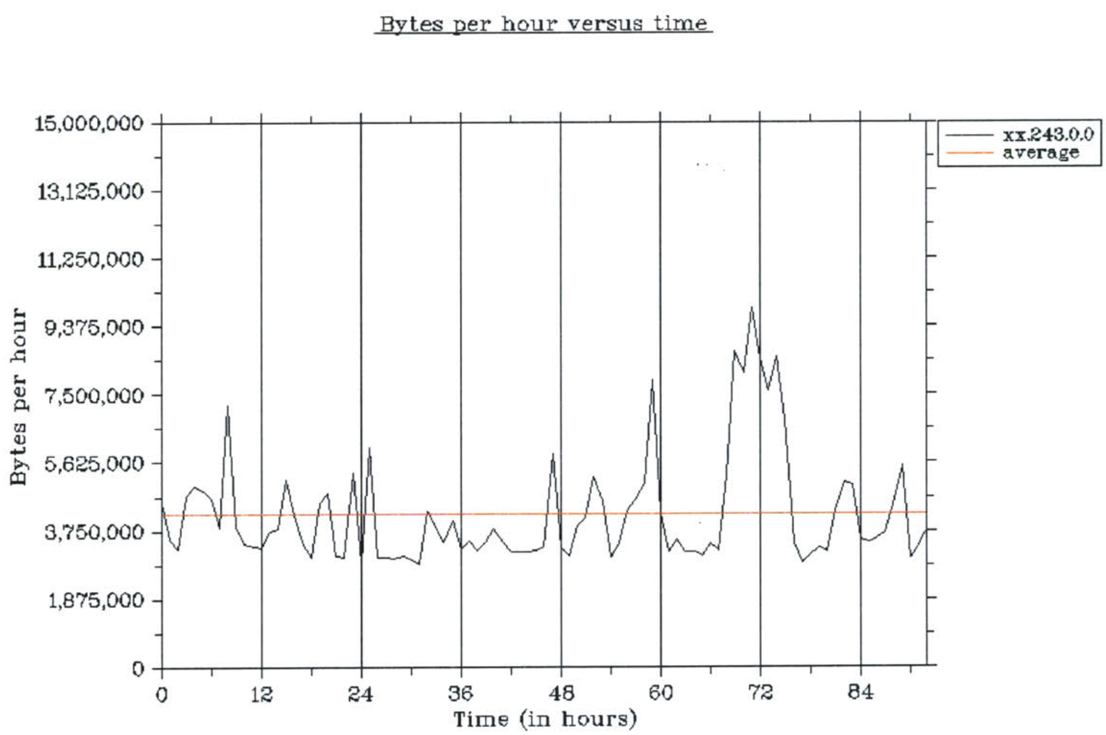

Figure A8-2 - Bytes per hour versus time in 243B.

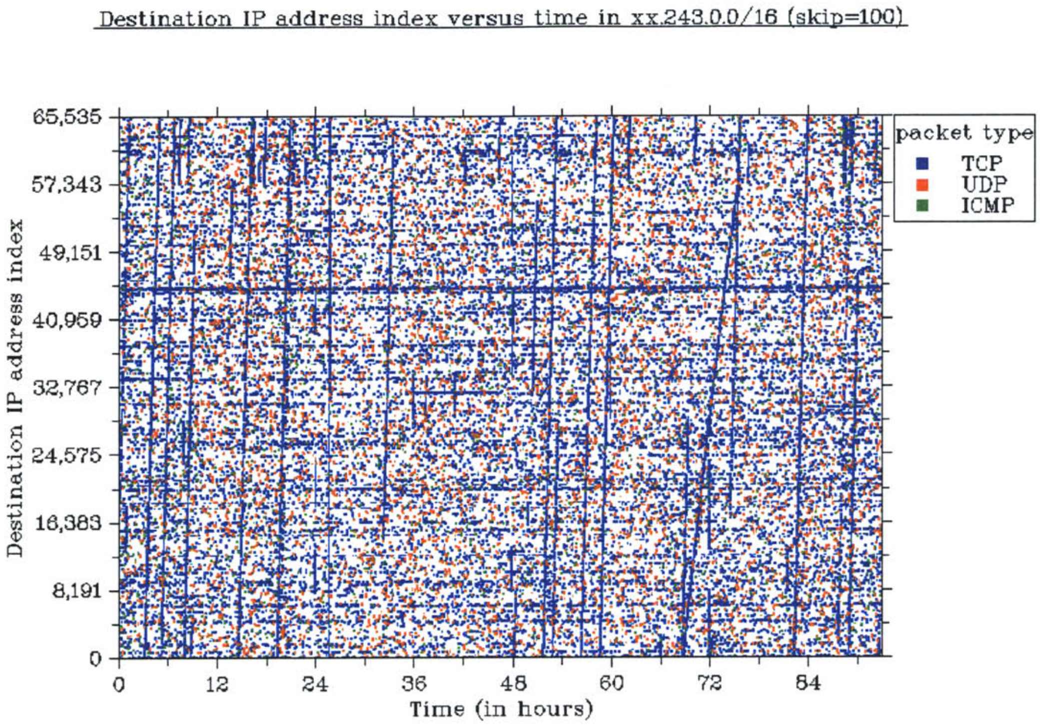

Figure A8-3 - Destination IP address index versus time in 243B.

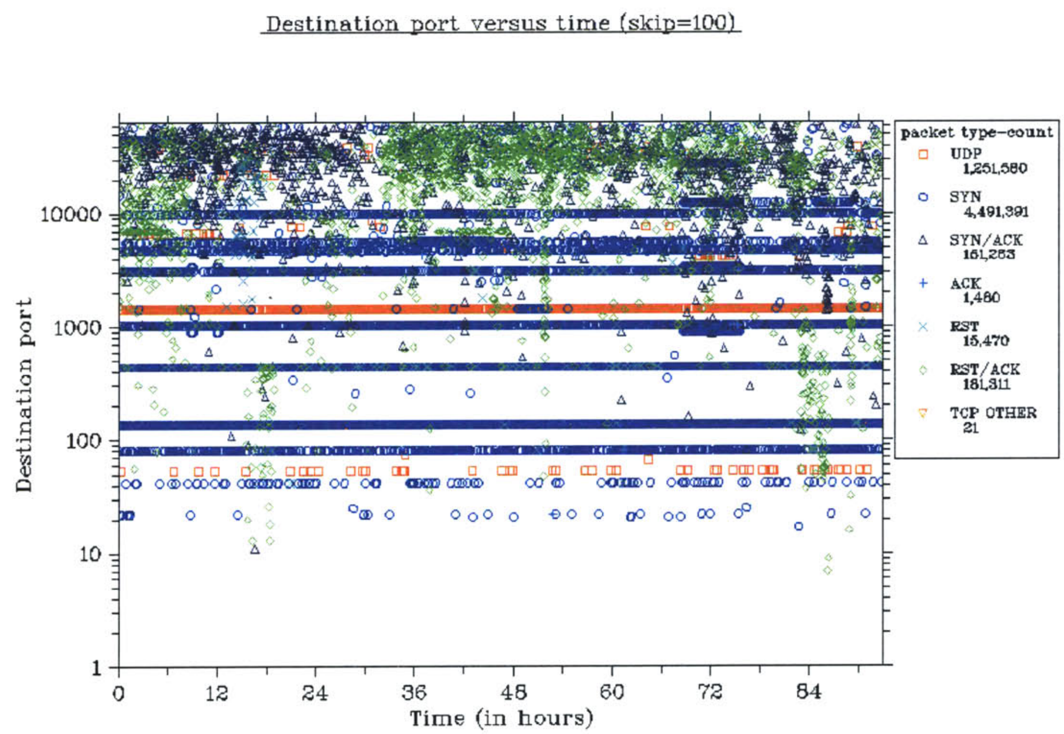

Figure A8-4 - Destination port versus time in 243B.

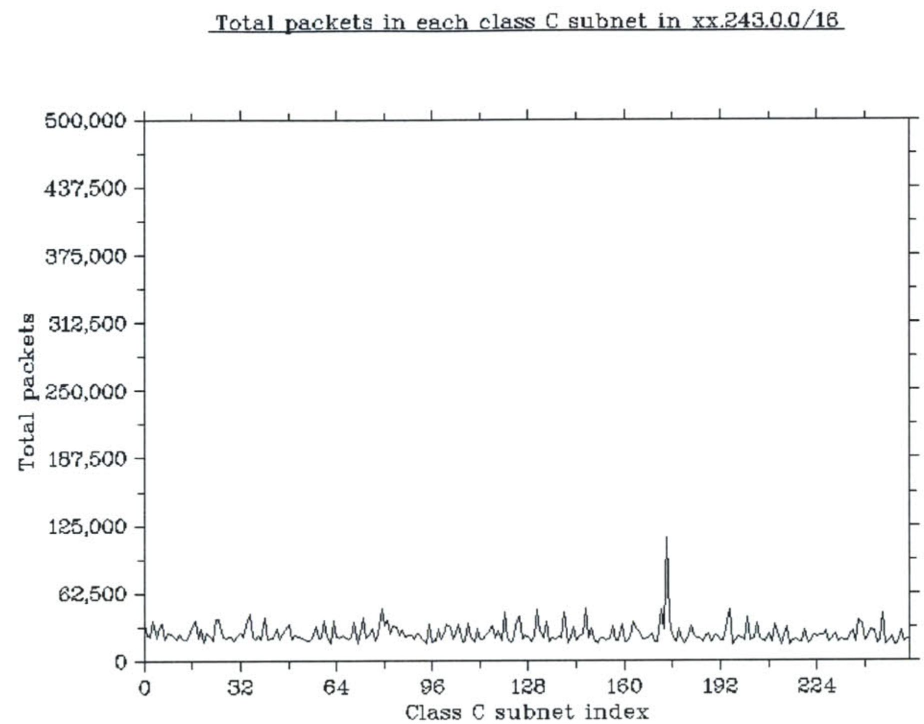

Figure A8-5 - Total packets in each class C subnet in 243B.

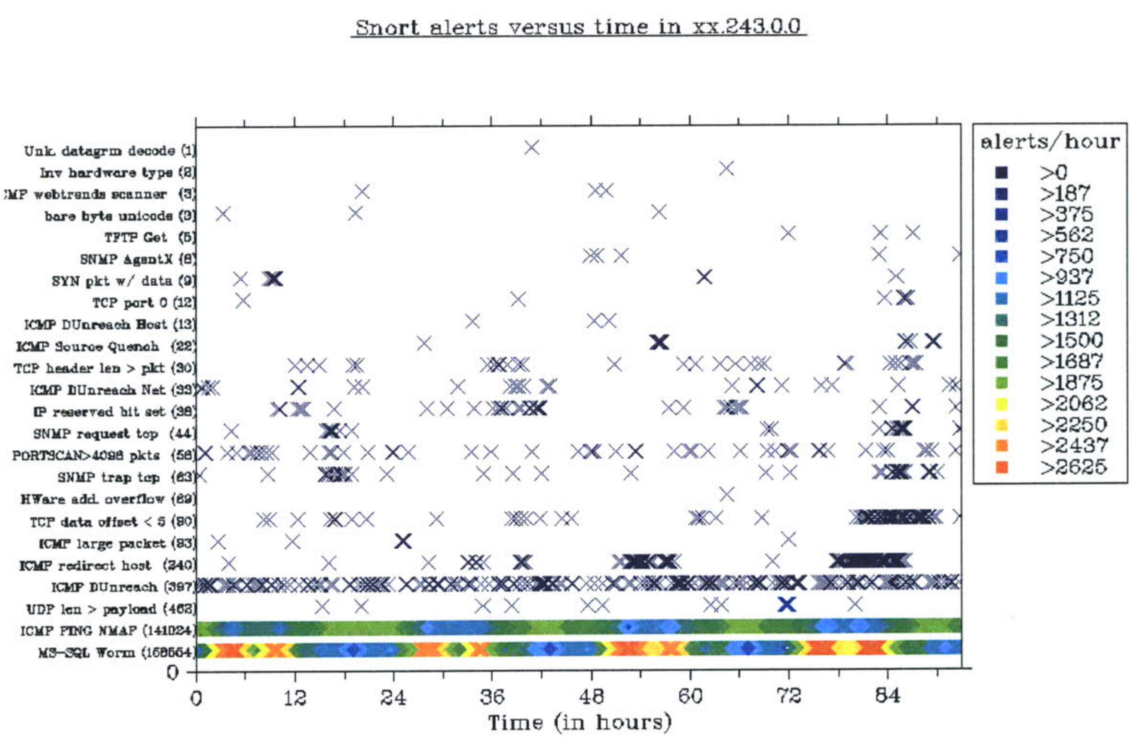

Figure A8-6 - Snort alerts versus time in 243B.

A.9 - XX.244.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	12,029,925	36	12,690	87.5	10.6	1.9
Bytes	626,345,354	1,871	508,750	74.7	24.1	1.2

Table A9-1 – Packet and byte statistics for 244B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	4,590,350	2,039,287	1,399	17,314	3,824,517	2,174

Table A9-2 – TCP packet types in 244B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	24	302K	972K (59)	53,087	397,024	30	1.6K	65,536	184	9.6K
90	X	X	X	18,326	48,597	223	11.7K	43,470	249	12.6K
50	X	X	X	21	35	172K	7.9M	6,634	907	41.6K

Table A9-3 – Statistics for all, the top 90%, and the top 50% of traffic in 244B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,793,459	14.9	86,361,152	13.8
UDP – 137	1,093,864	9.1	85,321,392	13.6
TCP – 135	1,088,412	9.1	52,728,327	8.4

Table A9-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 244B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.244.103.213	37,237	0.3	1,808,922	0.3
xx.244.214.245	36,960	0.3	1,785,738	0.3
xx.244.165.223	30,026	0.3	1,454,028	0.2

Table A9-5 – Top 3 destination IPs across all packet types by packet count, in 244B.

IP Source	Packets	Packet %	Bytes	Byte %
61.177.64.171	1,380,146	11.5	60,726,424	9.7
61.152.91.151	1,223,757	10.2	48,952,460	7.8
220.78.67.194	495,142	4.1	23,766,816	3.8

Table A9-6 – Top 3 source IPs across all packet types by packet count, in 244B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	157,742	52.2
ICMP Ping NMAP	142,389	47.1
ICMP Destination Unreachable Communication Administratively Prohibited	511	0.2

Table A9-7 – Top 3 alerts by alert count, in 244B.

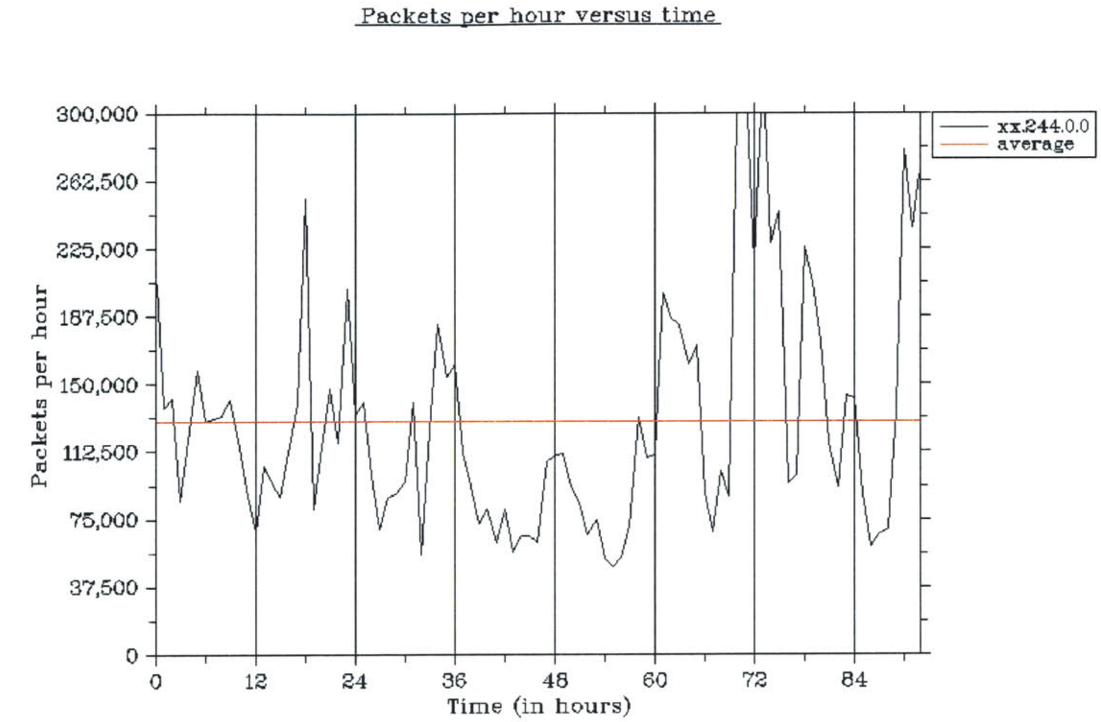

Figure A9-1 - Packets per hour versus time in 244B.

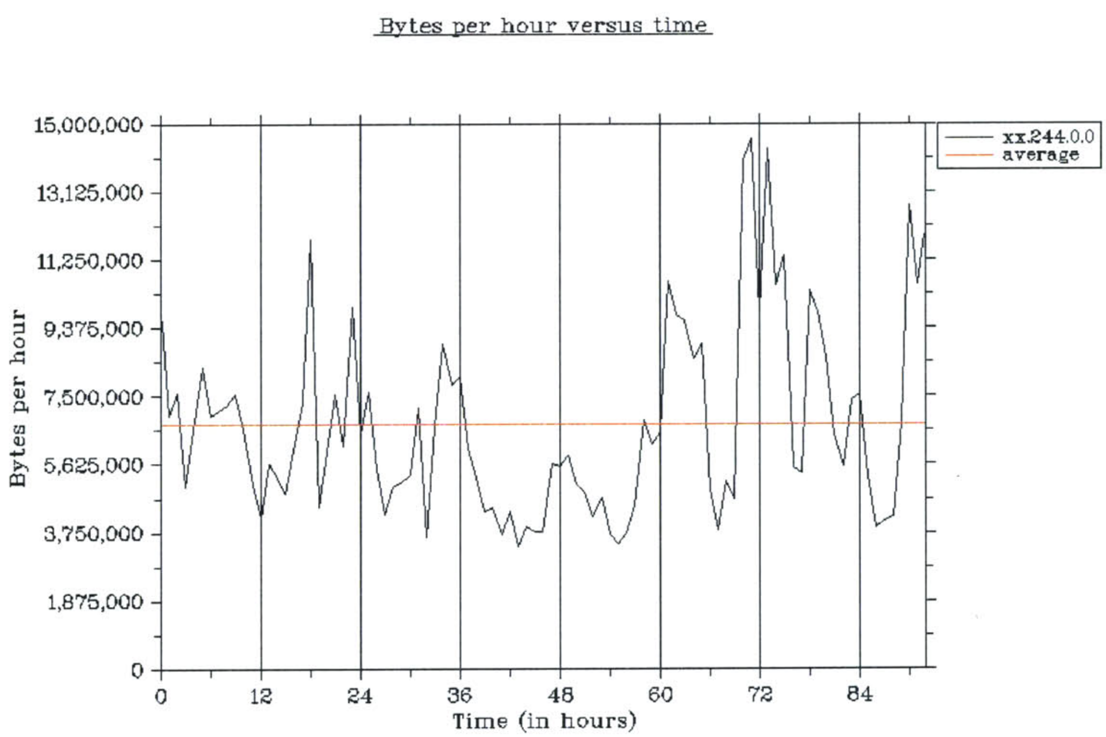

Figure A9-2 - Bytes per hour versus time in 244B.

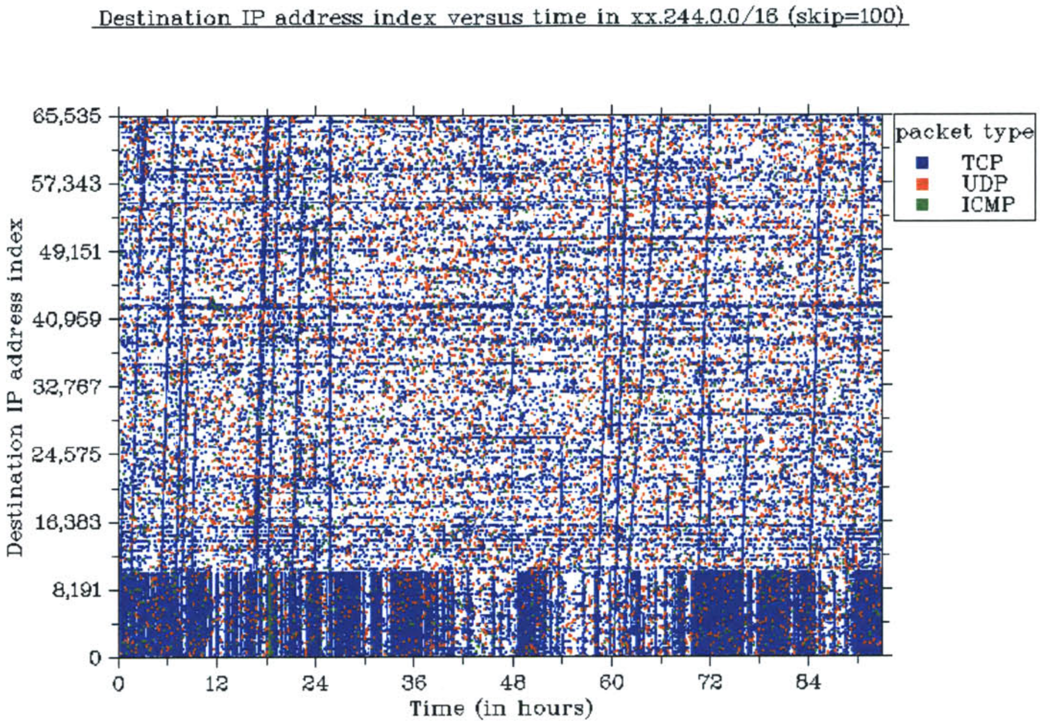

Figure A9-3 - Destination IP address index versus time in 244B.

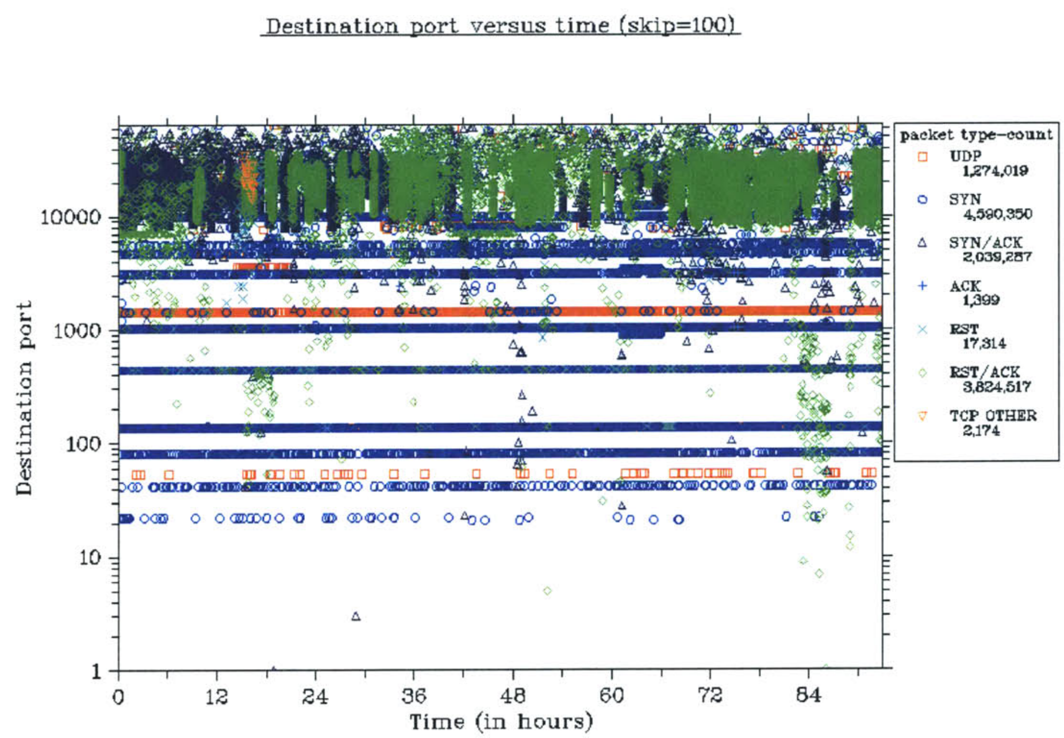

Figure A9-4 - Destination port versus time in 244B.

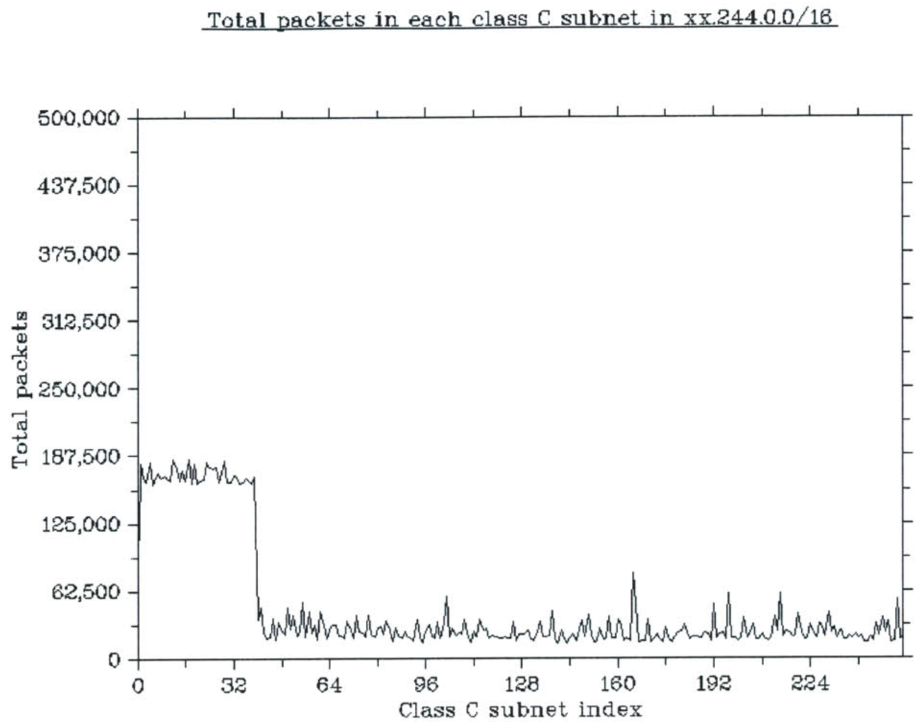

Figure A9-5 - Total packets in each class C subnet in 244B.

