A Novel Visualization Approach for Efficient Network Scans Detection

Zhang Jiawan[1], Li Liang[1], Lu Liangfu[1,2,*], Zhou Ning[1]
1. School of Computer Science and Technology, Tianjin University, Tianjin，P.R.China 300072;
2.School of Science, Tianjin University, Tianjin, P.R.China 300072
**Corresponding Author E-mail: liangfu79@tom.com*

Abstract

Network scans visualization provides very effective means for to detection large scale network scans. Many visualization methods have been developed to monitor network traffic, but all the techniques or tools still heavily rely on human detection. They seldom consider the importance of network event characteristics to the network data visualization, and cannot detect slow scans, hidden scans etc. In this paper a visual interactive network scans detection system called ScanViewer is designed to represent traffic activities that reside in network flows and their patterns. The ScanViewer combines the characteristics of network scan with novel visual structures, and utilizes a set of different visual concepts to map the collected datagram to the graphs that emphasize their patterns. Additionally, a new tool named Localport is designed for to capture large-scale ports information. The experiments show that ScanViewer can not only detect network scans, port scans, distributed port scans, but also can detect the hidden scans etc.

1. Introduction

Scanning a network is a very common step in a network intrusion attempt. In order to gain information about a potential network intrusion, it is beneficial to analyze these network scans. The process of scanning a network is usually performed in order to determine what exists on a network. Networks and systems are becoming increasingly more complex[1]. However, there is no absolute way to secure a network or system completely or indefinitely. All the current techniques or tools of securing a network or system still heavily rely on human detection. Most of them must have the user analyze and detect the anomalies or intrusions. Some visualization tools exist to detect scans recently [2-4]. Most of them concentrate on how to find novel visual structures. They seldom consider the importance of network event characteristics to the network data visualization, and they use visualization techniques only to the timing of network scans. They cannot detect the slow scans, hidden scans and spoofed scans etc.

In this paper a visual network scans detection system called ScanViewer is designed to represent traffic activities that reside in network flows and their patterns. The ScanViewer combines the characteristics of network scans with novel visual structures. The technique utilizes a set of different visual concepts to map the collected datagram to the graphs that emphasize their patterns. The global view and detail view interaction techniques are used in our system too. Additionally, a new tool, which we call it Localport, is designed to capture large-scale ports information. The new system can detect slow scan, distributed port scan and many kinds of TCP steal scan quickly and effectively.

The rest of the paper is organized as follows. Section 2 presents some of the related work in scanning visualization. We describe our approach in section 3, including details of data collection and processing, and their visualization. The features and design of the ScanViewer system is presented in section 4, and case studies in section 5. Finally, we give the conclusions and future work in section 6.

2. Previous work

Ultimately, the aim for all detection systems and tools is detecting as many attacks as possible. As the first step, all the users focus on the most popular intrusions for detection: port scans. Based on IP and the port number involved in the scans, there are three well known scan types: horizontal scan, vertical scan, and block scan [8].

The study of network scans has been popular for the last decade. Many research work has been done in

978-0-7695-3486-2/08 $25.00 © 2008 IEEE
DOI 10.1109/SecTech.2008.47

finding ways to work with the large numbers of alerts produced by various network scans detection tools using visualization. ScanVis [5] presents a means of facilitating the process of characterization by using visual and statistical techniques to analyze the patterns found in the timing of network scans. [6] uses a parallel coordinates technique to display scan details and characterize attacks. PortVis [7] contains three main frames: timeline, hour (main), and port, and the main visualization technique used is color map. But all these approaches focus on the novel visual structures detection of suspicious activity and not on the analysis of network event characteristics. The work presented here focuses on the combination the characteristics of network scans with novel visual structures. This make the new system effective in some difficult network scans detections such as slow scans, hidden scans etc.

3. The ScanViewer system

Network security visualization is a part of the larger field called information visualization. The main steps are data collection and processing, visual mapping, graphics generation. In this work, we focus on the above three steps. We will present the details of them for the design of system.

