Making Everything Easier!™

Lancope Special Edition

Incident Response with NetFlow

FOR DUMMIES®

A Wiley Brand

Learn to:

- Use NetFlow security monitoring to accelerate incident response
- Combat emerging cyberthreats and address IT trends with NetFlow
- Put together an effective incident response team, process, and toolkit

Compliments of

Lancope

VISION TO SECURE, INTELLIGENCE TO PROTECT™

Mike Chapple, Ph.D.

Lancope®

VISION TO SECURE, INTELLIGENCE TO PROTECT™

Lancope, Inc. is a leading provider of network visibility and security intelligence to defend organizations against today's top threats.

By collecting and analyzing NetFlow, IPFIX, and other types of flow data, Lancope's StealthWatch® System helps organizations quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats. Through pervasive insight across distributed networks, including mobile, identity, and application awareness, Lancope improves incident response, streamlines forensic investigations, and reduces enterprise risk. Lancope's security capabilities are continuously enhanced with threat intelligence from the StealthWatch Labs™ research team and its business partners.

Lancope helps organizations:

- Achieve complete network visibility and security intelligence
- Accelerate incident response and forensic investigations
- Detect and resolve advanced threats
- Reduce operational and enterprise risks

www.lancope.com

Incident Response with NetFlow

FOR DUMMIES®
A Wiley Brand

Lancope Special Edition

by Mike Chapple, Ph.D.

FOR DUMMIES®
A Wiley Brand

Incident Response with NetFlow For Dummies,® Lancope Special Edition
Published by
John Wiley & Sons, Inc.
111 River St.
Hoboken, NJ 07030-5774
www.wiley.com

ISBN 978-1-118- 88341-9 (pbk); ISBN 978-1-118- 88378-5 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgments

Some of the people who helped bring this book to market include the following:

Project Editor: Jennifer Bingham
Acquisitions Editor: Amy Fandrei
Editorial Manager: Rev Mengle
Business Development Representative: Melody Layne
Custom Publishing Project Specialist: Michael Sullivan
Project Coordinator: Melissa Cossell

Introduction

Network flow records provide a valuable source of information for security analysts seeking to respond to security incidents and implement other controls. I hope that this short book will get you started with NetFlow for incident response and whet your appetite for more information about this cutting-edge technology.

About This Book

Incident Response with NetFlow For Dummies, Lancope Special Edition, explains how NetFlow works, and shows how it can improve your organization's security controls.

This book takes you through the basics of NetFlow analysis for incident response purposes: the changing nature of incident response, what data sources you might use to assist with incident response, and how NetFlow can contribute to your response efforts.

It also provides you with pointers that you can use to align your incident response processes with industry-standard practices and tells you how you can use NetFlow to enhance your technical capabilities. The contents of this book were provided by and published specifically for Lancope.

Icons Used in This Book

The margins of this book sport several helpful icons that can help guide you through the content:

When I present something that can save you time and effort, I toss in this icon to highlight it.

This bit of info is worth remembering. No need to tattoo it on your forearm or anything, just keep it in mind.

This icon flags information to take note of because it could cause problems.

Chapter 1

The Changing Nature of Incident Response

In This Chapter

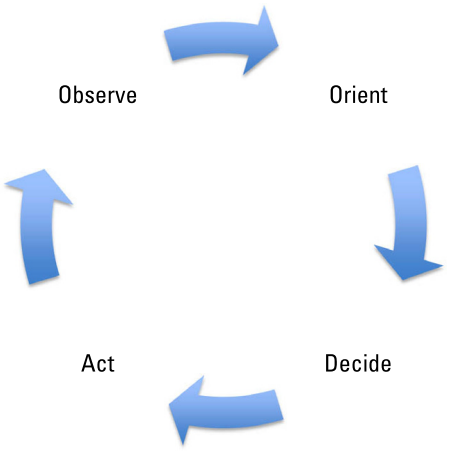
- Discovering the OODA loop and how it can guide incident response efforts
- Understanding the importance of audit trails in incident response
- Identifying the purpose of NetFlow and the role it may play in incident response
- Choosing audit sources

Security incidents are critical times for information security professionals. The minutes and hours following the first identification of a security incident can have a dramatic effect on the incident's severity and impact. In these stressful moments, it is important that incident responders have both access to critical information and a well-defined process to guide their actions.

In this chapter, I explore how a process known as the OODA loop can guide decision-making during incident response efforts, discuss the importance of audit trails in gathering critical information during an incident, and explain the role that NetFlow information plays in responding to security incidents.

Incident Response and the OODA Loop

Incident response professionals should embrace a process known as the OODA (which stands for observe, orient, decide, act) loop. The loop, shown in Figure 1-1, was originally developed by U.S. Air Force Colonel John Boyd as a model for fighter pilots to use when making quick decisions in the heat of armed conflict. It lends itself quite well to the fast-paced environment of incident response, which also requires rapid decision-making.



Source: Lancope, Inc.

Figure 1-1: The OODA Loop.

Incident responders may use each phase of the OODA loop as a guide in handling urgent security situations. Responders should consider the following questions in each phase:

- **Observe**: What is happening? What evidence exists and what is it telling us?
- **Orient:** Is there a bigger picture? Do environmental circumstances exist that might explain unusual observations?
- **Decide:** In light of your observations and the environment, what action should you take next?
- **Act:** While you're taking action, do you observe any effects of that action on the situation? Are other changes occurring that may require analysis?

Note that the questions asked during the *act* phase are actually aligned with the *observe* phase — this is the reason that the process is a loop. When you take action, you reach the end of one OODA iteration, but also begin the cycle anew, possibly resulting in additional action.

Importance of the Audit Trail

The first question asked during the incident response process, "What is going on?" is a critical question that requires information about past activity on systems and networks. An incident response process usually begins because someone observed an unusual symptom, such as network congestion, systems rebooting, or a defaced website. Incident responders normally turn first to records of recent activity, known as the *audit trail*, to explain the observed symptoms.

Audit trails consist of the log entries made by a variety of systems and devices during their normal course of activity. These log records often come from firewalls, intrusion prevention systems, Security Information and Event Management (SIEM) systems, and network devices.

Firewall logs

Firewalls serve as the border checkpoints of your network, controlling the types of traffic that are allowed to enter and leave your secured perimeters. This provides them with a unique perspective where they may observe, and log, every attempted and successful network connection that crosses the border.

The logs created by firewall devices provide important information to incident responders attempting to reconstruct a security event. Connection records provide insight into the inbound and outbound connections that may carry traffic related to the incident.

When relying on firewall logs for your audit trail, be sure that you configure the firewall to log *all* traffic, whether permitted or denied. Many firewall configurations only log traffic that is denied because it violates the firewall policy.

Intrusion prevention systems

Intrusion prevention system (IPS) technology plays an important role in protecting networks and systems against malicious activity. Network IPS devices monitor all traffic crossing a network segment, searching for signatures of malicious activity. Host-based IPS software may also run on individual systems, screening the traffic that reaches the system before allowing the system to act on it.

When an IPS identifies suspect traffic, it creates a log event recording the activity and, if configured to do so, will block the traffic from entering the network or system. Records from both host and network types of IPS technology are valuable components of the audit trail because they create a record of suspect activity that may be useful to analysts responding to security incidents.

Log management and SIEM

Many enterprises now rely on log management systems to collect and correlate the abundant sources of security information in their environments. These systems collect information from various operating systems, applications, and devices and store it for later analysis.

Some systems, known as SIEM systems, have advanced capabilities that include performing correlation of events from multiple sources. SIEMs contain logic that allows them to identify potential security incidents in progress and notify incident responders to take appropriate action.

Remember that log managers only capture and analyze the audit trail information that is sent to them. You must take steps to ensure that systems throughout your network are properly configured to send relevant log entries to the centralized collection point.

Network traffic

Incident response often requires knowing the types of traffic that occurred on a network during the incident. This may include summarized details of network connections contained

within NetFlow records or the packet payload contents obtained from a full packet capture. The remainder of this chapter covers the role of NetFlow in incident response.