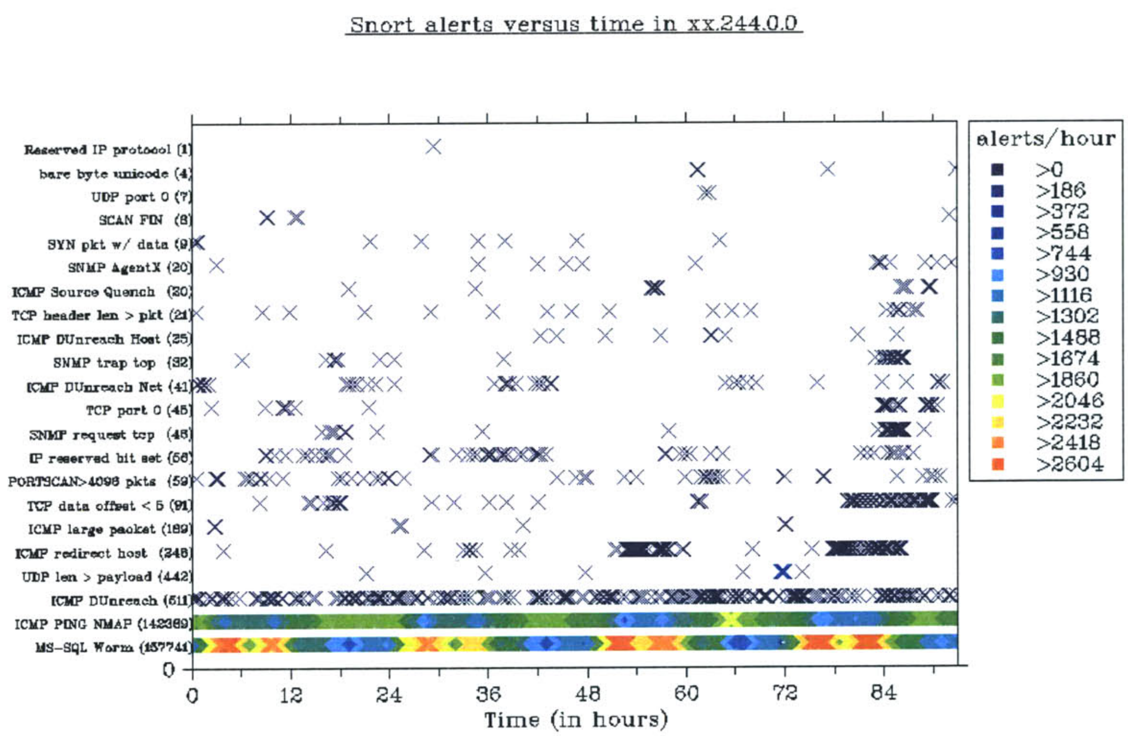

Figure A9-6 - Snort alerts versus time in 244B.

A.10 - XX.248.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	7,216,170	22	3,300	79.0	17.8	3.2
Bytes	435,681,460	1,301	145,000	63.3	34.8	1.9

Table A10-1 – Packet and byte statistics for 248B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	5,279,886	157,363	2,250	25,100	185,049	208

Table A10-2 – TCP packet types in 248B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 4K pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	25	295K	637K (51)	49,015	455,334	16	957	65,536	110	6.6K
90	X	X	X	16	161,093	40	2.5K	51,670	126	7.5K
50	X	X	X	3	3,845	938	62.8K	7,989	452	23.5K

Table A10-3 – Statistics for all, the top 90%, and the top 50% of traffic in 248B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,782,117	24.7	85,820,186	19.7
TCP – 135	1,168,738	16.2	56,572,837	13.0
UDP – 137	1,112,147	15.4	86,747,466	19.9

Table A10-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 248B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.248.246.112	692,920	9.6	33,349,840	7.7
xx.248.134.58	283,109	3.9	13,671,411	3.1
xx.248.18.222	80,480	1.1	3,882,780	0.9

Table A10-5 – Top 3 destination IPs across all packet types by packet count, in 248B.

IP Source	Packets	Packet %	Bytes	Byte %
220.87.74.65	471,795	6.5	24,533,340	5.6
83.129.66.115	114,492	1.6	5,953,584	1.4
68.72.89.180	60,719	0.8	2,914,512	0.7

Table A10-6 – Top 3 source IPs across all packet types by packet count, in 248B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	157,516	53.4
ICMP Ping NMAP	135,307	45.8
Short UDP Packet, Length Field > Payload Length	446	0.2

Table A10-7 – Top 3 alerts by alert count, in 248B.

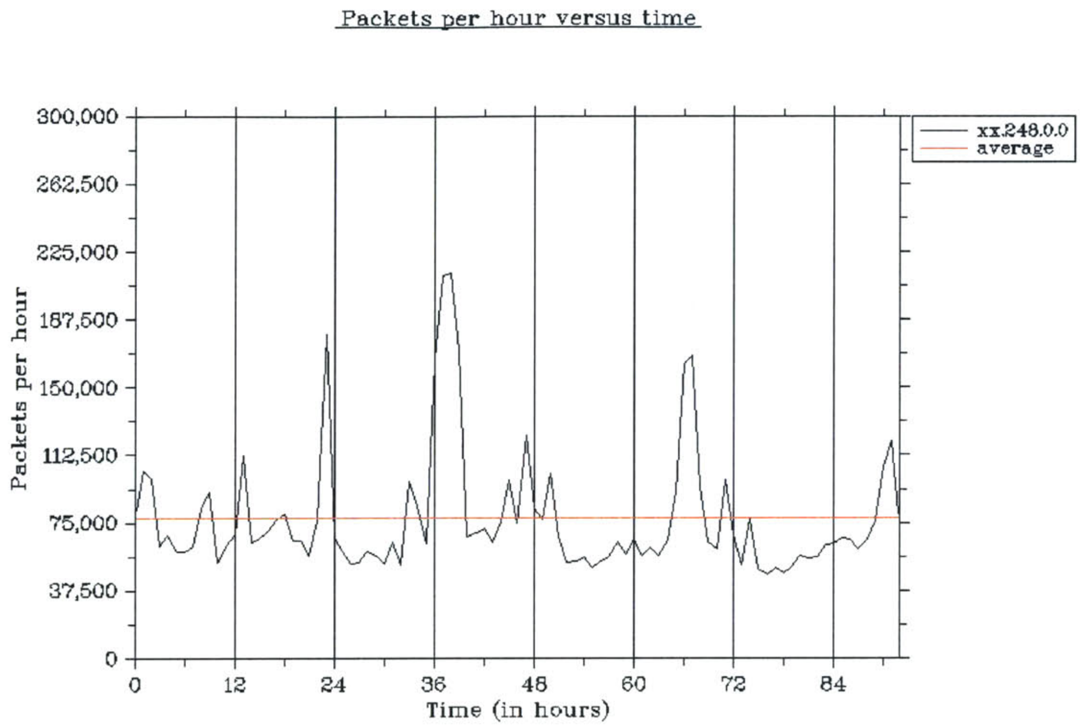

Figure A10-1 - Packets per hour versus time in 248B.

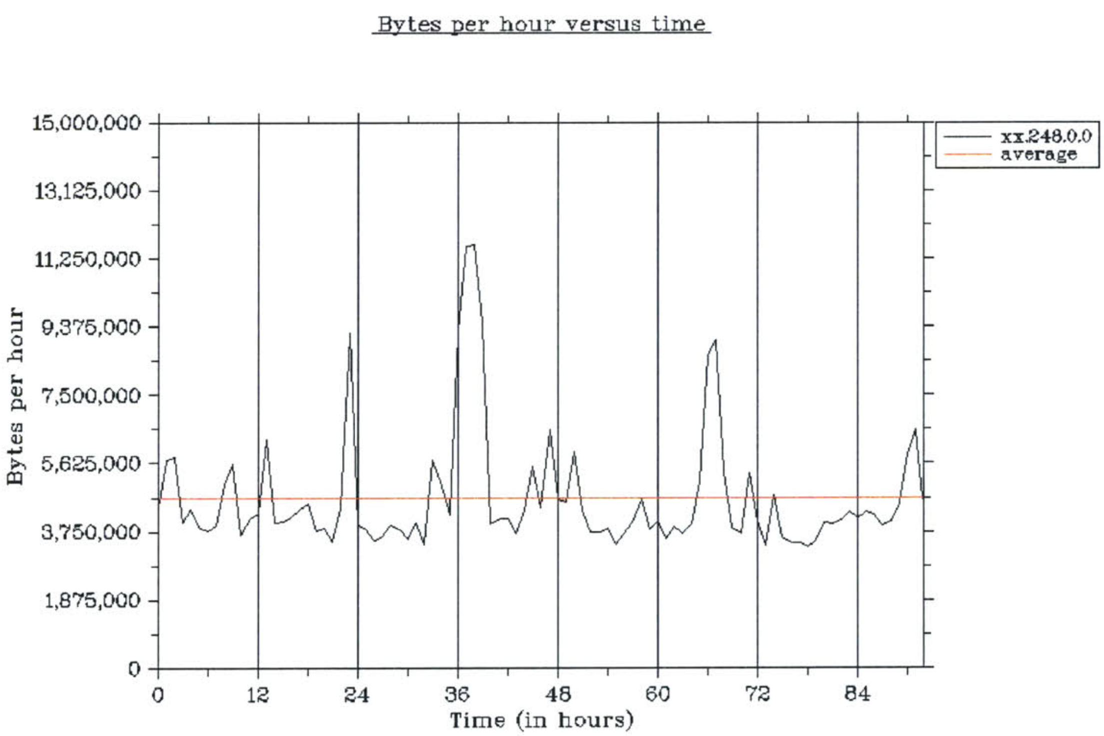

Figure A10-2 - Bytes per hour versus time in 248B.

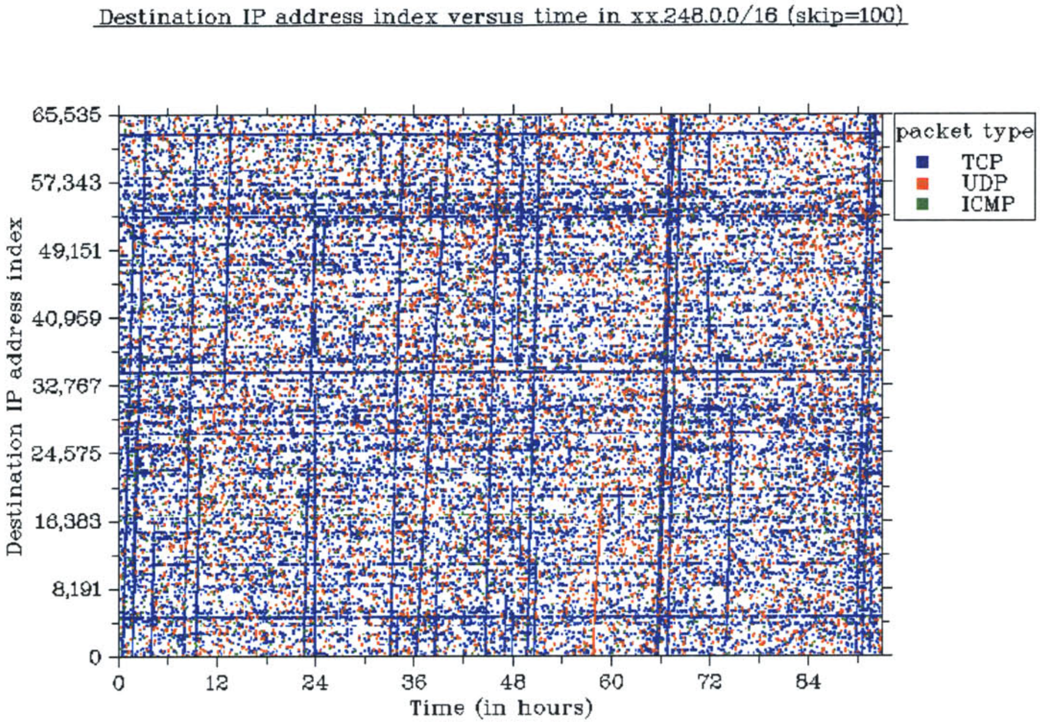

Figure A10-3 - Destination IP address index versus time in 248B.

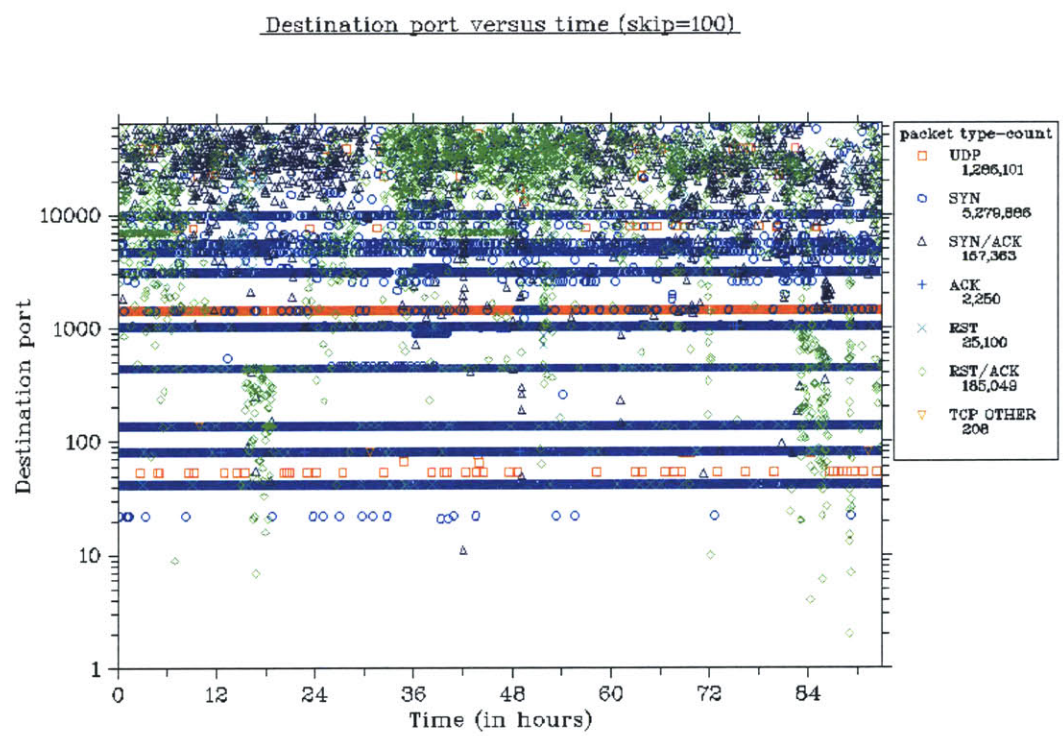

Figure A10-4 - Destination port versus time in 248B.

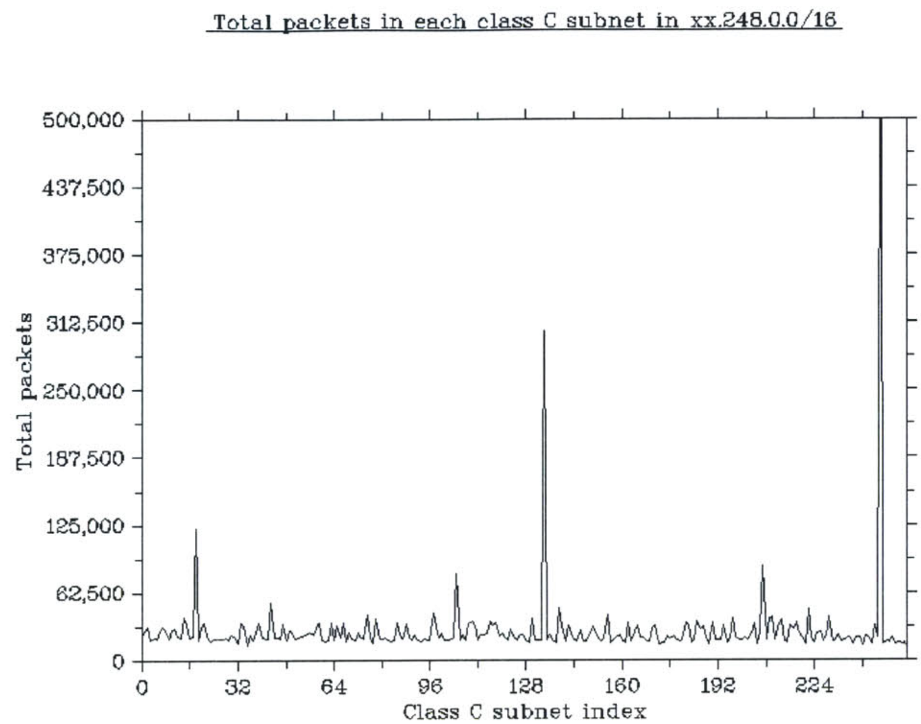

Figure A10-5 - Total packets in each class C subnet in 248B.

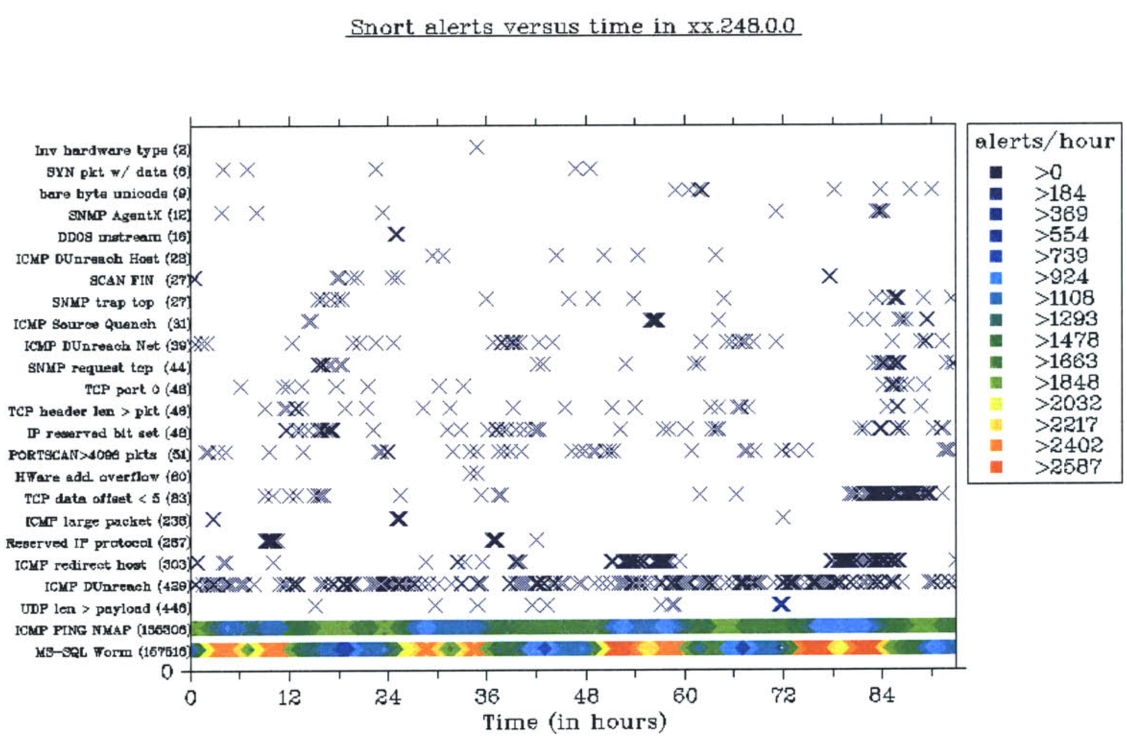

Figure A10-6 - Snort alerts versus time in 248B.

A.11 - XX.251.0.0/16

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	5,548,817	17	1,350	73.0	23.1	3.9
Bytes	352,415,753	1,052	64,653	55.1	42.8	2.1

Table A11-1 – Packet and byte statistics for 251B.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	3,651,252	149,694	1,322	15,063	180,622	67

Table A11-2 – TCP packet types in 251B.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 4K pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	25	297K	591K (43)	49,015	383,100	14	920	65,536	85	5.4K
90	X	X	X	12	139,494	36	2.3K	52,630	95	6.0K
50	X	X	X	2	3,214	863	61.4K	12,538	221	12.4K

Table A11-3 – Statistics for all, the top 90%, and the top 50% of traffic in 251B.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	1,673,220	30.2	80,599,136	22.9
UDP – 137	1,106,091	19.9	86,275,098	24.5
TCP – 135	846,056	15.3	41,066,937	11.7

Table A11-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 251B.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.251.72.243	95,372	1.7	4,608,147	1.3
xx.251.5.1	39,036	0.7	1,886,030	0.5
xx.251.200.186	23,973	0.4	1,155,027	0.3

Table A11-5 – Top 3 destination IPs across all packet types by packet count, in 251B.

IP Source	Packets	Packet %	Bytes	Byte %
217.94.211.66	114,762	2.1	5,508,576	1.6
83.129.64.175	111,785	2.0	5,812,820	1.7
61.153.17.25	106,688	1.9	4,694,272	1.3

Table A11-6 – Top 3 source IPs across all packet types by packet count, in 251B.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	157,331	53.0
ICMP Ping NMAP	137,691	46.4
ICMP Destination Unreachable Communication Administratively Prohibited	397	0.1

Table A11-7 – Top 3 alerts by alert count, in 251B.

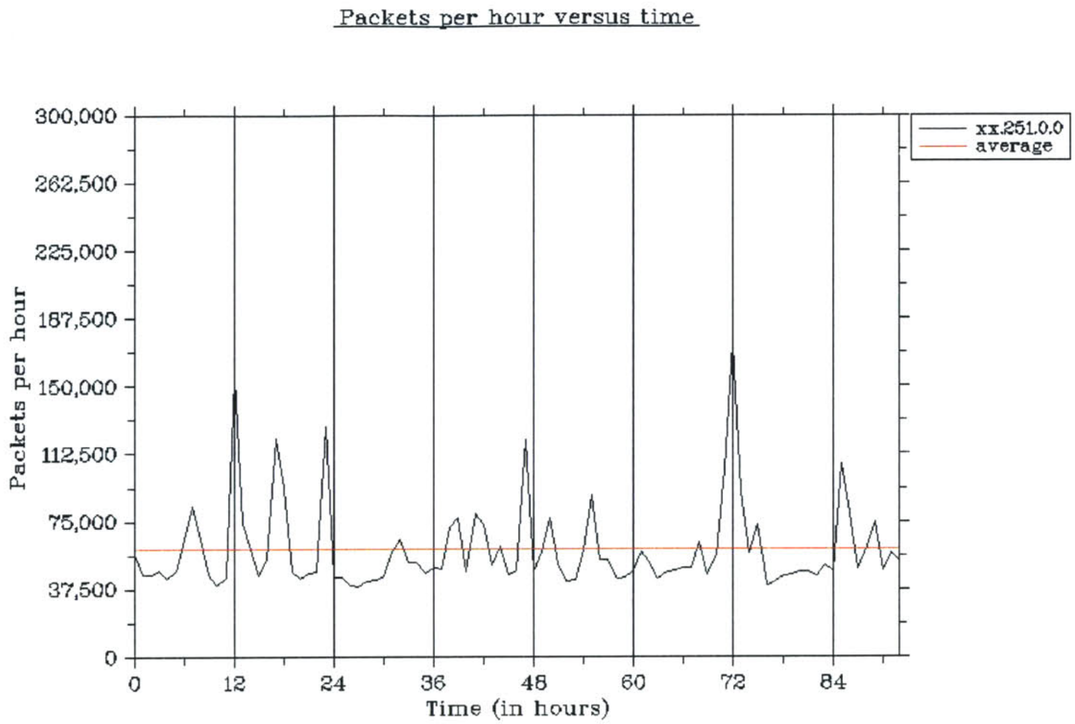

Figure A11-1 - Packets per hour versus time in 251B.

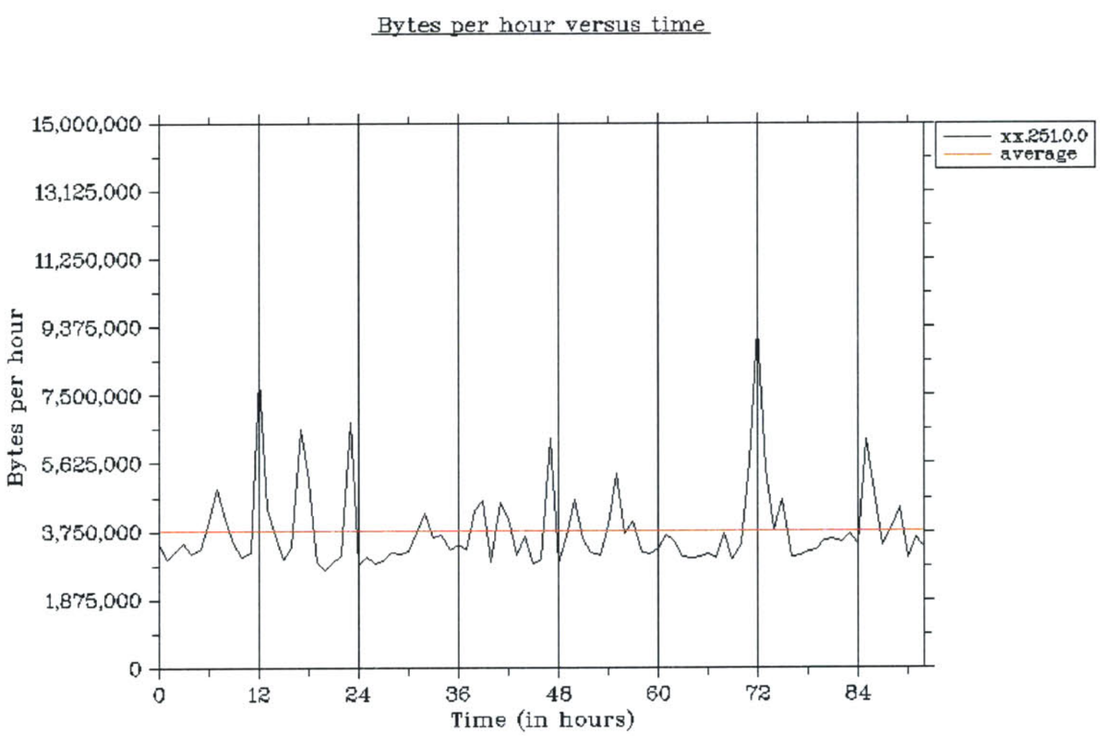

Figure A11-2 - Bytes per hour versus time in 251B.

