

# Effective Data Investigation on Cisco Routers

by: Ophelia Livingston, 07/20/2005

<http://www.securitydocs.com/library/3474>

## Abstract

As we move past the new millennium hackers and crackers continually find ways to break into network systems. An effective method to maintain a lead on security threats is to keep current on the Internetworking Operating System (IOS) versions used in routers. The main elements of any incident management include the ability to detect, respond and recover from an attack. Knowing the elements of the attack and vulnerabilities exploited provides an opportunity to understand critical points in your network infrastructure. Addressing the three security principles, confidentiality, integrity and availability suggests that network administrators should constantly review and update configurations in routers to maintain a concerted effort of providing due care and due diligence in the network. When performing router security, network administrators should never divulge more information that does not need to be shared. This document provides steps needed to perform effective data investigation on Cisco routers using the router show commands for analysis.

## Introduction

Routers have many responsibilities during a network data analysis. Many times routers are used as targets during an attack. During the investigative work, routers can provide valuable evidence that will enable investigators to resolve the how and the why during an incident. Defense-in-depth defines routers as being designed at the perimeter of most networks and providing the main resources as "core routers" for intranet, Internet, and remote access implementations. According to Andrew Mason (2001), the SAFE Axioms of router security include:

- Locking down Telnet Access to a router
- Locking down SNMP access to a router
- Controlling access to a router through the use of TACACS+
- Turning off unneeded services
- Logging at appropriate levels
- Authentication of routing updates

Before analyzing routers network engineers should develop a framework that will set the stage for effective analysis. To understand router investigation, one should note that routers lack "data storage and functionality" of many other network devices, therefore they are less likely to be the ultimate target of attacks. Understandably, routers control perimeter access to the network, therefore once compromised networks are very vulnerable. Routers make an excellent starting point for attackers to penetrate the network. Valuable information during footprinting can be monitored and used to attack other areas within a network infrastructure.

When creating the framework for router investigation it is advisable to develop structured guidelines before the review. Start with a security policy, and develop a plan to include collecting and defining data. Secondly, create a reconnaissance methodology; this information will be used to acquire information about the target. Thirdly, perform an analysis check to include incidents, review default passwords, default information, and protocol standards. Fourthly, develop an attack strategy to include commands to analyze the network, access control lists, firewalls and protocols. Fully integrate these steps during incident management on routers to detect, identify isolate and eradicate network attacks.

## Looking for Proof

When investigating router incidents, incident response personnel will analyze different types of collaborative effects of collusion. Router intrusions are mainly seen at the perimeter of most networks to include unauthorized access and

eavesdropping. Exploitation of services encompasses weaknesses in areas of security awareness training, non-compliance of IOS updates, and limited skilled engineer training. Proper incident response gathering is a very critical component of Information Security (InfoSec) framework. Incident response involves reviewing log files, probing for mundane information, documenting the reports and reporting the analysis to management. Early invention becomes an integral step in containment and reducing the risk exposed by malevolent attackers. Performing intrusion detection on routers should include:

- Analyzing direct compromise
  - Intruder gains privileged access to the router
- Analyzing routing tables for manipulation
  - Attacks involving routing table manipulation compromise the functionality of the router.
- Analyzing theft of information
  - Information on the router consists of network topology and access control, passwords, IP addresses, port numbers, and topology information.
- Analyzing Denial of Service attacks
  - Looking for sporadic router reboots and degrading performance

## Obtaining Volatile Data

When responding to a network attack, obtaining volatile data should be collected as early as possible. In Cisco routers non-volatile ram (NVRAM) is the stored configuration of the router and current configuration is called volatile data. This data is kept in Random Access Memory (RAM). If the intruder deletes the configuration or powers down the Cisco router while in RAM, all information is lost. Depending on the attack, the router may be used as a stepping stone in the attack, or the router may have played an active part in the intrusion. To retrieve RAM and NVRAM, first establish connection to the router. It would be better to have a direct connection using the console port using RJ-45-RJ-45 rolled cable (different from crossover cable) and an RJ-45-to-DB-9 female DTE adapter. If direct connection is not available then use the encrypted protocol Secure Shell (SSH) to remotely access the router. Make sure to log the entire session with Hyper Terminal. Select the capture text => start to begin the log session. Capture both volatile and non-volatile configuration for comparison changes and documentation purposes. A Cisco router has multiple modes, such as login prompt, enable, initial setup, configuration and interface. The two primary modes are user mode and enable (privilege) mode. To gain access to privilege mode the password must be known by the analyst.