Although full packet capture can provide important information about the actual contents of network traffic, it is impractical to capture full packets on an ongoing basis. I discuss the reasons behind this difficulty in Chapter 5. Full packet capture often comes into play after analysts detect an incident. If the incident is still in progress as the response effort begins, security professionals may deploy full packet capture on a just-in-time basis to capture and analyze incident-related traffic.

The tradeoff between NetFlow information and full packet capture is one between the richness of the content and the disk space required to retain the information. Furthermore, the cost to deploy full packet capture throughout the network can be cost prohibitive and expensive to store. Moreover, capturing packet-level data introduces a host of privacy concerns for the organization, which require additional governance and risk management measures.

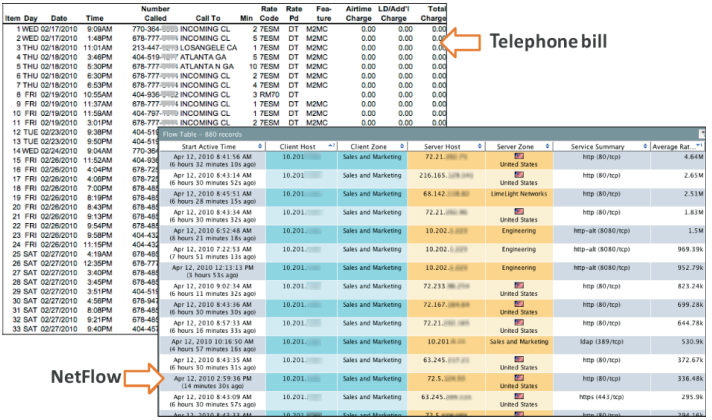
NetFlow's Role in Incident Response

NetFlow records are one of the most powerful information sources available to incident responders. They're capable of summarizing information about network traffic into brief records that may be maintained indefinitely, providing a running history of network connections that may be referenced during incident response.

What is NetFlow?

NetFlow is a feature built in to many network devices manufactured by Cisco, Juniper, Palo Alto, SonicWALL, and others. It captures basic information about every conversation that takes place through the monitored device, including the identities of the systems involved in the conversation, the time of the communication, and the amount of data transferred.

You might think of NetFlow records as a phone bill for your network, as shown in Figure 1-2. It can't tell you *what* was said on your network, but it gives you a good idea of who was talking and how much they said. NetFlow provides information about the "conversations" that take place on your network similar to the information phone bills provide about voice conversations.



Source: Lancope, Inc.

Figure 1-2: How NetFlow provides you with information similar to a phone bill.

Take a moment to think about the potential applications of these records. In addition to the obvious network diagnostic and maintenance uses of this data, NetFlow information can also be a critical tool for security analysts trying to identify anomalous activity or reconstruct the sequence of events when responding to an incident.

NetFlow records provide a rich source of data for security analysts to mine. Some of the most commonly used data elements generated by NetFlow include:

- Source IP address
- Destination IP address
- Source port
- Destination port

- Protocol
- Timestamps for the flow start and conclusion
- Amount of data passed

These are only a small sampling of the many data fields available to NetFlow analysts.

IP address information included in NetFlow records depends on the perspective of the NetFlow collector. If the collector is behind a firewall or other device using Network Address Translation (NAT), the true source IP address may not be available. With the right input data set, some NetFlow collection engines do provide NAT stitching capabilities to address this issue.

Take a look at Table 1-1 to see some of the different flavors of NetFlow that are available.

Table 1-1 NetFlow versions

NetFlow Version	*Benefits*	*Drawbacks*
V5	Defines 18 exported fields Fixed and compact format Most commonly used and supported	IPv4 only Fixed fields, fixed length fields only Single flow cache on exporter
V9	Template-based IPv6 flow data transported in IPv4 packets MPLS and BGP nexthop supported Defines multiple fields, including L2 fields Reports on flow direction	IPv6 flow data transported in IPv4 packets Fixed length fields only Uses more memory Slower performance Single flow cache

(continued)

Table 1.1 ***(continued)***

NetFlow Version	*Benefits*	*Drawbacks*
Cisco Flexible NetFlow Feature (FNF)	Template-based flow format (built on V9) Supports flow monitors (discrete caches) Supports selectable key fields and IPv6 Supports NBAR data fields	Less common Requires more sophisticated platform to produce Requires more sophisticated system to consume
IP Flow Information Export (IPFIX) aka NetFlow V10	Standardized – RFC 5101, 5102, 6313 Supports variable length fields, L7 fields can be exported Can export flows via IPv4 and IPv6 packets	Even less common Not widely supported

Sampled flow data and incident response

NetFlow records provide an extremely accurate accounting of the communications that take place on a network. This accurate recordkeeping requires that the NetFlow device analyze the details of each packet and fold it into the ongoing accounting of each connection. In many cases, this level of accuracy isn't needed, because the needs of network administrators may be met with approximations of the amount of data passed and they may be willing to miss some shorter communications.

Sampled flow data uses a "1 in *n*" approach to flow data. The NetFlow exporter simply samples every *n*th packet and includes the data from that packet in the NetFlow records.

Although sampled flow data may be appropriate for performance troubleshooting and other network administration tasks, it is *not* appropriate for incident response purposes. Incident responders need to be able to reconstruct *all* network traffic, not just a representative sample.

Where is NetFlow information available?

NetFlow data is available from a wide variety of sources, including both traditional NetFlow-enabled networking and security devices and special-purpose NetFlow collection appliances.

Traditional NetFlow

Although NetFlow was originally created by Cisco for use on their routers and switches, the networking community quickly adopted it as an Internet standard and many manufacturers now support NetFlow. Some of the major platforms that allow direct export of flow records include:

- Cisco routers and switches
- Cisco ASA firewalls
- Juniper routers and switches
- Citrix NetScaler
- Blue Coat PacketShaper
- Palo Alto Networks next-generation firewalls
- VMware vSphere

This is a small, representative list of the manufacturers and devices supporting NetFlow data collection. If you're using different devices on your network, consult with the manufacturer(s) to determine whether they're NetFlow-compatible.

If you're not running the current firmware on your network device, check whether upgrades are available. Many vendors added NetFlow support to their devices after the initial release, and a firmware upgrade may be all you need to get up and running.

NetFlow generation

In some cases, security analysts may not be able to gain access to NetFlow data from the organization's network devices. This might be because the devices aren't capable of generating NetFlow exports, network engineers are unwilling to provide access to those records, or concerns exist about the overhead introduced on the networking device.

If this is the case in your organization, you may wish to consider the use of dedicated NetFlow exporters to collect the same information — sometimes enhanced with application performance metrics. These devices can be attached to the network in the following ways:

- Switched Port Analyzer (SPAN)
- Mirror port
- Ethernet Test Access Port (TAP)
- Installed as a virtual machine on VMware ESX server

Although purchasing a NetFlow exporter will require an additional investment in hardware or software, you can gather the same NetFlow information without modifying your network configuration.

Choosing Audit Sources

Security professionals seeking to design an audit trail infrastructure to support incident response have a wide variety of log sources at their disposal. When selecting the mix of audit sources that will support a broad range of security incidents, they should combine records related to system, network, and security device activity that will paint a full picture of the state of the computing environment.

Although many log sources contain information about network activity, only NetFlow records are capable of providing a ledger of each and every transaction that takes place on a network over an extended period of time.