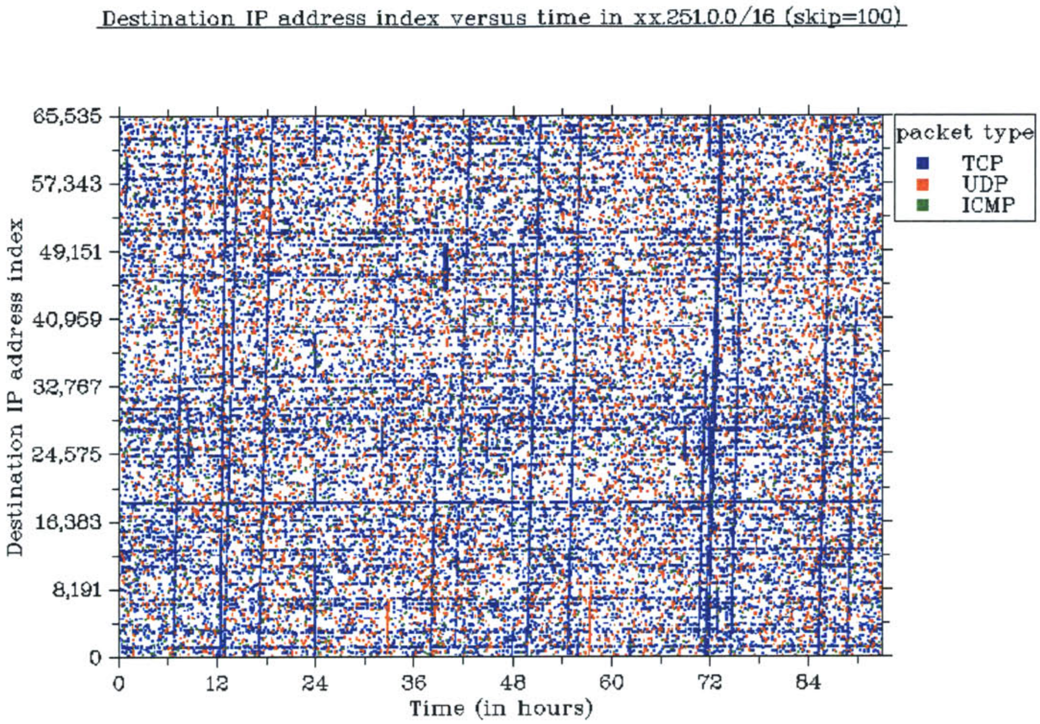

Figure A11-3 - Destination IP address index versus time in 251B.

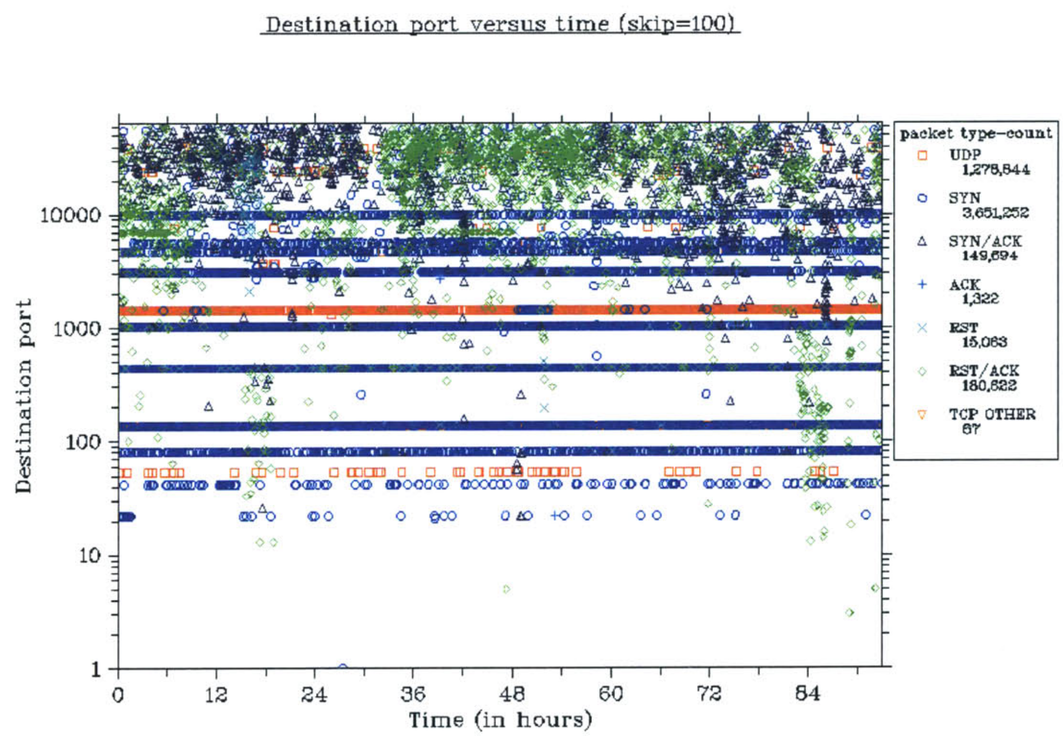

Figure A11-4 - Destination port versus time in 251B.

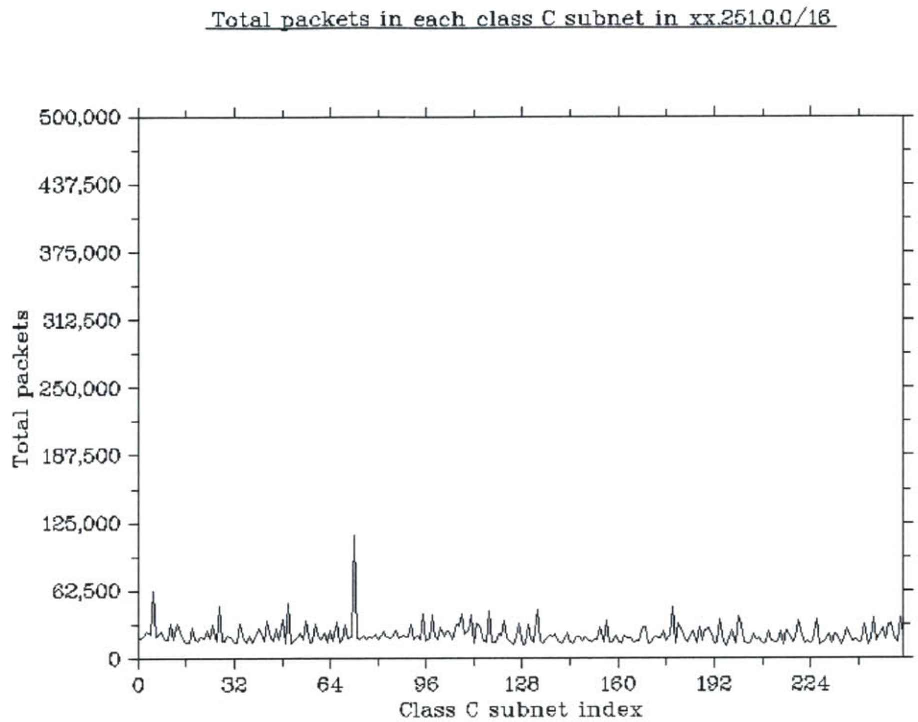

Figure A11-5 - Total packets in each class C subnet in 251B.

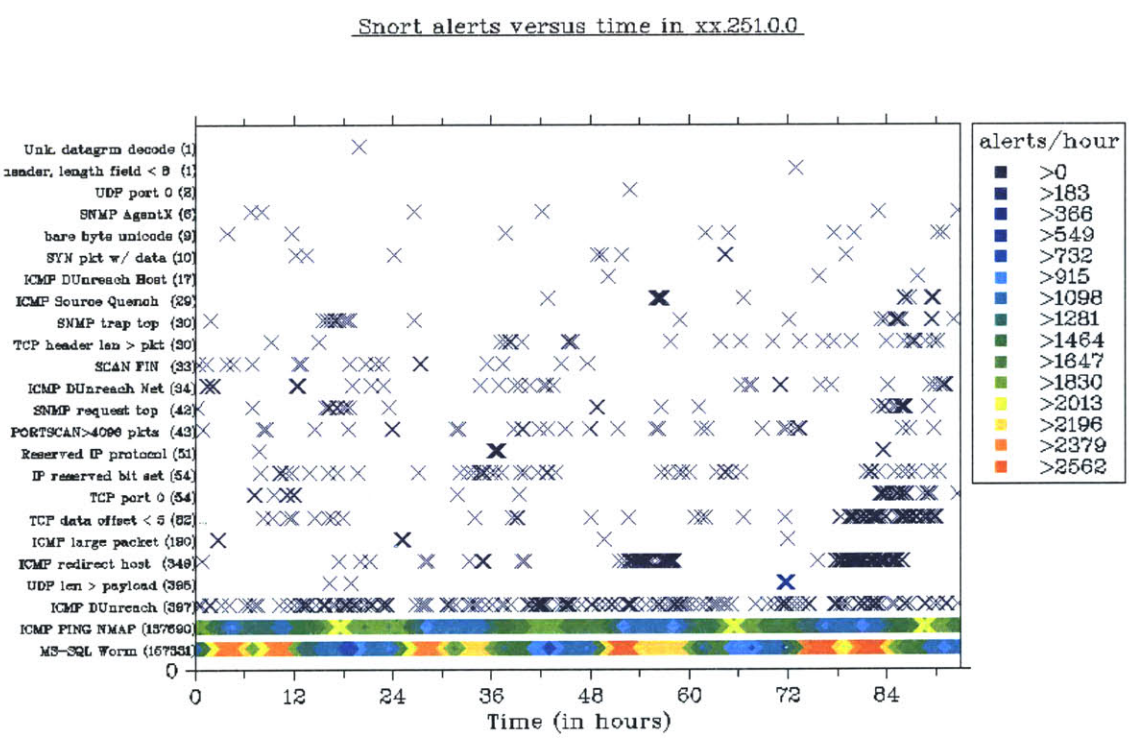

Figure A11-6 - Snort alerts versus time in 251B.

Appendix B:

Tables and Plots for Class C Subnets

B.1 - XX.55.145.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	23,037	0.07	254	76.3	20.8	2.9
Bytes	1,415,624	4.6	51,283	58.2	40.2	1.6

Table B1-1 – Packet and byte statistics for 55.145C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	11,869	3,588	27	32	1,845	0

Table B1-2 – TCP packet types in 55.145C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	6	963	7.5K (30)	681	1,870	12	757	256	90	5.5K
90	X	X	X	147	512	41	2.6K	220	94	5.8K
50	X	X	X	4	38	308	18.8K	97	119	7.1K

Table B1-3 – Statistics for all, the top 90%, and the top 50% of traffic in 55.145C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 135	5,078	22.0	243,752	17.2
UDP – 137	4,146	18.0	323,388	22.8
TCP – 445	1,724	7.5	83,044	5.9

Table B1-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 55.145C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.55.145.202	871	3.8	43,144	3.1
xx.55.145.143	211	0.9	13,592	2.7
xx.55.145.44	206	0.9	10,266	2.5

Table B1-5 – Top 3 destination IPs across all packet types by packet count, in 55.145C.

IP Source	Packets	Packet %	Bytes	Byte %
61.152.241.175	970	4.2	42,696	3.0
61.234.250.206	890	3.9	38,692	2.7
211.219.84.18	722	3.1	34,656	2.5

Table B1-6 – Top 3 source IPs across all packet types by packet count, in 55.145C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	602	62.5
ICMP Ping NMAP	327	34.0
Portscan > 16 Packets	30	3.1

Table B1-7 – Top 3 alerts by alert count, in 55.145C.

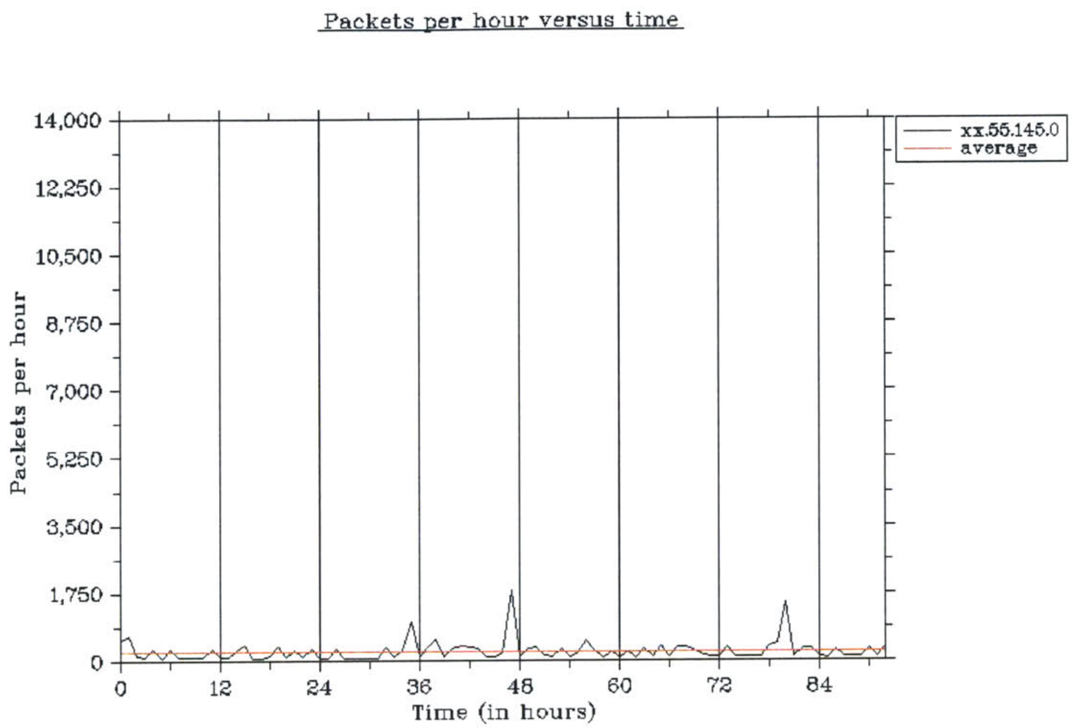

Figure B1-1 - Packets per hour versus time in 55.145C.

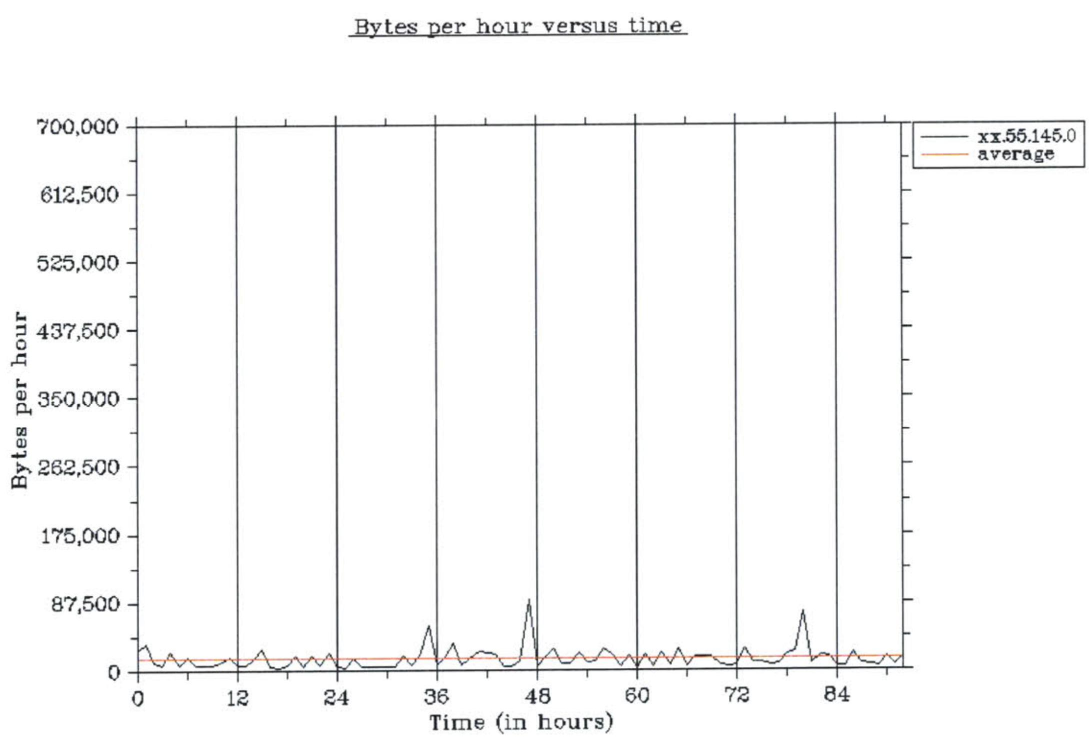

Figure B1-2 - Bytes per hour versus time in 55.145C.

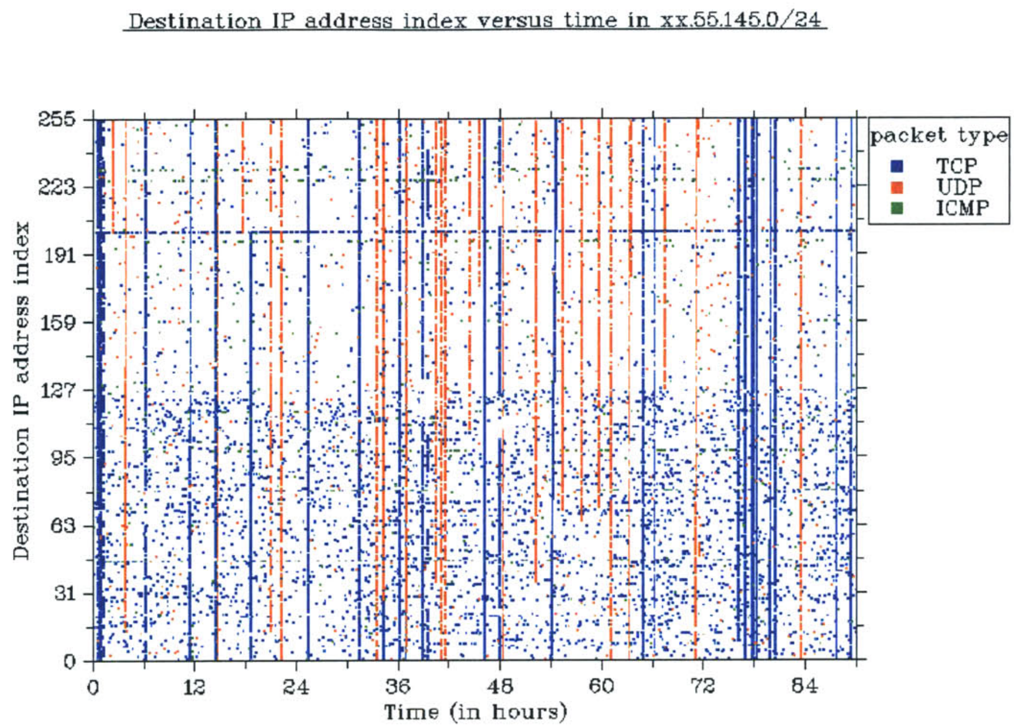

Figure B1-3 - Destination IP address index versus time in 55.145C.

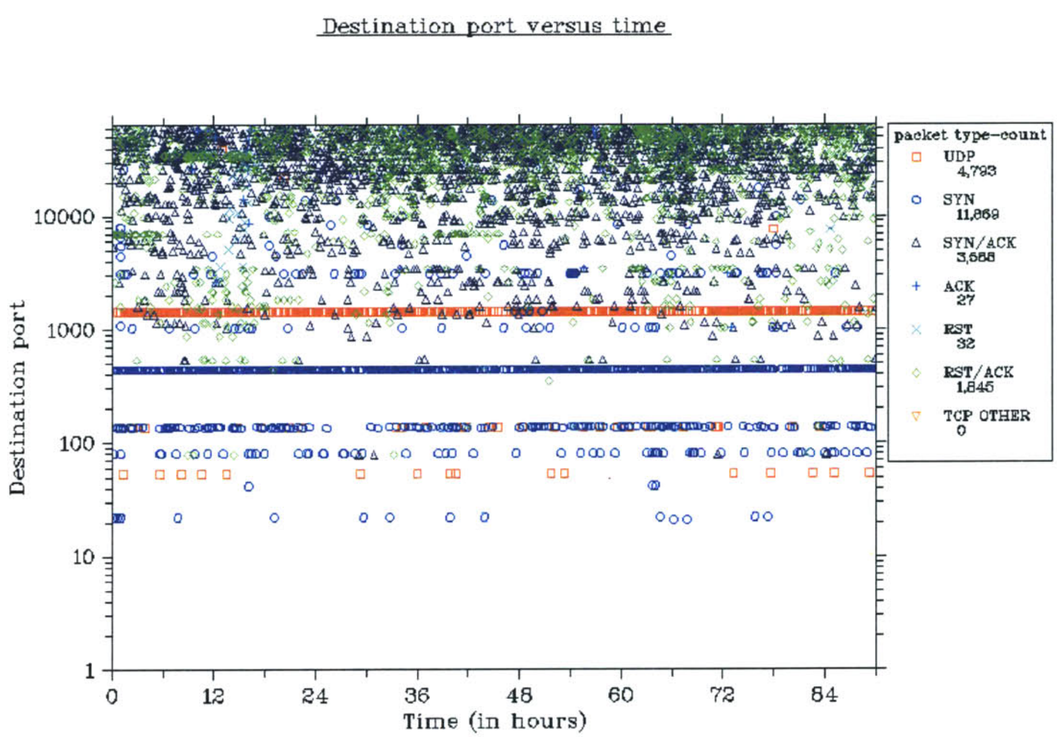

Figure B1-4 - Destination port versus time in 55.145C.

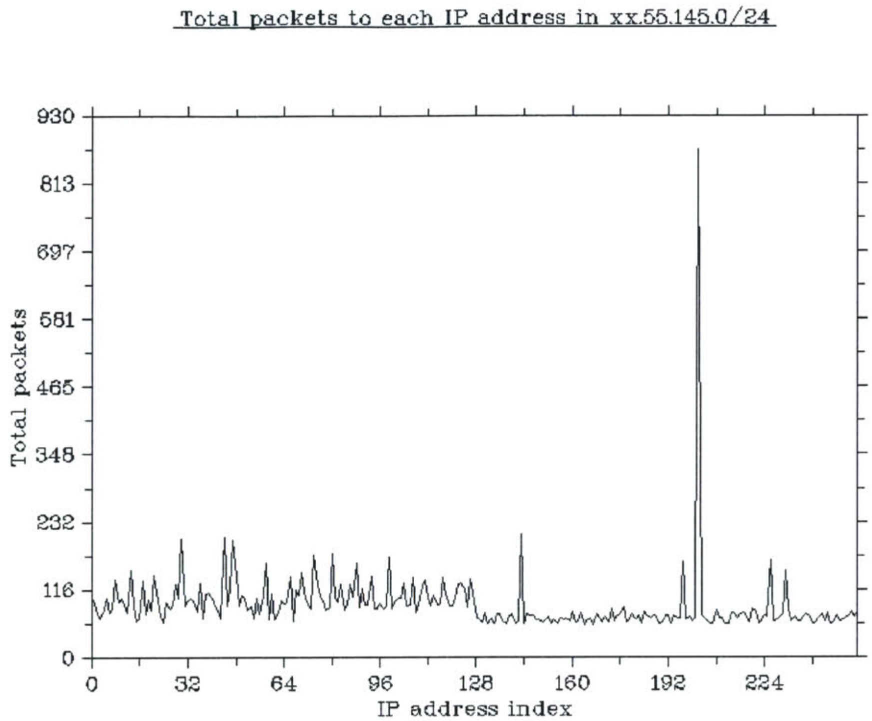

Figure B1-5 - Total packets to each IP address in 55.145C.

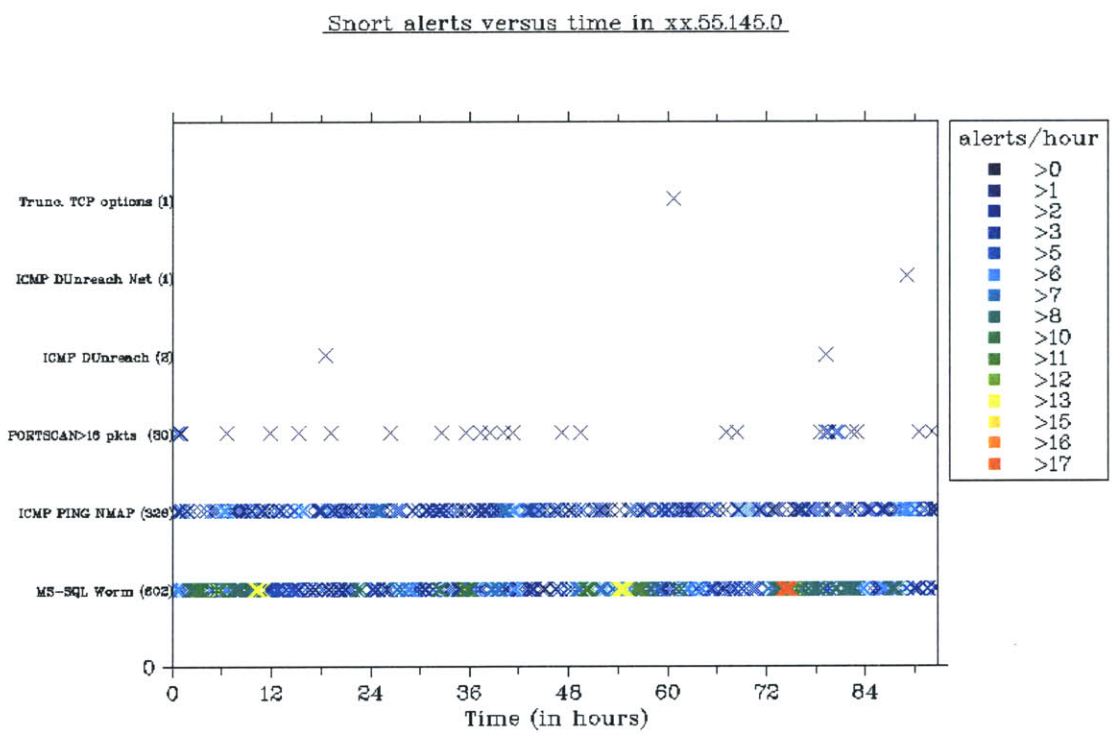

Figure B1-6 - Snort alerts versus time in 55.145C.