## What to Analyze First?

When conducting an investigation on a router, there are many show commands that can be used. Once in the router, an attacker can change the enable password stored in memory. Without knowing the current privileged password, authorized users will have to reboot the system, losing the attacker's configuration command, and losing comprehensive reporting of the router. The following show commands will be reviewed in this paper:

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

## Show clock and Show version

Recording the system time will be critical when cross-referencing data during an incident. Using the *show clock* command in the router records the investigative start time. The slide capture in **figure 1**, illustrates the *show clock* command. The output from *show clock* indicates a recorded time of 03:02:37 UTC on June 3, 2005. Next record the system uptime. This command is

critical when cross-referencing data and determining the time the incident may have occurred. Another reason to use the above command is for pin pointing the time that the system router has been online since the last reboot providing a timeline of current history of the router. To obtain system uptime information, use the `show version` command. As observed in **figure 2** the red arrow points to the system uptime of the router. The `show version` provides a significant amount of hardware and software about the router. The platform is Cisco 3640 router, Cisco IOS version is 12.2(13b) the system image file is c3640-ik8os-mz.122-13b.bin, router interfaces, 64,000 K of DRAM memory, 2 fast Ethernet port, 4 serial network interfaces, and 2 Voice FXO interfaces, 2 Voice FXS interfaces, 24 Megabytes flash memory and configuration register 0x2102. Analyzing these features will provide a significant understanding of router in question.

```
Livingston#show clock
09:02:37.047 UTC Fri Jun 9 2005
Livingston#
```

Figure 1: Show Clock command

```
ROM: System Bootstrap, Version 11.1(20)AA2, EARLY DEPLOYMENT RELEASE SOFTWARE (FC1)

Ophelia uptime is 6 minutes
System returned to ROM by power-on
System image file is "flash:c3640-ik8os-mz.122-13b.bin"

cisco 3640 (R4700) processor (revision 0x00) with 64416K/5120K bytes of memory.
Processor board ID 16828277
R4700 CPU at 1800Mhz, Implementation 33, Rev 1.0
Bridging software.
X.25 software, Version 3.0.0.
SuperLAT software (copyright 1990 by Meridian Technology Corp).
2 FastEthernet/IEEE 802.3 interface(s)
4 Serial network interface(s)
2 Voice FXO interface(s)
2 Voice FXS interface(s)
DRAM configuration is 64 bits wide with parity disabled.
125K bytes of non-volatile configuration memory.
24576K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102
```

Figure 2: Show Version Command

## Show users

If the network analyst is directly connected to the console port of the router, an attacker may be unaware of this event. To determine who is logged into the router use the `show users` command. This command is very useful to determine what host IP address is in the router.

```
Livingston#show users
Line          User             Host(s)          Idle           Location
* 0 con 0      User              135.25.9.1      00:00:00
-198 vty 0     User              idle            00:00:00 195.25.9.1

Interface    User             Mode              Idle           Peer Address
```

Figure 3: Show users command

The output shows that two users are currently logged onto the router.

- The first entry shows that someone is logged in at the console port with host IP address 135.25.9.1
- The second entry is a virtual terminal connection. The asterisk (\*) on the far left indicates the current connection has been made to IP address 135.25.9.1.

This is useful information when investigating incidents. When an unauthorized user is logged on to the victim's system, reevaluate and review the chain of evidence before proceeding with the investigation. At this point the attacker may realize that an investigation is under way. To avoid lost configuration, save the configuration to NVRAM.

## Show startup-configuration

Router configuration files are stored in a single configuration files. These router files controls all aspects of the router's behavior and stored in NVRAM. The router will use these stored configuration files to boot the router. The router's configuration file can be modified using the active configuration file called RAM. The attacker may change files located in RAM to manipulate and modify the system files. Use the show startup-config command to compare the show running-config two files on the router. To compare active and stored configurations in Cisco routers use the following commands;

```
Router_A# show running-config

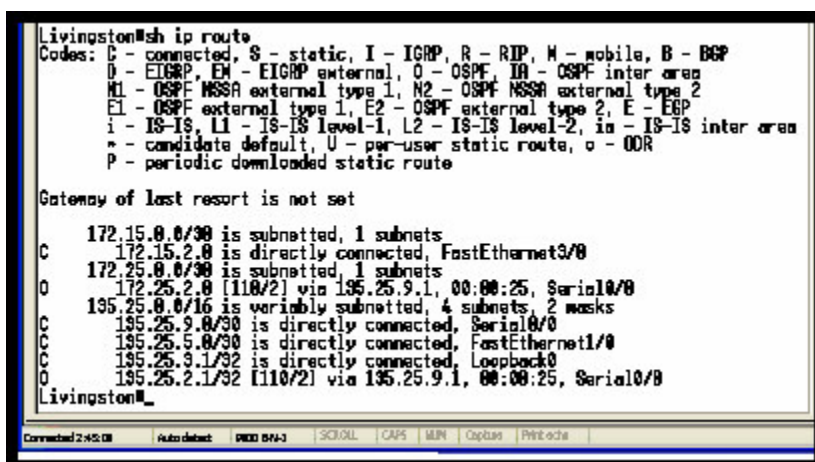
Router A# show startup-config
```

