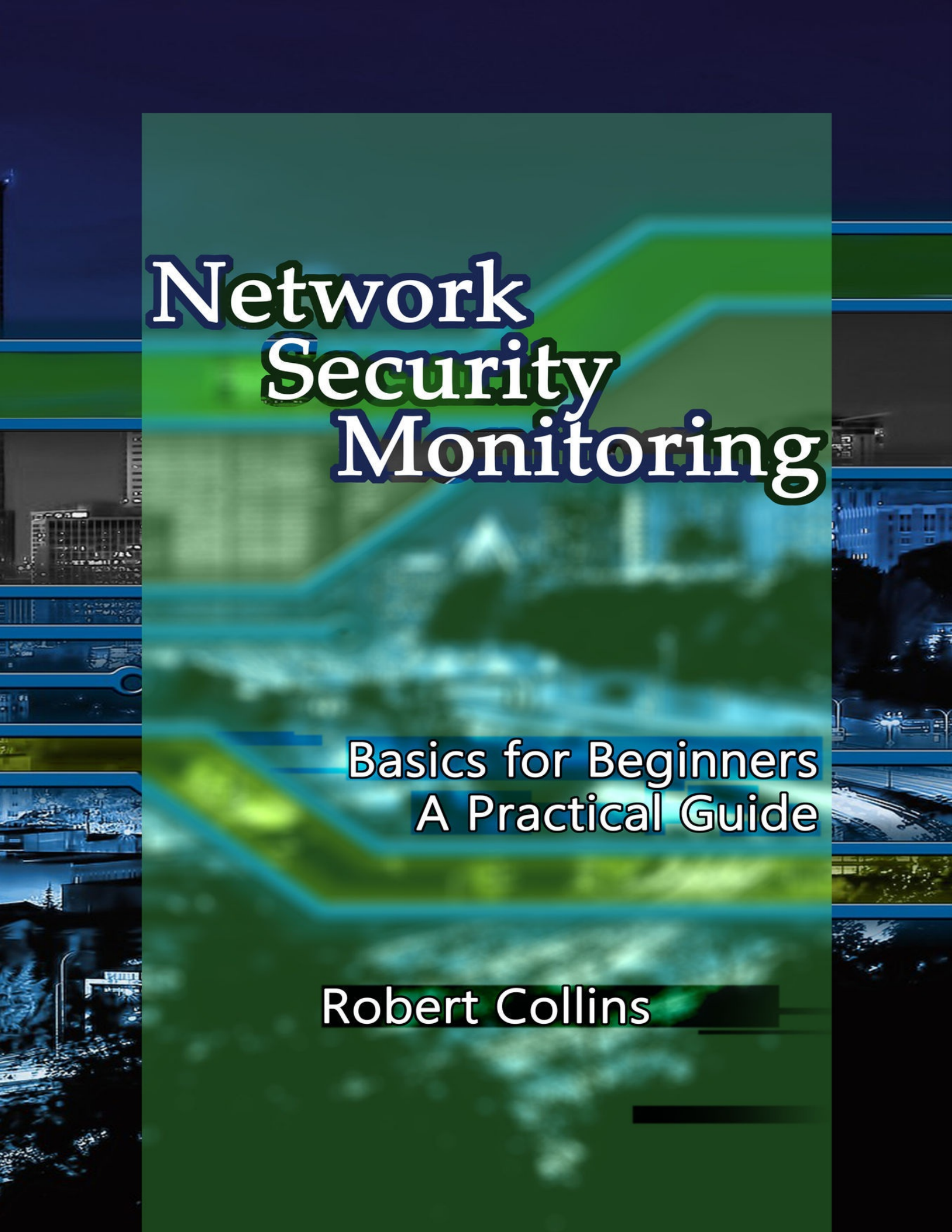
Network Security Monitoring
Basics for Beginners
A Practical Guide
Robert Collins

Network Security Monitoring

Basics for Beginners

A Practical Guide

Robert Collins

Table of Contents

Disclaimer

While all attempts have been made to verify the information provided in this book, the author does assume any responsibility for errors, omissions, or contrary interpretations of the subject matter contained within. The information provided in this book is for educational and entertainment purposes only. The reader is responsible for his or her own actions and the author does not accept any responsibilities for any liabilities or damages, real or perceived, resulting from the use of this information.

The trademarks that are used are without any consent, and the publication of the trademark is without permission or backing by the trademark owner. All trademarks and brands within this book are for clarifying purposes only and are the owned by the owners themselves, not affiliated with this document.

Introduction

Every organization has data. Some data is very sensitive, so that if it leaks to the public, the operations of the organization may have to be terminated. A good example is a banking institution. If the information about the bank customers leaks to the public, they may leave the bank and go to another bank. This data is normally transmitted over the network. Without proper network security, attackers may modify this data when it is in transit. There is a need for each organization to monitor its network and identify any network security loopholes. Such loopholes should be closed immediately when they are discovered. Any attempt to attack an organization's network should be detected as early as possible and the appropriate action taken. This book guides you on the various ways one can monitor a network's security.

Chapter 1- Network Monitoring Basics

Initially, networks were flat, meaning that they only had a small number of elements. Everything on a network is now connected to a complex design using elements such as wireless, cloud, remote users, IoT (Internet of Things), mobile devices, VPN, etc.

With this evolvement, there is a need for network monitoring. With network monitoring, the network administrators are able to know what is happening or going on in their network, may it be a WAN, VoIP, LAN, MPLS, or other types of connections. The network administrator can also discover the state of the network elements such as routers, servers, access, distribution and core switches, firewalls, client systems, and others.

Before we can dive into network monitoring, it is good for you to have a basic understanding of networking and networking elements. You should also know the essentials of the Windows operating system which is widely used across enterprises in the world. With a good knowledge about networking and the network elements, it becomes easy for you to understand network security monitoring and management.

What is networking?

A network refers to a connection of many devices which are capable of communicating with one another via a communication protocol common transport. Communication in this case can refer to the exchange of data between users or the exchange of instructions between the network nodes. The nodes can be computers, output devices, mobile devices, servers, management elements, switching and routing devices.

Networks are normally categorized according to size of area that they span, and they can be a LAN, WAN, or the Internet. Also, the topology or the design of a network differs from one organization to another depending on the requirements of the organization, and this can be star, mesh, ring, bus

the requirements of the organization, and this can be star, mesh, ring, bus, or other types of network topologies.