3.1. Data collection and processing

The current security visualization techniques require the data to be displayed as efficient as possible, and it can present sufficient amounts of information. Different security visualization techniques deal with their essence of high dimension data in different ways. There are always two primary sources of data as input for visualizations. Raw scan data captured by the tools such as tcpdump, is the first source. The second one is preprocessed netflow data. The netflow data is unidirectional stream of packets between a given source and destination, both of which are defined by a network-layer IP address and transport-layer source and destination port numbers. They can help the analysts reduce the amount of data, but they can not provide additional information for the visualizations. On the contrary, the raw scan data can provide the whole information for us, and it can help us obtain an intuitive understanding of network patterns. So in this paper we introduce two strategies to get raw scan data, which consists of router-level network traffic traces. Using windump to capture raw scan data is the one method, the other is using Jpcap. From our analysis, the latter is better for the filtering of data and the capture rules of data packets.

Though large amount of raw data makes it hard to be analyzed, and the real-time processing of large volume of traffic data becomes more difficult, we can use data reduction and filtering techniques to make the network traffic data more manageable. Thus, many scans are performed quickly and noisily using an automated tool or script. This kind of activity can be easily and automatically detected by monitoring a network stream for connections to many destinations in a small space of time. When a certain threshold of destinations per unit time is detected, it is usually a trivial task to extrapolate forwards and back wards in time to extract the entire scan. Of course, it is possible to miss a scan if it is being performed at a rate lower than the threshold, and also make a normal traffic as a scan if the threshold is low. According to the three principles of port scans detection: the time X of attack in time slot Y; connection with unopen ports; abnormal TCP flags. We can get datagram of TCP, UDP, ICMP protocols after filter the datagram of ARP、IGMP protocols which have few relations to the security information. Finally the data used in security visualization techniques are IP addresses, time, ports, protocols, connection information, TCP flags and so on.

3.2. Visual structures and interaction techniques

There are many security visualization techniques. Each has its unique way to display data. The most common techniques include: glyphs, color maps, parallel coordinate plots, histograms and scatterplots [10]. SeeNet[11] displays network traffic on a colored grid. Each point on the grid represents the level of traffic between a traffic source and a traffic destination. PortVis [7] produces visualizations of network traffic using 2D plots with time and port number as axes, and summarizing the network activity at each location in the plot (a time/port pair) using color. Users can drill down to display traffic information at finertemporal and port resolutions. VisFlowConnect [1] uses a simple application of parallel coordinates to display incoming and outgoing network flow data as links between two machines or domains. It also employs a variety of visual cues to help detect attacks.

Unlike previous systems, ScanViewer displays port activities by use of scatterplots, parallel coordinates, histograms and color maps. There are multiple levels of details. Scatterplots is used as a basic technique in the paper that combines nodes and lines to represent hosts with their connections. Parallel coordinates is a widely used technique for plotting high-dimensional data. The X coordinate in the gird is denoted by the different ports of one host, and the Y coordinate is denoted by the other host. This can enable the user to

visualize the correlation between the two hosts, the patterns that are generated. The histograms is used to be numbers of different types of datagram. It can help us easily find the scans. Different color maps shall one common ground and represent patterns in the paper.

Interaction is the key to performing deep analysis with ScanViewer. The technique contains two views: the global view and detail view. Each view provides different information in their display. In the global view, network flows are represented in multitude of lines. The nodes represent different hosts in the web.

From the visualization, we can easily find that the patterns of traffic data. The detail view in the paper provides the connection between ports of one host and another host. From this, we can see the attack easily on every host. So detail view provides a more precise and accurate view of data. Additional information can also be shown in the color of the nodes.

3.3. The design of ScanViewer

ScanViewer is designed to help Internet security experts inspect their netflow data visually and perform deep analysis. Figure 1 displays the framework of our ScanViewer. The first step is the data collection and filtering. We introduce two strategies, windump and Jpcap, to capture raw scan data. The information visualization framework is used and it is the key to ScanViewer. We use the famous MVC frame to design our system, and toolkits of information visualization [12] is used in the interaction techniques. Because the large-scale ports and hosts always change, a new tool named Localport is designed to get port. Figure 2 is the communication guidelines of the Localport.