Chapter 2

Examining Trends Addressed by NetFlow

In This Chapter

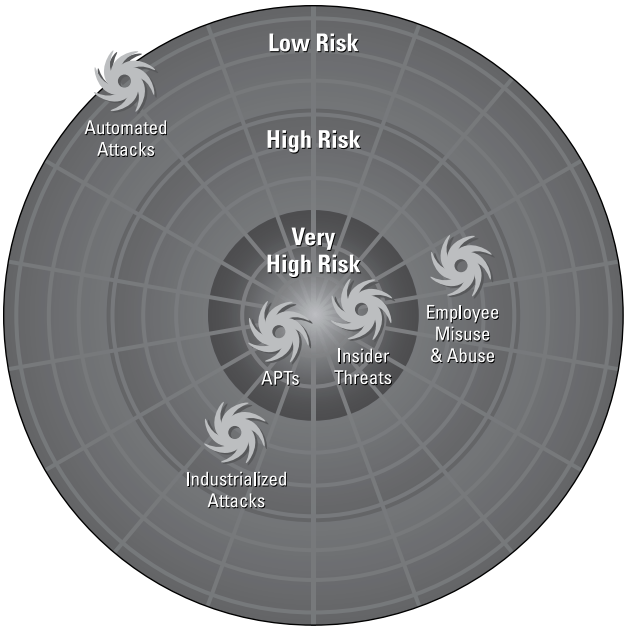
- Understanding the risks posed to enterprises by the evolving threat landscape
- Exploring the security impact of IT consumerization, mobility, virtualization, and cloud computing
- Learning to adapt NetFlow usage in the face of evolving network technologies such as IPv6 and SDN

Today, incident responders turn to NetFlow as a tool to inform the response they make to security incidents. In this chapter, I look at the trends driving the adoption of NetFlow as an incident response tool.

Evolving Threat Landscape

The nature of information security threats has changed dramatically over the past few years. As shown in Figure 2-1, the familiar automated attacks of worms and viruses have given way to more advanced and insidious threats.

Several threats warrant particular attention from security analysts: the advanced persistent threat (APT), the insider threat, malware/zero-day threats, and distributed denial-of-service (DDoS) attacks.



Source: Lancope, Inc.

Figure 2-1: The evolving threat landscape includes two very high risk items: advanced persistent threats and the threats posed by insiders.

Advanced persistent threats

Advanced persistent threats are targeted attacks against a particular organization. An attacker might single out a company, government agency, or even an individual who has desirable information or resources and use advanced, stealthy attack techniques to slip in under the radar and carry out an attack.

APTs are especially insidious because they're carried out by determined attackers with the time and resources to deliberately target an organization. Security practitioners previously associated APTs strictly with government agencies engaged in cyberwarfare, but now these attacks are affecting a wide range of organizations around the world

Don't underestimate the risk of APTs against your organization. In a recent Ponemon Institute study, 83 percent of respondents believed that their organization was the target of an APT. State-sponsored attackers are now targeting a wide range of corporate and government entities to carry out cyberespionage.

APT1: State-sanctioned threat?

In February 2013, Mandiant released an investigative report entitled "APT1: Exposing One of China's Cyber Espionage Units," concluding that APT1 "is likely government-sponsored and one of the most persistent of China's cyber threat actors."

The capabilities of APT1 are quite robust and include several large networks in the Shanghai region that appear to be dedicated to waging electronic warfare. During their investigation, Mandiant observed the compromise of 141 different organizations and the exfiltration of hundreds of terabytes of information. Of the organizations attacked, 87 percent were based in English-speaking countries. Once APT1 infiltrated an organization, they were able to maintain access for 356 days, on average, with the longest attack lasting for 1,764 days.

The nature of APTs means that the carefully constructed perimeter security controls put in place by enterprise security professionals are simply insufficient. The persistent hacker leveraging advanced techniques will likely find an opportunity to breach that perimeter and find a path onto the internal network. In this case, NetFlow data can play a critical role both in detecting the presence of an APT and conducting post-incident forensic analysis. NetFlow-based security analysis leverages behavioral analysis and pattern recognition techniques that allow for rapid detection of undocumented attack vectors, often revealing APT attackers early in the attack lifecycle.

Insider threat

In many cases, the greatest risk to an organization's security comes not from far-away hackers but from trusted individuals with access to sensitive information. The federal government experienced this in 2013 when the alleged actions of a single employee of a major defense intelligence contractor led to a massive disclosure of classified information about the National Security Agency and its operations.

As with APTs, perimeter controls aren't effective against the insider threat because those controls are designed to *permit* insiders access to sensitive information! NetFlow technology can identify signs of insider attacks in progress, such as internal or external data transfers that are unusually large or to atypical destinations.

Zero-day malware

New malware variants appear on the threat landscape on a daily basis. Some of these variants are simple tweaks of existing malware strains while others are insidious attacks that take advantage of previously unknown vulnerabilities. In either case, traditional antivirus software is unable to identify and defend against these attacks until the vendor obtains a sample of the malware and develops signatures to detect it.

NetFlow information can identify zero-day malware outbreaks immediately, without requiring signature updates. Infections may be identified by locating network flows that are unusual in size and/or destination and investigating the originating system for signs of infection.

Distributed denial-of-service attacks

Organized hacker groups, such as Anonymous, are now using DDoS attacks to bring large websites to their knees by simply exhausting all available capacity. NetFlow analysis can help identify that a DDoS attack is in progress and allows responders to identify the source and destination systems. NetFlow tools may also have the ability to identify slow connection floods that consume resources in a stealthy manner.

Changes in Information Technology

As the threats to information security evolve, information technology continues to change. Some important IT trends driving the adoption of NetFlow in enterprises include the widespread adoption of consumer technologies, mobile computing, the increased use of virtualization technology, and cloud computing.

Mobility and the vanishing perimeter

Mobile computing use has skyrocketed in recent years, to the point where smartphones, tablets, and other portable Internet-enabled devices are nearly ubiquitous and the phrase BYOD (bring your own device) is part of the IT language. You'd be hard-pressed to find a business traveler without at least one mobile device in his pocket that is capable of reaching back through his employer's firewalls to access sensitive corporate information.

This trend keeps security practitioners awake at night. All it takes is a single lost or stolen device to render significant investments in security controls moot. This leads to a trend, known as the *vanishing perimeter,* where security architects must consider all those mobile devices as part of their front-line security defenses, and design controls with that in mind.

NetFlow technology plays an important role in identifying and reacting to the risks posed by mobile devices. As traffic to and from these devices traverses the internal network, NetFlow captures the patterns of their network behavior and can quickly alert security professionals to any anomalous activity, triggering an appropriate incident response. No other monitoring technology provides such rapidly deployable, broad coverage at such a low cost to the organization.

Your organization should adopt formal policies about the use of personally owned devices on your networks and within your enterprise information systems. If you don't adopt such a policy, users will bring their devices anyway and not know the proper way to secure them.

Virtualized data centers

Organizations are quickly embracing the use of virtualization technology to host many virtual servers on a single hardware platform. This provides many apparent benefits to the enterprise, including:

- Recapture of computing resources (CPU cycles, memory, storage) that would otherwise go unused

- Reduced hardware footprint, allowing greater data center density
- Smaller environmental impact, reducing carbon emissions

But virtualization does present challenges to network security analysts. Communications between guest systems running on the same virtual host never touch an actual hardware switch or cross a network wire. Instead, they're routed through a virtual switch that exists in the memory of the virtualization host.

The communications taking place over virtual switches are difficult to protect with conventional security tools, and are invisible to traditional NetFlow technology. For this reason, many organizations are adopting NetFlow solutions that have specialized virtual network collectors, such as Lancope's StealthWatch FlowSensor VE (virtual edition).

Cloud computing

Organizations around the world are rapidly adopting cloud computing infrastructure, platforms, and software services. In order to manage this migration, security teams require insight into the organization's use of the cloud. This includes knowledge of the applications, data, and workloads that move into cloud environments, the location of stored data, and details about who accesses it. Organizations need real-time access to this information as they work to prevent breaches, as well as a store of historical records for use in forensics and incident response.

The NetFlow-provided details of every conversation that takes place on the network can fill this need. These details offer a permanent record of the connections made by internal systems to cloud providers. Analysts conducting a cloud risk assessment may use this information to help build the inventory of cloud services used by an organization and estimate the extent of that use through volumetric analysis.

Evolution of the Network

Advances in networking technology also complicate the jobs of security professionals seeking visibility into enterprise networks. In addition to the challenges addressed in the

previous section, three additional trends play important roles in shaping the future of network monitoring: new networked applications, IPv6 deployment, and software-defined networking (SDN). Each of these technologies has the potential to disrupt current network monitoring solutions if not properly managed.

Changing traffic types

As networks increase in speed and reliability, organizations are deploying a wide range of new applications on those networks. In addition to traditional computer systems, data networks now often carry VoIP telecommunications traffic, support embedded systems, and manage industrial processes.