Whatever the network design that is used, each network adheres to a reference design described in an OSI model for communication and data transmission. The OSI (Open Systems Interconnection) is a reference model for networks which describes how information flows from an application installed on a system or device through the nodes in the network to some other device located in the same network or in an external network. A number of components take part in facilitating communication between various nodes in a network, including transport and communication protocols, network addresses, as well as the methods which facilitate the transfer of packets within a network or between different networks.

Below are the basic networking elements which form the basis for network monitoring:

1. IP address and subnetting
   The IP address refers to the reference label which is assigned to network nodes, and other network nodes use this label when they need to locate and communicate with the node. The IP addresses are binary numbers, but they are usually written in a form readable by humans, either IPV4 or IPV6 address. The elements on a network which have been assigned an IP address can be divided into smaller sub networks depending on the type of the device, its location, its access, etc. Note that all the devices residing in the same subnet share a common prefix in their IP addresses.

2. Switching and routing
   Switching is the process through which data is divided into small packets before it can be sent and transported over a network. Routing is the process of finding the path through the network for transmission of a packet from source node to destination node located in a different network.

3. DNS (Domain Name System)

Other than is the IP address, each element contained on a network can have a reference name? Research has shown that people easily remember names compared to numbers. With DNS, people can use reference names for communication instead of numbers which are hard to remember. The purpose of DNS is to resolve the name to an IP address or the IP address to a name. For example, once you type www.facebook.com on your browser, the DNS will translate it into the necessary IP address so as to locate the server.

4. DHCP (Dynamic Host Configuration Protocol)
   This is a network protocol which allows the DHCP server (the management server) to assign IP addresses to the network hosts dynamically. If it were not for DHCP, the network administrators will have to assign the IP addresses to the hosts manually and this would bring much difficulty as far as the management of IP addresses is concerned.

Basic Windows Monitoring Elements

There are various business applications installed on the servers of a datacenter or enterprise network for provision of services to organization's hosts. There are also additional services for managing the network and users, which include DHCP, DNS, Active Directory, and others and these are provided from the servers. The organization users also need a computer operating system. Among all the available computer operating systems, Windows-based operating systems are commonly used in both the servers and hosts of organizations.

There are various business applications which run on servers, and this calls for monitoring of resource usage such as disk space, memory, CPU, cache, and so on. With monitoring, one can also identify issues which might be affecting the performance of the servers. The client devices should also be monitored so that the end-users do not experience issues when using them.

The systems based on Windows can provide data to the monitoring systems which will then process the data and report any issues related to the health of the servers and the host machines. Below are some of the ways through which the monitoring data can be collected from the Windows machines:

1. Performance counters
   The Microsoft Windows Server comes with OS performance counters which are enabled by default. Such counters will provide the data related to system performance such as data on memory, cache, processor, disk, etc. Such data can be used by the server performance monitoring applications.

2. Windows Management Instrumentation (WMI)
   This is a Microsoft feature which allows for the access of management information about statuses of computer systems. This feature also supports actions such as configuration and changing of the system properties, scheduling processes, permissions, and others. This feature can be used to manage both servers and the host machines running locally or remotely.

3. Eventlog
   The Windows OS usually generates a number of event logs which normally shows the events which occur on a system such as application events (example, data loss or problems with performance), security events (security log tempering, failed logon attempts, and attempts to access the secure files) and system events. Such logs can be monitored by use of a monitoring system so as to determine any issues with the server and client systems.

Basic Monitoring Tools and Protocols

In this section, we will be exploring the basic monitoring techniques and tools which are commonly used by the network administrators. For you to be able to monitor your network or the servers, you should have the

be able to monitor your network or the servers, you should have the following:

1. Data or information from the various network nodes. The data should have details such as the current status and performance as well as the health of the element which is being monitored.

2. The monitoring software should be able to process, collect, and present the data in a format which is readable. The software should also be capable of alerting or notifying the users in cases in which it senses some danger somewhere within the system.

3. A protocol should exist which should facilitate the transfer of information between the element which is being monitored and monitoring software.

Once the information has been collected from the network, it can help in management and control of the network, identification of any issues to do with the network before they can result into a downtime and a quick resolution of problems when something goes wrong. With constant monitoring of the network, the organization will stay safe and the network will have a better performance.

Below are some of the basic tools which can be used for network monitoring:

1. Ping
   This is a tool for network administration used for testing the availability and reach ability of a host running on an IP network. The data obtained after running this utility can tell whether a particular network host is active or not. It can also give information about data loss and transmission time from one host to another.

2. SNMP (Simple Network Management Protocol)
   This is a protocol for network management used for exchange of information between the hosts running on a network which is using a

information between the hosts running on a network which is using a network monitoring software. It is the common protocol for use in

monitoring of networks and some of its components include the following:

- Managed Device- this is the network node which supports SNMP and the access to the specific information.

- Agent- this is software program which is part of a device under monitoring. The agent is capable of accessing the Management Information database (MIB) of this device and it will allow the SNB to read and write data to MIB.

- NMS (Network Management System)- this is an application running on a system which monitors and controls managed devices via an agent by the use of SNP commands.

The SNP data is usually collected or sent to the managed device by use of either traps or polling. With traps, the agent is allowed to send information to the NMS about the events on device. The MIB usually holds the information about the structure of data on the device for management. The MIB should have the object identifier (OID) which identifies the variable which is to be read from your device or be set on the device.

3. Syslog
   This refers to a message logging system which allows a device to send event notifications in the IP networks. The information obtained from such messages can be used for the purpose of managing the system and security auditing. There are a number of devices which support syslogs, including firewalls, printers, and routers.

4. Scripts
   Some networks lack NMS, which can be used for monitoring. In some other networks, the available NMS does not have some functionality. There could also be a need to extend the functionality of the available

NMS. In such cases, the network administrators can use scripts. Such scripts usually make use of common commands such as ping, lynx,

netstat, snmpwalk, etc. These commands are supported by most networking elements for performance of actions such as collection of data from networking elements, implementing changes to the device configurations, or performing tasks which are scheduled. Perl and Bash scripts are some of the scripts commonly used by the network administrators.