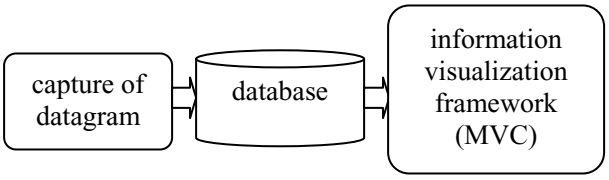

Figure 1. Three main modules of ScanViewer

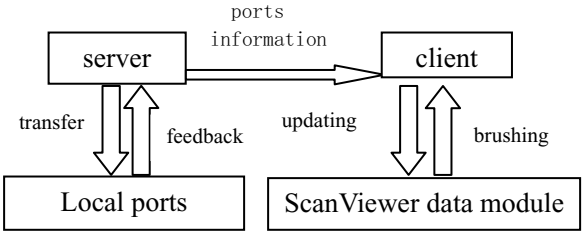

Figure 2.Communication guidelines of Localport

4. Case studies

In this section we describe several examples using ScanViewer to detect anomaly scans. ScanViewer can easily detect the ports scans in the local area networks. For example, Figure 3 is a visualization of two ports scans. As we all know, one host seldom has connection with all of the hosts in local area networks. But there are many connections between all of the hosts in 202.113.180.* and 59.67.33.124. The same is 202.113.188.164. So we can easily consider the 59.67.33.124 and 202.113.188.164 to be the attackers.
If we want to have a more precise and accurate view of data, we can use the detail view on two hosts. We can get the pattern: one host scans all of the open ports of other hosts, so this can be considered as ACK scans. The latter only scans 135 port of all the other hosts, so it is SYN half-open scans. Though the time slot of slow scan always is delayed, it can be quickly displayed on our ScanViewer. Figure 4 show the patterns of slow scans. One host sends many datagram to another host though its ports are unopened. If we do further analysis, we can find that the flags are SYN flags. So they are SYN scans. Most of current tools can not find the patterns when there are few datagram. ScanViewer can quickly and effectively displays the patterns though there is only one datagram. From Figure 5, the red histograms show the numbers of datagram of different types. Figure 5 displays that there are 215 FIN datagram. They are FIN hidden scans.

