Executive Summary

Though network devices have primitive storage capabilities compared to computers, the information stored in their configuration and logs can be pieced together with a map of the network to identify evidence that cannot be attained otherwise. Because network devices are the point of entry into a network and they are targets. It is critical that the Forensic Investigator (FI) use the information from network devices to assess the extent of a compromise.

DF Purpose

Network Devices Distinctions

It is not possible in this paper to cover the basics of networking but I think it would be useful to mention some differences between the various classes of network devices. A router is a device that connects two networks. When it receives a packet on an interface it looks at the destination IP address of that packet and forwards it to the appropriate network. A packet is a basic unit of network traffic and an IP address corresponds to the address for a particular computer on a network. A router can also offer security through the use of Access Control Lists (ACL). Using ACL a router can act as a firewall (which filters traffic). This simply means that there are rules for what types of traffic the router will allow. A switch is a less sophisticated device than a router. It looks at the MAC address of a packet and determines which port it should send that traffic to. The MAC address is the unique address that each network interface (or network card) has. A hub is the most primitive network device that doesn’t analyze traffic at all. When a hub receives traffic on one port it will broadcast that traffic to all of its other ports. The nuances of each of these different devices have security implications that the FI must fully understand in order to effectively conduct Network-Centric Forensics.

Live Collection and Analysis

The information collected from network devices is not always directly decisive. Often it requires deductive conclusions based on a plethora of information from various sources (e.g. network topology, logs, startup configuration, running configuration, ARP tables, routing tables, etc.). To start with the FI need not only have an extremely high level of knowledge in networking but also experience with the devices under investigation. This is especially true when it comes to intricate devices like routers, VPN Concentrators,
Firewalls, Intrusion Detection devices, etc. The reason being most useful conclusions require an aggregate analysis of network device configurations. If a device has been compromise typically it will be reconfigured in a way to allow or perpetuate some kind of malicious activity. The strategy used by the perpetrator might be extremely subtle and clever. If the FI does not understand the consequences of each configuration setting as well as the collective configuration these clues are likely to be missed. For instance, the Cisco IOS, has functionality to set up ACL. These are a sequence of rules that allow or deny specific types of network traffic. Because ACL are processed sequentially if the very first rule allows all types of traffic the rest of the rules are never processed. Consequently, a single rule in an ACL could cause the entire network to be vulnerable [1]. It is therefore critical that the FI be very familiar with the particular device that is under investigation.

What can be collected from network devices? Generally most network devices do not have permanent storage (e.g., hard drive) like computers do. One exception is that a computer can be configured to act as a router. A typical network device has storage for configuration similar to how a computer saves the BIOS setting. Subsequently, there is typically no storage device that can be removed and analyzed in a lab. Usually, the Forensics Investigator will be required to perform a live analysis of the device. Furthermore, typically network devices are part of the critical infrastructure to an organization that can not be removed or taken off line but for a brief period of time. This is yet another reason why the FI must be a skilled with the device under investigation.

Many network devices have logging capabilities. This can be a very useful source of data but this is contingent upon a few factors. First, has logging been enabled on this device? Because of the extra overhead involved with logging, most network devices do not have logging enabled by default. If the device has been compromised the logs may have been erased. There should be evidence that of this. But let’s say that the FI comes on the scene and logging on a particular device is turned off. Can the FI conclude that it was turned on at one time and that a perpetrator has turned it off? It will depend on whether the organization has trustworthy documentation on all accesses and configuration to this device. Many network devices are able to send the log activity to another device for long term storage. For instance, a router might send its logging information over the network to a computer that receives and stores this information. Depending on the level of detail, these logs can be a wealth of useful information for the FI. The drawback to looking trough logs can be time consuming and tedious to extract useful information from them.

Another source of information is the current running configuration. Many network devices can have two different configurations, the current configuration (e.g. running configuration) that the device is using and a configuration that used when the device is booted up (e.g. startup configuration). It is very useful for the FI to compare these two configurations. If the device has been compromised and if the perpetrator is trying to covering their tracks they might only change the running configuration and leave the start up configuration as it was. One of the common tactics of network administrators when debugging network issues is to reboot a network device. Thus, if the perpetrator changed a setting that caused a noticeable issue, then the network administrator might reboot the
device and the evidence of compromise will have been lost. Consequently, it is very important that the FI capture the running configuration before the device is rebooted or this information will not be recoverable. Subsequently, any difference between the running configuration and the startup configuration should raise a flag for the FI. It is possible that the perpetrator changed the password on the router. With Cisco routers the only way to recover the password is to reboot the devices. If this is the case the current running configuration will certainly be lost. But in this scenario the FI will also know immediately that the device has been compromised.

