Chapter 6

Router Forensics

by Michael Gregg

Solutions in this chapter:

- Network Forensics
- Searching for Evidence
- An Overview of Routers
- Hacking Routers
- Router Attacks
- Investigation of Routers
- Incident Forensics

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

Introduction

This chapter examines router and network forensics. This chapter is important as many attacks will require the analyst to look for information in the router or require network forensics. This requires you to have an understanding of routers and their architecture. It is important to understand where they reside within the OSI model and what role they play within network communications.

Anytime you work with forensic evidence it is critical that the concept of chain of custody be understood. How evidence is handled, stored, accessed, and transported is critical, because if basic control measures are not observed the evidence may be ruled inadmissible in court.

Network Forensics

Network forensics can best be defined as the sniffing, recording, and analysis of network traffic and events. Network forensics are performed in order to discover the source of security incidents and attacks or other potential problems. One key role of the forensic expert is to differentiate repetitive problems from malicious attacks.

The Hacking Process

The hacking process follows a fixed methodology. The steps a hacker follows can be broadly divided into six phases:

1. Reconnaissance
2. Scanning and enumeration
3. Gaining access
4. Escalation of privilege
5. Maintaining access
6. Covering tracks and placing backdoors

The Intrusion Process

Reconnaissance is considered the first preattack phase. The hacker seeks to find out as much information as possible about the victim. The second preattack phase is scanning and enumeration. At this step in the methodology, the hacker is moving from passive information gathering to active information gathering. Access can be gained in many different ways. A hacker may exploit a router vulnerability or maybe

social engineer the help desk into giving him a phone number for a modem. Access could be gained by finding vulnerability in the web server's software. Just having the access of an average user account probably won't give the attacker very much control or access to the network. Therefore, the attacker will attempt to escalate himself to administrator or root privilege. Once escalation of privilege is complete the attacker will work on ways to maintain access to the systems he or she has attacked and compromised. Hackers are much like other criminals in that they would like to make sure and remove all evidence of their activities, which might include using root kits to cover their tracks. This is the moment at which most forensic activities begin.

Searching for Evidence

You must be knowledgeable of each of the steps of the hacking process and understand the activities and motives of the hacker. You many times will be tasked with using only pieces of information and playing the role of a detective in trying to reassemble the pieces of the puzzle. Information stored within a computer can exist in only one or more predefined areas. Information can be stored as a normal file, deleted file, hidden file, or in the slack or free space. Understanding these areas, how they work, and how they can be manipulated will increase the probability that you will find or discover hidden data. Not all suspects you encounter will be super cyber criminals. Many individuals will not hide files at all; others will attempt simple file hiding techniques. You may discover cases where suspects were overcome with regret, fear, or remorse, and attempted to delete or erase incriminating evidence after the incident. Most average computer users don't understand that to drop an item in the recycle bin doesn't mean that it is permanently destroyed.

One common hiding technique is to place the information in an obscure location such as C:\winnt\system32\os2\dll. Again, this will usually block the average user from finding the file. The technique is simply that of placing the information in an area of the drive where you would not commonly look. A system search will quickly defeat this futile attempt at data hiding. Just search for specific types of files such as bmp, tif, doc, and xls. Using the search function built into Windows will help quickly find this type of information. If you are examining a Linux computer, use the grep command to search the drive.

Another technique is using file attributes to hide the files or folders. On a Macintosh computer, you can hide a file with the ResEdit utility. In the wonderful world of Windows, file attributes can be configured to hide files at the command

line with the attrib command. This command is built into the Windows OS. It allows a user to change the properties of a file. Someone could hide a file by issuing attrib +h secret.txt. This command would render the file invisible in the command line environment. This can also be accomplished through the GUI by right-clicking on a file and choosing the hidden type.

Would the file then be invisible in the GUI? Well, that depends on the view settings that have been configured. Open a browse window and choose tools/folder options/view/show hidden files; then, make sure Show Hidden Files is selected. This will display all files and folders, even those with the +h attribute set. Another way to get a complete listing of all hidden files is to issue the command attrib /s > attributes.txt from the root directory. The attrib command lists file attributes, the /s function list all files in all the subdirectories, and > redirects the output to a text file. This text file can then be parsed and placed in a spreadsheet for further analysis. Crude attempts such as these can be quickly surmounted.

An Overview of Routers

Routers are a key piece of networking gear. Let's know the role and function of a router.