Chapter 2- Packet Analysis

When using a tool named Wireshark, it is possible for you to capture the packets being transmitted on a network in real time and then display them in a format readable by humans. The tool includes color coding and filters, as well as other tools which can help you explore the network traffic and inspect the packets.

In this chapter, you will know how to capture packets, filter, and inspect them. You can use the wireshark tool to inspect the network traffic of a suspicious program analyze how the traffic flows in your network and troubleshoot any problems with your network.

Getting Wireshark

You can visit the official Wireshark website and download the tool for either Windows or Mac OS. For those using a Unix-like operating system such as Linux distros, Wireshark can be obtained from the package repositories. If you are using Ubuntu, for example, you can find the Wireshark tool in the Ubuntu software center. Note that a number of organizations do not allow this tool to be used into their networks, so avoid using it in your company network, as it can cost your job.

Capturing the Packets

Once you have downloaded and installed the Wireshark tool, just double click so as to open it. Double click on the name of the network interface below Capture so as to begin capturing the packets on the interface. For example, if your aim is to capture the packets traversing your wireless network, then click on the wireless network interface. If you need to configure it for advanced settings, you can click on Capture -> Options. After clicking on the name of the interface, you will observe the packets begin to appear in a real time fashion. The Wireshark tool will be able to capture all packets leaving your system as well as those entering your

capture all packets leaving your system as well as those entering your system.

In case the promiscuous mode is enabled, noting that it comes enabled by default, you will be able to see all the packets on the network other than those which have been addressed to your network adapter. If you need to verify whether this option is enabled, just click on capture -> Options, and then check to see whether the checkbox for “Enable promiscuous mode on all interfaces” has been checked or not. This can be found at the bottom of the window.

If you need to stop the traffic capturing process, then click the red button labeled “Stop” and the top left corner of the window.

Color Coding

The packets you see will be highlighted using different colors. In Wireshark, colors are used to help you differentiate the different kinds of traffic. By default, the light purple color is used to mark TCP traffic, light blue to mark UDP traffic, while black marks packets with errors, for example, the packets might have been delivered while out of order.

If you want to know the meaning of the color codes, click on View -> Coloring Rules. You may also choose to modify the coloring rules, and it is possible for you to do it from here.

Filtering Packets

You might need to monitor something specific, such as the traffic which a program sends while phoning home, in which case it will help you to close all the other applications which are using the network so that you can narrow down the traffic. Despite this, you will have many packets for you to sift through. The Wireshark filters come to help in this case.

The easiest way for you to apply a filter is for you to type it into filter box found at the top part of the window, and then presses Enter or clicks on

found at the top part of the window, and then presses Enter or clicks on Apply. For example, if you type dns, you will only see the DNS packets.

Wireshark will also help you by auto completing your filter once you begin to type it.

You may also choose to click on Analyze -> Display Filters so as to choose the filter you need from the default ones which are provided by Wireshark. It is also possible for you to add your own filters and save them so that you can be able to access them with ease in the future.

You can also right click on a packet and then choose Follow -> TCP Stream. After that, you will be in a position to view the full conversation between client and server. If you need to have a view of the other conversations, just click on the protocol you need from the Follow menu. Close the window and the filter will be applied automatically. The Wireshark tool will show you all the packets which make up the conversation.

Packet Inspection

You can click on a packet so as to choose it and dig down so as to view its details. It is possible for you to create filters from there. Identify one of the details, right click it, and then use the submenu for Apply as Filter so as to create the filter based on that.

Wireshark is a very powerful tool. Most professionals use the tool so as to debug the implementations of network protocols, inspect internals of network protocol, and inspect any problems with network security.

Chapter 3- Detecting the Heartbleed Bug

The Heartbleed protocol usually runs on the top of the Record layer protocol, which is defined in the SSL (Secure Sockets Layer). The Heartbleed bug occurs in some OpenSSL versions implementing the Heartbleed protocol. The bug is a serious vulnerability which normally allows attackers to be able to read big portions of memory, including passwords and the private keys during the Heartbleed response.

Heartbleed Wireshark Filter

The Heartbleed protocol usually runs on the top of the Record layer which is identified as the record type (24) in SSL/TLS. When using Wireshark, we can use the "ssl.record.content_type == 24" display filter so as to show the Heartbleed message. The Heartbleed messages include the Heartbleed Request and the Heartbleed Response.

Heartbleed Wireshark Analysis

Launch the packet capture file named "heartbleed.pcap" in the Wireshark. The display filter should then be set to "ssl.record.content_type == 24." The Wireshark will only display the heartbleed messages which have been encrypted. The first one will be the Heartbleed Request message. In the message, the length of the Heartbleed message, that is, sl.record.length == 112, is normally set to 112 bytes.

After sending a Heartbleed Request message to the server, the server responds with a Heartbleed Response message.

If you find the length of the Heartbleed response, that is, ssl.record.length == 144, has been set to 144, it is an indication that the server has returned more data than it was expected to, that is, 32 more bytes will be returned. The extra information is the one known as Heartbleed. Note that the bleed may have very sensitive information such as private keys and passwords

may have very sensitive information such as private keys and passwords.

Testing for Heartbleed

The following are the steps necessary for one to test for Heartbleed using the Woreshark software:

1. Install the OpenSSL version (1.0.1c) from openssl library. You can do this by running the following command:

   openssl version

2. Create a self-signed SSL certificate by running the following two commands:

   openssl req -sha256 -new -newkey rsa:2048 -nodes -keyout ./server.key -out ./server.csr -subj "/C=PU/ST=Anish/L=Test/O=Security Analysus /OU=Heartbleed/CN=host_name.com"

   openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.pems

3. Launch the TLS server by use of the OpenSSL version which has been affected:

   openssl s_server -www -cipher AES256-SHA -key ./server.key -cert ./server.pem -accept 443

4. You can then begin to capture the packets:

   tcpdump port 443 –s0 –w heartbleed.pcap &

If the SSL/TLS server can be reached through a public network, you can use an online flippo. There are also other tools which can be used for this purpose, for example, Heartbleed Detector.It is recommended that patches should be applied to the OpenSSL as advised. After addressing the vulnerability, make sure that you change the

Chapter 4- Session Data

Session data refers to the summary of the communication between any two network devices. It can also be referred to as a flow or conversation, and it can help in network security monitoring. However, when compared to packets, session data only provides fewer details for network security monitoring, but it is very useful to network security specialists. With session data, you can learn which individuals took part in a communication, their location, and the times they communicated.