B.2 - XX.128.8.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	858,412	2.7	1,050	1.2	98.6	0.2
Bytes	136,753,757	426	278,750	0.4	99.5	0.1

Table B2-1 – Packet and byte statistics for 128.8C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	8,175	791	13	272	967	0

Table B2-2 – TCP packet types in 128.8C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	7	2,907	4.5K (20)	985	2,437	352	56.1K	256	3.4K	534K
90	X	X	X	1	84	9.2K	1.5M	1	840K	135M
50	X	X	X	1	25	18.6K	3.5M	1	840K	135M

Table B2-3 – Statistics for all, the top 90%, and the top 50% of traffic in 128.8C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
UDP – 1037	839,327	97.8	135,382,959	99.0
UDP – 137	5,599	0.7	436,722	0.3
TCP – 135	3,859	0.5	183,444	0.1

Table B2-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 128.8C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.128.8.14	840,247	97.9	135,479,180	99.1
xx.128.8.82	848	0.10	41,468	0.03
xx.128.8.33	350	0.04	19,942	0.01

Table B2-5 – Top 3 destination IPs across all packet types by packet count, in 128.8C.

IP Source	Packets	Packet %	Bytes	Byte %
192.12.94.30	58,592	6.8	2,368,412	1.7
192.55.83.30	42,695	5.0	1,828,498	1.3
192.42.93.30	39,887	4.7	1,629,782	1.2

Table B2-6 – Top 3 source IPs across all packet types by packet count, in 128.8C.

Alert Name	Alert Count	Alert %
Short UDP Packet, Length Field > Payload Length	1,602	55.1
MS-SQL Worm Propagation Attempt	630	21.7
ICMP Ping NMAP	584	20.1

Table B2-7 – Top 3 alerts by alert count, in 128.8C.

Packets per hour versus time

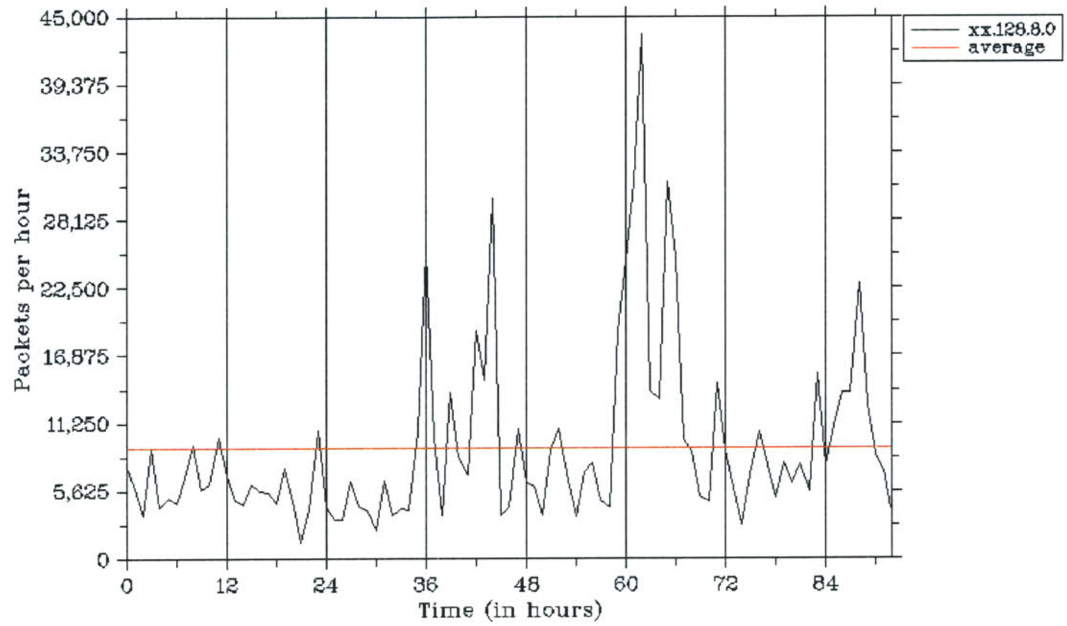

Figure B2-1 - Packets per hour versus time in 128.8C.

Bytes per hour versus time

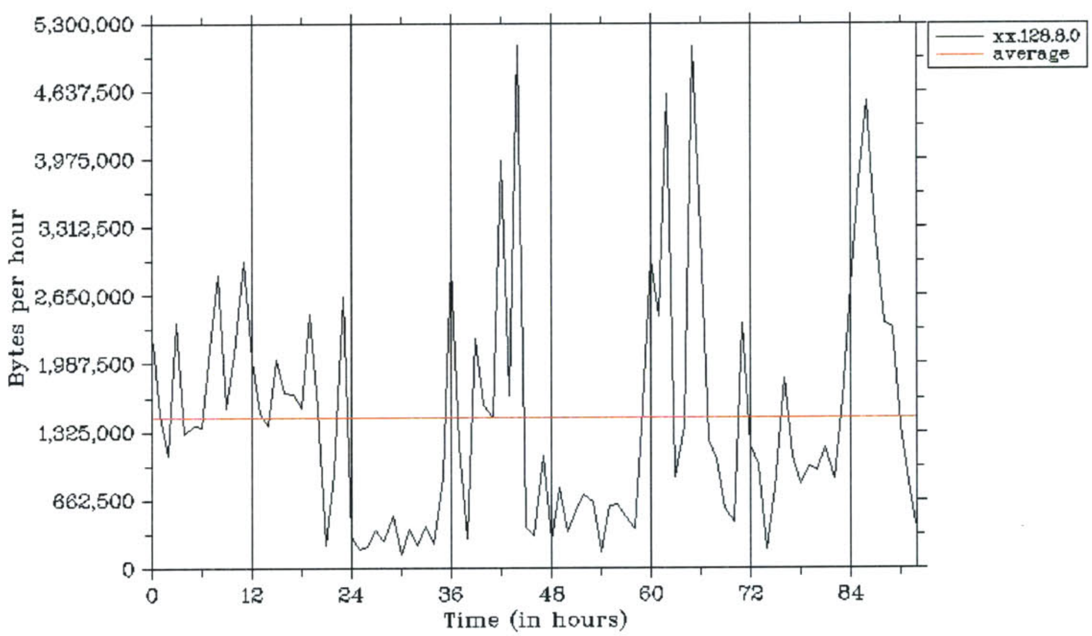

Figure B2-2 - Bytes per hour versus time in 128.8C.

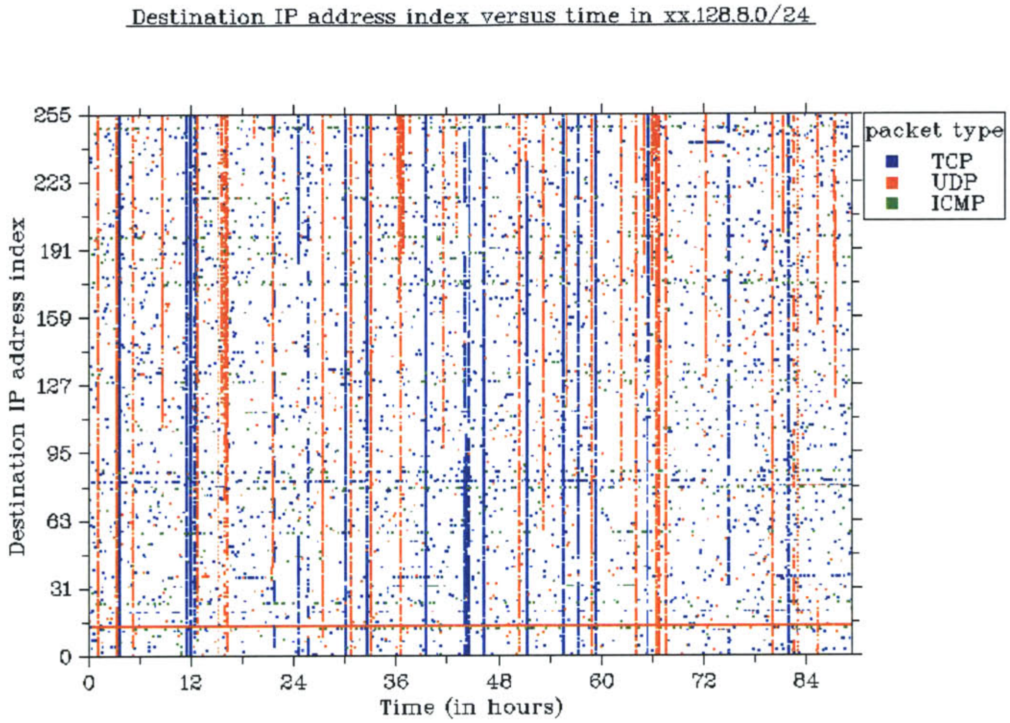

Figure B2-3 - Destination IP address index versus time in 128.8C.

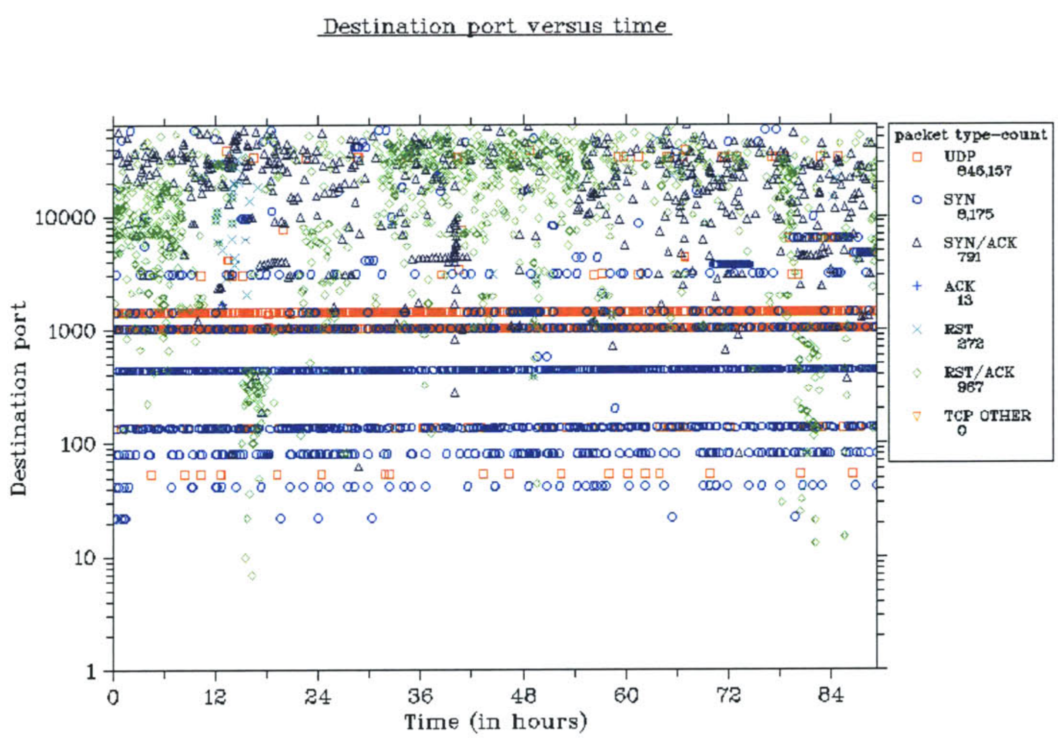

Figure B2-4 - Destination port versus time in 128.8C.

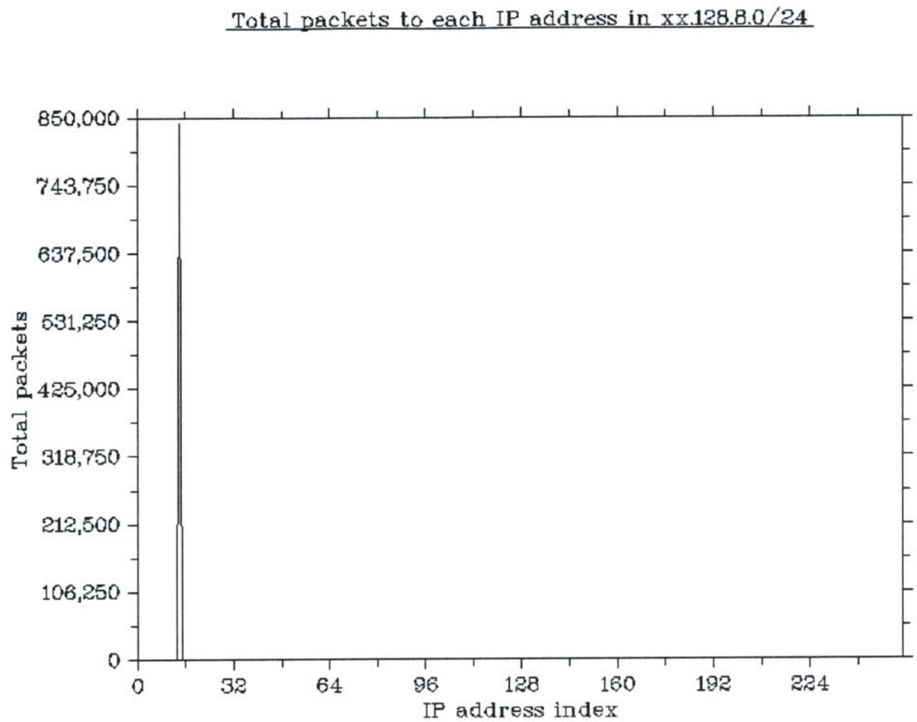

Figure B2-5 - Total packets to each IP address in 128.8C.

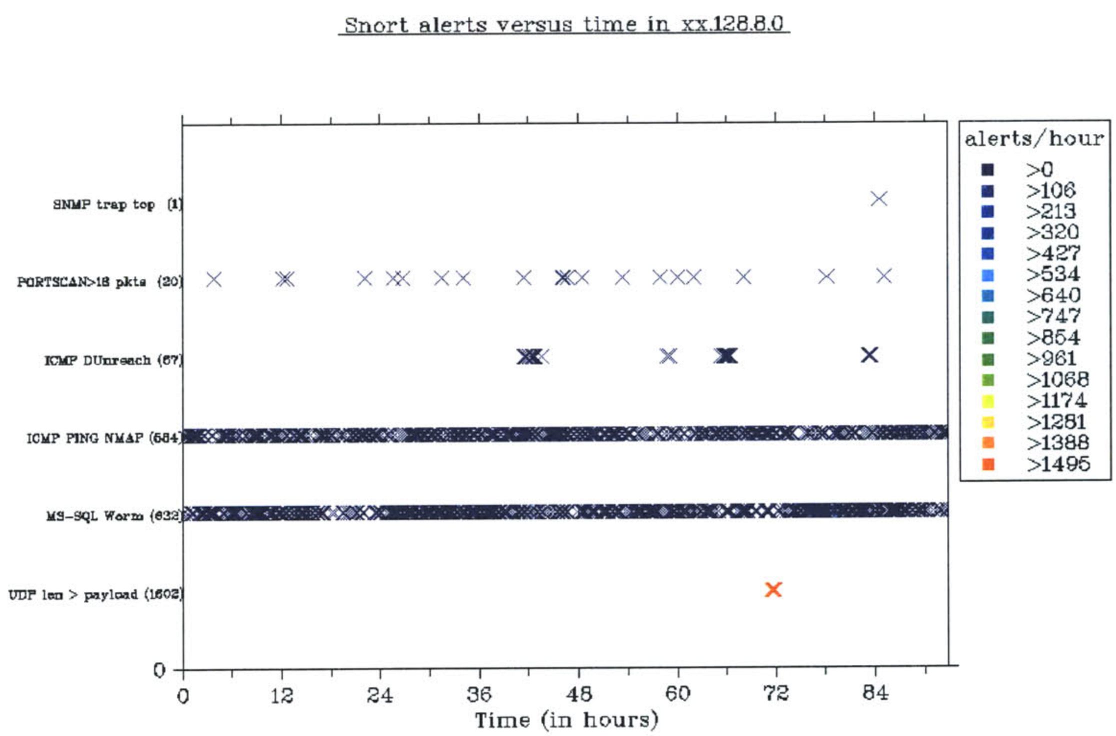

Figure B2-6 - Snort alerts versus time in 128.8C.

B.3 - XX.198.188.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	584,973	1.8	353	98.0	1.1	0.9
Bytes	24,797,791	74	16,896	95.9	2.8	1.3

Table B3-1 – Packet and byte statistics for 198.188C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	39,605	138,992	1,852	208	392,590	17

Table B3-2 – TCP packet types in 198.188C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	9	941	6.8K (22)	13,323	8,672	67	2.9K	256	2.3K	96.9K
90	X	X	X	8,196	59	8.9K	368K	1	537K	22M
50	X	X	X	2,339	6	49.3K	2.0M	1	537K	22M

Table B3-3 – Statistics for all, the top 90%, and the top 50% of traffic in 198.188C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 445	16,871	2.9	812,605	3.3
UDP – 137	5,780	1.0	450,840	1.8
ICMP – Destination Unreachable	4,500	0.8	305,967	1.2

Table B3-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 198.188C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.198.188.220	537,113	91.8	22,108,578	89.2
xx.198.188.96	16,798	2.9	811,838	3.3
xx.198.188.6	14,961	2.6	722,049	2.9

Table B3-5 – Top 3 destination IPs across all packet types by packet count, in 198.188C.

IP Source	Packets	Packet %	Bytes	Byte %
61.152.108.4	106,312	18.2	4,254,316	17.2
210.245.191.90	61,258	10.5	2,450,332	9.9
61.129.70.220	47,611	8.1	1,938,756	7.8

Table B3-6 – Top 3 source IPs across all packet types by packet count, in 198.188C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	624	66.3
ICMP Ping NMAP	229	24.3
TCP Port 0 Traffic	30	3.2

Table B3-7 – Top 3 alerts by alert count, in 198.188C.

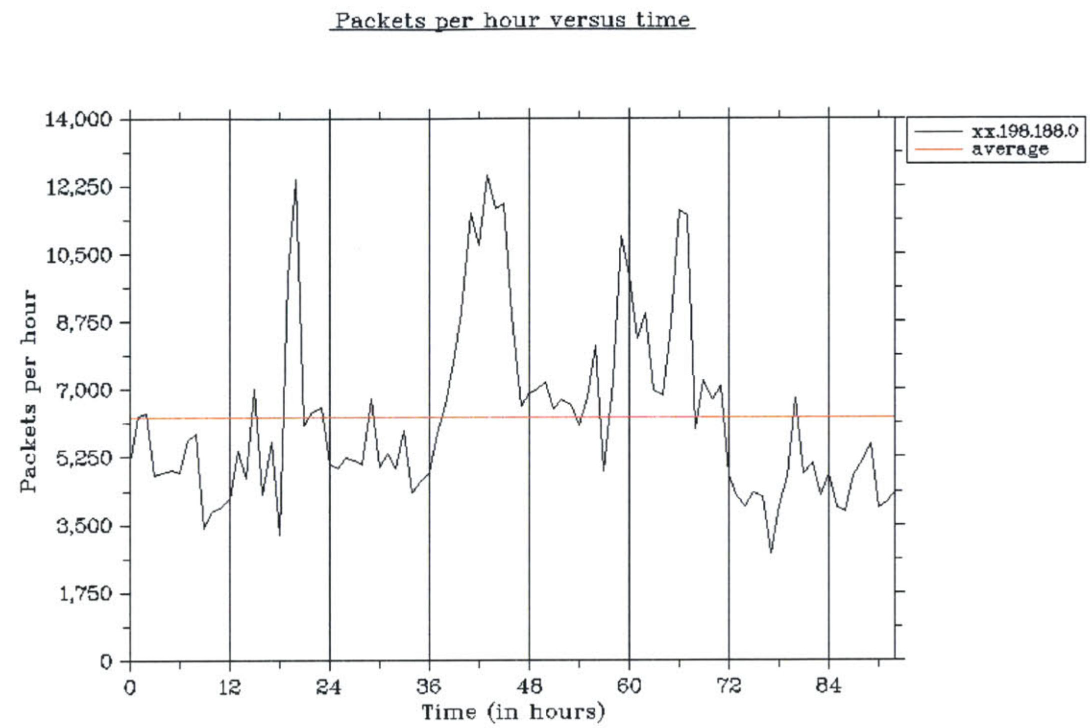

Figure B3-1 - Packets per hour versus time in 198.188C.

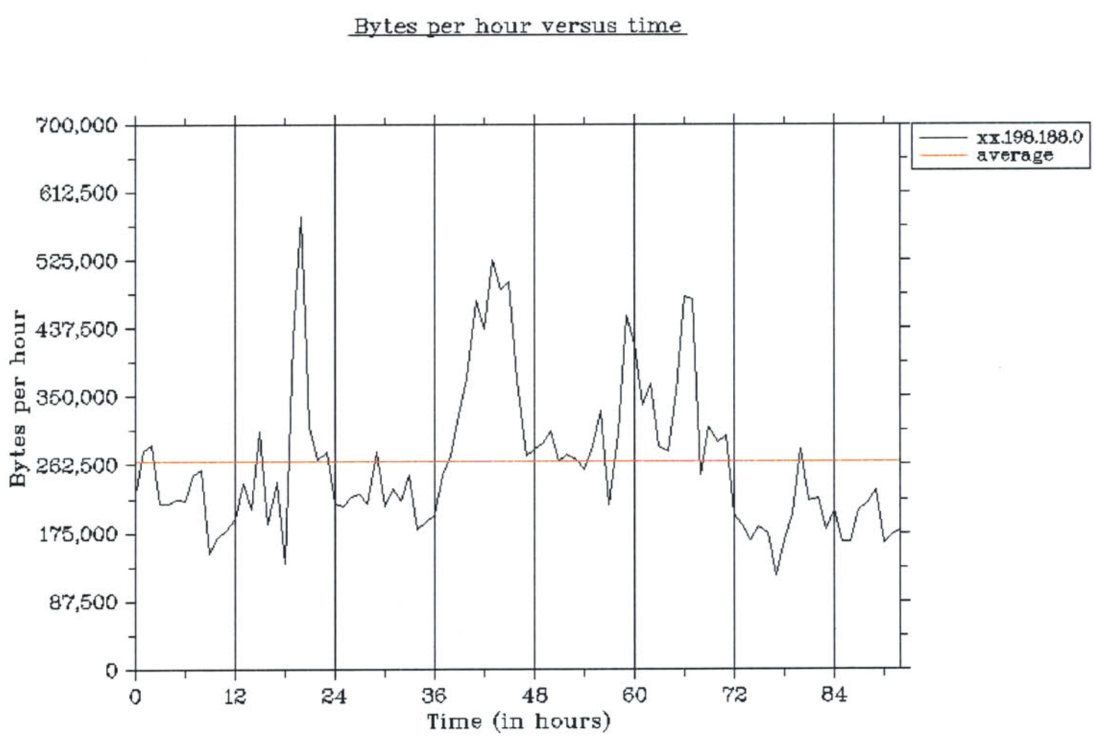

Figure B3-2 - Bytes per hour versus time in 198.188C.

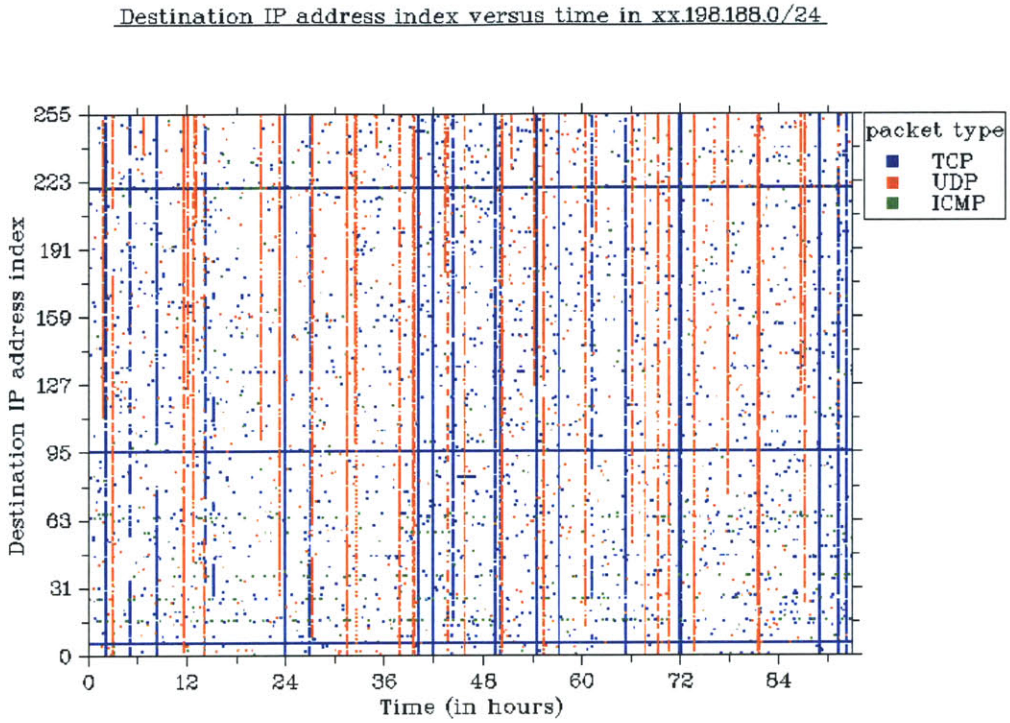

Figure B3-3 - Destination IP address index versus time in 198.188C.