This increase in network uses requires a scalable NetFlow analysis system capable of monitoring massive amounts of data in real time.

IPv6 deployment

The rapid depletion of available IP address space is beginning to drive the long-anticipated adoption of IPv6 networking, especially in larger organizations. Those enterprises with IPv6 networking in place or planning deployment of such networks in the near future should be sure to select a NetFlow solution that accommodates IPv6 addressing.

Flow-based network monitoring solutions can help ease the transition to IPv6 by tracking how network devices and applications behave before, during, and after the cutover, helping to mitigate any anomalies before they become a serious issue.

Software-defined networking (SDN)

Recent advances in networking technology have led to a new technology strategy, known as software-defined networking (SDN). SDN uses the power of abstraction to separate network control functions from the actual physical devices that handle traffic. Network administrators seeking to configure devices

do so through a controller that then configures the physical devices to implement the administrator-defined policy, as shown in Figure 2-2.

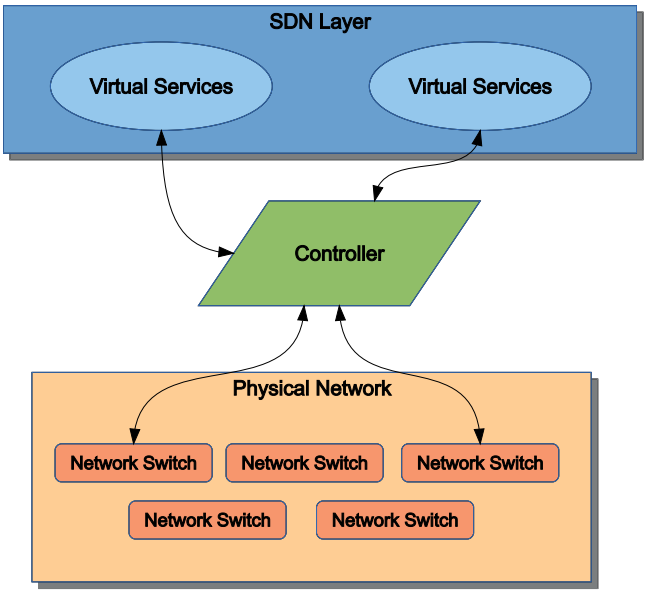


Figure 2-2: Software-defined networking abstracts network control functions from the manipulation of physical network devices.

SDN provides network administrators with unprecedented flexibility to reconfigure networks dynamically, but it doesn't help them identify optimal ways to *design* that network architecture. That's where NetFlow can help. Network architects can incorporate valuable network usage information generated by NetFlow into the network designs that they implement through SDN.

Chapter 3

Aligning Incident Response Along the Kill Chain

In This Chapter

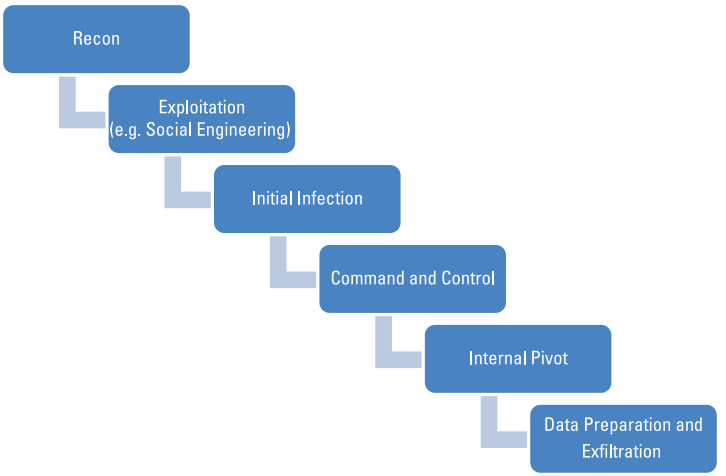
- Understanding the kill chain and how it can be applied to cybersecurity
- Learning about the six phases that make up the kill chain

The analysis of activity that takes place during security incident response provides critical information to an organization. First, it provides the attacked organization with perspective on the actual activities of the attacker, so that you know exactly what the attacker accomplished — and didn't accomplish. This information is critical in deciding what response is necessary and who needs to be notified.

Plus, reconstructing the details of a successful attack provides important information that can be used to prevent future attacks from succeeding. By determining the path that attackers followed to compromise a system or network, responders can identify the specific vulnerabilities exploited during the attack and remediate them to prevent similar future exploitation. Additionally, analysis of attacker behavior can help to quickly identify subsequent attack attempts by the same attacker.

Understanding the Kill Chain

When attacking traditional targets, the military uses a model known as the *kill chain* that describes the steps taken — from finding a suitable target through executing the attack and assessing the results. Lancope adapted this model to apply to computer intrusions in an approach shown in Figure 3-1, the *kill chain*. Lancope's model is an adaptation of work originally performed by Lockheed Martin.



Source: Lancope, Inc

Figure 3-1: The kill chain includes six phases.

Examining the Kill Chain Process

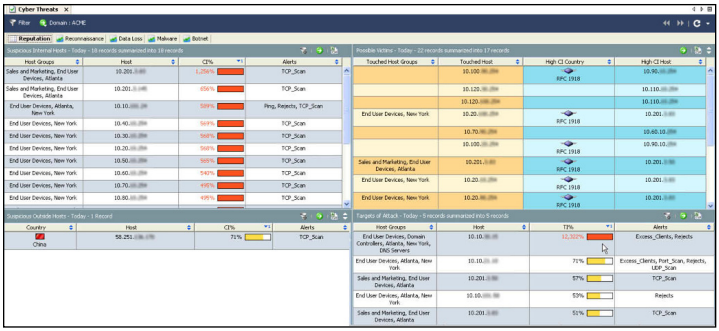
The kill chain includes six phases: reconnaissance, exploitation, initial infection, command and control, internal pivot, and data exfiltration. The remainder of this chapter explores the activities that take place during each of these phases.

Reconnaissance

During the reconnaissance phase of an attack, the attacker searches for and evaluates potential targets based on their perceived value and the likelihood of a successful attack. The types of reconnaissance conducted may depend on the attacker's objective. For example, if the attacker is simply seeking computing resources to conduct distributed denial-of-service (DDoS) attacks, the reconnaissance may

cast a wide net across large portions of the Internet seeking systems that have a specific vulnerability that the attacker knows how to exploit. On the other hand, if an attacker is targeting a specific organization, the reconnaissance may include scans of that organization's network address space, seeking systems that contain any vulnerability in a large database of potential weaknesses.

Incident responders seeking to reconstruct the reconnaissance phase of an attack should look for records of horizontal and/or vertical system scans that took place prior to the attack itself. Horizontal scans may include attempts to connect to every IP address in the organization's address space, regardless of whether the address is in use. Vertical scans may include repeated unsuccessful attempts to connect to large numbers of ports on the same system. NetFlow data is an excellent source of information that may show the signs of this type of reconnaissance. Figure 3-2 shows an example of detecting reconnaissance scans using Lancope's StealthWatch System.



Source: Lancope, Inc.

Figure 3-2: Using Lancope's StealthWatch System to detect TCP and UDP scans.

Exploitation

During the exploitation phase, the attacker exploits a vulnerability detected during reconnaissance. Examples of the types of vulnerabilities an attacker might exploit include:

- **Operating system vulnerabilities:** For instance, missing patches, which allow buffer overflows, malformed requests, or other attacks providing access to the underlying OS on a targeted system.
- **Application vulnerabilities:** For instance, SQL injection or improper access controls, which allow attackers to gain unauthorized access to an application, which may lead to access to underlying databases or other systems.
- **Human vulnerabilities:** For instance, social engineering or spear phishing, which exploit human weaknesses to gain passwords or other sensitive information that may be used to bypass access controls and gain entry to a system.

Attackers may use exploits from one or more of these categories to get an initial foothold on a system located on the organization's network. The system that they access through this initial exploit may not be the actual target system but may instead be simply a way of gaining initial access to the network.