Flow or session records are usually generated. Such records usually include the source and destination IP addresses the source and destination ports, a timestamp which shows the time the communication started and the time that it ended, and the amount of the data which was transferred between the communicating devices.

A flow record refers to many packets aggregated together. The aggregation in this case can be done differently based on the kind of tool being used.

Collection of Session Data

There are different ways which one can collect session data. A collector and a flow generator must be used regardless of the kind of method applied. The flow generator refers to the software or the hardware which generates the flow records. This can be done by collection of the network data directly from the network interface or by parsing some other data. The flow collector is the software responsible for receiving the flow records from the generator, and storing them in a format which is retrievable.

The best way for one to generate session data is by capturing it directly from the wire. This is the same way that NIDs alert data or FPC data is generated. It can be done by use of a software program running on a server, or by use of a network device such as a router.

Generation using Hardware Devices

In some cases, it is possible for you to leverage the hardware that you have and generate some version data. You are only expected to configure a router by adding the network address of the destination collector. The router should have the flow enabled. After that, the flow records from the interface of the router will be forwarded to the destination.

Generation using Software

There are numerous advantages of using software for flow generation, and this is why most network security monitoring experts rely on software for the generation of flows. One of the advantages is that software deployment is very flexible. The processing of adding a software program for generating the flow on a network is easy compared to changing the network layout so as to add a router to help in generating the flow.

For one to use software to generate flows, a daemon must be executed on the sensor responsible for collecting and forwarding the flow records depending on a specific configuration. The data which passes through the software will be used to generate the flow.

Yet Another Flowmeter (YAF)

This is a tool for generating flow, and it provides an IPFIX output. It was designed to be used in the generation of records to be used with SiLK. The YAF offers a bidirectional flow and is good for keeping up with the increasing bandwidth. With YAF, you can also use IPFIX template architecture together with the SiLK application labels so as to get a more refined analysis. The installation of this tool is easy, but it will be good for you to first read its documentation.

Fprobe

This tool is available in most Linux distribution repositories. One can use package management systems such as apt and yum so as to install it on a sensor. If your sensor location does not have outside network connections, you can compile and then install the package manually. Once the installation is completed, you have to initiate it. You just have to run the fprobe command together with network location and the port you will be directing the flow data to.

Example:

Suppose you need to generate flow data on the eth1 network interface, and then send this to the collector running on the host 172.168.160.1 and listening on port 2880, the following command will help you achieve this:

fprobe -i eth1 172.168.160.1:2880

Collection and Analysis of Flow Data

The System for Internet-Level Knowledge (SiLK) is good tool for analysis of security across computer networks. It can be used for collection of flow data. The tool can also be used for storing, accessing, parsing, and displaying the flow data. It provides network security analysts with a way to parse the flow in an efficient way, without using scripts which are CPU intensive.

The SiLK has two components, namely the analysis suite and the packing system. The packing system provides a way through which the SiLK collects and then stores the flow data in a manner which is a consistent and native format. Packing refers to the process of compressing the data into a binary format which is space efficient so that it can be passed through the analysis suite of SiLK. The SiLK's analysis suite is made up of a collection of tools

suite of SiLK. The SiLK's analysis suite is made up of a collection of tools good for filtering, sorting, displaying, grouping, counting, mating, and

more. The tools come with a great level of flexibility. All of these tools are powerful, but you can pipe the outputs from various tools to another depending on what you want.

For you to be able to use this analysis feature, you should pass data from the flow generator to it. Once the records have been received, they are separated in a logical manner depending on type of flow.

A tool known as rwflowpack is used to parse the flow type, determining the sensor where the data is coming from and adding the flow data which has been parsed into the database. Other tools within the analysis toolset can then parse the flow from there. The configuration details for the tool are contained in a file named rwflowpack.conf. For you to initiate the tool, run the following command:

service rwflowpack start

If all the configurations are okay, the tool will show you the verification screen.

Using Rwfilter for Filtering

Consider the command given below:

rwfilter --any-address = 1.2.3.4 --start-date = 2017/06/09:08 --end-date = 2017/06/09:13 --type = all --pass = stdout | rwcut

Note that we have narrowed the frame time to what we need. In the command, we need to know the extent of harassment by the host with the IP address that you specify.

Chapter 5- Application Layer Metadata

When doing network security monitoring, there are two types of data on which we rely on the network layer, and these are session data (Netflow) and full content data (PCAP). These two types of data can be easily generated if the sensor placement is okay and one can get good value from the data.

The Netflow is the session data which shows details about network traffic including "who, when, what, and where." With this type of data, one can get a lot of value without experiencing a disk overhead. The majority of commercial firewalls and routers usually generate Netflow, but one can also use tools such as SiLK for the purpose of generating Netflow. However, note that Netflow does not give a complete picture of the data, and that is why it is mostly used to complement the full content data.

Full Content Data (PCAP)

Our previous type of data, that is, Netflow, can be seen to be similar to call logs. The PCAP, or the full content data, can be seen to be similar to having the full recordings of all the calls.

This type of data has become very universal and there are several tools, both commercial and open sources, which can be used to collect it. Examples of such tools include Tcpdump, Dumpcap, Wireshark, and others. Most intrusion detection systems such as Snort normally use the full content data. PCAP data is very helpful to analysts, as it provides them with the highest level context during the investigation of an anomaly. However, it has a disadvantage that one experiences a high disk overhead when relying on full content data and this is deterrence to a number of organizations from collecting and using this type of data. Also, if you don't find the specific thing you are looking for in a specified range, locating things can be difficult, and this can make analysis inflexible.

Application Layer Metadata

When you are monitoring network security, you can realize that most of the traffic is formed by application layer data from a number of common protocols. Examples of such protocols include HTTP, SMTP, SSL, and DNS.

It is easy for you to save some disk space from any data that you don't want. There are a number of ways through which you can do this. You can use Tcpdump so as to read the PCAP data, and you will get ASCII formatted data and store it in a file. The Unix strings command can help you to read the binary data that you are unable to read. You can then apply timestamps to your data and format it so as to look prettier.

With such a bash script, you can generate the application layer metadata in the form of a packet string, or the PSTR file. The script should run as a cron job and parse the generated PCAP files continually so as to generate the accompanying PSTR files. Once you have the application layer metadata, you can use it in different ways.