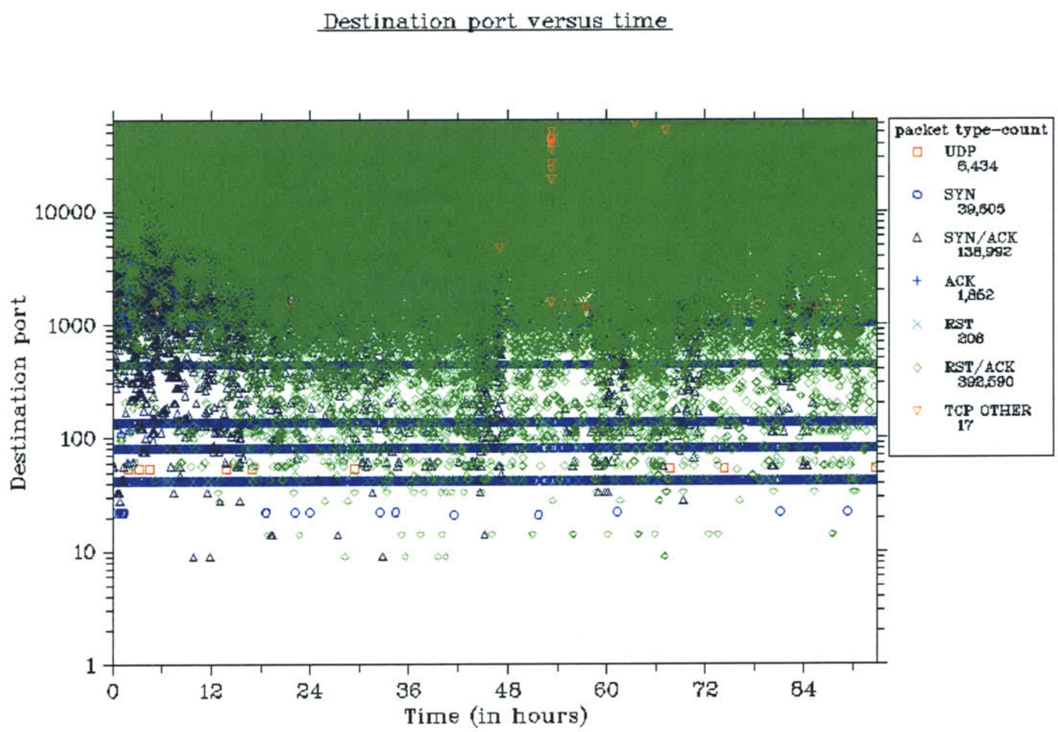

Figure B3-4 - Destination port versus time in 198.188C.

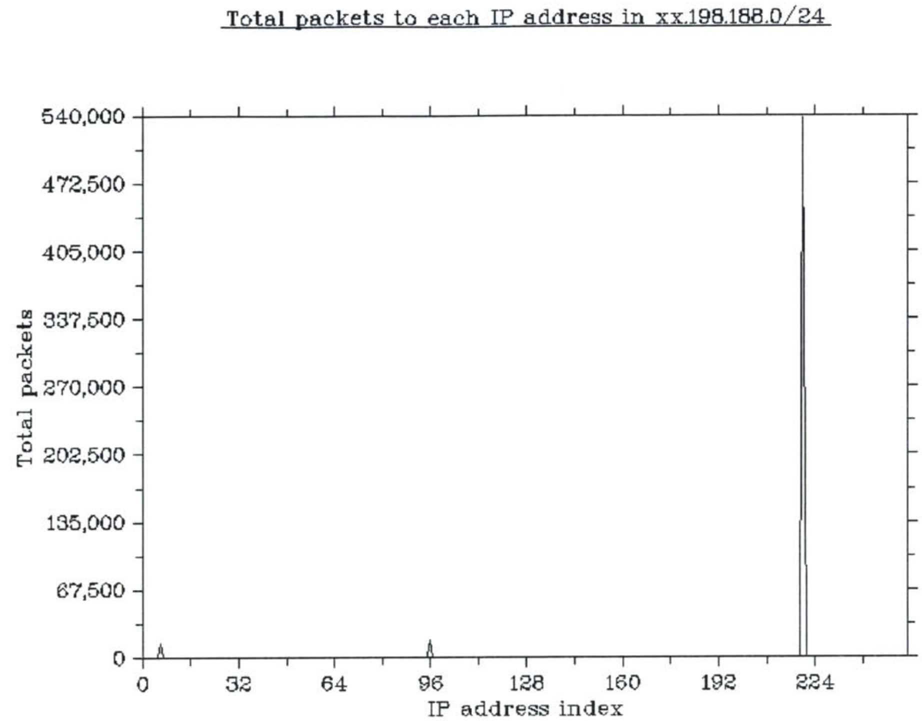

Figure B3-5 - Total packets to each IP address in 198.188C.

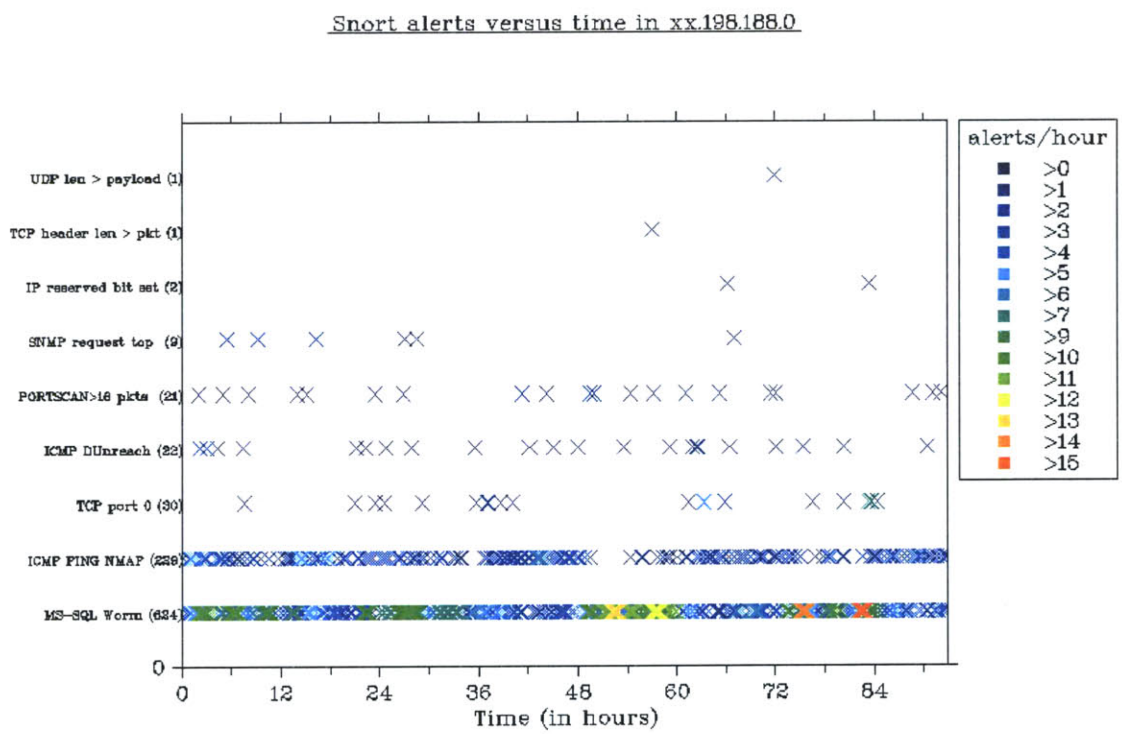

Figure B3-6 - Snort alerts versus time in 198.188C.

B.4 - XX.209.239.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	23,029	0.07	235	65.3	30.1	4.6
Bytes	1,473,260	4.7	11,280	49.1	48.6	2.3

Table B4-1 – Packet and byte statistics for 209.239C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	13,811	417	8	38	527	0

Table B4-2 – TCP packet types in 209.239C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 16 pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	4	1,408	6.4K (28)	482	2,397	10	615	256	90	5.8K
90	X	X	X	10	751	28	1.8K	223	93	6.0K
50	X	X	X	2	41	285	18.2K	105	110	7.0K

Table B4-3 – Statistics for all, the top 90%, and the top 50% of traffic, in 209.239C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 135	5,959	26.0	291,360	19.8
UDP – 137	5,898	25.6	460,044	31.2
TCP – 3127	3,200	13.9	153,708	10.4

Table B4-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 209.239C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.209.239.167	695	3.0	35,064	2.4
xx.209.239.5	369	1.6	15,237	1.0
xx.209.239.154	249	1.1	12,558	0.9

Table B4-5 – Top 3 destination IPs across all packet types by packet count, in 209.239C.

IP Source	Packets	Packet %	Bytes	Byte %
221.160.90.43	734	3.2	35,232	2.4
67.82.117.166	691	3.0	33,168	2.3
84.171.134.66	611	2.7	29,328	2.0

Table B4-6 – Top 3 source IPs across all packet types by packet count, in 209.239C.

Alert Name	Alert Count	Alert %
ICMP Ping NMAP	784	55.8
MS-SQL Worm Propagation Attempt	593	42.1
Portscan > 16 Packets	28	2.0

Table B4-7 – Top 3 alerts by alert count, in 209.239C.

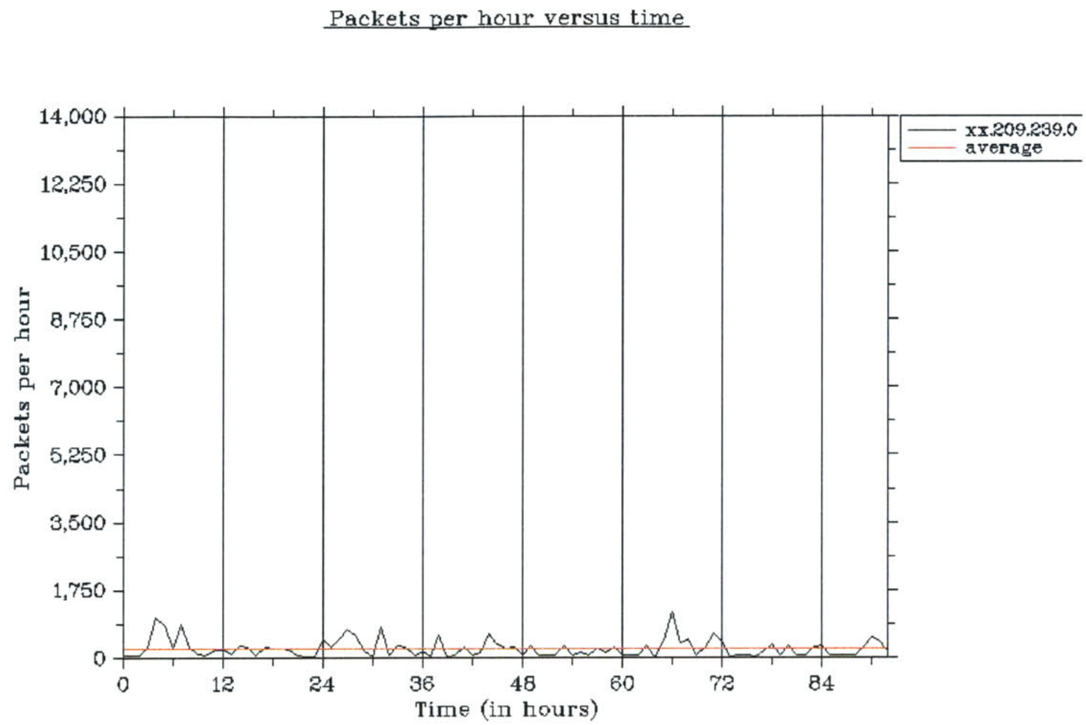

Figure B4-1 - Packets per hour versus time in 209.239C.

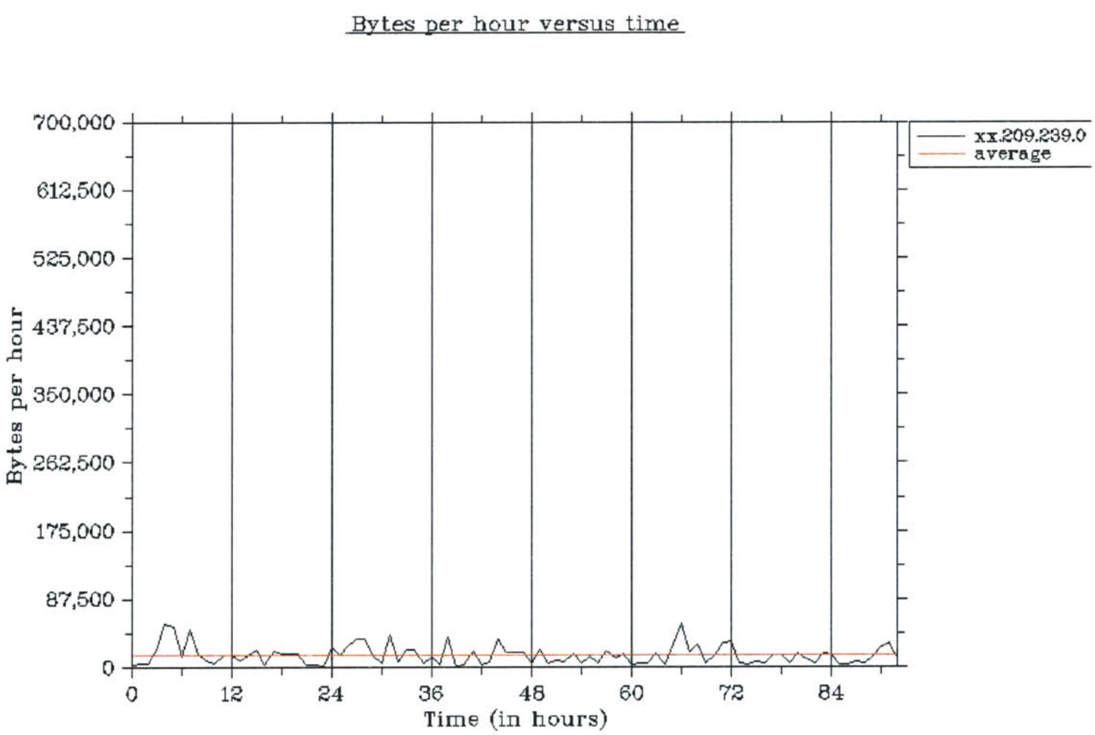

Figure B4-2 - Bytes per hour versus time in 209.239C.

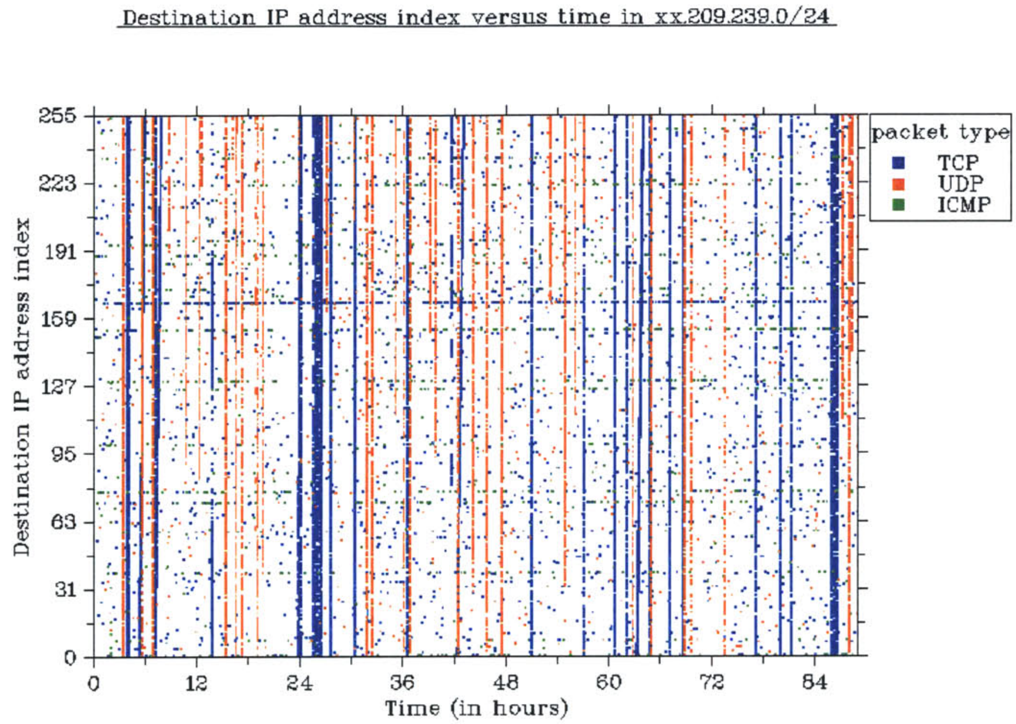

Figure B4-3 - Destination IP address index versus time in 209.239C.

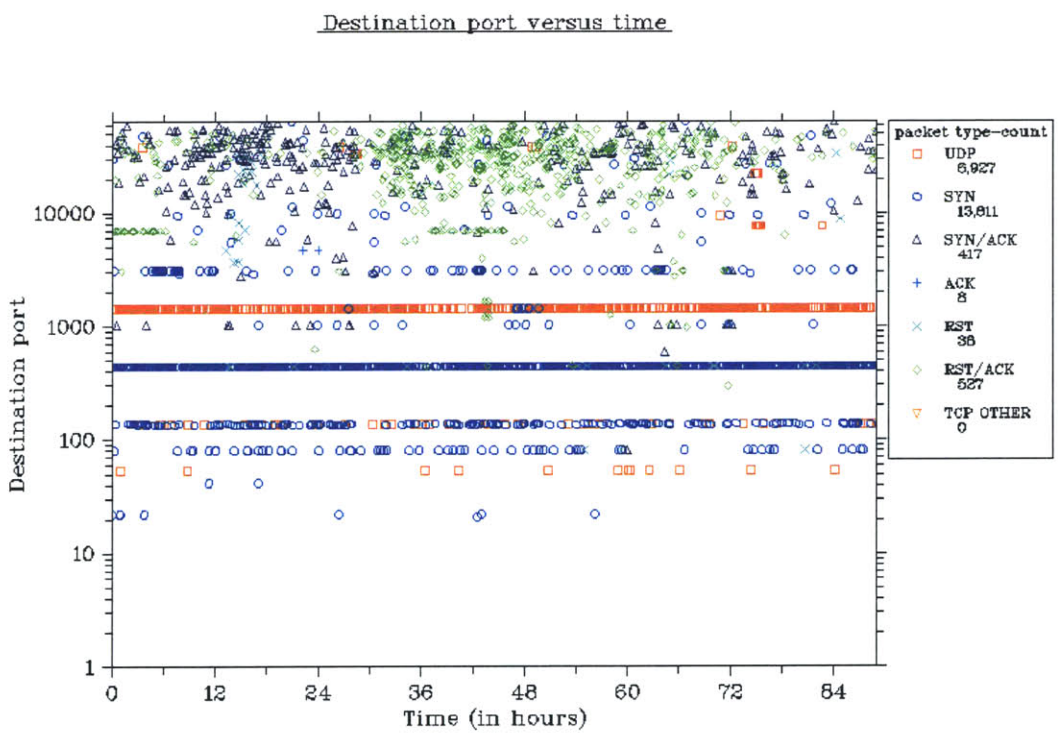

Figure B4-4 - Destination port versus time in 209.239C.

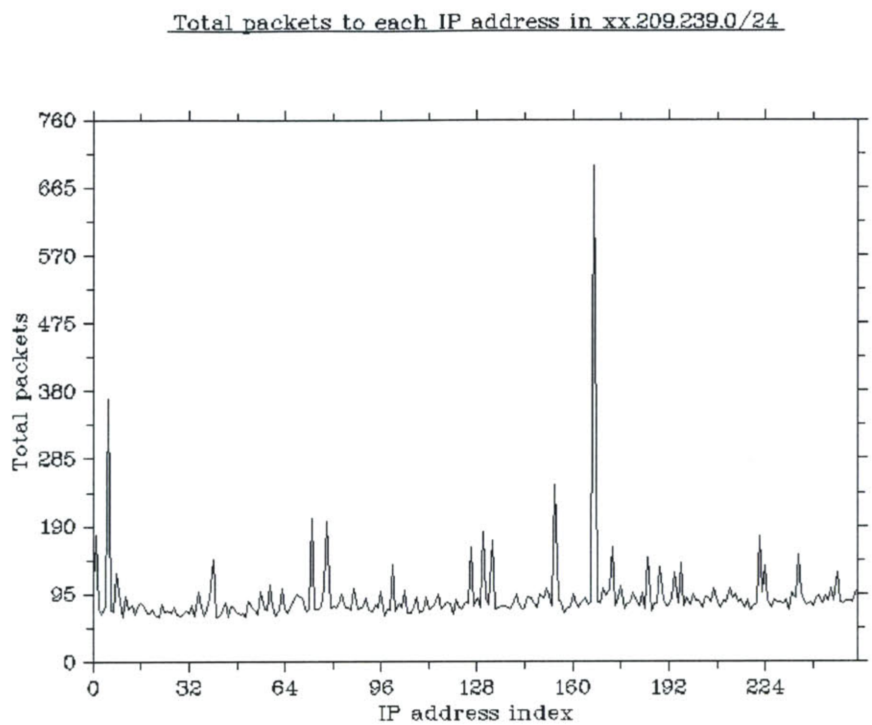

Figure B4-5 - Total packets to each IP address in 209.239C.

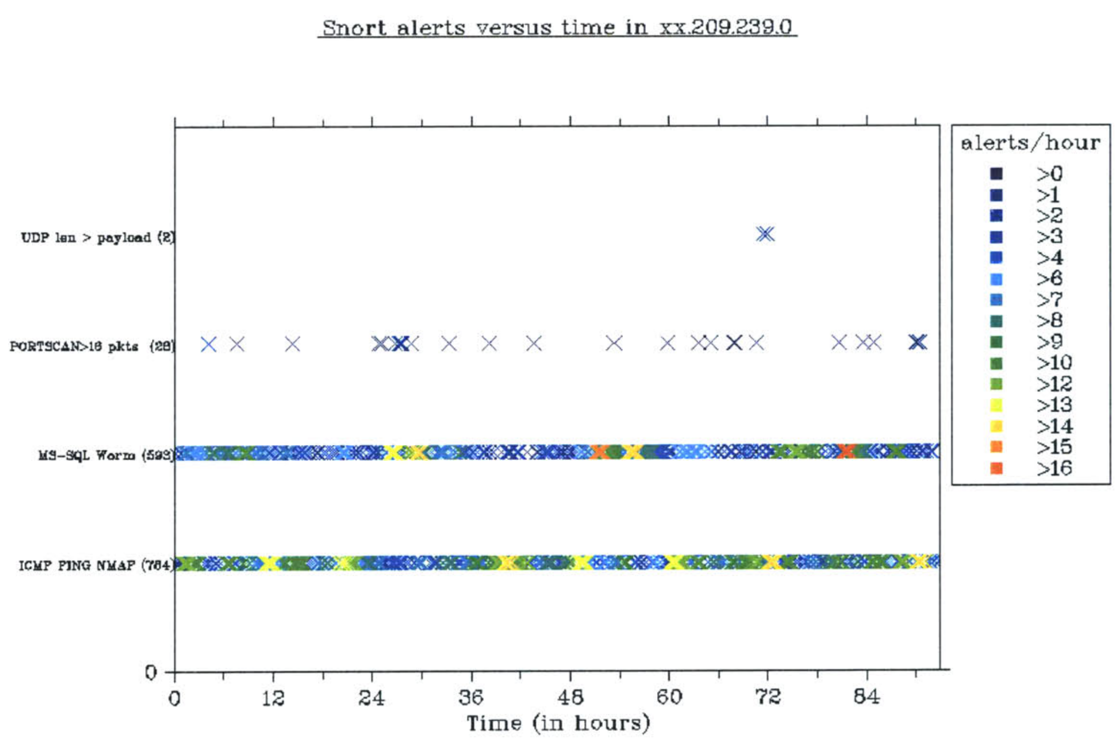

Figure B4-6 - Snort alerts versus time in 209.239C.

B.5 - XX.218.68.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	504,197	1.5	280	98.8	1.1	0.1
Bytes	24,810,656	75	13,428	97.4	2.5	0.1

Table B5-1 – Packet and byte statistics for 218.68C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	495,351	892	10	485	968	2

Table B5-2 – TCP packet types in 218.68C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	7	1,226	4.9K (18)	870	36,964	14	671	256	2.0K	96.9K
90	X	X	X	1	21,485	21	1.0K	1	486K	24M
50	X	X	X	1	5,051	50	2.5K	1	486K	24M

Table B5-3 – Statistics for all, the top 90%, and the top 50% of traffic, in 218.68C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 4662	486,016	96.4	23,589,016	95.1
UDP – 137	4,629	0.9	361,062	1.5
TCP – 445	3,693	0.7	178,218	0.7

Table B5-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 218.68C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.218.68.212	486,226	96.4	23,599,560	95.1
xx.218.68.7	2,869	0.57	138,901	0.56
xx.218.68.20	229	0.05	9,702	0.04

Table B5-5 – Top 3 destination IPs across all packet types by packet count, in 218.68C.

IP Source	Packets	Packet %	Bytes	Byte %
217.217.141.2	702	0.14	33,696	0.14
82.235.3.100	522	0.10	25,056	0.10
219.54.84.76	488	0.10	23,424	0.09

Table B5-6 – Top 3 source IPs across all packet types by packet count, in 218.68C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	630	51.4
ICMP Ping NMAP	571	46.6
Portscan > 16 Packets	18	1.5

Table B5-7 – Top 3 alerts by alert count, in 218.68C.

Packets per hour versus time

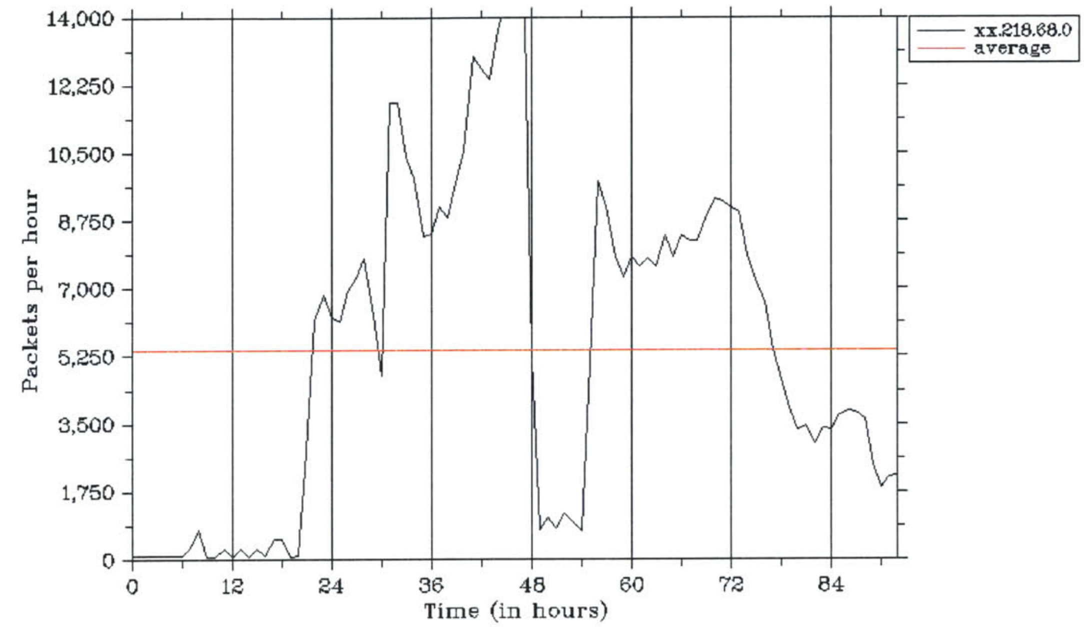

Figure B5-1 - Packets per hour versus time in 218.68C.