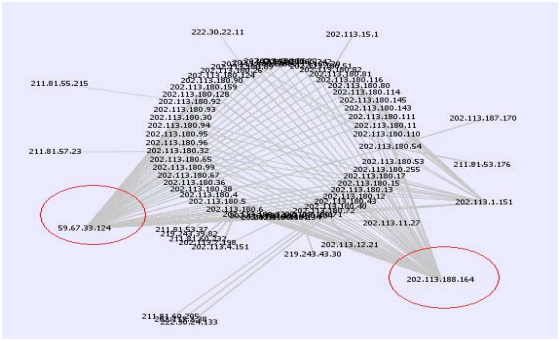

Figure 3. Pattern of network scans in ScanViewer

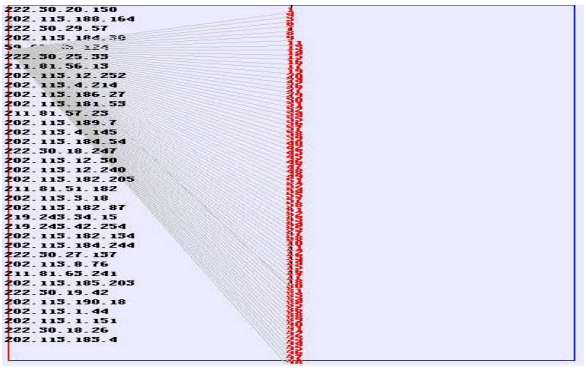

Figure 4. Pattern of port scans in ScanViewer

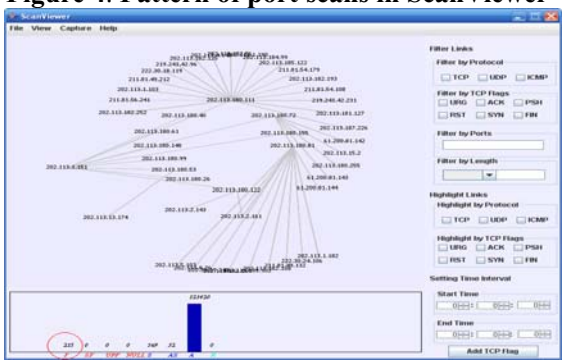

Figure 5. Pattern of hidden scans in ScanViewer

5. Conclusion and future work

In this paper a visual interactive network scan detection system called ScanViewer is designed by combining the characteristics of network scans with novel visual structures. We have demonstrated that ScanViewer can not only detect network scans, port scans, distributed port scan, but can also detect the hidden scans. Additionally, a new tool has been designed to capture large-scale ports information. In future work, we plan to introduce more visual mappings and more interaction techniques , such as linking and brushing techniques, it will greatly increase the usability of ScanViewer.

6. Acknowledgments

This work has been supported by National Natural Science Foundation of China under Grant No.60673196； Natural Science Foundation of Tianjin, P.R. China, under Grant No. 07F2030.

7. References

[1]X.Yin, W. Yurcik, et al. (2004). "VisFlowConnect: NetFlow Visualizations of Link Relationships for Security Situational Awareness." *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*. Washington, DC, USA, ACM Press.

[2]R.F.Erbacher. "Visual traffic monitoring and evaluation". *In Proceedings of the Conference on Internet Performance and Control of Network Systems II,* 2001,pp 153–160.

[3]L.Girardin and D. Brodbeck. "A visual approach for monitoring logs".*In Proceedings of the 12th Usenix System Administration conference*, 1998, pp 299–308.

[4] C. Muelder, Kwan-Liu Ma and Tony Bartoletti, "A Visualization Methodology for Characterization of Network Scans", *Visualization for Computer Security*, 2005, pp.29-38

[5]C.Muelder, , Ma, K.L., Bartoletti, T.: A visualization methodology for characterization of network scans. Visualization for Computer Security, IEEE Workshops, pp. 4 – 4 (2005)

[6]G.Conti,Abdullah, K.: "Passive visual fingerprinting of network attack tools". *VizSEC/DMSEC ' 04: Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security, 2004*,pp. 45 – 54

[7]J.McPherson, ,Ma, K.L., Krystosk, P., Bartoletti, T., Christensen,M.: Portvis: "A tool for port-based detection of security events". *In: ACM VizSEC 2004 Workshop,* 2004,pp. 73 – 81

[8]Pin Ren, Yan Gao and Zhichun Li, "IDGraphs: Intrusion Detection and Analysis Using Histographs", *Visualization for Computer Security,* 2005, pp.39-46

[9]K. Stuart Card, Jock D. Mackinlay and Ben Shneiderman, *"Readings in information visualization: using vision to think",* Morgan Kaufmann Publishers, 1999

[10] Rawiroj Robert Kasemsri, "A Survey, Taxonomy, and Analysis of Network Security Visualization Techniques"：[Master Paper], USA，Georgia State University, 2005

[11] Richard A. Becker, Stephen G. Eick, and Allan R. Wilks. "Visualizing network data". *IEEE Transactions on Visualization and ComputerGraphics*,1995 1(1):pp. 16–28.

[12] Prefuse: http://www.prefuse.org/

[13]Mukosaka, S.;,Koike, H., "Integrated visualization system for monitoring security in large-scale local area network *Visualization"APVIS '.2007 6th International Asia-Pacific Symposium,* 2007,pp.41– 44

[14]Musa,Shahrulniza,Parish,etc."Visualising Communication Network Security Attacks", *Information Visualization[J].IV '07. 11th International Conference*, 2007,pp.26-733