Using PSTR as a Data Source

Our initial goal of generating the PSTR file was to get a way of generating a data format with low disk overhead and one capable of providing value to analysts as a data source for network security monitoring. Let us discuss some of the use cases of the PSTR in network security monitoring:

Malware Infection

Suppose you receive a notification from the intrusion detection system that the internal system has received some symptoms of an infection. The cause of this might be a signature detecting a malicious GET request which is associated with a botnet C2 server. After examination of the host, the GET request appears to match the result of a signature which fired, so one can know with certainty that there was an infection of the box.

know with certainty that there was an infection of the box.

After a further examination, you may find the infected host sent an HTTP POST with a unique string. This is a sign of malicious activity, but none of your signatures fired on. Through the use of the GREP command, one can find similar occurrences of this string in the HTTP header data for the traffic on the monitored networks. With PSTR data, you can easily find the infected boxes in the networks being monitored.

Targeted Phishing

Your users may receive a suspicious email, specifically targeting your company. In such a case, they have to contact the security team of your company. The email might ask the employee about their payroll information, and prompt them to login using their employee ID and password.

Once you examine the email carefully, you notice that it has been sent from a spoofed email address and the subject line used is almost unique for each recipient. The emails may have been sent over a close duration. First, you should determine the individuals in your organization who have received the email. You should then warn them not to click the link provided in the email and determine why they were chosen from the many employees in the organization.

For instance, you can choose to search through Postfix and Exchange logs and see if it is possible for you to find the recipients. Your organization should provide adequate logging and a proper retention of those logs. However, with string, it is hard for one to query the data sources. When using PSTR data, it is possible for you to create a regular expression which will match the semi-unique subject lines and then execute a query which will provide you with the results.

Using PSTR for Detection

The PSTR file can be used for second level detection. With second level

The PSVR file can be used for second level detection. With second level detection and analysis, we refer to movement past near real-time detection

to a point in which the analysts begin to review traffic retrospectively so as to find the things the signature doesn't match. In most cases, this involves an anomaly and statistical based detection using large data sets. PSTR is perfect in doing this.

User Agent

Each HTTP header has the user agent field, and it can help in detecting malware infections in networks. In most malware, a custom value is used in this field, and this normally deviates from the standard browser identifying strings. Most of the security techniques deployed to detect such malware infections rely on the IDS/IPS signatures.

However, this has a problem in that the rate at which malware is generated is faster, making it hard to detect them. Due to this, there are numerous user agents which have not been detected. Some of the malware agents also make use of user agent strings which are generated randomly, making it hard for one to write enough signatures to be detected.

You can write a simple script to parse the PSTR data for a site, get all the user agent strings, and then sort how unique they are. There will be several occurrences of Explorer and Firefox user agents, but you will notice there are some user agents who occurs a handful of times and they are not related to any browser. When such user agent strings are well analyzed, you will realize that they have been infected with malware.

E-mail Subject

It is also possible for us to do an analysis of the subject line of an email. You can create a user agent parsing code so as to look at the PSTR data so as to look for the email subject lines which are related.

The good thing with the application layer metadata is that it can be easily stored, and one can easily search through it. You can also do the following

stored, and one can easily search through it. You can also do the following with this data:

1. Search for the unique values with DNS, SMTP, HTTP and SSL headers. This calls for you to sort the unique values within some specific fields and then identify any additional outliers which need an additional investigation.

2. Byte entropy of some fields. You can perform entropy calculation on both the GET and POST requests so as to locate the encrypted data so as to find the one which is not located where it should be.

3. Checking field lengths for anomalies
   With a statistical analysis, you can find that there are some fields whose length falls within a particular range. With this, it will be easy for you to flag any outliers, that is, fields which are too short or too long, and you will be able to find anomalies in them.

4. Enumerating the Downloads for some types of files
   With this, you can choose to list all files of a particular type, example, PDF or executable files, which have been downloaded within a particular time span. This can be achieved by the analysis of the HTTP headers within the PSTR files.

Chapter 6- URL Search

You can search for a URL (uniform resource locator) by use of network traffic as the data source. A URL string is just a subset of URI (Uniform Resource Identifier) which specifies the location of an identified device and the mechanism which can be used to retrieve it.

The difference between a URL and a URI is that a URI may have some additional information such as an anchor link used by the client side for an automatic navigation to a section of a web page.

Mostly, a search for a URL involves searching for a full or partial name of a website so as to know the person accessing it.

Building the Search URL

There is a need for a more sophisticated analysis and more visible Internet links. This is due to security concerns, rich activity visibility, and continuous monitoring. Also, most of the applications which are used across organizations are hosted by organizations externally; hence there is a need to use such links.

Before searching for the URL strings, a data source is needed. Some of the common data sources include the following:

1. Capturing packets on a local laptop or PC.
2. Capturing packets on the network through mirror ports, SPAN, or TAPs.
3. Analyzing log files on proxy servers or firewalls.

Local Packet Capture

You can capture packets on your local laptop or PC and use them to learn more about packet capture as well as how to use them to search for the URL

strings. This can be best done by use of Wireshark, which is a good tool for you to use for capturing network traffic as it enters and leaves network adapters on a PC or laptop.

If you need to search for a URL, you can use display filter in Wireshark so as to search for a specific text string. We will not go into more details about this, as we discussed how to do it previously.

However, you can easily overload the system in case you begin to capture the traffic at very high data rates. If you need to store data for the long term, there is a need for extra disk storage. It is also very complex, making it hard for one to read and interpret.

Network Traffic Capture with Mirror Port or SPAN or Mirror

TAPs or SPAN ports can help those who need to scale up from local network traffic capture. With this approach, you will be able to capture all the network traffic flowing in and out of your network. With this approach, you will get a data source for all the web activity happening on your network.

You should begin by setting up a SPAN port and then use a tool such as NetFort LANGuardian for the processing of the packet data. The NetFort DPI engine is responsible for extracting application level details such as the URL strings from traffic flows. The remaining details of the packets will be removed before they can be stored in the database which comes built-in.