What Is a Router?

Routers can be hardware or software devices that route data from a local area network to a different network. Routers are responsible for making decisions about which of several paths network (or Internet) traffic will follow. If more than one path is available to transmit data, the router is responsible for determining which path is the best path to route the information.

The Function of a Router

Routers also act as protocol translators and bind dissimilar networks. Routers limit physical broadcast traffic as they operate at layer 3 of the OSI model. Routers typically use either link state or hop count based routing protocols to determine the best path.

The Role of a Router

Routers are found at layer three of the OSI model. This is known as the networking layer. The network layer provides routing between networks and defines logical

addressing, error handling, congestion control, and packet sequencing. This layer is concerned primarily with how to get packets from network A to network B. This is where IP addresses are defined. These addresses give each device on the network a unique (logical) address. Routers organize these addresses into classes, which are used to determine how to move packets from one network to another. All types of protocols rely on routing to move information from one point to another. This includes IP, Novell's IPX, and Apple's DDP. Routing on the Internet typically is performed dynamically; however, setting up static routes is a form of basic routing. Dynamic routing protocols constantly look for the best route to move information from the source to target network.

Routing Tables

Routers are one of the basic building blocks of networks, as they connect networks together. Routers reside at layer 3 of the OSI model. Each router has two or more interfaces. These interfaces join separate networks together. When a router receives a packet, it examines the IP address and determines to which interface the packet should be forwarded. On a small or uncomplicated network, an administrator may have defined a fixed route that all traffic will follow. More complicated networks typically route packets by observing some form of metric. Routing tables include the following type of information:

- **Bandwidth** This is a common metric based on the capacity of a link. If all other metrics were equal, the router would choose the path with the highest bandwidth.
- **Cost** The organization may have a dedicated T1 and an ISDN line. If the ISDN line has a higher cost, traffic will be routed through the T1.
- **Delay** This is another common metric, as it can build on many factors including router queues, bandwidth, and congestion.
- **Distance** This metric is calculated in hops; that is, how many routers away is the destination.
- **Load** This metric is a measurement of the load that is being placed on a particular router. It can be calculated by examining the processing time or CPU utilization.
- **Reliability** This metric examines arbitrary reliability ratings. Network administrators can assign these numeric values to various links.

By applying this metric and consulting the routing table, the routing protocol can make a best path determination. At this point, the packet is forwarded to the next hop as it continues its journey toward the destination.

Router Architecture

Router architecture is designed so that routers are equipped to perform two main functions: process routable protocols and use routing protocols to determine best path. Let's start by reviewing routable protocols. The best example of a routed protocol is IP. A very basic definition of IP is that it acts as the postman of the Internet—its job is to organize data into a packet, which is then addressed for delivery. IP must place a target and source address on the packet. This is similar to addressing a package before delivering it to the post office. In the world of IP, the postage is a TTL (Time-to-Live), which keeps packets from traversing the network forever. If the recipient cannot be found, the packet can eventually be discarded.

All the computers on the Internet have an IP address. If we revert to our analogy of the postal system, an IP address can be thought of as the combination of a zip code and street address. The first half of the IP address is used to identify the proper network; the second portion of the IP address identifies the host. Combined, this allows us to communicate with any network and any host in the world that is connected to the Internet. Now let us turn our attention to routing protocols.

Routing Protocols

Routing protocols fall into two basic categories, static and dynamic. Static, or fixed, routing is simply a table that has been developed by a network administrator mapping one network to another. Static routing works best when a network is small and the traffic is predictable. The big problem with static routing is that it cannot react to network changes. As the network grows, management of these tables can become difficult. Although this makes static routing unsuitable for use on the Internet or large networks, it can be used in special circumstances where normal routing protocols do not function well.

Dynamic routing uses metrics to determine what path a router should use to send a packet toward its destination. Dynamic routing protocols include Routing Information Protocol (RIP), Border Gateway Protocol (BGP), Interior Gateway Routing Protocol (IGRP), and Open Shortest Path First (OSPF). Dynamic routing can be divided into two broad categories: link-state or distance vector dynamic routing protocols, which are discussed in greater detail later in the chapter.

RIP

RIP is the most common routing protocol that uses a hop count as its primary routing metric. RIP is considered a distance vector protocol. The basic methodology of a distance vector protocol is to make a decision on what is the best route by determining the shortest path. The shortest path is commonly calculated by hops. Distance vector routing is also called routing by rumor.

