GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Detecting and Stopping Internal Attacks

By

Clifford Kobashigawa
Username: clkobas001

GIAC Security Essentials Practical Assignment v1.4.b (option 1)

December 6, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1. Abstract.

This paper presents a tutorial or "how to" on detecting and stopping internal attacks in a Cisco Switched wide area network. This paper will take you through the various stages of trouble shooting a network slowdown symptom and explain how to close in on the real problem by providing detailed step-by-step instructions in locating a suspect internal workstation. The problem being referenced within this paper is a workstation infected with the W32.Welchia.Wom (nachi virus), issuing ICMP echo requests. The following instructions, however, are not specific to the nachi virus and may be used in other situations.

In essence, this paper is intended to help network security personnel detect and stop a disruptive workstation. This is not new information but rather a collection of valuable information that should be shared amongst network personnel, responsible for a virus free network.

2. Trouble Shooting Introduction and Phases

As mentioned above, this tutorial will focus on providing detailed instructions to detect and stop an internal attack. This will be accomplished by presenting the entire topic in a trouble call format broken down into the following sections. This approach is intended to set the stage and logic for each instructional phase:

- Understanding the existing network environment.
- The reported disruptive symptoms.
- Beginning the initial trouble shooting.
- Escalating the problem.
- Searching for clues and symptoms.
- Narrowing down the possibilities.
- Focusing on a true lead (determine the MAC address from the ip address).
- Locating the workstation (step by step instructions).
- Stopping the internal attack.
- Paying a friendly but quick visit.
- Closing the incident.

Note: The subsequent trouble call scenario actually occurred. For this paper, however, the referenced ip addresses have been changed to simulate the actual event.

Hopefully you will never be faced with infected workstations on your internal network. Should that happen, please remember that the following instructions do work and may help you detect then stop a malicious internal attack.

3. Understanding the existing network environment.

Below is the baseline network infrastructure that the detailed instructions are applicable to:

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Four major and 20 remote sites all interconnected.
- A 2,000+ workstation environment.
- Several Cisco 7206 Routers, Cisco Catalyst 6500 Switches, many Cisco 3500 and 2900 edge switches, and 2 Checkpoint Firewalls.
- Internal ip addresses are all within the private 10.0.0.0 range.
- Workstation ip addresses are issued by dhcp.
- Workstations are a combination of various Microsoft and other vendor platforms.
- Windows workstations run antivirus software.
- Windows workstation OS (operating system) updates are pushed to the workstation.

Let's begin with the simulated trouble call. The step-by-step instructions will be explained as the investigation effort escalates.

4. The reported disruptive symptoms.

Your pager vibrates and the help desk's message says "users cannot get their email". You stop working on that overdue project and proceed to check your email. You retrieve your mail although it seemed a bit slow. After completing some simple email sends and receives, you feel quite confident the email servers are operational. Your initial assessment is that it was just a period of heavy email activity.

5. Beginning the initial trouble shooting.

After several minutes another page is received regarding widespread reports of users having problems retrieving their email. You access email again and this time you can't reach the server. Subsequent attempts are sometimes successful. Since you are able to intermittently process email, you feel somewhat confident the servers are operational. To be sure though, you next attempt to access the servers from the internet.

How do you access your network from the internet? In our case, we've subscribed to and installed a cable modem connection to our office. This allows us to access our network from a workstation through the cable modem's Internet Service Provider. Because it is not protected by a true firewall, workstations are physically attached only when necessary. This connection has become one of our major tools in testing and trouble shooting external connectivity to or from our network.

Back to the scenario. From the internet, you discover connections to email is quick and consistently successful. You now know your email system is OK but internal access to those servers fail intermittently. You begin to suspect some internal routing problem or failing network segment. Time to dig deeper.

6. Escalating the problem.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

At this point you believe the network is being disrupted although you're not sure where such activity could be taking place. You try accessing other servers on the same dmz segment as the email server. Symptoms are similar. Access from the internal network is slow or inaccessible while access from the internet is fine. You report the problem and it's seriousness to your supervisor and associates, and ask if there were any recent network changes. None are reported so you enlist everyone's help in locating and identifying the problem.