The data reduction feature is very useful for a long life and historical storage of user and network activity, and this is very useful in planning, reporting, and forensics. All critical information such as user name, IP addresses, URI, domain names, and the bandwidth consumed will be stored in the database. This way, one is able to access historical and real-time web usage reports. If you are considering using other types of tools

time web usage reports. If you are considering using other types of tools,

then ensure that the tool supports historical and real-time reporting features so as to match the data retention abilities that you need.

Analysis of Log Files on Proxy Servers and Firewalls

Most proxy servers and firewalls provide logging options. These become very useful when one needs to check if any changes made to the firewall rules are working or not. However, the server log files have a number of limitations associated with them. The purpose of the log files is to provide the administrators with information regarding the server behavior but not the user information such as the URLs that they access.

This technique is very useful if you need to check whether any changes made to the block rules are functioning or not. However, note that once you enable logging, the performance of the proxy or firewall will be impacted. The devices were not designed to capture information for the long term. Also, if your proxy or firewall develops some performance issues, you will not be in a position to access the logs so as to troubleshoot the issue.

Chapter 7- Intrusion Detection and Prevention

Intrusion detection refers to the process of monitoring the activities taking place on a network and checking them for any signs of violations, incidences, or imminent attacks. Intrusion prevention refers to performing the intrusion detection and stopping any detected incidences.

Each business network has several access points to the other networks, and these access points can be either private or public. There is a big challenge for any business to maintain a secure network while at the same time keeping it open to its customers. Most of the network attacks are sophisticated, and they are able to thwart any security mechanisms, especially those relying on encryption and the use of network firewalls. The use of encryption and network firewalls alone is not enough for an organization to have a secure network.

The IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems) usually monitor the network constantly, identifying any possible incidences and logging information regarding them. Such incidences are then reported to the network security administrators. Some organizations rely on the IDS/IPS systems so as to identify any problems with their security policies and prevent people from violating these policies. These systems are becoming very popular in most organizations due to their ability to detect attackers, deter them from attacking the network, and report it to the security administrators.

How IDS works

There are three IDS detection methodologies which can be used for detection of incidences. These include the following:

1. Signature Based Detection
   This method compares the signatures against the observed events so as to identify any possible incidences. It forms the simplest form of

as to identify any possible incidences. It forms the simplest form of intrusion detection, since it only compares the current activity unit

such as a log entry or a packet to a signature list, by the use of string comparison operations.

2. Anomaly Based Detection
   This detection technique compares the definition of what is known to be a normal activity with the observed events so as to identify any significant differences. It is a very good technique for detection of any threats which are previously unknown.

3. Stateful Protocol Analysis
   This technique compares the predetermined profiles of the generally accepted definitions for a benign protocol activity for every protocol state against the observed events so as to detect any variations.

Implementation of Signature Based Detection with Snort

In this section, we will discuss how one can implement a signature based intrusion detection system. We should begin by installing some network security tools including BASE, Snort, and TCP Relay.

Snort is simply a system for network detection and intrusion, and the tool is open source. You can use this tool to analyze traffic and data flow in real time as it flows on your network. The tool is also capable of checking traffic analysis and detecting various types of attacks. The tool uses a rule which is written by a user so as to analyze the packets. Such rules can be written by the use of various languages, and modification of the same is also easy. In the case of buffer overflow attacks, the snort tool is capable of detecting the attack by use of the patterns of the previous tools, and then takes any action so as to prevent the attack from occurring. In signature based intrusion detection, if an old attack occurs, the system is able to detect the pattern, but if a new attack occurs, it can be a challenge to detect it. However, the Snort rule can overcome this by analyzing the traffic in a real-time manner. If a new packet come into the network, and the performance of the network

If a new packet come into the network, and the performance of the network

goes down, the packet is discarded and its details are stored in the signature database.

The Snort tool is made up of the following components:

- Packet Decoder
- Preprocessors
- Detection Engine
- Logging and Alerting System
- Output Modules

The patterns for intrusion attacks are well known, so they are encoded properly and then used to match the user behavior.

The packet decoder is responsible for collecting the packets from different interfaces and sending it to the preprocessor or the detection engine. The preprocessor is responsible for arranging the packets in a way before they can be sent to the detection engine for analysis. The detection engine usually finds if an intrusion activity exists in the packet. Once the activity is found, then an alert is raised or it is logged by the logging and alert system. By default, the logs are kept in the folder /var/log/snort, but one can use the –l option so as to change the location of the command. The output modules are responsible for saving the output obtained from the alert and logging system according to the operations that the user wants to perform on the output.

The Structure of Snort Rules

The Snort rules are created by the known intrusion signature system. The rule is normally divided into two parts, namely the rule header and the rule option. The rule can be modified according to the need. The rule header has to follow the following pattern:

Action + protocol + source address+ S-port + direction +

Action + protocol + source address + S-port + direction + destination address + D-port

Alert ip any any -> any (msg : "IP Packet Detected ";)

One can use an intrusion detection system so as to protect the network. The system can be deployed within hosts, switches, or server firms. In this case, we will be placing the Snort tool between hosts.

Setting up the System

We will be using a Debian operating system running on a Linux box so as to detect any intrusion attempts into our system placed in the network. If Snort detects an intrusion attempt, it will generate an alert.

Installing the Components

We have to install Snort, BASE, and Postgresql database. In Debian, configurations must be made for BASE (Basic Analysis and Security Engine) and Snort-pgsql so that the user can be provided with a user-friendly web front user interface for analysis of the Snort alerts. One should also configure the Postgresql database, Apache Http server, Secure Shell, and the PHP.

Begin by downloading the Snort-pgsql. The following are the installation steps:

1. Begin by downloading the Snort-pgsql from the Snorts official website. The following command can help you achieve this from the terminal:

   dpkg -i snort-pgsql_2.8.5.2-8_i386.deb

2. Install the following from the synaptic:

   postgresql-8.4(server)
   postgresql-common
   postgresql-client-common

postgresql-client-8.4

3. Next, create the Snort database:

   # su postgres
   $ createdb database_name(snortdb)
   $ zcat /usr/share/doc/snort-pgsql/create_postgresql.gz | psql snortdb(database_name)
   $ createuser -P user_name(snortuser)

Next, create a password for your new user. In the next prompts, type n for No.