Head of the Class…

What Is a Hop Count?

A hop count is the number of routers that a packet must pass through to reach it destination. Each time a packet passes through a router, the cost is one hop. So, if the target network you are trying to reach is two routers away, it is also two hops away. The major shortcoming of distance vector protocols is that the path with the lowest number of hops may not be the optimum route. The lower hop count path may have considerably less bandwidth than the higher hop count route.

OSPF

OSPF is the most common link state routing protocol and many times, it is used as a replacement to RIP. Link state protocols are properly called Dijkstra algorithms, as this is the computational basis of their design. Link state protocols use the Dijkstra algorithm to calculate the best path to a target network. The best path can be determined by one or more metrics such as hops, delay, or bandwidth. Once this path has been determined, the router will inform other routers as to its findings. This is how reliable routing tables are developed and routing tables reach convergence. Link state routing is considered more robust than distance vector routing protocols. One reason is because link state protocols have the ability to perform faster routing table updates.

NOTE

Convergence is the point at which routing tables have become synchronized. Each time a network is added or dropped, the routing tables must again resynchronize. Routing algorithms differ in the speed at which they can reach convergence.

Hacking Routers

Full control of a router can often lead to full control of the network. This is why many attackers will target routers and launch attacks against them. These attacks may focus on configuration errors, known vulnerabilities, or even weak passwords.

Router Attacks

Routers can be attacked by either gaining access to the router and changing the configuration file, launching DoS attacks, flooding the bandwidth, or routing table poisoning. These attacks can be either hit-and-run or persistent. Denial of Service attacks are targeted at routers. If an attacker can force a router to stop forwarding packets, then all hosts behind the router are effectively disabled.

Router Attack Topology

The router attack topology is the same as all attack topologies. The steps include:

1. Reconnaissance
2. Scanning and enumeration
3. Gaining access
4. Escalation of privilege
5. Maintaining access
6. Covering tracks and placing backdoors

Tools & Traps…

Hardening Routers

The Router Audit Tool can be used to harden routers. Once downloaded, RAT checks them against the settings defined in the benchmark. Each configuration is examined and given a rated score that provides a raw overall score, a weighted overall score (1-10), and a list of IOS commands that will correct any identified problems.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks fall into three categories:

- **Destruction**. Attacks that destroy the ability of the router to function.
- **Resource consumption**. Flooding the router with many open connections simultaneously.
- **Bandwidth consumption**. Attacks that attempt to consume the bandwidth capacity of the router's network.

DoS attacks may target a user or an entire organization and can affect the availability of target systems or the entire network. The impact of DoS is the disruption of normal operations and the disruption of normal communications. It's much easier for an attacker to accomplish this than it is to gain access to the network in most instances. Smurf is an example of a common DoS attack. Smurf exploits the Internet Control Message Protocol (ICMP) protocol by sending a spoofed ping packet addressed to the broadcast address and has the source address listed as the victim. On a multiaccess network, many systems may possibly reply. The attack results in the victim being flooded in ping responses. Another example of a DoS attack is a SYN flood. A SYN flood disrupts Transmission Control Protocol (TCP) by sending a large number of fake packets with the SYN flag set. This large number of half-open TCP connections fills the buffer on victim's system and prevents it from accepting legitimate connections. Systems connected to the Internet that provide services such as HTTP or SMTP are particular vulnerable.

DDoS attacks are the second type of DoS attack and are considered multiprotocol attacks. DDoS attacks use ICMP, UDP, and TCP packets. One of the distinct differences between DoS and DDoS is that a DDoS attack consists of two distinct phases. First, during the preattack, the hacker must compromise computers scattered across the Internet and load software on these clients to aid in the attack. Targets for such an attack include broadband users, home users, poorly configured networks, colleges and universities. Script kiddies from around the world can spend countless hours scanning for the poorly protected systems. Once this step is completed the second step can commence. The second step is the actual attack. At this point the attacker instructs the masters to communicate to the zombies to launch the attack. ICMP and UDP packets can easily be blocked at the router, but TCP packets are difficult to mitigate. TCP-based DoS attacks comes in two forms:

- **Connection-oriented**. These attacks complete the 3-way handshake to establish a connection. Source IP address can be determined here.
- **Connectionless**. These packets SYN are difficult t trace because source

An example of a DDOS tool is Tribal Flood Network (TFN). TFN was the first publicly available UNIX-based DDoS tool. TFN can launch ICMP, Smurf, UDP, and SYN flood attacks. The master uses UDP port 31335 and TCP port 27665. TFN was followed by more advanced DDoS attacks such as Trinoo. Closely related to TFN, this DDoS allows a user to launch a coordinated UDP flood to the victim's computer, which gets overloaded with traffic. A typical Trinoo attack team includes just a few servers and a large number of client computers on which the Trinoo daemon is running. Trinoo is easy for an attacker to use and is very powerful in that one computer is instructing many Trinoo servers to launch a DoS attack against a particular computer.