Incident responders seeking to reconstruct the exploitation phase of an incident are likely to turn to log entries created by the exploited system that indicate both successful and unsuccessful attack attempts. Intrusion prevention systems also provide important records to reconstruct system exploits.

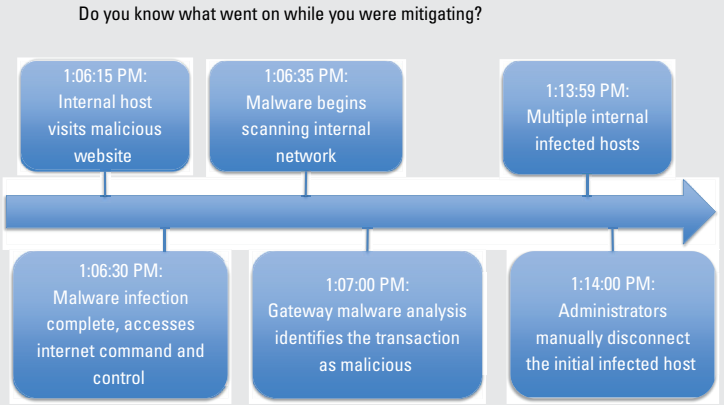
Initial infection

During the initial infection phase of an attack, the intruder installs software on the exploited system to gain permanent access to the attacked environment. This may include the use of a *remote access Trojan (RAT)* — software that allows the attacker to gain unrestricted access to the system from a remote location or a *backdoor* that allows access through methods that bypass traditional security controls.

NetFlow records may contain important information showing the initial infection of an exploited system. This typically manifests itself as inbound administrative connections to a system from unusual locations.

Timeline of an attack

Attacks may take place over a very short period of time, quickly moving from the reconnaissance phase through the other steps of the kill chain. Some steps may be omitted depending upon the objectives of a particular attack. For example, if an attacker is able to gain access to a system containing sensitive information during the exploitation phase, the attack may immediately jump to the data exfiltration phase. See the accompanying figure, which shows the timeline of an example attack taking place over an eight-minute period.



Source: Lancope, Inc.

The figure shows an example of an attack that occurred when an individual on the target network visited a malicious website. The exploitation, initial infection, and C&C objectives were all achieved in the first 15 seconds of the attack. Over the next seven minutes, the internal pivot stage of the attack took place. Administrators believe that they ended the attack during that stage, avoiding data exfiltration.

Command and control

Once an attacker gains a permanent foothold in the environment through an initial infection, the goal of the attack shifts to gaining command-and-control (C&C) access to the network. With C&C access, the attacker installs software that allows systems to be remotely controlled using outbound connections that easily traverse the organization's firewall.

C&C connections are more difficult to detect than initial infections because they don't normally use the inbound connections that are typical of initial infections. NetFlow records can provide important information to help detect C&C links by comparing the destination addresses of outbound flow records to the addresses of known C&C networks.

Internal pivot

Once an attacker has established C&C access to an organization's network, the attack moves on to the internal pivot phase. During this phase, the attacker seeks to expand access throughout the targeted organization's network. Remember that the system used for the initial infection may not be the actual target of the attack. During the internal pivot stage, the attacker leverages the system(s) under outside control to attack other system(s) on the network, including the actual target of the attack.

Once again, NetFlow data may be used to identify the internal pivot phases of an attack. The records of this phase are similar to those generated during the reconnaissance phase of the attack, with the distinction that they originate *inside* the organization's network, rather than outside. Analysts should look for flow records that indicate internal systems scanning the intranet, seeking systems with vulnerabilities, and exploiting them.

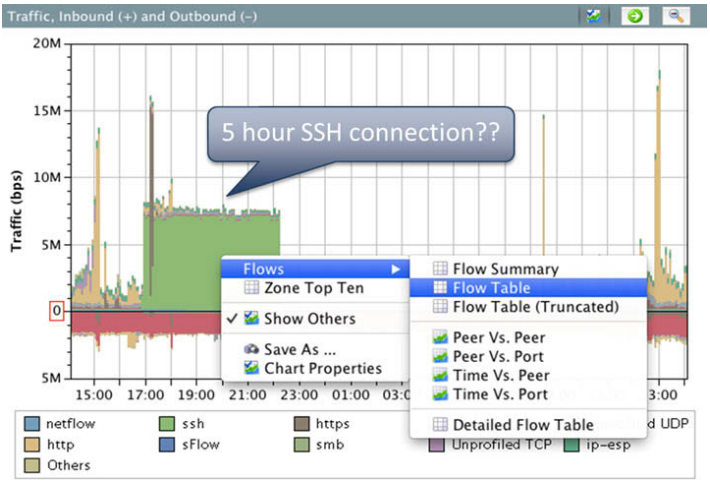
Data exfiltration

During the final phase of the attack, the attacker has gained access to the ultimate target system and may now seek to steal sensitive information, a process known as *data exfiltration*. There are three specific activities that take place during this phase:

- Identification of relevant data, which may be stored in files, databases, or other data stores.
- Preparation of the data, including extracting the desired data from the source, compressing it to reduce transfer time, and encrypting it to hide from data loss prevention systems performing keyword searches.
- Exfiltration of the data by transferring it from the target system to a system under the attacker's complete control.

Information on the identification and preparation steps of this phase is most likely found in operating system and application logs. The exfiltration step leaves indelible footprints in NetFlow records, showing transfers of information from the attacked system to an external destination.

See Figure 3-3 for a visual.



Source: Lancope, Inc

Figure 3-3: Lancope's StealthWatch System reveals data exfiltration through NetFlow analysis.

The Five Ws

When your network is compromised, there are five main questions you need to answer.

- **Who did this?** See if you can find usernames and IP addresses.
- **What did they do?** What behavior did they engage in?
- **Where did they go?** What hosts on my network were accessed?
- **When?** Have we investigated the full intrusion timeline?
- **Why?** What is their objective?

Chapter 4

Responding to Security Incidents Today

In This Chapter

- Building an incident response team
- Putting together an incident response process based on critical metrics
- Creating an incident response technology toolkit

Responding to a security incident is a complex undertaking requiring careful coordination among the people, processes, and technology required to successfully restore operations. In this chapter, I cover the roles that each of these components plays in incident response.

Involving the Right People

When responding to a security incident, an organization must consider many different facets of the response. In addition to the technical investigation and recovery tasks that immediately spring to the minds of IT professionals, the organization must also consider the operational, legal, human resources, and public relations angles of the event. Involving the right people in your incident response team from the start can save you significant hardship down the road.

Building response teams

The first planning step that you should consider is the creation of appropriate security incident response teams. These include both an operational computer security incident response team (CSIRT) and a multidisciplinary threat management group.

The CSIRT consists of the technical staff who conduct the tactical response to a security incident. CSIRTs are typically led by the information security function and include representation from many technical functions, including:

- Networking
- System engineering
- Application development
- Operations
- Change/configuration management
- Database administration

The specific composition of the CSIRT will vary based upon the technology organization's structure. In addition, team members may be included on an *ad hoc* basis depending upon the nature of the incident.

The threat management group is also typically chaired by information security leadership but consists of leaders from throughout the organization. The composition of each team will vary based upon the nature and composition of an organization, but should include as a minimum:

- **Information security team leaders** with responsibilities related to the incident response function
- **Operations leaders** responsible for critical functions of the business
- **Technical leaders** representing the major technology functions expected to be involved in incident response
- **Legal representation** to advise the team on compliance obligations related to security incidents
- **Public relations staff** to handle media inquiries, press releases, and news conferences
- **Human resources team members** to advise on appropriate steps if disciplinary action against staff results from the incident

The threat management group provides a strategic response to security incidents and also facilitates organization-wide risk assessments.

Err on the side of inclusion. If you're not sure whether a group should be represented on your response teams, invite them to the table anyway. In the worst case, if their role isn't needed, you can identify that together and change the team composition. On the other hand, if you fail to include a critical stakeholder, you risk damaging both the effectiveness of the incident response process and an important relationship.