7. Searching for clues and symptoms

Someone checks the firewall logs, since the email server's dmz is connected to the firewall. Another checks the Cisco Core switches and internal routers for high activity. Yet another conducts test from various segments, attempting to find general patterns of inaccessibility. The help desk is also contacted to reconfirm if the trouble is enterprise wide or confined to a specific user segment. While all of these activities are occurring, you also consider the possibility of being under some denial of service attack.

After several minutes, your associates report the following significant findings:

1. For a brief period, a particular Cisco Catalyst 6500 core switch was running at 99%.
2. The firewall logs show sporadic yet high amounts of icmp echo requests (pings) from 3 workstations. The entries' timestamps are close to the time of the initially reported problems.
3. Oddly, internal access to email is available once again.

From these reports, you determine the problem was intermittent and feel certain it will reoccur. You decide to pursue the matter.

8. Narrowing down the possibilities

At this point your best source of information is from the firewall log. You review the high amount of icmp traffic from 3 workstations and notice one workstation sent ICMP traffic to the entire range of addresses on the email server's dmz segment. You also notice that these 3 workstations are on the same internal ip segment connected to the core switch which was running at 99%. You decide to locate the 3 workstations.

Because the firewall is the default gateway, it only records traffic that passes through it. This accounts for traffic to the internet and most dmzs. In this scenario, the infected workstations were issuing ICMP echo requests to various DMZ segments. As a side note, the nachi virus reportedly sends ICMP requests to an entire class B segment. For the details, go to the Symantec's Security Response – W32.Welchia.Worm (Nachi Virus). Oct. 8, 2003. web site listed in References.

Granted, the firewall logs were informative, however detecting the ICMP requests via the firewall is not the solution. We can assume there was a significant amount of ICMP

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

traffic traversing all internal segments prior to the firewall's logged events. Perhaps the huge internal bandwidth made the internal ICMP echo request traffic go unnoticed.

Before proceeding further, there are 5 cisco commands and 1 cisco configuration statement that will be presented.

> Information on the following 3 commands and 1 statement can be found at the Catalyst 6500 Series Cisco IOS Command Reference, 12.1 E reference.
>
> > "ip route-cache flow" (configuration statement)
> > "sho ip cache flow" (show command)
> > "sho cdp neighbor detail" (show command)
> > "sho mac-address-table address" (show command)
>
> Information on the following 2 commands can be found at the Catalyst 6000 Family Switch and ROM Monitor Commands reference.
>
> > "sho cam" (show command)
> > "sho port" (show c ommand)

To detect specific traffic within your internal network you could query the Cisco MSFC (MultiLayer Switch Feature Card). The MSFC requires the following configuration statement in each vlan interface that you seek information from. Cisco's **"**NetFlow on Logical Interfaces" is the IOS software that provides this feature. Netflow is listed as a reference.

```
"ip route-cache flow"
```

Below is an interface configuration example for vlan 99 in the MSFC:

```
Interface Vlan99
 Description Vlan 99 segment
 Ip address 10.100.50.254 255.255.255.0
 Ip access-group 110 out
 Ip helper-address 10.75.1.1
 Ip route-cache flow
 No ip redirects
```

With the statement added, run the following command at the MSFC to specifically seek ICMP echo requests:

```
 "sho ip cache flow | include 0800"
```

If a workstation is infected and issuing ICMP echo requests, you should see all virus initiated requests to various addresses within a class B segment. The infected workstation's ip address will be listed as the source. Below is an example of the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

command and the MSFC's response. The sending workstation (10.100.50.1) is on vlan 99 and the pinged ip is 10.50.25.11:

```
B01_MSFC#sho ip cache flow  |  include 0800
Vl99            10.100.50.1    Null         10.50.25.11    01  0000  0800
```

In the above example, the protocol type is 01 (ICMP), ICMP packet type and code is 0800 (echo request). More ICMP header information may be found in Volume 1, chapter 3 of the SANS Security Essentials with CISSP CBK Text. This is listed as a reference. This tool will help you track down a malicious workstation.