4. Next, log into your database:

   $ psql snort

5. Grant all the privileges to the Snort user on all the tables and the preferences:

   psql>grant all privileges on database snortdb to snortuser;
   psql>GRANT ALL ON TABLE data, detail, event, icmphdr, encoding, iphdr, opt, reference, reference_system_ref_system_id_seq, schema, reference_ref_id_seq, reference_system, sensor, sensor_sid_seq, sig_class_sig_class_id_seq, sig_class, sig_reference, signature, signature_sig_id_seq, udphdr TO snortuser, tcphdr;

6. Edit the database.conf file:

   # getit /etc/snort/database.conf
   add a line

   output database: alert, postgresql, user=snortuser password=snort-password dbname=snortdb host=postgresql-host-ip

7. Edit the snort.conf file:

   getit /etc/snort/snort.conf After the line that reads: #var HOME_NET any
   Add line
   var HOME_NET host-ip-address

8. Next, you have to configure the postgresql. Open its configuration file:

   # gedit /etc/postgresql/8.4/main/postgresql.conf

Search the line with the directive for listen address and then set the IP address of the host which is running the Postgresql database. Make sure you uncomment it:

listen_addresses = postgresql-host-ip

Next, run the following command to open another configuration file:

 # gedit /etc/postgresql/8.4/main/pg_hba.conf

Find the line:

host all all 127.0.0.1/32 md5

Then add the following below it:

host snortdb snortuser snort-sensor-host-ip/32 password

Restart the Postgresql so as to apply the changes you have made:

/etc/init.d/postgresql restart

```
/etc/init.d/postgresql restart
```

Configuration of Snort

1. Use etho to launch Snort in an interactive mode:

   # snort -i etho -c /etc/snort/snort.conf

2. For you to check whether all the needed services are running as expected, run the following command:

   # ps -ef |grep <SERVICE>

The <SERVICE> in this case can be apache, snort, postgresql, etc. You can test to see whether the database is logging the alerts by sending some suspicious traffic to the Snort sensor host. You can use a tool such as nessus or nmap to do this.

 # su postgres
$ psql snort -c "select count (*) from event"

Once you send some suspicious traffic then you execute an SQL query, you should get a value which is increasing.

Setting up the BASE Pre-requisites

Install PHP 4 or 5, Apache 2, the PGP adodb library, and the PHP GD extension. There are various configuration options whose specifics can be known from their documentation.

 # apt-get install apache2 libapache2-mod-php4 php4-gd php4-pgsql libphp-adodb

Create a file named test.php in the /var/www/ directory and add the following to it:

```
<?php
phpinfo();
```

?>

Open the file /etc/php4/apache2/php.ini and then ensure that the following lines are added and uncommented:

Extension = pgsql.so
extension = gd.so

Restart the Apache 2 so as to enable the PHP scripts which have been installed:

 # /etc/init.d/apache2 restart

Open your browser, and then open the URL: **http://web-server-ip-address/test.php.** This should give you all the information regarding your system, PHP, Apache, postgres, and gd.

Next, you should install and then configure BASE. Begin by downloading it, making sure that you download its latest version. Login as the root user and then run the following commands so as to add the BASE to the /var/www/base directory:

 # mv base-1.2.tar.gz /var/www/
 # cd /var/www/
 # tar xvzf base-1.2.tar.gz
 # rm base-1.2.tar.gz
 # mv base-1.2 base
 # cd /var/www/base

You should then copy the file named "base_conf.php.dist" to "base_conf.php" so that if you do anything wrong, you can begin from the start:

 # cp base_conf.php.dist base_conf.php

 # vi base_conf.php

We should then adjust a number of variables. If you need to have a user authentication system, then don't forget to add a user before you can set it to 1:

$Use_Auth_System = 1;(you will be prompted for Login and Password)

$Use_Auth_System = 0;(The BASE will be opened directly in the browser)

$BASE_urlpath = '/base'; $DBlib_path = '/usr/share/php/adodb';

$DBtype = 'postgres';
$alert_dbname = 'snortdb';
$alert_host = 'postresql-host-ip';
$alert_port = '';
$alert_user = 'snortuser';
$alert_password = 'snort-password';

Since we have no archive database, we can set the following to zero:

$archive_exists = 0;

Open the base_main.php page in a browser. If there are any database changes which are required, the BASE will prompt you for an action. Click the "Setup page" so as to open the DB configuration page, that is, configuration page, that is, base_db_setup.php.

Click the buttons for "Create BASE AG." The purpose of BASE tables is to add the tables which will extend the Snort DB so as to support BASE functionality.

If you have not installed the PEAR:: Image-Graph, just install it. The installation can be done by running the following command:

 # apt-get install php-image-graph

We need the PEAR::Image_Color, but you may have to install it based on the version of Linux distribution you are using. This should be installed in the /usr/share/php/Image/. The following commands will help you achieve this by setting the proxy first:

pear config-set http_proxy
http://Login:Password@192.20.4.254:80
 # apt-get install php4-pear
 # pear install Image_Color

Depending on the version of BASE you are using, there could be a bug in /var/www/base/base_qry_common.php. This can prevent the display of graphs. To solve this is, just doing away with the empty line which occurs immediately after "?>". You will be done with the installation process!

When sending traffic from one host to another, Snort should be running. The TCP relay can help achieve this. We can also use Snort so as to send the packets and check for alerts in the BASE. To relay the traffic, we can use either TCP Relay or Snort.

TCP Relay

The TCP Relay is a suite of Unix system utilities which can be used to edit and replace network traffic, and such traffic is usually captured using tools such as tcpdump or wireshark/ethernal. With the tool, one can classify the traffic as either client or server, edit the packets at layers 2-4, and then replay the traffic at an arbitrary speed onto the network through a device for sniffing. The process takes three steps as follows:

1. Determine the packets which are server->client and the ones which are client->server.

2. Rewrite the IP addresses according to their direction.

3. Send the packets through an inline device.

3. Send the packets through an inline device.

We can use tcpprep so as to split the traffic according to source/destination port. The following command can help us achieve this:

$ tcpprep --port --cachefile=example.cache --pcap=example.pcap

With the above, all the packets which are directed to a UDP or TCP port <1024 will be considered to be client->server, while the rest will be considered to be server->client. The information will then be stored in a tcpprep cache file named example. Cache so that it may be used later.

The tcprewrite command can be used for the purpose of changing the IP addresses to a local network. The following command demonstrates this:

$ tcprewrite – endpoints=192.29.14.50:192.20.14.48 --cachefile=example.cache --infile=example.pcap --outfile=new.pcap

In the above command, our aim is to have traffic appear as if it is between the two IP addresses. One of the IP addresses should be the client, while the other should be the server, and we have used the cache file which we created previously.