Training the CSIRT

Members of the CSIRT will require training that covers both the broad functioning of the CSIRT as well as the specific functions they're expected to perform during an incident response effort. In addition to an initial training program that brings the newly formed team up to speed on its responsibilities, the CSIRT process should include (at least) annual refresher training for all team members and induction training for members who join the team after it's formed.

Members of the CSIRT should also participate in technical professional development programs, including both education on emerging technologies used by the organization and awareness of the tools available for incident response. As you deploy NetFlow as an incident response tool, you may wish to conduct seminars for CSIRT participants making them aware of NetFlow's capabilities and the fields available for incident analysis.

Calling in outside help

In some cases, the circumstances of an incident will call for expertise that doesn't exist on your team, or will require a commitment of staff time beyond the organization's existing capabilities. When this occurs, you should consider bringing in incident response specialists capable of supplementing your own CSIRT. The most common use of outside help during an incident response is bringing in outside forensic consultants who have skills and tools beyond those available within your organization.

Negotiating contracts with forensics experts and other incident response specialists can be a time-consuming process. You should try to anticipate the needs you may have in the event of an incident and develop agreements in advance that you can activate when an incident occurs.

Creating a Measurable Process

IT organizations today need to provide increasingly efficient results with dwindling resources, so it is important to demonstrate the value of IT processes through understandable metrics. I suggest using four time-based metrics for your incident response program, based on a model proposed by Forrester Research.

Mean time to identify

The mean time to identify (MTTI) is the amount of time required to recognize that an incident has taken place. The initial notice of an incident may come from a user or technician report of suspicious activity.

Mean time to know

The mean time to know (MTTK) is the time required from the point an incident occurs until analysts understand the root cause of the incident. Depending on the information available, the MTTK may vary from minutes to days.

Remember that these are measures of *elapsed* time. Therefore, the MTTK includes both the time required to recognize the incident and the time required to identify the root cause.

Mean time to fix

The mean time to fix (MTTF) begins at the point an incident occurs and continues until the root cause is repaired and the incident is successfully resolved. MTTF is an important measure because it indicates the actual time required to return operations to normal in the wake of an incident.

Mean time to verify

The mean time to verify (MTTV) includes the time that elapses between an incident occurring and the team confirming with customers and other stakeholders that the incident has been successfully resolved.

The use of NetFlow, IDS/IPS, and other automated tools allows for the rapid detection of potential incidents, increases the

efficiency of analysis and repair efforts, and contributes to the verification of incident resolution. These benefits serve to reduce MTTI, MTTK, MTTF, and MTTV.

Benchmarking incident response metrics

In January 2014, the Ponemon Institute published "Cyber Security Incident Response: Are we as prepared as we think?" Of the 674 IT professionals surveyed about the incident response capabilities of their organizations, following were some interesting highlights:

- Thirty-four percent of organizations don't have a fully functional CSIRT, and those that do often lack full-time staff.
- Fifty percent of respondents say their organization doesn't have meaningful operational metrics to measure the overall effectiveness of incident response activities.
- It takes about a month, on average, to work through the entire process of incident investigation, service restoration, and verification.

Understanding the typical incident response timelines and procedures found in other organizations can help you assess the effectiveness of your own incident response program.

Building Your Technology Toolkit

Once you have the appropriate teams and processes in place to respond to security incidents, you should turn your attention to the tools available to responders and ensure that you've laid the foundation for successful incident response.

The tools used within your organization may vary based on your resources and business needs, but you should consider implementing a SIEM, NetFlow, and packet capture capabilities as a minimum base.

Security Information and Event Management

Security Information and Event Management (SIEM) systems are capable of collating logs from a wide variety of sources.

They then allow security professionals to analyze and correlate those disparate information sources in an effort to identify and/or investigate security incidents.

A SIEM is only as good as the information feeding it. For that reason, organizations implementing SIEM as part of their incident response toolkit must also dedicate sufficient time to the log configuration of each monitored component. This ensures that, in the event of an incident, the necessary information will be stored in the SIEM's database and ready for analysis.

NetFlow

NetFlow information, as discussed in Chapter 1, plays a critical role in incident response by keeping a phone bill style ledger of all communications that took place on a network. Organizations seeking to implement a sound incident response process should have NetFlow exporters deployed throughout the network at any point where they might encounter network connections relevant to the investigation of a security incident.

Furthermore, the organization must have a NetFlow collector in place that is capable of receiving flows from throughout the network and retaining them for an extended period of time. I discuss the design of a NetFlow system in Chapter 5.

Packet capture

Although packet capture isn't appropriate for long-term collection on an organization's network (see Chapter 5), it plays an important role in incident response efforts. Packet capture may be used as a point-in-time technique to peer inside a network during an investigation. Packet capture is the only way to discover the actual contents of traffic traveling on a network through payload analysis. Having this capability at your disposal may provide important information that allows you to reduce your MTTK.

Because you won't be able to run packet capture on an ongoing basis, your incident response plan should include the steps that you will take to activate capture on an as-needed basis. You must also ensure that you have network taps, capture systems, and software ready to go in your incident response toolkit. Time is of the essence during an actual incident, and you won't want to miss capturing critical packets because you were fumbling around looking for an Ethernet cable!

Chapter 5

Enabling Incident Response with NetFlow

In This Chapter

- Identifying the objectives of your NetFlow deployment and selecting an appropriate solution
- Designing a scalable NetFlow infrastructure able to accommodate the flows generated by your network
- Leveraging advanced analysis techniques and security context to mine significant information from NetFlow data

NetFlow provides a valuable source of information about activity on your network in a consistent, standardized format supported by many networking and security vendors. Collecting data, however, is where the standardization stops. Many different systems provide the ability to collect and analyze NetFlow data, ranging from open-source packages with limited functionality to commercial systems with advanced analysis capabilities.

What's Your Objective?

As you begin to select a NetFlow analysis solution, you should have a clear understanding of the objectives of your deployment. The fact that you're reading this book indicates that you're interested in using NetFlow for incident response, but you likely have other objectives as well. Some possibilities include:

- Monitoring your network for anomalous activity that may indicate a security event
- Creating a forensic audit trail to assist in post-incident analysis following a security breach

- Providing network engineers with a robust tool for troubleshooting network performance issues
- Complying with regulatory requirements to retain network connection information

As you consider various NetFlow collection and analysis platforms, keep your objectives front-of-mind and allow them to drive your product selection process.

Maintaining a forensic audit trail

Organizations seeking to implement NetFlow for incident response typically make their first objective with NetFlow the creation of a forensic audit trail: They simply enable NetFlow exporting to a NetFlow collector and then allow the data to accumulate over time. This data set then becomes a valuable source of information for post-incident assessment in the event of a security breach. NetFlow acts as a continuous, 24x7 audit trail of all communications that occur within the network.

Analysts can retrieve NetFlow data from Lancope's StealthWatch System to assist with forensic analysis. For a given pair of systems, the analyst can identify the number of communication sessions that took place, the duration of those sessions, the amount of data passed and additional technical details.

Improving compliance

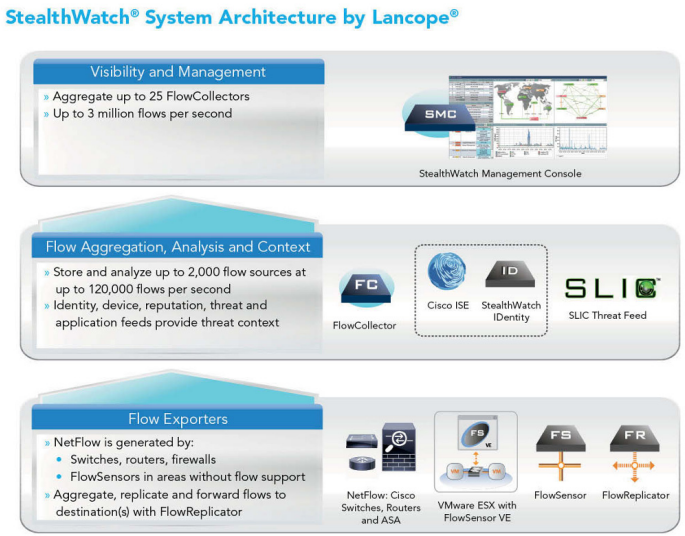
Many industries are subject to information security laws and regulations that require the use of strict security controls to protect the confidentiality, integrity, and availability of sensitive information. NetFlow data can help in these cases by providing security analysts the tools they need to proactively monitor the compliance status of a network, conduct forensic investigations, identify malicious software in use on the network, and assess the effectiveness of other security controls.