As a side note: Our staff learned this capability shortly after the initial nachi virus was detected. Subsequently, a workstation became infected and upon running this query, we immediately saw hundreds of ICMP echo requests being issued from the infected workstation. With this information, we were able to quickly locate the workstation and shutdown its edge switch port.

9. Focusing on a true lead (determine the MAC address from the ip address)

Back to the scenario. The 3 suspect workstations listed in the firewall's log were issued ip addresses by dhcp. This meant the workstations could be anywhere. Regardless, the key to finding a workstation in a Cisco switched network lies in knowing the workstation's media access control (MAC) address. Once the MAC address is known, there are ways to physically locate the workstation.

10. Locating the workstation (step by step instructions)

The step by step instructions will focus on the following commands assuming the ip address is known. Details of each command will follow.

1. From a windows workstation's dos prompt, enter the "nbtstat" command to obtain the suspect workstation's MAC address. This will work if the suspect workstation is another windows workstation or server.

2. If the workstation is not running windows, query the dhcp server's leases addresses file. Each leased address entry should include the MAC address.

3. At a Cisco core switch, enter the "sho cam" command with the MAC address to find a trunk or workstation port that knows of the MAC address.

4. Lastly, if the "sho cam" command identified a trunk port, telnet to each edge switch on that trunk and enter the "sho mac-address-table address" command to find the port on the edge switch that knows the MAC address.

10.1. Using NBTSTAT

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Once the ip address of a Windows workstation or server is known, its MAC address can be found by running the following DOS command:

“nbtstat –A <workstation’s ip address>”

The “-A” sends a query directly to the workstation. A fictional example is shown below targeting ip 10.100.50.1. Note the MAC Address, 00-50-08-92-C4-B9, at the very bottom. Additionally, the workstation’s hostname, ABC-123456, is also shown. A good practice is to use meaningful information (inventory tag#) in the hostname field.

```
C:\>nbtstat  –A  10.100.50.1

Local Area Connection 3:
Node IpAddress: [10.200.50.10] Scope Id: [ ]

          NetBIOS  Remote  Machine  Name  Table

     Name                     Type           Status
     ------------------------------------------------------------------
     ABC-123456       <00>     UNIQUE         Registered
     XYZ              <00>     GROUP          Registered
     ABC-123456       <03>     UNIQUE         Registered

     MAC Address  -  00-50-08-92-C4-B9
C:\>
```

Nbtstat details may be found at the Reference URL for Microsoft Technet – Nbtstat.

10.2 Viewing DHCP Server’s Leases

If the suspect workstation is not running windows (perhaps an Apple workstation), you could find the MAC address in the dhcp server. Query the dhcp server’s lease addresses file. Look for the ip address and you should find the corresponding MAC address. Details may be found at the Windows 2000 Server – Displaying DHCP server Information reference site. Below is an example of an entry format typically found in a Windows 2000 dhcp server.

```
10.100.50.1     ABC-123456.XYZ.COM      11/22/2003  3:37:08 PM     DHCP     00500892c4b9
```

Note the information:
Ip address: 10.100.50.1
Hostname: ABC-123456.XYZ.COM
Lease renew date and time: 11/22/2003 3:37:08 PM
MAC address: 00500892c4b9

© SANS Institute 2004, Author retains full rights.

In a Redhat Linux 7.2 dhcp server, look for the /var/lib/dhcp/dhcpd.leases file. Copy the file to a word document then search for the ip address. You'll be presented with similar information as above. Details may be found at the Red Hat Linux 7.2 Bible reference.

10.3 SHO CAM COMMAND (at the Cisco core switch)

Once the MAC address is known, you can begin tracking down the workstation. Start at the Cisco core switch and enter the following command:

"sho cam 00-50-08-92-C4-B9"

Below is an example of the command and its reply. For this example, the reply has been shortened to show only significant information. Note the details identifying the trunk port that knows of this MAC address. You'll need to determine where the trunk port (3/22) goes to by relying on well documented port configuration descriptions.

```
B01_6006> <enable>  sho cam 00-50-08-92-C4-B9
* = Static Entry. + = Permanent Entry. # = System Entry.  R = Router Entry.
X = Port Security Entry $ = Dot1x Security Entry

VLAN   Dest Mac/Route Des   [CoS]  Destination Ports or VCs / [Protocol Type]
99     00-50-08-92-C4-B9           3/22  [All]
Total matching CAM Entries Displayed   =1
```

In the above "sho cam" example, the Destination Port is 3/22. Below is the subsequent query of port 3/22 to learn its description as "Trunk_to_Sales". This means 3/22 is a trunk port to a possible edge switch or stack of edge switches in the Sales Office. Be prepared to telnet to each of these edge switches for further querying.