Bytes per hour versus time

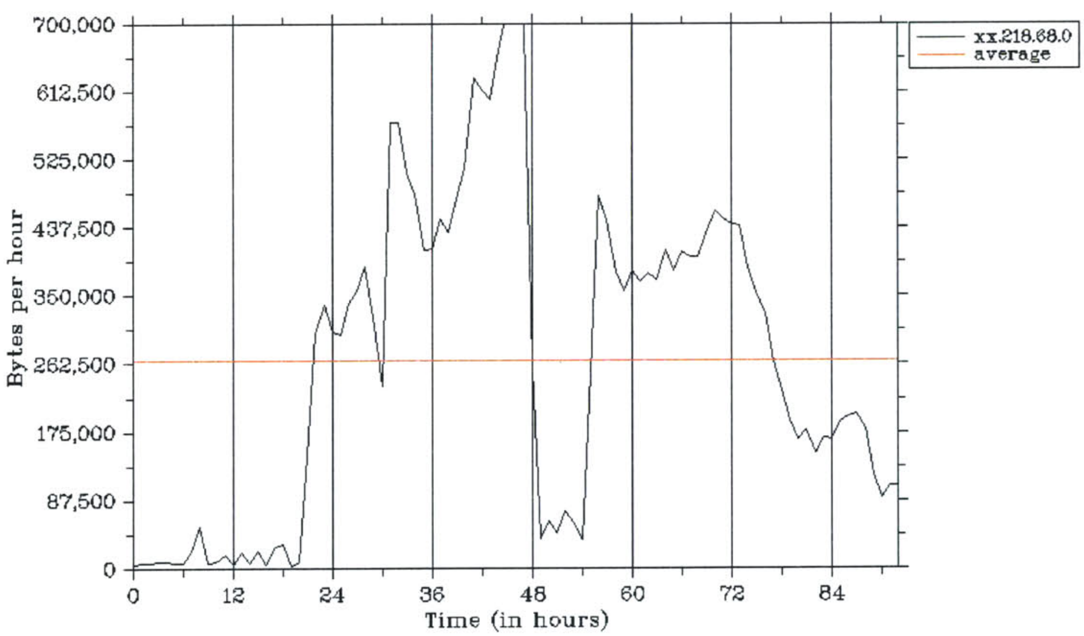

Figure B5-2 - Bytes per hour versus time in 218.68C.

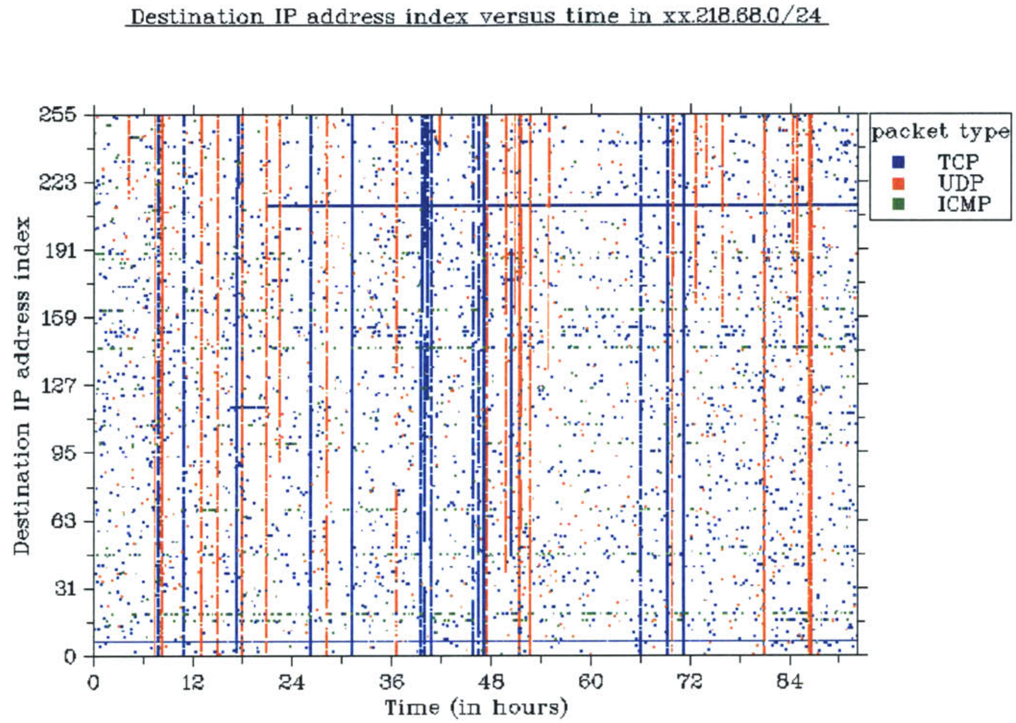

Figure B5-3 - Destination IP address index versus time in 218.68C.

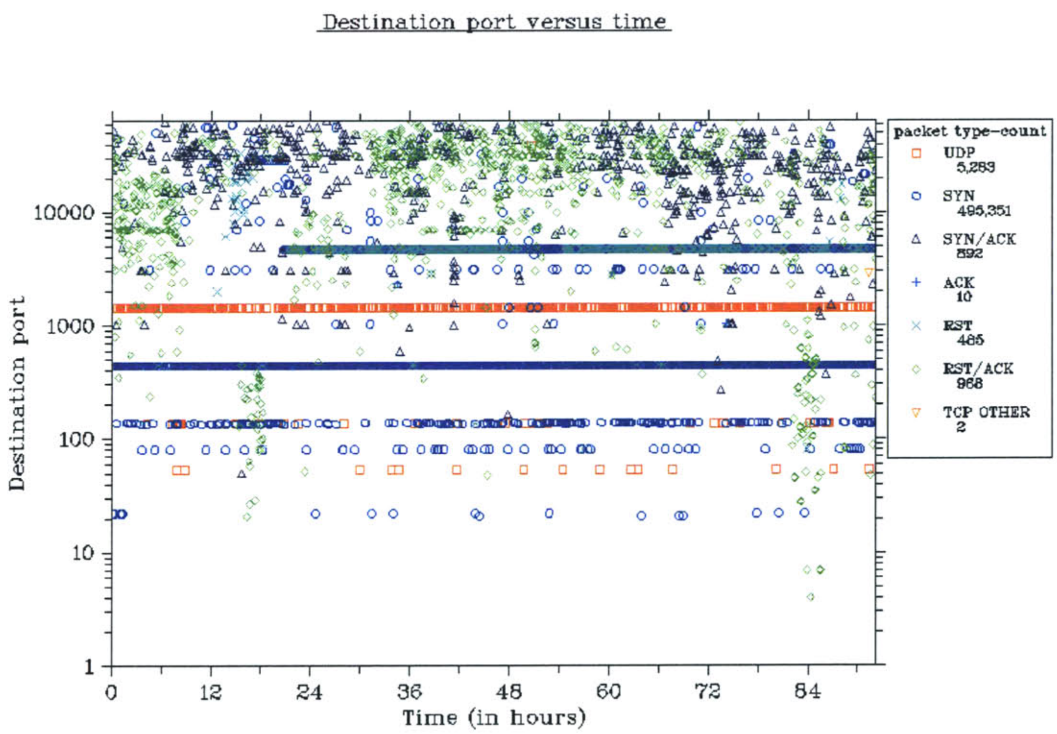

Figure B5-4 - Destination port versus time in 218.68C.

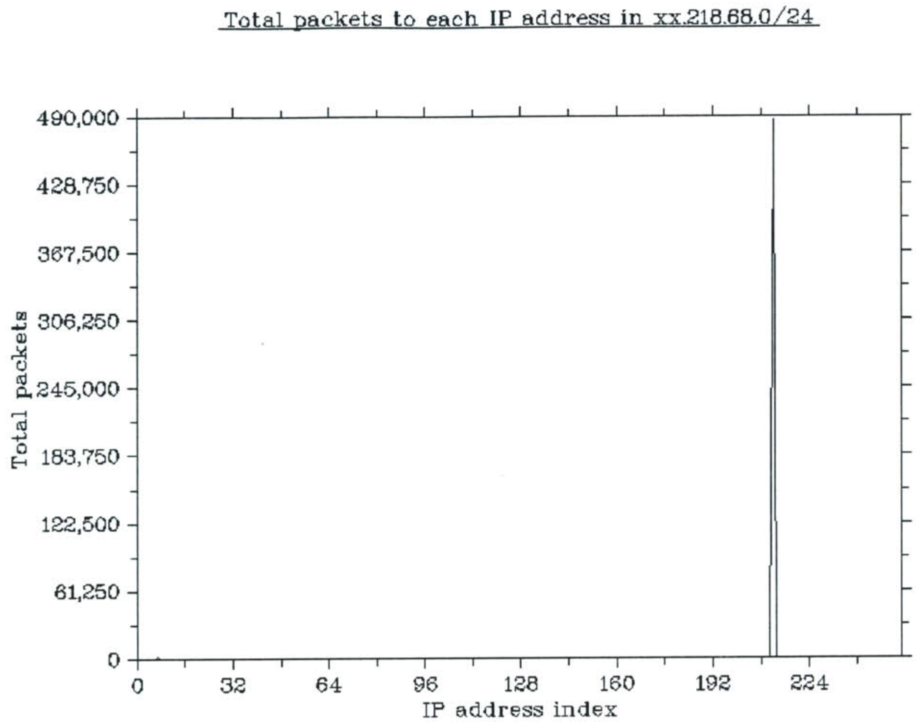

Figure B5-5 - Total packets to each IP address in 218.68C.

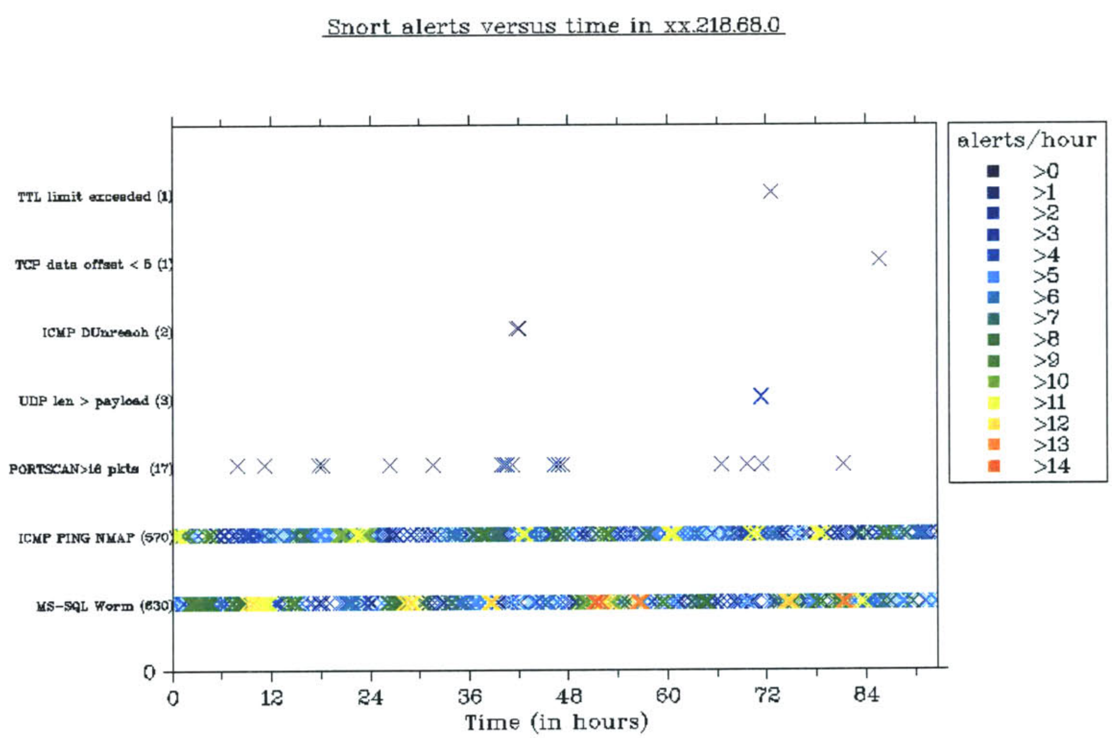

Figure B5-6 - Snort alerts versus time in 218.68C.

B.6 - XX.220.236.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	9,223	0.03	454	57.9	36.4	5.7
Bytes	737,756	2.8	55,350	34.5	63.2	2.3

Table B6-1 – Packet and byte statistics for 220.236C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	4,143	470	4	24	516	0

Table B6-2 – TCP packet types in 220.236C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	5	928	1.9K (9)	408	1345	7	548	256	36	2.9K
90	X	X	X	36	614	14	1.1K	222	37	3.1K
50	X	X	X	2	26	182	13.9K	106	44	3.6K

Table B6-3 – Statistics for all, the top 90%, and the top 50% of traffic in 220.236C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
UDP – 137	2,700	29.3	210,600	28.6
TCP – 135	2,188	23.7	106,824	14.5
TCP – 445	681	7.4	32,936	4.5

Table B6-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 220.236C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.220.236.113	112	1.2	6,750	0.9
xx.220.236.111	108	1.2	4,796	0.7
xx.220.236.130	93	1.0	4,624	0.6

Table B6-5 – Top 3 destination IPs across all packet types by packet count, in 220.236C.

IP Source	Packets	Packet %	Bytes	Byte %
83.129.46.113	444	4.8	23,088	3.1
24.72.12.113	431	4.7	20,688	2.8
66.135.248.40	242	2.6	11,616	1.6

Table B6-6 – Top 3 source IPs across all packet types by packet count, in 220.236C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	627	97.6
ICMP Ping NMAP	286	30.9
Portscan > 16 Packets	9	1.0

Table B6-7 – Top 3 alerts by alert count, in 220.236C.

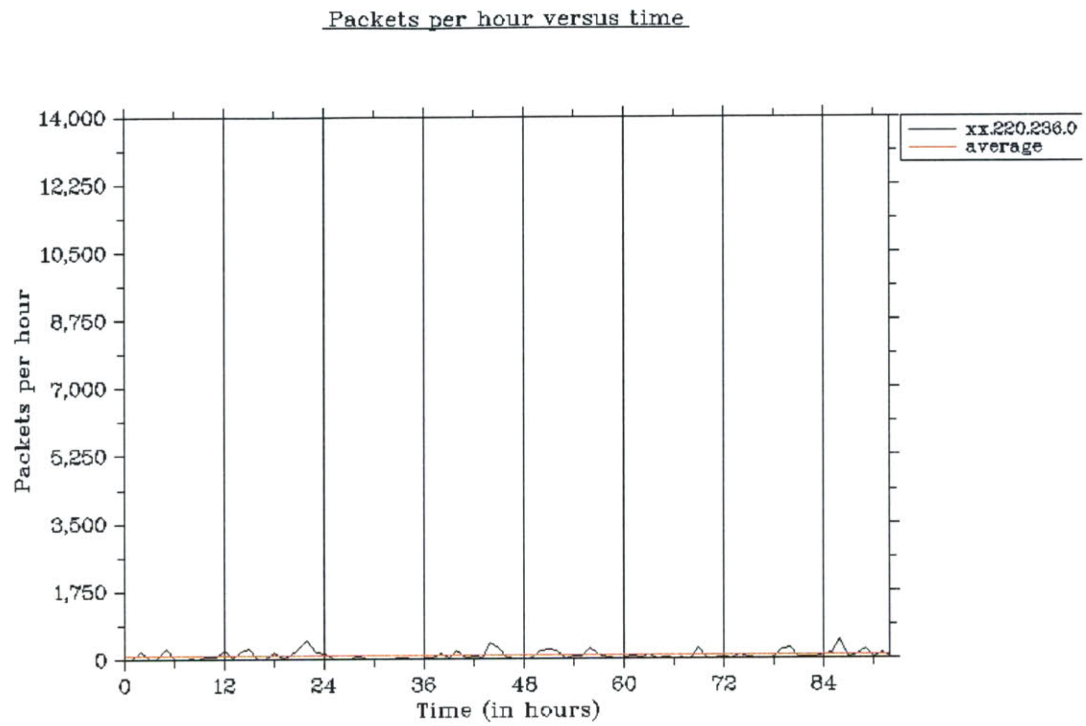

Figure B6-1 - Packets per hour versus time in 220.236C.

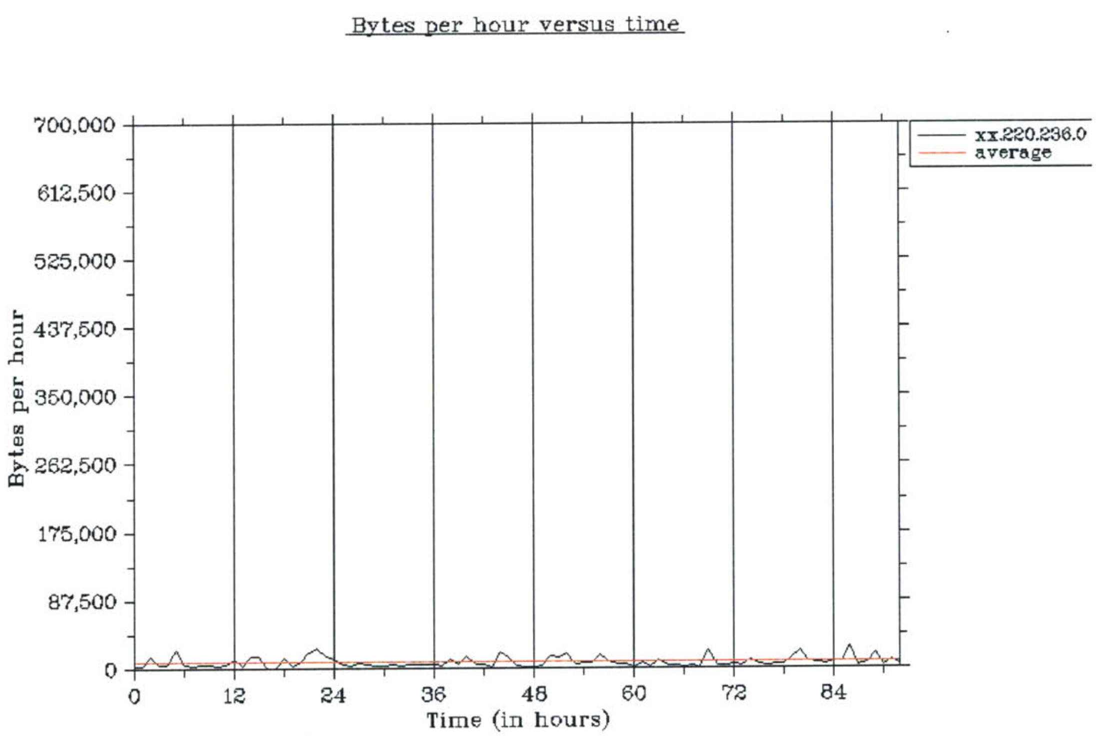

Figure B6-2 - Bytes per hour versus time in 220.236C.

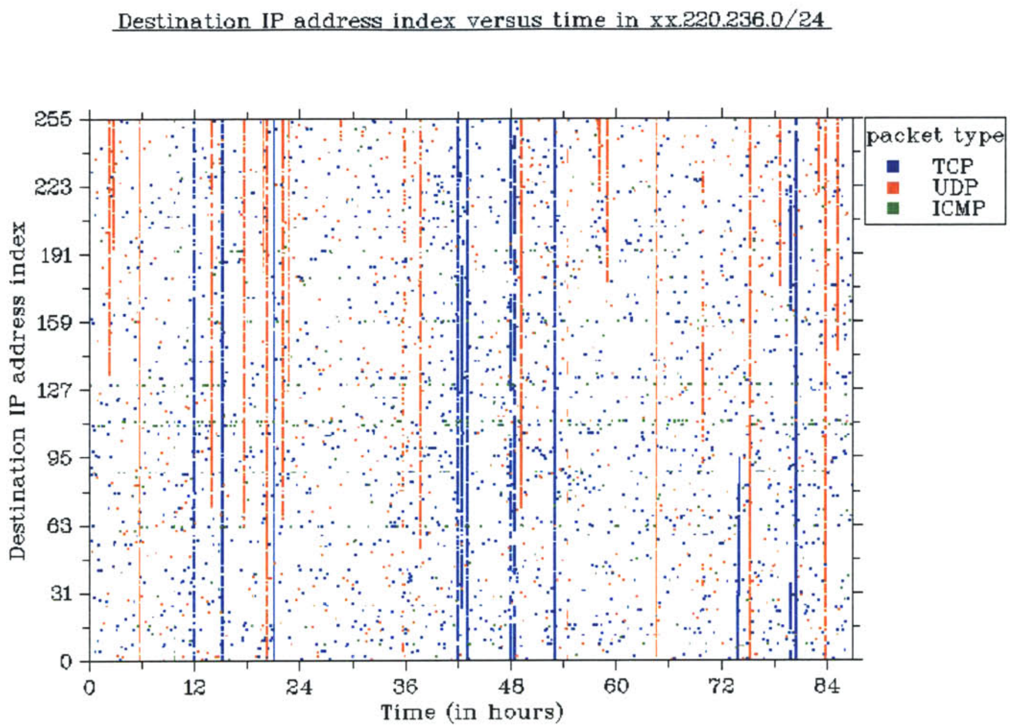

Figure B6-3 - Destination IP address index versus time in 220.236C.

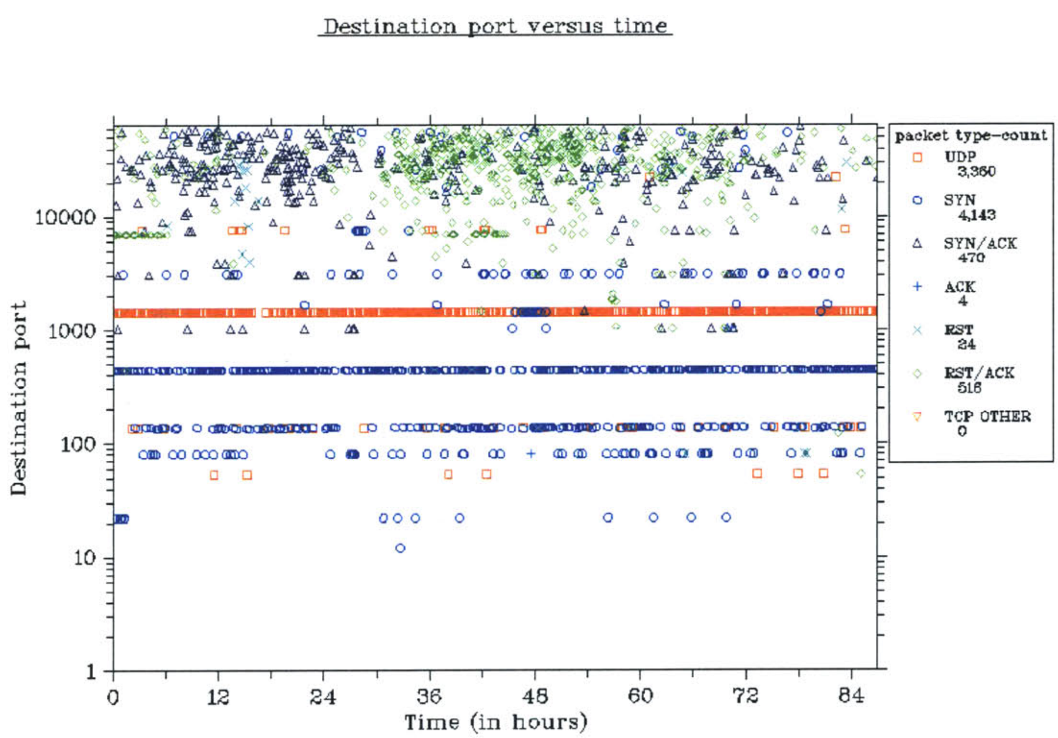

Figure B6-4 - Destination port versus time in 220.236C.

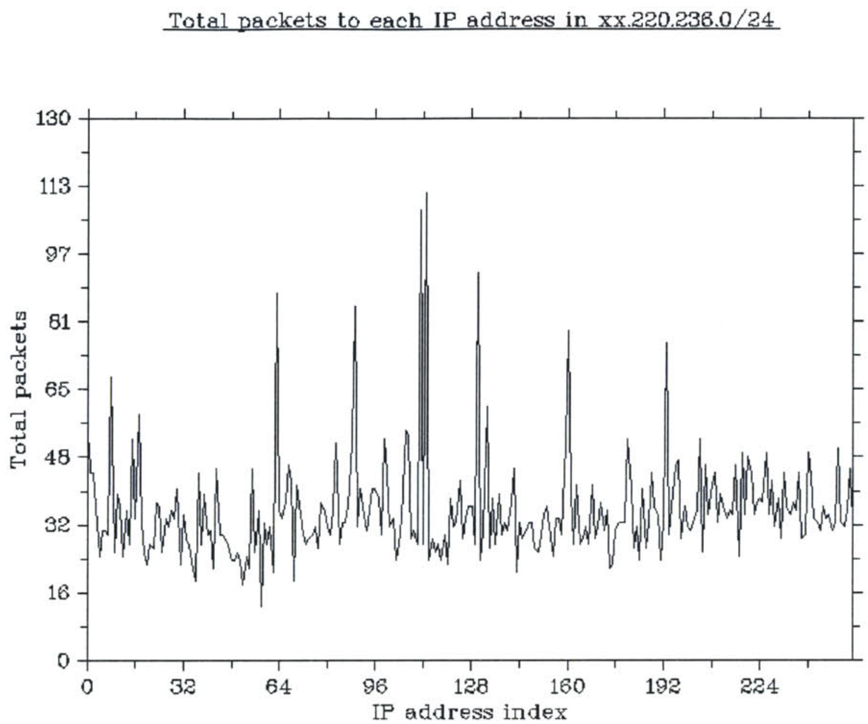

Figure B6-5 - Total packets to each IP address in 220.236C.