NetFlow data can assist organizations seeking to comply with the Payment Card Industry Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley Act (SOX), Control Objectives for

Information and related Technology (COBIT), and the National Institute of Standards and Technology (NIST) 800 series, among others.

Designing for Scalability

Conducting NetFlow analysis in large environments requires solutions that offer a scalable architecture not found in open-source products or software-only solutions. Figure 5-1 provides an example of a scalable architecture consisting of three components: NetFlow exporters, flow collectors, and a management console. Administrators can add capacity at any layer as needed.



Source: Lancope, Inc.

Figure 5-1: Scalable NetFlow analysis platforms use three layers of devices: NetFlow exporters, flow collectors, and a management console.

NetFlow exporters

A wide variety of devices are capable of generating NetFlow data and exporting it to a flow collection system. There are three basic categories of NetFlow exporters:

- **Routers, switches, and firewalls:** Network infrastructure components are in a unique position to capture and export NetFlow information due to their central location in the network. In many cases, an organization's existing network infrastructure is already capable of generating NetFlow records and exporting them to a collection system.
- **Dedicated flow sensors:** NetFlow collection system vendors also offer passive flow sensors that may be connected to a network tap in a manner similar to an intrusion detection system. They then monitor traffic on the tap, generating flow records for each connection encountered.
- **Virtual flow sensors:** Specialized flow sensors operate in virtualized networking environments, monitoring the traffic passing through a virtual switch and exporting flow records to the collection system.

Flow collectors

Flow collectors are the workhorses of the NetFlow analysis system. They receive NetFlow records from exporters and perform a number of critical tasks, including:

- **Flow deduplication:** In networks with multiple flow exporters, the same network connection may be captured multiple times. Flow collectors must watch for this and remove duplicate records before performing security analysis. Without deduplication, traffic volume can be misreported and false positives would occur. Deduplication is necessary for accurate host-level reporting and allows for the efficient storage of flow data.
- **Flow stitching:** NetFlow generates unidirectional records, resulting in two different records for each network session. The flow collector puts these back together again, giving analysts the full picture of each connection.
- **Behavioral analysis and pattern recognition:** Security-oriented flow collectors will provide algorithms and mechanisms for easy visualization and analysis of flows to detect security threats.
- **Flow retention:** The flow collector will store weeks, months, perhaps years worth of NetFlow data. The collector's flow database is used to perform detailed forensics and incident response.

The number of flow collectors you need will depend upon the amount of NetFlow data generated on your network. This is normally measured in flows per second (FPS).

Management console

In large networks, multiple flow collectors are needed to collect flows. When multiple collectors are used, a central management console is a must. The management console provides the day-to-day interface used by networking and security professionals to interact with and manage the NetFlow analysis platform. Management consoles typically offer a wide set of features, including:

- Dashboards providing analysts with quick overviews of network activity
- Advanced analytic capabilities to visualize abnormal behavior
- Alarms that immediately alert analysts when certain suspicious conditions occur
- A management interface that allows the reconfiguration of the NetFlow analysis system
- Management of the security policy across multiple collectors
- Per-user access restrictions to the flow data

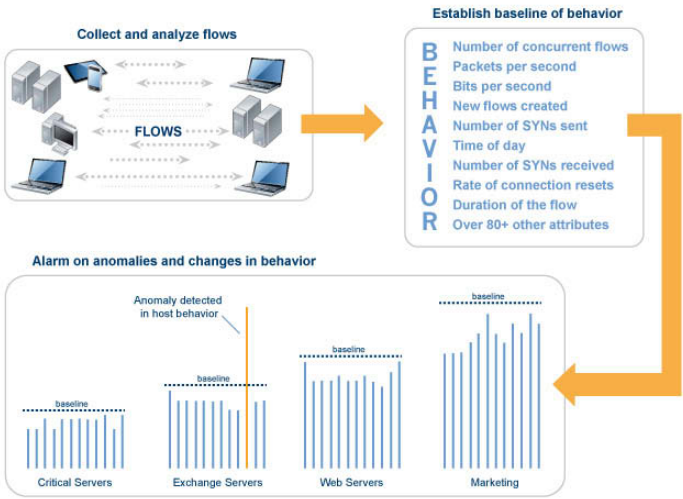
Before selecting a system, be sure to give the management console a test drive. It's helpful to go back to your objectives and prepare a list of common tasks that you expect analysts will perform and then walk through those tasks in the management console. There's nothing like hands-on experience to help you evaluate a product.

Enhancing Analysis Capabilities

One of the true differentiators of NetFlow collection systems is the sophistication of the analysis tools provided through their management consoles. Some systems offer advanced features, such as behavior analysis, security indexes, and activity alarms to facilitate network security monitoring.

Network behavior analysis

NetFlow records provide a uniquely valuable data source for identifying anomalous behavior. Most systems, especially critical servers, are creatures of habit — they engage in the same types of activity with the same systems from day to day. Figure 5-2 provides an illustration of how this activity can be baselined to develop a picture of your network under normal conditions.



Source: Lancope, Inc.

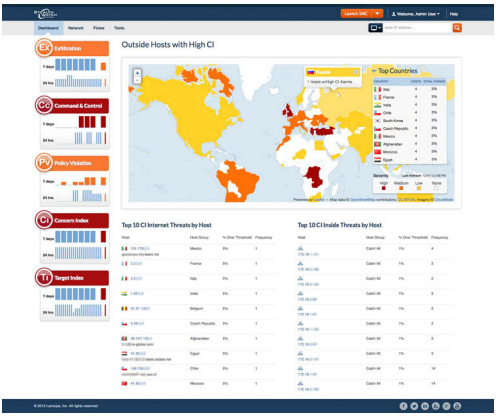
Figure 5-2: Network behavior analysis algorithms allow you to baseline normal behavior for a host and alert security analysts to future deviations from that baseline.

After you've developed a baseline of network activity, your NetFlow analysis system can identify anomalies by watching for deviations from that baseline. Security analysts can then use that information to proactively identify potential security incidents requiring further investigation.

Security indexes and alarms

NetFlow analysis platforms have access to a large amount of data about anomalous connections and analysts may struggle to identify the significant data that requires their immediate attention.

One of the most important features of a NetFlow analysis system is its capability to run in an unmanned mode, freeing analysts to perform other tasks. This is done through the use of security indexes and alarms that may be triggered by violations of an organization's security policy or significantly anomalous network behavior (see Figure 5-3).



Source: Lancope, Inc.

Figure 5-3: With the StealthWatch Concern Index, administrators can easily determine which issues need to be dealt with first for optimum network protection.

Delivering greater operational network and security intelligence, Lancope's StealthWatch System alarms correspond with the kill chain to provide greater security context. Aligning alarms with attacker behaviors turns network and security data into actionable intelligence for faster, more effective troubleshooting.

- **Concern Index (CI)** tracks hosts that appear to pose a threat to the integrity of your network.
- **Target Index (TI)** tracks hosts that the system suspects may be the victims of suspicious activity.
- **C&C (Command & Control)** indicates the existence of bot-infected servers or hosts in your network attempting to contact a C&C server.

- **Data exfiltration** tracks inside and outside hosts to whom an abnormal amount of data has been transferred.
- **Policy violation** identifies hosts exhibiting behaviors that violate established network policies.

Can't I just capture everything?