We can then use the trcpreplay command so as to send the traffic through intrusion prevention system (IPS). This is shown below:

 # tcpreplay --intf1=eth0 --intf2=eth1 --cachefile=example.cache new.pcap

Our aim is to split the traffic between the two interfaces, that is, eth0 and eth1. We have used the cache file and the new.pcap which we have created in our previous step. The cache file can be used for various pcap files because even though the IP addresses might have changed, the semantics and order remain the same.

Using Snort

Using Snort

We have to pass the name of the tcpdump file and the alerts will be seen in the BASE.

$ snort --pcap-single=outside.tcpdump -c /etc/snort/snort.conf

The outside.tcpdump will test the DARPA dataset. It is the one which facilitates the generation of alerts in BASE.

Chapter 8- Security Onion

This is a Linux distribution used for network security monitoring, intrusion detection, and log management. The distribution is based on Ubuntu and it comes with Suricata, Snort, Sguil, Bro, Snorby, Squert, NetworkMiner, Xplico, ELSA, and other tools for network security. With Security Onion, you are able to monitor your network so as to discover security alerts. The platform is very simple, and you can run it on simple platforms.

In this chapter, we will guide you on how to set up a Security Onion, configure Snort, and then use Squil for management and viewing of alerts. I will have two network cards, one for monitoring and the other one for management. The monitoring interface will be connected to a SPAN port (network mirroring) on a switch.

Installation of Security Onion

1. First, begin by downloading Security Onion. You can use a direct link from source forge.

2. Security Onion is based on Ubuntu 64-bit. If you are installing it on a VMWare, then ensure that you choose the 64-bit architecture.

3. After booting the system for the first time, then choose the option for a live system. You will be able to play around with the system. You can also install the system directly into the hard drive once the system boots.

4. When you get ready to install the system, choose the install script on desktop. This will take you through some steps and you will be able to permanently install the system.

5. You will also be asked to choose the way you need to partition your hard drive. If you are running a virtual machine, just allow the install to format the hard drive and use it completely. You should also

remember the username that you choose for your system. The system doesn't cache the usernames during the reboots.

6. You may also want to encrypt your home folder, so feel free to choose that option.

7. Security Onion will then try to put the interface in a monitoring mode so that it can monitor the security events. The native operating system may ask you to allow this to be done.

Once the installation process completes, you will be asked to reboot the system. Once the system reboots, you will be expected to reboot both the Ubuntu and the Security Onion components. You can move to the menu bar, and then click "Check for updates." After the process runs completely, move to the menu bar and then click "Install all updates." Note that you may have to do this for several times so that you can have all the updates installed. Again, after a complete installation of all the updates, just restart the system.

For those using the Security Onion on VMWare, install the VMWare tools, but this is optional.

You should ensure that you are logged in as the root user. The Security Onion components should be updated. The update will be done to the security tools and scripts running inside the platform. The standard Ubuntu package management tools can help you to update all the packages.

There is a possibility that you will be prompted to update both the PF-RING and the kernel packages at once. This is not good, as the former may only be installed for the current kernel as opposed to the newly created kernel, and the services may fail during a reboot. The best way is to install only the PF_RING kernel module on its own, and then install the kernel and other modules which you might need. The following onliner will help you achieve this:

sudo apt-get update ; sudo apt-get install securityonion-pfring-module ; sudo apt-get dist-upgrade

However, if you had installed the packages at once and the Snort and Suricata services fail, go ahead and re-install the securityonion-pfring-module package. Use the following command:

sudo apt-get install –reinstall securityonion-pfring-module

Note that the use of sudo –i provides me with root privileges.

Security Onion Setup

1. Move to the desktop the double click the install script.

2. Enter the root password, and then choose "yes" so as to configure the network interfaces.

3. The next step will be for you to choose the management interface. This is the interface with an IP address, and it will be used for management of the system.

4. The next step will be for you to configure the interface for DHCP or static IP settings. Mostly, you will have to configure the static IP addresses. If you need to use DHCP, well and well.

5. In the next step, you will have to configure the monitoring interface. The security tools will use this interface so as to monitor the network traffic. Once done, you will be prompted to reboot the system.

6. After the reboot, click the setup icon found on the desktop.

7. The network setup has already been completed, so you may skip it.

8. The installation of the Security Onion can be done either as a Quick Setup or Distributed option, and you will have to choose one. Choose the Quick Setup option.

9. You will then be prompted to choose the network interface which is

9. You will then be prompted to choose the network interface which is being monitored. Choose the right one.

10. Next, you will be asked to create a username which you will be using so as to log into the system and use Squert, Sequill, and the ELSA tools.

11. Next, you will be prompted to provide an email address, which is the username which you will be using so as to log into Snorby. Next, you will have to create a password. Note that only alphanumeric passwords are accepted.

12. Enable the ELSA. The configuration of the security onion tools will be completed.

You will then have completed the installation of the Security Onion.

How to use Security Onion

You should begin by updating the Snort rules in the Security Onion. Launch a new terminal while ensuring that you are logged in with root privileges. You can use the sudo –i command so as to change to the root. Use the following command so as to update the rules:

/usr/bin/rule-update

In this step, you should launch the Snorby. You only have to double the Snorby icon which on your desktop. Use the email address and the password which you created previously so as to login. At this point, you may not see many alerts. Navigate to the "Events" menu bar, and you will be able to see some traffic.

Note that the alerts you will get should be based on the Snort rules. It is possible for you to disable or modify the rules. You can create security incidences based on the rules.

You have not setup the Security Onion, or configured Snort for data monitoring, and you are now using Snorby to view the alerts.

monitoring, and you are now using Shorby to view the alerts.

Conclusion

This is the end of this book. At this point, you should be acquainted with various network security monitoring techniques. Each organization should monitor its network so as to ensure that they are secure. Organization data should remain safe and secure and it should only be accessed by the authorized individuals. The sensitive organization data should not be allowed to get to the public or the competitors. If an intruder gets access into the organization network, then any data being transmitted over the network may be modified. Network security monitoring helps an organization detect and prevent such attacks. There are various ways through which an organization can monitor the security of its network.