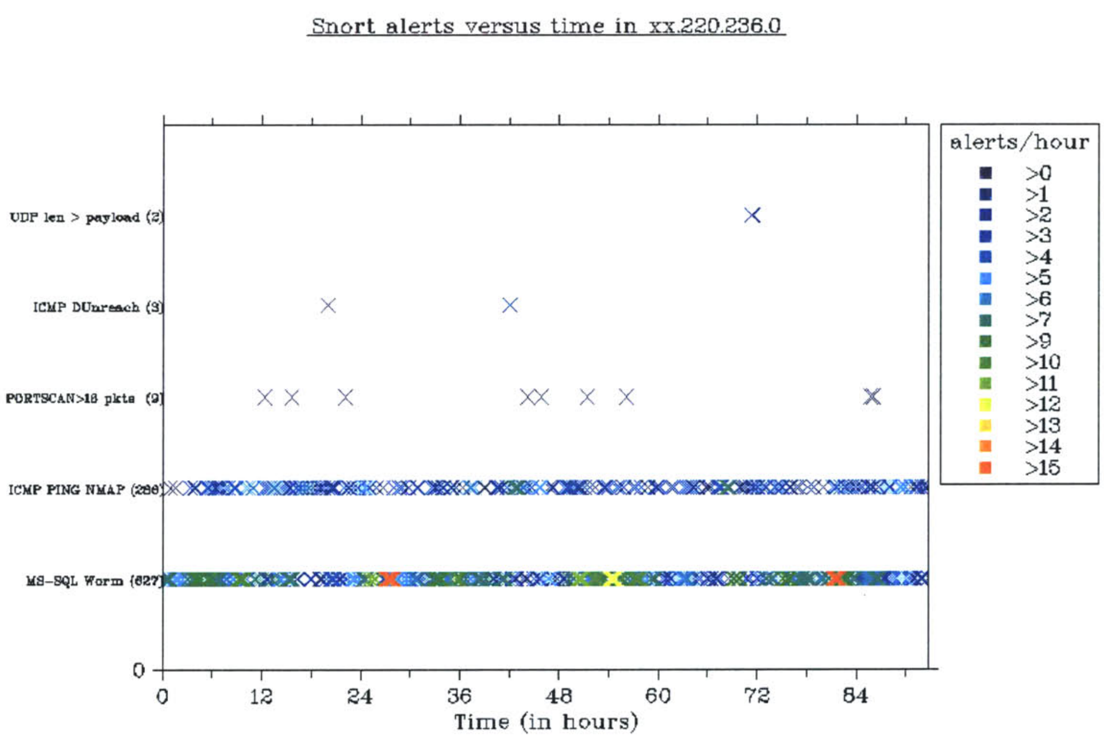

Figure B6-6 - Snort alerts versus time in 220.236C.

B.7 - XX.226.255.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	10,543	0.04	224	46.7	51.1	2.2
Bytes	825,213	2.8	10,753	29.0	70.0	1.0

Table B7-1 – Packet and byte statistics for 226.255C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	4,552	69	4	43	50	0

Table B7-2 – TCP packet types in 226.255C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 16 pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	4	666	1.5K (3)	241	1,707	6	483	256	41	3.2K
90	X	X	X	8	1,009	9	770	205	46	3.6K
50	X	X	X	2	19	280	19.6K	43	123	8.0K

Table B7-3 – Statistics for all, the top 90%, and the top 50% of traffic in 226.255C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
UDP – 137	3,011	28.6	234,858	28.5
TCP – 445	2,546	24.2	122,600	14.9
UDP – 38293	1,688	16.0	74,272	9.0

Table B7-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 226.255C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.226.255.212	2,174	20.6	105,566	12.8
xx.226.255.255	1,729	16.4	77,153	9.4
xx.226.255.217	106	1.0	6,906	0.8

Table B7-5 – Top 3 destination IPs across all packet types by packet count, in 226.255C.

IP Source	Packets	Packet %	Bytes	Byte %
168.171.13.3	1,286	12.2	56,584	6.9
220.117.199.6	740	7.0	35,520	4.3
222.121.11.249	573	5.4	27,504	3.3

Table B7-6 – Top 3 source IPs across all packet types by packet count, in 226.255C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	658	98.8
Short UDP Packet, Length Field > Payload Length	4	0.6
Portscan > 16 Packets	3	0.5

Table B7-7 – Top 3 alerts by alert count, in 226.255C.

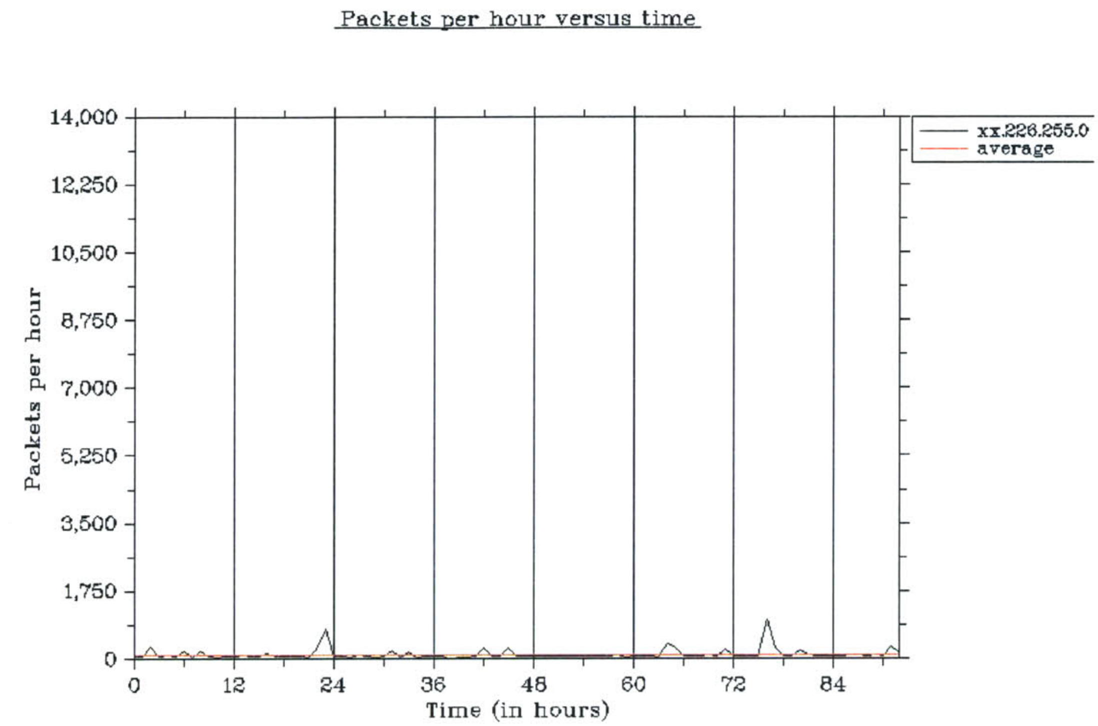

Figure B7-1 - Packets per hour versus time in 226.255C.

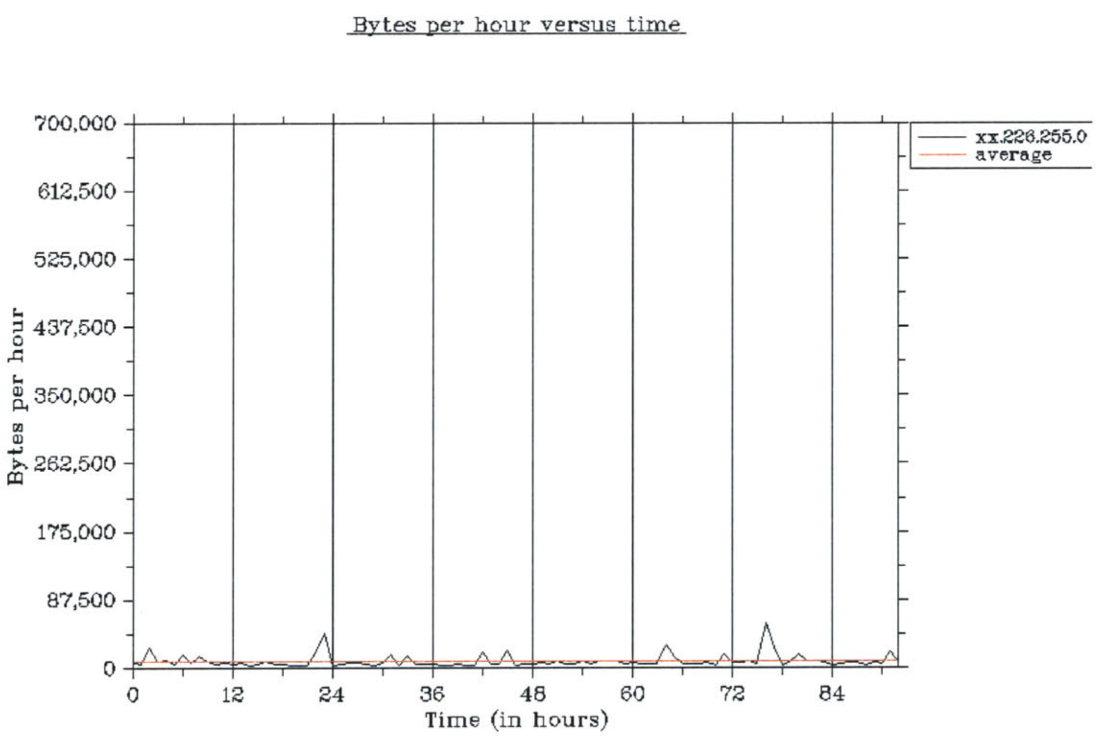

Figure B7-2 - Bytes per hour versus time in 226.255C.

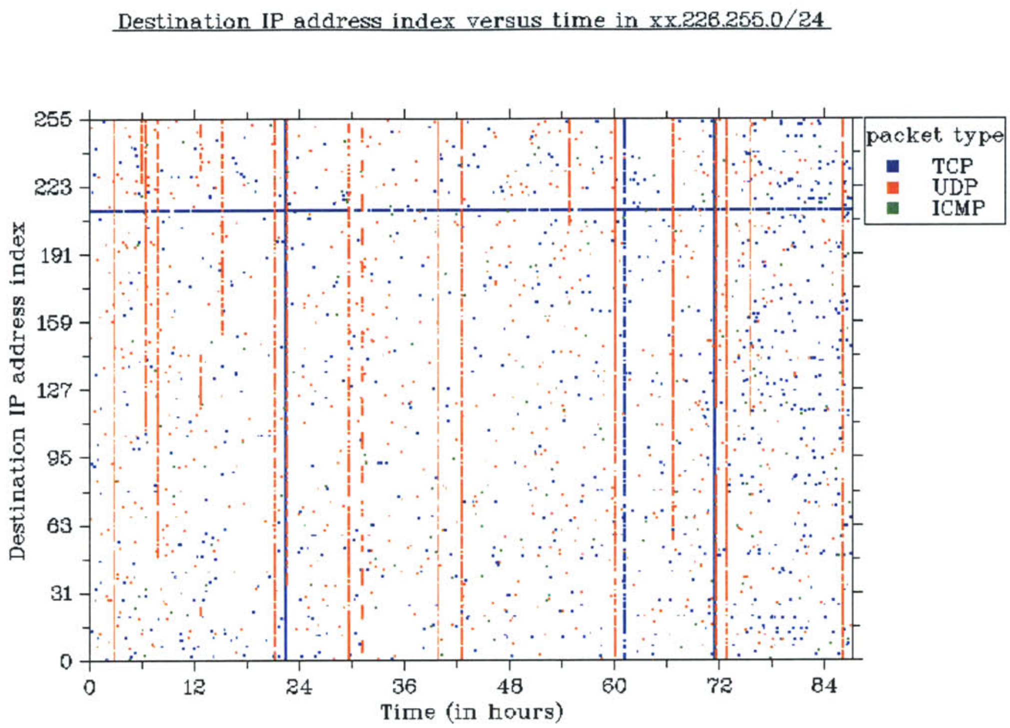

Figure B7-3 - Destination IP address index versus time in 226.255C.

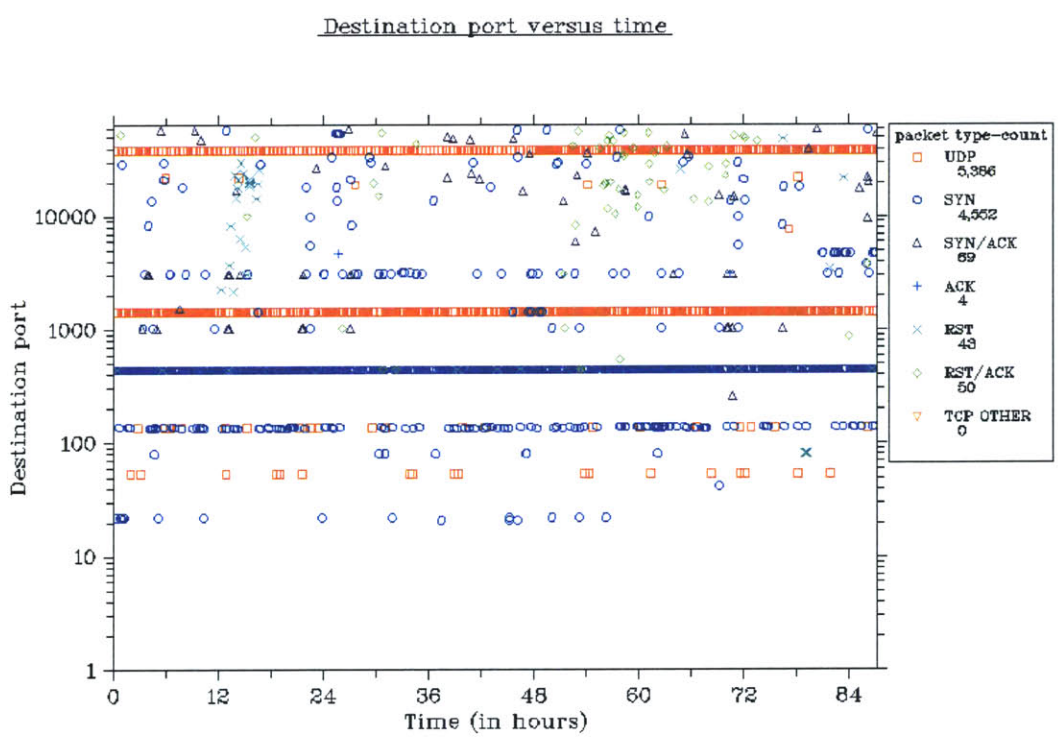

Figure B7-4 - Destination port versus time in 226.255C.

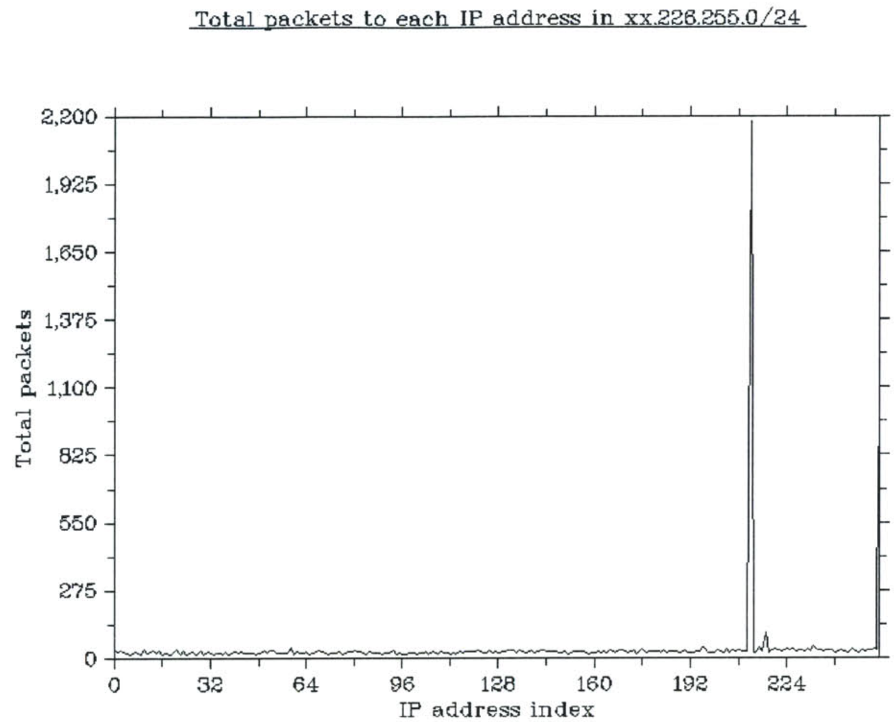

Figure B7-5 - Total packets to each IP address in 226.255C.

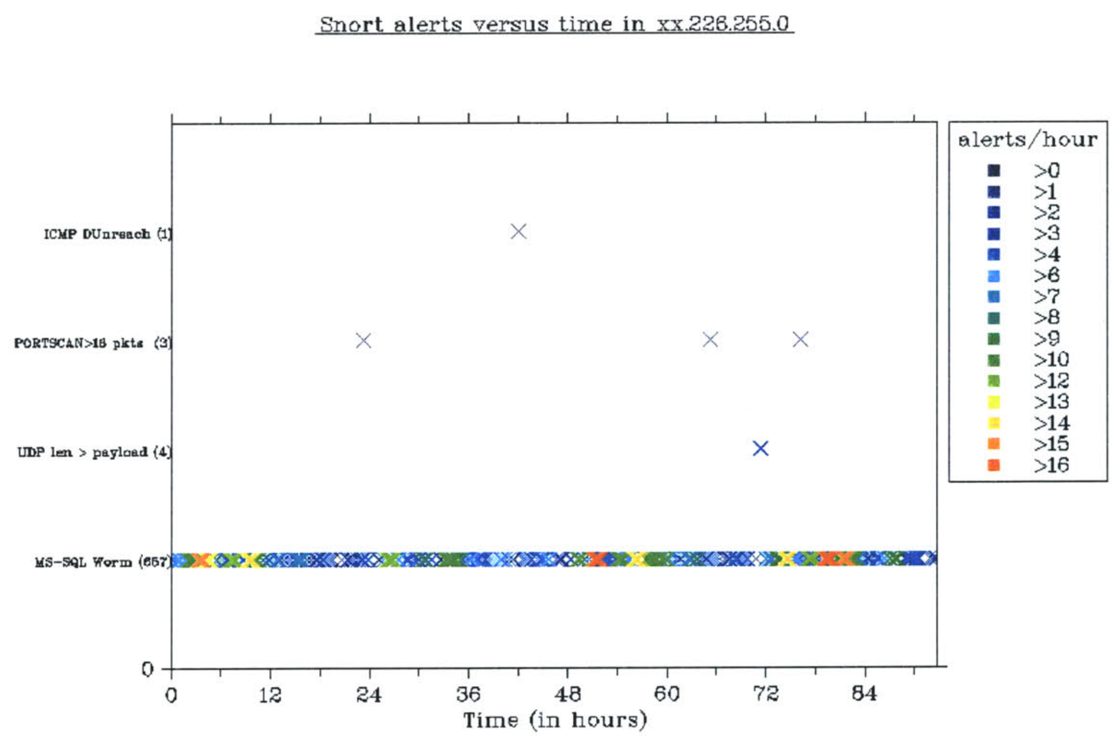

Figure B7-6 - Snort alerts versus time in 226.255C.

B.8 - XX.239.255.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	8,150	0.03	445	16.5	80.6	2.9
Bytes	731,397	2.7	19,608	9.1	89.8	1.1

Table B8-1 – Packet and byte statistics for 239.255C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	990	78	8	31	50	1

Table B8-2 – TCP packet types in 239.255C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	Unique	Total	Packets (Scans > 16 pkts)	Total	Hosts	Avg Pkts /Src	Avg Bytes /Src	Hosts	Avg Pkts /Dest	Avg Bytes /Dest
100	4	622	0 (0)	238	869	9	842	256	32	2.9K
90	X	X	X	7	357	21	1.9K	211	35	3.2K
50	X	X	X	1	16	259	19.1K	74	55	4.5K

Table B8-3 – Statistics for all, the top 90%, and the top 50% of traffic in 239.255C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
UDP – 137	4,230	51.9	329,940	45.1
UDP – 38293	1,692	20.8	74,448	10.2
UDP – 1434	619	7.6	250,076	34.2

Table B8-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 239.255C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.239.255.255	1,737	21.3	77,998	10.7
xx.239.255.82	151	1.9	9,532	1.3
xx.239.255.217	85	1.0	5,428	0.7

Table B8-5 – Top 3 destination IPs across all packet types by packet count, in 239.255C.

IP Source	Packets	Packet %	Bytes	Byte %
168.171.13.3	1,290	15.8	56,760	7.8
201.252.46.157	229	2.8	17,862	2.4
85.96.117.162	229	2.8	17,862	2.4

Table B8-6 – Top 3 source IPs across all packet types by packet count, in 239.255C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	616	99.0
Short UDP Packet, Length Field > Payload Length	4	0.6
ICMP Destination Unreachable Communication Administratively Prohibited	1	0.2

Table B8-7 – Top 3 alerts by alert count, in 239.255C.

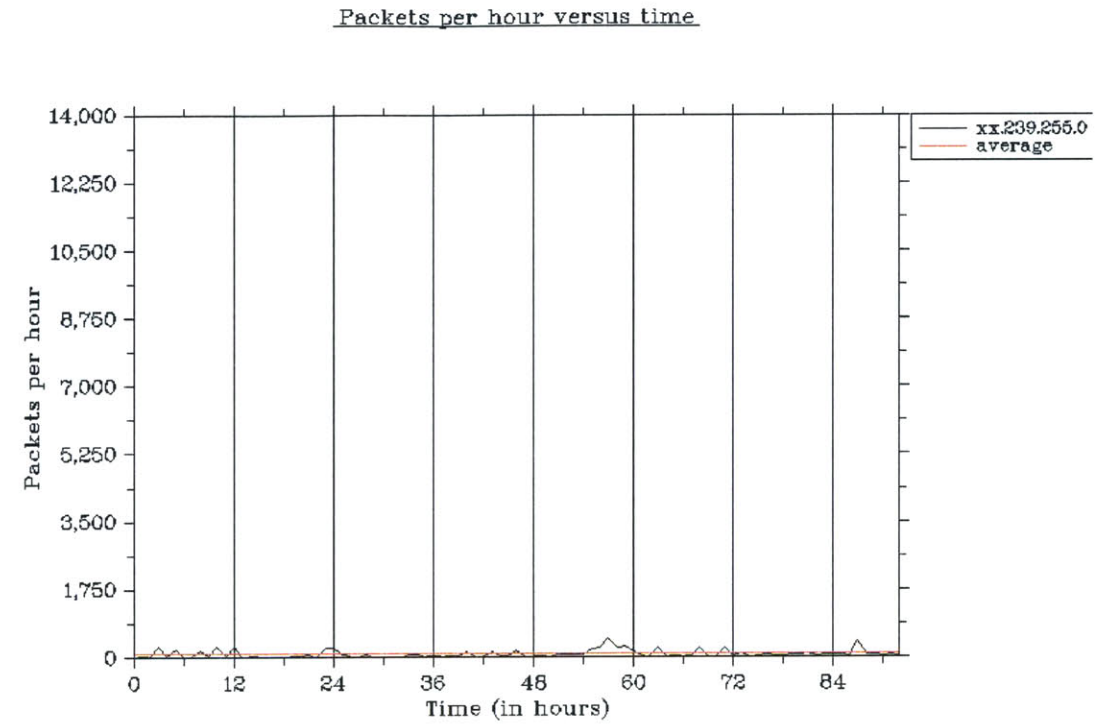

Figure B8-1 - Packets per hour versus time i n 239.255C.

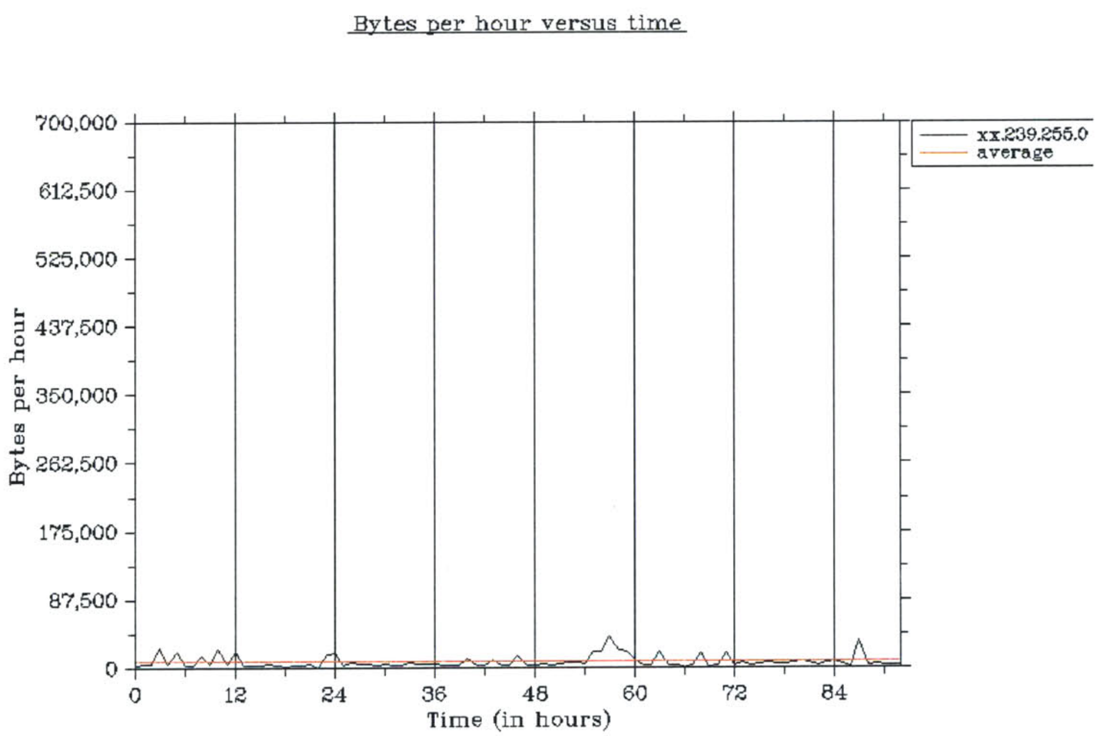

Figure B8-2 - Bytes per hour versus time in 239.255C.