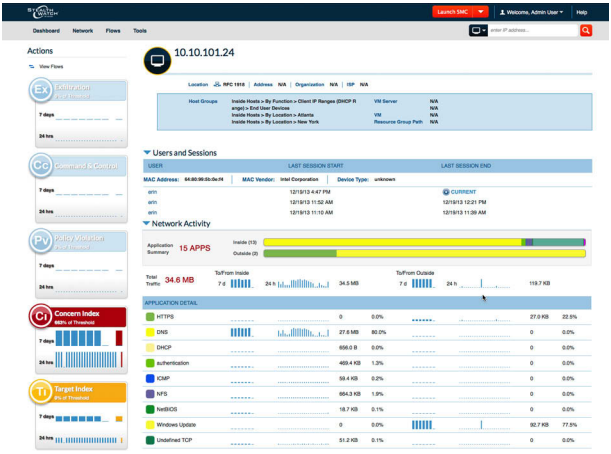
Many security professionals considering NetFlow deployment for the first time do so after first considering capturing all traffic on a network. This is often driven by a desire to retain forensically valuable information or comply with stringent security requirements.

Although full packet capture is technically possible and would provide undeniably valuable information in the event of a security incident, it's simply not feasible. The amount of storage required to retain data captured across even a low bandwidth connection over a long period of time is tremendous.

For example, if you wanted to capture all of the data crossing a circuit that averages 100Mbps, you would be collecting 12.5 megabytes of data every second, or 45 terabytes per hour!

Correlating Flows with Context

Another powerful feature of NetFlow analysis tools is their ability to integrate additional context — including identity and application awareness — for increased situational awareness. See Figure 5-4.



Source: Lancope

Figure 5-4: Gain critical context with user identity and application awareness for expedient incident response.

Identity awareness

Almost every security investigation that begins with NetFlow records at some point requires identifying the individual user and/or system involved in a communication. Unfortunately, generic NetFlow doesn't provide this information, because NetFlow exporters don't have access to information not found in the packets comprising the flow.

Some NetFlow systems provide security analysts with the added ability to correlate identity information from other sources, such as the identity of an individual user retrieved from a Windows domain controller, proxy server, or a VPN concentrator. Identity-aware NetFlow collectors bridge the gap between IP addresses and users. Lancope offers identity awareness through its own StealthWatch IDentity appliance, or through integration with Cisco's Identity Services Engine (ISE), Cisco Adaptive Security Appliance (ASA), and Palo Alto Networks next-generation firewalls.

Application awareness

Incident responders can also achieve significant benefits from including application context in NetFlow analysis. For example, some NetFlow systems embed URL information in the records they generate. This provides responders with the ability to see not only the destination systems accessed by internal hosts but also to identify the specific websites users were accessing. With the increased use of shared cloud hosting providers, this information is more important than ever before.

Chapter 6

Five Myths about NetFlow

In This Chapter

- Recognizing five commonly held myths about the use of NetFlow in incident response

NetFlow is an important tool for incident responders, providing valuable insight into the activities that took place on a network. In this chapter, I dispel five common myths about NetFlow's role in incident response.

Myth 1: Complex Attacks Can't Be Detected with NetFlow

On the contrary, NetFlow records are often used to identify complex attacks, allowing responders to identify indicators of compromise across a large amount of network traffic in a timely fashion. Furthermore, because NetFlow can see deep into the network, it can be used for behavioral analysis that identifies anomalous traffic patterns, network reconnaissance, policy violation, internal pivots, and more.

Myth 2: Full Packet Capture Makes NetFlow Irrelevant

Full packet capture is simply not a sustainable practice. Maintaining these records for an extended period of time requires extensive deployment of probes and massive storage capacity. Furthermore, analyzing records of full packet capture is very time consuming compared to the preprocessed data available from NetFlow.

Myth 3: NetFlow Provides Insufficient Information

One of the biggest mistakes made in incident response is failing to conduct sufficient monitoring and surveillance to inform the response effort. NetFlow logs every communication taking place through a monitored device and provides information essential to incident responders. In its most basic configuration, NetFlow logs timestamps, source/destination IP addresses and ports, and the amount of information exchanged. Advanced configurations may include additional information requested by incident responders.

Myth 4: NetFlow Is Not Admissible Evidence

Incident responders can rest assured that NetFlow records can indeed be admissible in court. These records, gathered during the normal course of business, are often relied on as evidence in both criminal and civil trials. Various courts have repeatedly accepted NetFlow as a valid form of evidence of network activity.

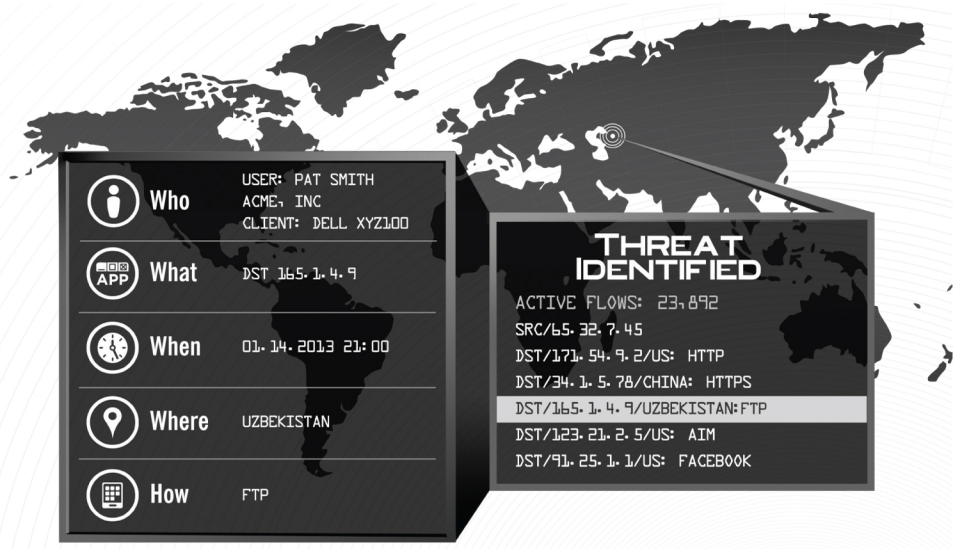
Myth 5: NetFlow Degrades Performance

When NetFlow first came to market over 15 years ago, it had a significant impact on router and switch CPU consumption. However, NetFlow is now a core capability of network devices, which are optimized to perform NetFlow operations without significant performance impact.

Generally speaking, networking devices operating under a 50 percent utilization rate should see an impact of less than 2 percent on CPU performance after NetFlow is enabled. From a bandwidth perspective, network overhead is usually between 0.1 percent and 0.3 percent of the monitored traffic.

Lancope®

Vision to Secure, Intelligence to Protect™



By collecting and analyzing NetFlow, IPFIX and other types of flow data, Lancope's StealthWatch® System helps organizations quickly detect a wide range of attacks from APTs and DDoS to zero-day malware and insider threats.

www.lancope.com

Use NetFlow to accelerate incident response and forensic investigations!

Security incidents are time sensitive and stressful. Incident response teams must have access to critical information and a well-defined process to guide their actions. NetFlow data provides a full audit trail to expedite forensic investigations and reduce time-consuming manual analysis. This book explains how NetFlow analysis can dramatically accelerate incident response by delivering complete network visibility to discover, investigate, and counteract a wide variety of cyberattacks including APTs, insider threats, zero-day malware, and DDoS.

- ***Incident response basics* — find out how network audit trails and NetFlow analysis help you respond faster and more precisely to security incidents**
- ***Why NetFlow, why now* — take a look at the trends driving the adoption of NetFlow as an incident response tool**
- ***Respond quickly to security incidents* — learn how to build an efficient incident response team**
- ***Find out more about NetFlow* — learn the role that NetFlow information plays in a network security infrastructure and how to put NetFlow to work**

Open the book and find:

- **How NetFlow combats the modern threat landscape and addresses emerging IT trends**
- **Best practices for building an effective incident response team, process, and toolkit**
- **How to use NetFlow to align incident response along the kill chain**
- **How NetFlow fills the visibility gap for faster incident response**

Go to Dummies.com®
for videos, step-by-step examples, how-to articles, or to shop!

Mike Chapple, Ph.D. Senior Director for IT Service Delivery at the University of Notre Dame. Mike is the author of several books, including the *CISSP Prep Guide*.

FOR DUMMIES®
A Wiley Brand

ISBN: 978-1-118-88341-9
Not for resale