It is also very useful to know how long the router has been running. Some network devices are very vulnerable when they are first booting up. Thus some exploits capitalize on this small window of time to take control of the device. Another critical piece of data that the FI should look for is who is logged in to a network device and from where (locally, remotely)? It is very possible that the perpetrator is still logged into a compromised device. If this is the case and the FI wants to be undetected then the desired data should quickly be extracted before the perpetrator notices someone else logged in. Of course it might be the case that because of policy or legal issues that a compromised device be taken offline until the security flaws have been identified and eradicated.

Some of the more elaborate attacks on network devices do not require that a malicious users login to the network device. For instance, if a router is configured to accept updates that affect its routing table without first authenticating this information, then a wily hacker could manipulate a router by sending it a routing update causes it to send traffic destined for a particular network to a different network. A routing table is a mapping that a router uses to determine which network to send traffic to. The consequence could be that the traffic destined for www.mybank.com is now going to www.hackedbank.com. Another consequence could be that traffic destined for multiple networks is now sent to one particular network. This would then funnel large amount of network traffic to a single network possibly overwhelming the network devices for that network and rendering it unreachable. Subsequently, the router can become a weapon used by a malicious user to overwhelm and thus render a particular network unreachable (e.g. a Denial of Service attack or DoS attack). What if the target network is part of a critical infrastructure for a city’s power grid?

Thus far we have focused on routers. Many of the techniques used on routers apply to other devices but the way at which the information is accessed might be very different. Another class of network device that is common on most networks is a switch. It is becoming more common for higher end switches to have advanced management and monitoring features that were once only available to routers. Many of these features can be used to for gathering valuable forensic evidence. Typically this information is similar to that found on routers but limited to the functionality of the switch class. For instance, switches do not “route” traffic thus they do not have a routing table. One of the classic attacks on a switch is “ARP poisoning”. This is the process of manipulating the switch to send traffic to ports that traffic is not intended for. This might be done in conjunction with a Man-in-the-Middle attack where a malicious user inserts themselves between the
victim and the victim target during a sensitive transaction (e.g. while you are logging into your bank).

Other Sources of Data

Aside from information directly related to the network devices there are other sources that are necessary when analyzing an incident. Network topology is the map of the network and its devices. When analyzing router ACL or logs, the implication of these items required comparing them to the topology. Without an understanding of the topology the FI will not be able to infer the consequences of information gathered from the network devices.

Setting up a network monitoring systems and sniffing traffic can be a useful source of information. Though, this is not a substitute for analyzing the configuration and logs. Still, how a network device is handling network traffic can be very insightful. This type of empirical evidence might be able to guide the FI as to what to look for.

State of Practice

In [1] chapter 16 an excellent job is done taking one through a step by step analysis of a Cisco router. Though I think this exercise is very useful, I would caution the reader that there are many subtleties to the Cisco IOS that can not be fully understood from a simple step by step check list. The Cisco IOS is unintuitive and more intricate than it appears on the surface. If one is interested in learning the Cisco IOS there is an open source project [2], that emulates a Cisco 7200 router. Using this software one could learn the Cisco IOS with needing access to a multi-thousand dollar device. Though many of the techniques discussed should be platform independent most of my experience is with Cisco equipment so the some of the specifics discussed might be different for other vendors’ devices.

The two main sources of data that is gathered from a network device are configuration and log data. How these are collected is specific to the device. Generally configuration is captured by logging into the device. Logs can be either stored on the device or elsewhere. Analysis tools can be very useful for parsing through log data. The downside is that there is no standard logging format and the FI must rely on vendor specific tools, use whatever standard string extraction methods are available.

The best set of tools that a FI has at their disposal when investigating a network device is a solid understanding of networking as well as experience with the common devices. The latter is a very specific skill set that requires access to expensive equipment. If the members of the FI lack experience with the devices under investigation but are knowledgeable in networking one option would be to collaborate with the on-sight network administrator. Ultimately, when it comes to analyzing a sophisticated network device there is no substitute for experience.
Works Cited

[1] Incident Response and Computer Forensics – Mandia, et.al