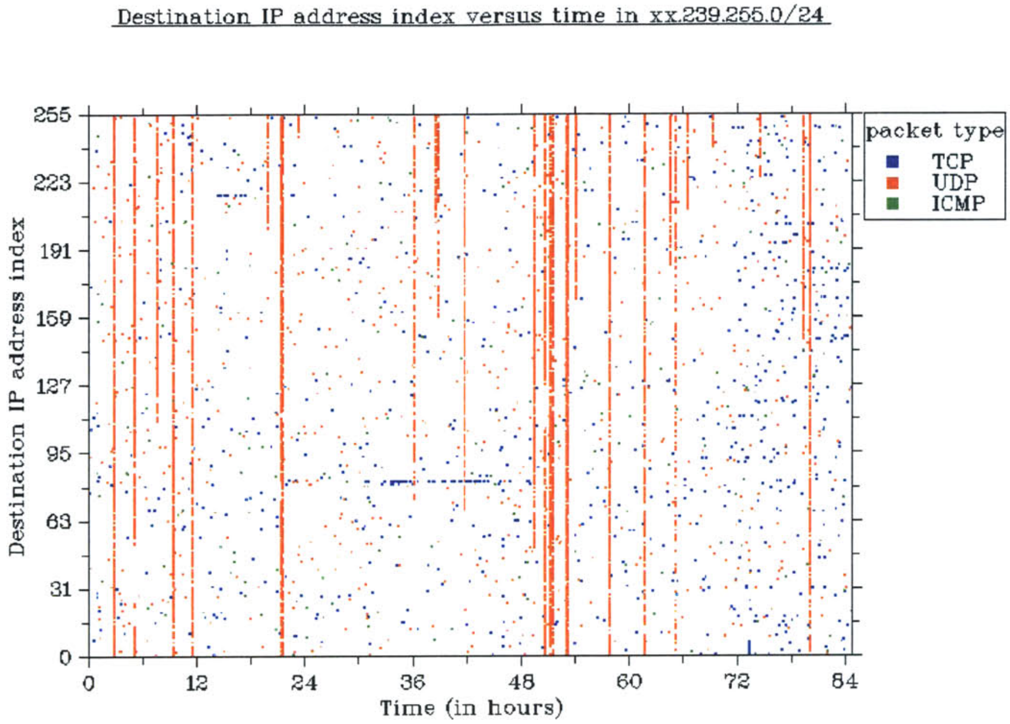

Figure B8-3 - Destination IP address index versus time in 239.255C.

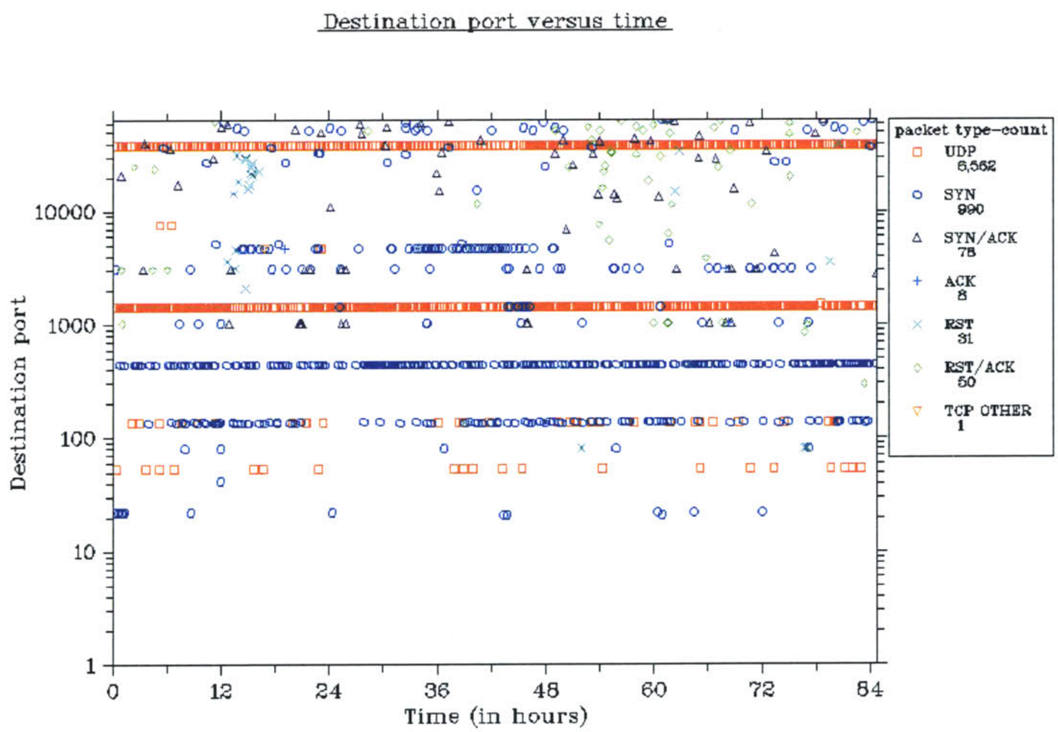

Figure B8-4 - Destination port versus time in 239.255C.

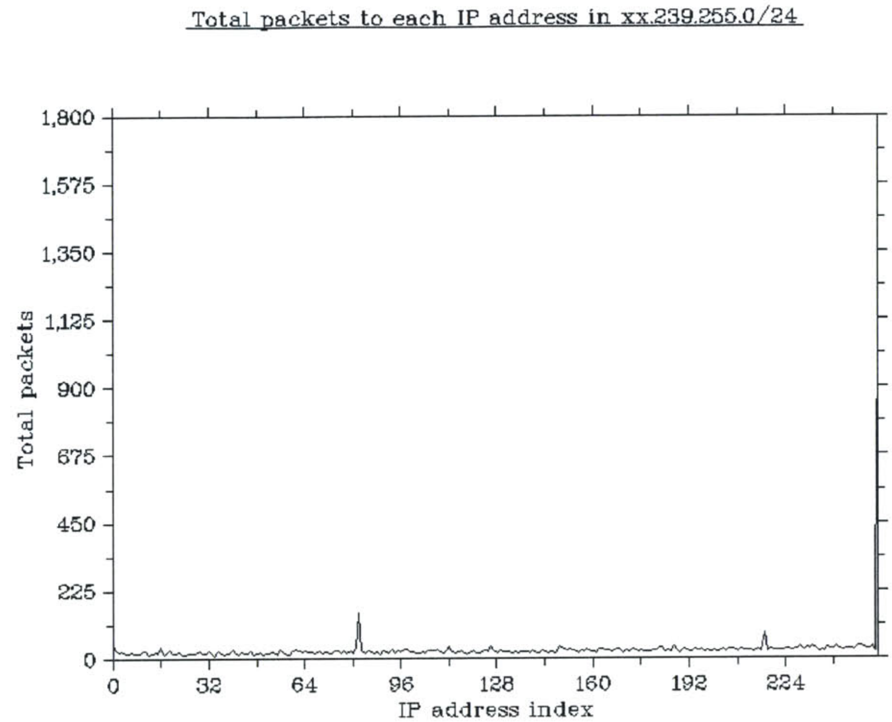

Figure B8-5 - Total packets to each IP address in 239.255C.

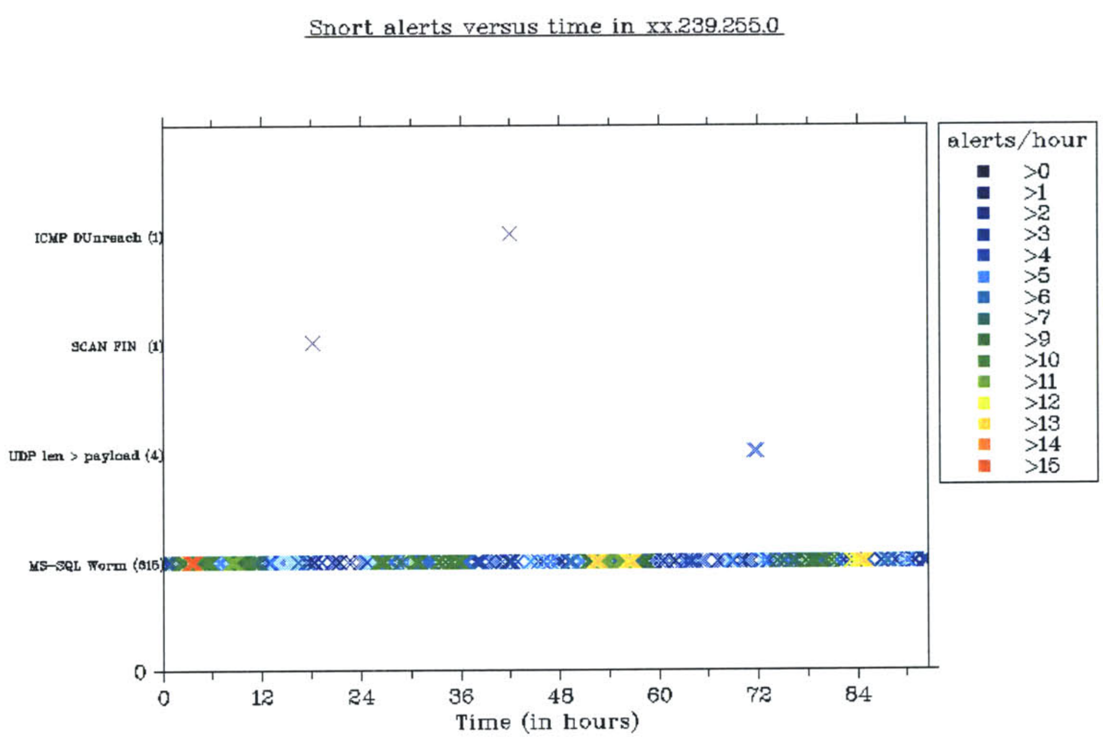

Figure B8-6 - Snort alerts versus time in 239.255C.

B.9 - XX.248.246.0/24

	Total	Avg Rate	Peak Rate	%TCP	%UDP	%ICMP
Packets	707,941	2.1	181	99.2	0.7	0.1
Bytes	34,403,749	103	8,688	98.2	1.7	0.1

Table B9-1 – Packet and byte statistics for 248.246C.

TCP TYPE	SYN	SYN/ACK	ACK	RST	RST/ACK	OTHER
PKT COUNT	692,595	524	582	7,183	812	119

Table B9-2 – TCP packet types in 248.246C.

	Snort Alerts		Scans	Ports	Sources			Destinations		
%	**Unique**	**Total**	**Packets (Scans > 16 pkts)**	**Total**	**Hosts**	**Avg Pkts /Src**	**Avg Bytes /Src**	**Hosts**	**Avg Pkts /Dest**	**Avg Bytes /Dest**
100	10	1,078	5.7K (41)	433	51,238	14	671	256	2.8K	134K
90	X	X	X	5	27,819	23	1.1K	1	693K	33M
50	X	X	X	3	4,177	85	4.1K	1	693K	33M

Table B9-3 – Statistics for all, the top 90%, and the top 50% of traffic in 248.246C.

Protocol - Port/ICMP Type	Packets	Packet %	Bytes	Byte %
TCP – 1025	150,797	21.3	7,257,139	21.1
TCP – 42	149,216	21.1	7,181,840	20.9
TCP – 80	135,969	19.2	6,548,915	19.0

Table B9-4 – Top 3 packet types across ICMP, TCP, and UDP traffic by packet count, in 248.246C.

IP Destination	Packets	Packet %	Bytes	Byte %
xx.248.246.112	692,920	97.9	33,349,840	96.9
xx.248.246.249	202	0.03	9,534	0.03
xx.248.246.94	139	0.02	6,952	0.02

Table B9-5 – Top 3 destination IPs across all packet types by packet count, in 248.246C.

IP Source	Packets	Packet %	Bytes	Byte %
207.157.30.46	2,621	0.4	125,736	0.4
193.170.238.69	2,413	0.3	115,824	0.3
193.224.106.40	2,311	0.3	110,928	0.3

Table B9-6 – Top 3 source IPs across all packet types by packet count, in 248.246C.

Alert Name	Alert Count	Alert %
MS-SQL Worm Propagation Attempt	609	56.5
ICMP Ping NMAP	391	36.3
Portscan > 16 Packets	41	3.8

Table B9-7 – Top 3 alerts by alert count, in 248.246C.

Packets per hour versus time

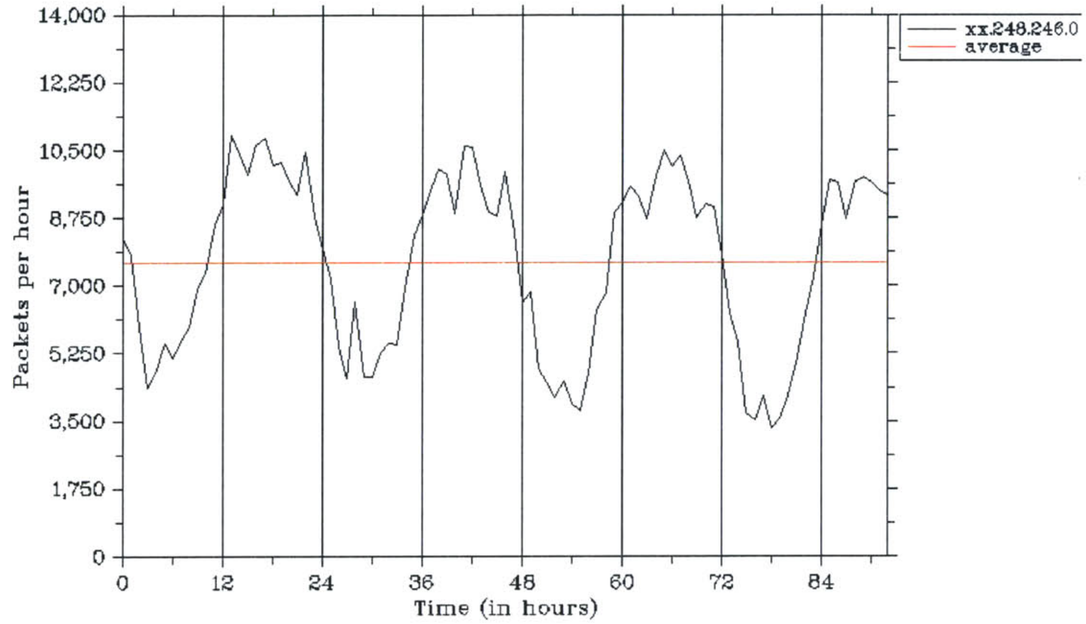

Figure B9-1 - Packets per hour versus time in 248.246C.

Bytes per hour versus time

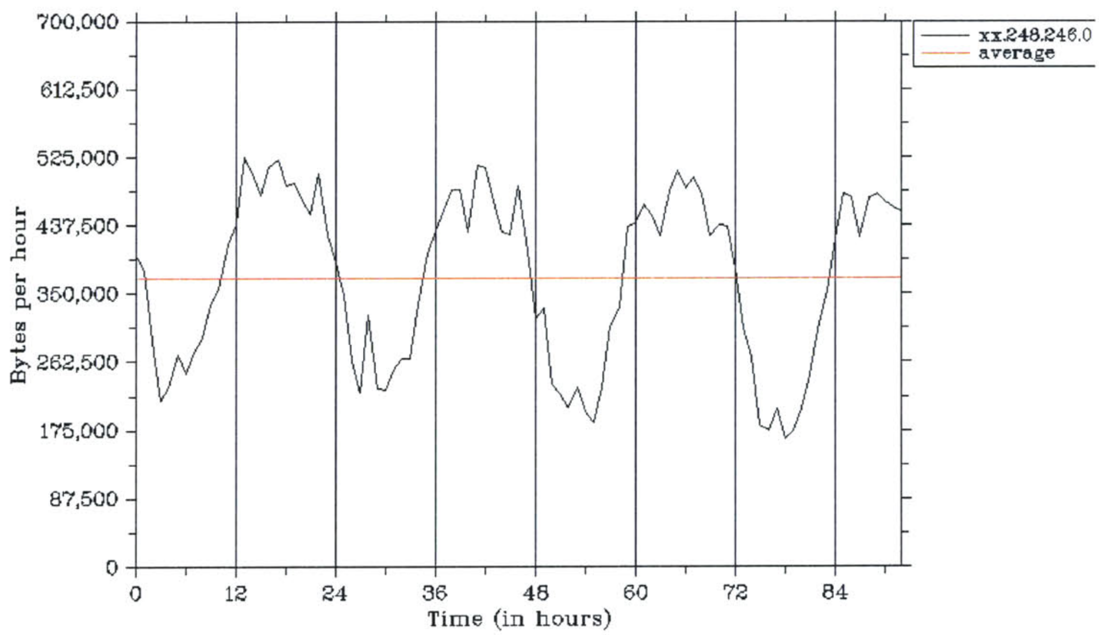

Figure B9-2 - Bytes per hour versus time in 248.246C.

Destination IP address index versus time in xx.248.246.0/24

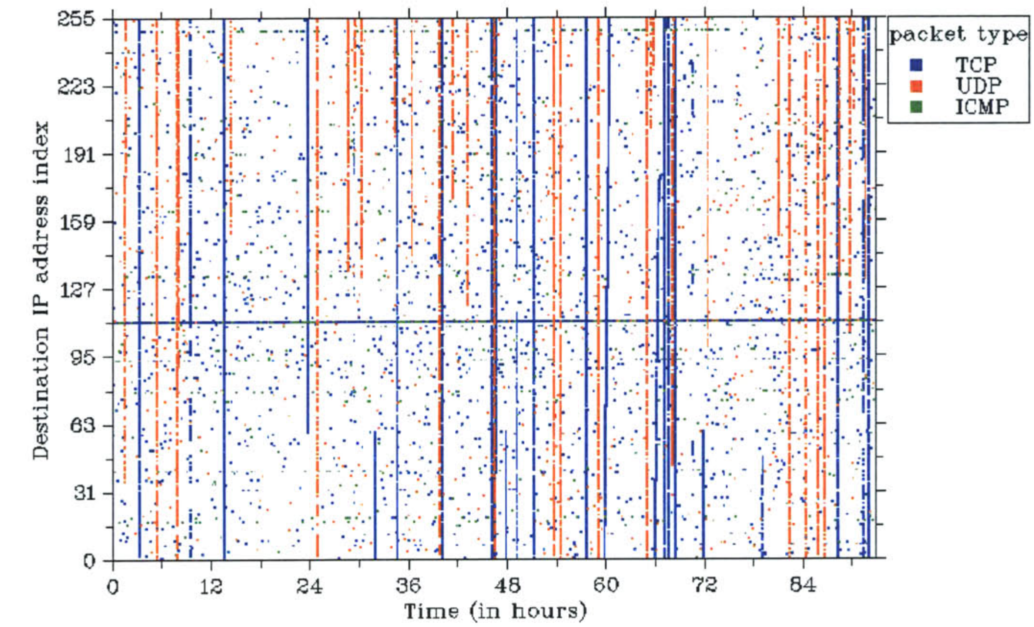

Figure B9-3 - Destination IP address index versus time in 248.246C.

Destination port versus time

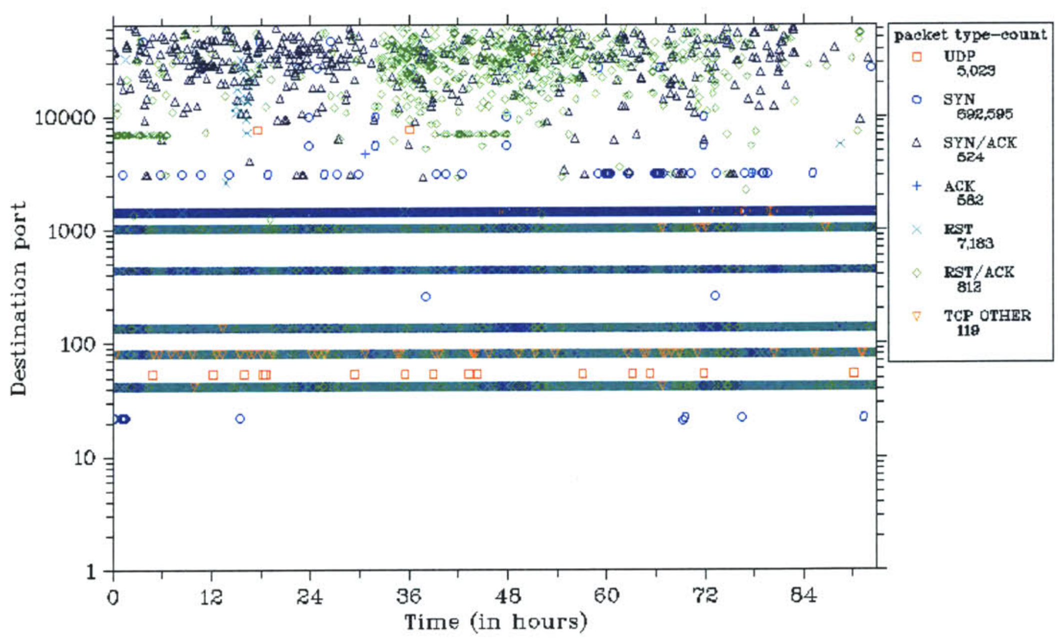

Figure B9-4 - Destination port versus time in 248.246C.

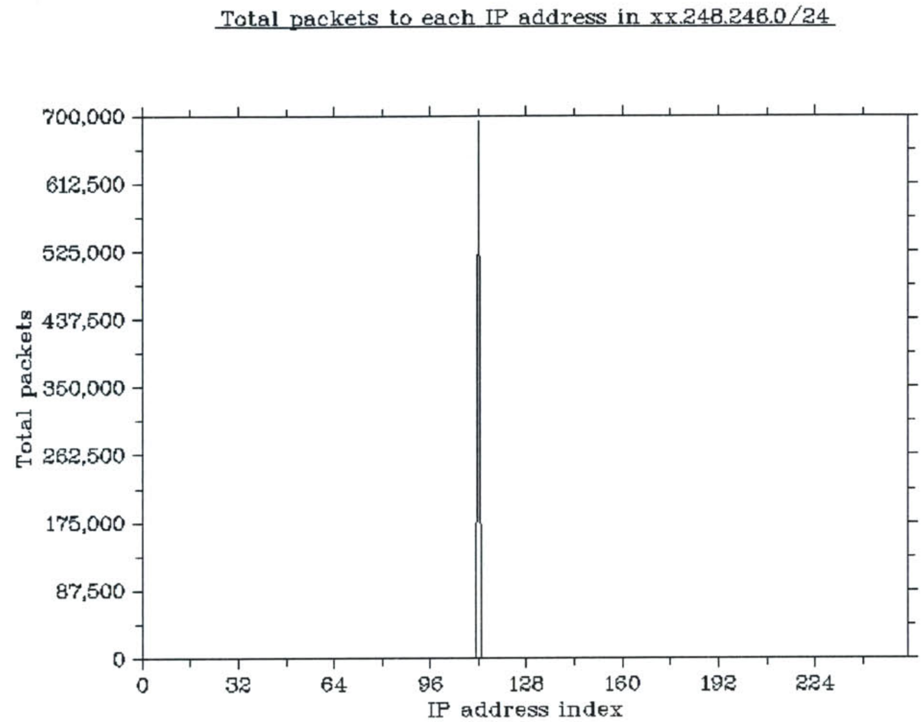

Figure B9-5 - Total packets to each IP address in 248.246C.

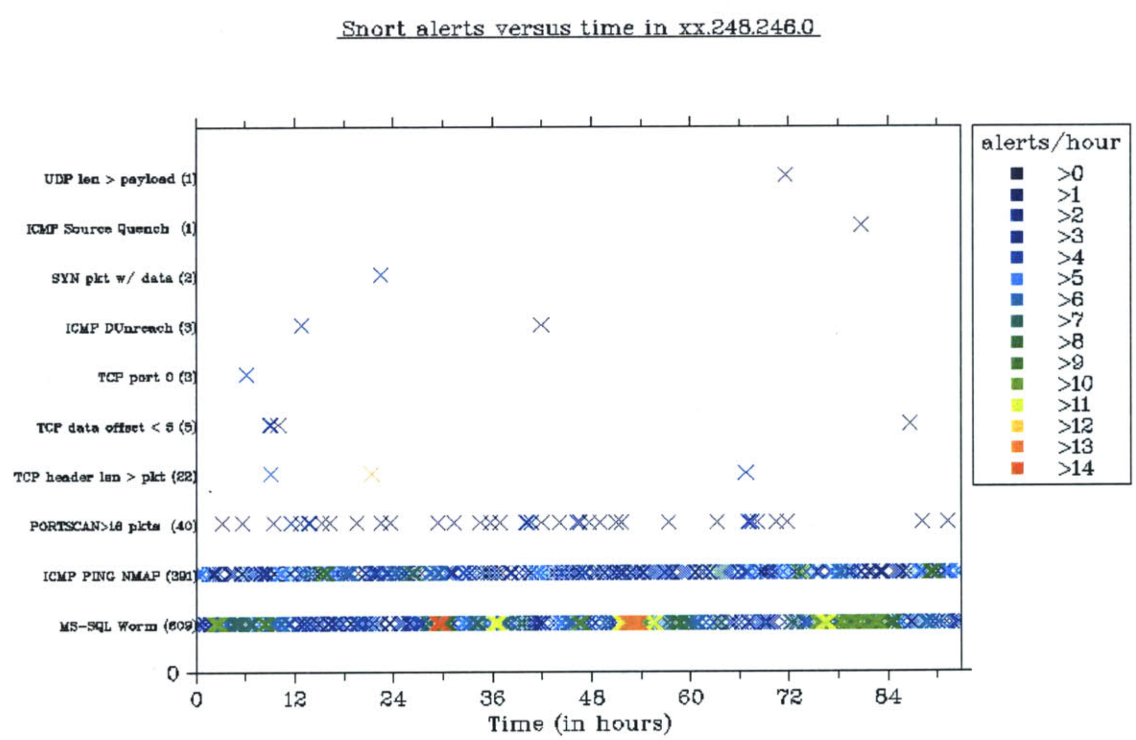

Figure B9-6 - Snort alerts versus time in 248.246C.

3382-90