Routing Table Poisoning

Routers running RIPv1 are particularly vulnerable to routing table poisoning attacks. This type of attack sends fake routing updates or modifies genuine route update packets to other nodes with which the attacker attempts to cause a denial of service. Routing table poisoning may cause a complete denial of service or result in suboptimal routing, or congestion in portions of the network.

Hit-and-Run Attacks and Persistent Attacks

Attackers can launch one of two types of attacks, either-hit and-run or persistent. A hit-and-run attack is hard to detect and isolate as the attacker injects only one or a few malformed packets. With this approach, the attacker must craft the attacks so that the results have some lasting damaging effect. A persistent attack increases the possibility for identification of the attacker as there is an ongoing stream of packets to analyze. However this attack lowers the level of complexity needed by the attacker as they can use much less sophisticated attacks. Link state routing protocols such as OSPF are more resilient to routing attacks than RIP.

Damage & Defense…

Forensic Analysis of Routing Attacks

During a forensic investigation the analyst should examine log files for evidence such as IP address and the protocol. It is a good idea to redirect logs to the syslog server. This can be accomplished as follows:

```
#config terminal
Logging 192.168.1.1
```

Investigating Routers

When investigating routers there are a series of built-in commands that can be used for analysis. It is unadvisable to reset the router as this may destroy evidence that was created by the attacker. The following show commands can be used to gather basic information and record hacker activity:

- Show access list
- Show clock
- Show ip route
- Show startup configuration

- Show users
- Show version

Chain of Custody

The chain of custody is used to prove the integrity of evidence. The chain of custody should be able to answer the following questions:

- Who collected the evidence?
- How and where is the evidence stored?
- Who took possession of the evidence?
- How was the evidence stored and how was it protected during storage?
- Who took the evidence out of storage and why?

There is no such thing as too much documentation. One good approach is to have two people work on a case. While one person performs the computer analysis, the other documents these actions. At the beginning of an investigation, a forensic analyst should prepare a log to document the systematic process of the investigation. This is required to establish the chain of custody. This chain of custody will document how the evidence is handled, how it is protected, what process is used to verify it remains unchanged, and how it is duplicated. Next, the log must address how the media is examined, what actions are taken, and what tools are used. Automated tools such as EnCase and The Forensic Toolkit compile much of this information for the investigator.

Volatility of Evidence

When responding to a network attack, obtaining volatile data should be collected as soon as possible. Although all routers are different, you will most likely be working with Cisco products as Cisco has the majority of the market share. Cisco routers store the current configuration in nonvolatile ram (NVRAM). The current configuration is considered volatile data and the data is kept in Random Access Memory (RAM). If the configuration is erased or the router powered down all information is lost. Routers typically are used as a beachhead for an attack. This means the router may play an active part in the intrusion. The attacker uses the router as a jumping off point to other network equipment.

When starting an investigation you should always move from most volatile to least volatile. The first step is to retrieve RAM and NVRAM. To accomplish this you may use a direct connection to the console port using RJ-45-RJ-45 rolled cable and an RJ-45-to-DB-9 female DTE adapter. In instances when a direct connection is not available a remoter session is the next preferred method. Insecure protocols such as FTP should not be used; an encrypted protocol Secure Shell (SSH) is preferred. You should make sure to capture both volatile and nonvolatile configuration for comparison changes and documentation purposes. Cisco routers have multiple modes, so to gain privilege mode the password must be known by the analyst.

Case Reports

Case reporting is one of the most important aspects of computer forensics. Just as with traditional forensics everything should be documented. Reporting should begin the minute you are assigned to a case. Although it may sometimes seem easier to blindly push forward, the failure to document can result in poorly written reports that will not withstand legal scrutiny.