There are times when it is crucial to save the aforementioned configurations to a remote server using a Trivial File Transfer Protocol (TFTP) server on the network. There are many software TFTP server packages available on the Internet. An example of configuring the TFTP server is listed below using the IP address of 192.168.1.2:

```
Router_A# copy running-config tftp
Remote host [] ? 192.168.1.2
Name of configuration file to write [IA8040]? ENTER
Write file IA840 on host 192.168.1.10? [confirm] ENTER
Building configuration...
Writing IA8040 !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!! [OK]
```

## Show ip route

The routing table contains the path of how a router forwards packets. If an attacker changes the routing table, then the attacker can dictate the packet flow. Session hijacking occurs when packets are diverted to an unauthorized path called a covert channel. Manipulating the routing table is the primary reason attackers' compromise routers. To view the routing table, use the `show ip route` command. In **figure 4**, there are directed connected route, and ospf routes.



```
Livingston#sh ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

 172.15.0.0/30 is subnetted, 1 subnets
 C    172.15.2.0 is directly connected, FastEthernet3/0
 172.25.0.0/30 is subnetted, 1 subnets
 O    172.25.2.0 [110/2] via 135.25.9.1, 00:00:25, Serial0/0
 135.25.0.0/16 is variably subnetted, 4 subnets, 2 masks
 C    135.25.9.0/30 is directly connected, Serial0/0
 C    135.25.5.0/30 is directly connected, FastEthernet1/0
 C    135.25.3.1/32 is directly connected, Loopback0
 O    135.25.2.1/32 [110/2] via 135.25.9.1, 00:00:25, Serial0/0
Livingston#
```

Figure 4: Show ip route command

This information is very easy to follow. At this point an attacker can spoof the network, affecting the integrity of routing

information and the router. If a malicious static route appears, the attacker can manipulate the router's configurations.

## Using Routers as Response Tools

During an incident response, reviewing the router's access control lists provides a listing of protocols, source/destination IP addresses, TCP or UDP port activity, ICMP message types and more. Access control lists are used to implement security policies in the network and create rules. A well-configured router is often used to supplement a firewall creating defense-in-depth. Access control lists can be used to eliminate traffic by denying traffic to the specific interface. All access control lists are based on six principles:

- Deny traffic which is not specifically permitted
- Access list control traffic in one direction (inbound or outbound) on the interface.
- Every packet is examined against an applied access list in the direction of that particular packet.
- Packets are compared against the access list using the top-down approach. There is an implicit deny statement at the end of every access list.
- Outbound packets are routed to appropriate physical interfaces before being applied.
- Inbound packets are compared to the access list, and if permitted are routed to the appropriate physical interface.
- Only one access list may be applied to one physical interface using either outbound or inbound traffic.

```
Livingston#show access-list
Extended IP access list 105
  permit udp any any range 16984 16484
  permit tcp any any eq 1720
Livingston#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Livingston(config)#_
```

Figure 5: Show access-list

IP address spoofing is one of the oldest and most dangerous techniques used by an attacker. If an attacker can masquerade as a trusted network address, then the attacker's goal has been accomplished which is to get inside of the network. One of the main reasons to spoof a routes IP address is to perform a Denial of Service (DoS) Attack on a network denying the availability for authorized users to access data. As stated in Incident Response & Computer Forensics, "if an attacker can force a router to stop forwarding packets, then all hosts behind the router are effectively disable". If a router is sporadically rebooting itself, or there is performance degradation, possibly attempts to over utilize a network router is being performed. Filtering the router's perimeters at both the ingress and egress boundaries will reduce this attack.

## Summary

A router's main function in a network is to discover the "best path" for packet flow through the network. Routers become targets during an intrusion because these devices control access at the ingress and egress points of networks. As a security analyst, monitoring router vulnerabilities requires expertise and technical skills to reduce network weaknesses against draconian attacks. Many Cisco Router show commands may be used to provide detailed information about a router's IP addresses, access-lists, interfaces, and packet routes when investigation incident responses. Routers will remain critical to network access, seemingly router attacks will always abound. In the midst of a computer or network crime security analysts should recognize the capabilities of a router to circumvent and reduce the amount of vulnerabilities and attacks.

## References

Mandia, K., Prorise, C., & Pepe M. (2003). *Incident response & computer forensics*. Emeryville, CA. McGraw-Hill/Osborne.

Mason, A. G., Newcomb. (2001). *Cisco secure internet security solutions*. Indianapolis, IN. Cisco Press.

Schultz, E., & Shumway, R. (2002). *Incident response. A strategic guide to handling system and network security breaches*. Boston, MA. Newriders.

Tanase, M. (2003). IP spoofing: an introduction. Retrieved on June 15, 2005 from website:  
<http://www.securityfocus.com/infocus/1674>.

Tiller, J. S. (2005). *The ethical hack*. Boco-Raton, WA. Auerbach Publications.