Let's face it, not all aspects of computer forensics are exciting and fun. Most of us view paperwork as drudgery. It is a somewhat tedious process that requires an eye for detail. Don't allow yourself this fallacy. In the end, the documentation you keep and the process you follow will either validate or negate the evidence. The report is key in bringing together the three primary pieces of forensics: acquisition, authentication, and analysis.

The case report will be the key to determining one of the following actions:

- Employee remediation
- Employee termination
- Civil proceedings
- Criminal prosecution

When the investigation is complete a final written report is prepared. Some of the items found in this report will include:

- Case Summary
- Case Audit Files
- Bookmarks

- Selected Graphics
- File Location Path
- File Location Properties

Although this is not an all-inclusive list it should give you some indication of what should be included. Depending on the agency or corporation, the contents of the report will vary. What is consistent is that anyone should be able to use the logs and the report to recreate the steps performed throughout the investigation. This process of duplication should lead to identical results.

Incident Response

Incident response is the effort of an organization to define and document the nature and scope of a computer security incident. Incident response can be broken into three broad categories that include:

- **Triage**. Notification and identification
- **Action/Reaction**. Containment, analysis, tracking
- **Follow up**. Repair and recovery, prevention

Compromises

Before a compromise can be determined, investigators must be alerted that something has happened. It is best if the alert function is automated as much as possible. Otherwise, the sheer volume of log information would be overwhelming for an employee. Even with a high level of automation someone must still make a judgment regarding the validity of the alert. Once an attack has been validated it is important to reduce the damage of the attack as quickly as possible and work to restore normal business functions.

Summary

In this chapter, we reviewed how routers can play an important part in forensics. Readers were introduced to routed protocols such as IP and we discussed how routed protocols work. In many ways, IP acts as a "postman" since its job is to make the best effort at delivery. In a small network or those that seldom change, the route that the IP datagrams take through the network may remain static or unchanged. Larger networks use dynamic routing. Administrators use routing protocols such as RIP for dynamic routing. We also looked at how attackers attack routers and how incident response relates to routers and router compromises.

Solutions Fast Track

Network Forensics

- ☑ Network forensics is the process of examining network traffic for the purpose of discovering attacks and malicious events.
- ☑ Network forensics is commonly performed with a sniffer or packet capture tool.

Overview of Routers

- ☑ Routers are designed to connect dissimilar protocols.
- ☑ Routers deal with routing protocols.
- ☑ Common routing protocols include RIP and OSPF.

Hacking Routers

- ☑ Routers can be attacked by exploiting misconfigurations or vulnerabilities.
- ☑ Routers need to have logging enabled so sufficient traffic is captured to aid in forensic investigations.

Incident Response

- ☑ Monitoring for incidents requires both passive and active tasks.
- ☑ Incident response requires development of a policy to determine the proper response.

Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to **www.syngress.com/solutions** and click on the **"Ask the Author"** form.

Q: Why is network forensics important?

A: Network forensics are important because so many common attacks entail some type of misuse of network resources.

Q: What are the different ways in which the network can be attacked?

A: Attacks typically target availability, confidentiality, and integrity. Loss of any one of these items constitutes a security breach.

Q: Where is the best place to search for information?

A: Information can be found by either doing a live analysis of the network, analyzing IDS information, or examining logs that can be found in routers and servers.

Q: How does a forensic analyst know how deeply to look for information?

A: Some amount of information can be derived from looking at the skill level of the attacker. Attackers with little skill are much less likely to use advanced hiding techniques.

Q: Where do routers reside in relationship to the OSI model?

A: Routers are a layer 3 device.

Q: Do routers pass physical addresses?

A: No, not by default since routers are layer 3 devices and physical addresses are found at layer 2.

Q: What do routers do with broadcast traffic?

A: Routers block physical broadcast traffic.

Q: Why target routers?

A: Routers can sometimes be overlooked by security professionals since so much time is placed on securing workstations and servers.

Q: What is the first thing an attacker does when targeting a router?

A: An attacker must first identify the device and be able to verify it is a router. With this done the attacker must next determine the version and model of the router.

Q: What is the most important preplanning aspect of router forensics?

A: You must make sure good policies and procedures are in place that specify adequate logging is taking place.

Q: What type of skills are required for incident response?

A: Incident response requires technical skills, investigative skills, and leadership skills.

Q: How would you best define the incident response process?

A: Incident response is the process of detecting a problem, determining its cause, minimizing the damage.