10.4. SHO PORT COMMAND (at the Cisco core switch)

```
B01_6006> <enable>  sho port 3/22
Port   Name              Status      Vlan    Duplex   Speed    Type
3/22   Trunk_to_Sales    Connected   Trunk   full     1000     1000BaseSx

        (Remaining sho port details omitted for this example)
```

10.5. SHO CDP NEIGHBOR CAM COMMAND (at the Cisco core switch)

In addition to learning where port 3/22 goes, you can obtain details of port 3/22 by running the "sho cdp neighbor detail" command at the core switch. This command

© SANS Institute 2004, Author retains full rights.

gives you details of every port including details of the distant switch device that is connected to each port. Below is an example of the “sho cdp neighbor detail” response. Most important is the ip address (**10.0.2.38**) of the distant switch connected to port 3/22.

```
B01_6006> <enable>  sho cdp neighbor detail

Port  <Our Port>:  3/22
Device-ID:  Sales_2924
Device Addresses:
   IP Address:  10.0.2.38
Holdtime:  161 sec
Capabilities:  SWITCH  IGMP
Version:
   Cisco Internetwork Operating System Software

        (remaining details not shown)
```

10.6. SHO MAC-ADDRESS-TABLE ADDRESS

The “sho cam” command above, identified a trunk port. You must now telnet to each edge switch connected to the trunk port and run the “sho mac-address-table address” command. Below is an example of the command and its reply.

In the example below, assume you’ve just telneted to the only Cisco 3524 edge switch in the Sales Office.

```
Sales_3524#sho mac-address-table address 0050.0892.C4B9
Non-static Address Table:
Destination Address   Address Type   VLAN    Destination Port
0050.0892.c4b9         Dynamic        99      FastEthernet0/7
Sales_3524#
```

11. Stopping the internal attack.

Note the how the specific port (FastEthernet0/7) is identified above.

Now that you know the edge switch port, must decide whether the port should be immediately shutdown or not. If it is not causing further harm, you may want to keep it operational while you dispatch personnel to find the workstation and perhaps even a malicious user. Shutting down the port may signal a malicious user that someone’s detected their activity. In most situations, you will choose the immediate shutdown.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

To actually locate the workstation, you must physically start from the switch port and follow the cabling back to the workstation. Once at the workstation, you can verify its ip and MAC addresses. However, following cable to a workstation is not an easy task especially if your documentation does not explicitly show wall outlet locations. Another solution is to place equipment inventory information in the workstation's hostname. If you recall, the hostname appears in the dhcp addresses file. If the inventory information is known, it could be looked up by the inventory manager for the workstation's location and assigned user.

11.1. Shutting down the specific port

To shutdown a specific Cisco 3524 interface port, telnet to the remote switch and enter the configuration terminal mode. In this mode, access the specific interface and enter the "shutdown" command. This will immediately shutdown the port. Save your change and exit the switch. Details may be found at the Cisco Catalyst 3500 Series XL Switches – Cisco IOS Commands reference site. Below is an example of fast ethernet port 0/7 (fa0/7) being shutdown and the configuration change being saved.

```
Sales_3524#config t
Sales_3524<config>#interface fa0/7
Sales_3524<config-if>#shutdown
Sales_3524<config-if>#exit
Sales_3524<config>#exit
Sales_3524#write memory
Sales_3524#exit
```

In addition to dispatching IT Network personnel, if the site is some distance away, you may choose to contact a trusted user at the site. Having that user quickly walkthru the area looking for any suspicious activity or person is worth it.

Remember, you have the option of shutting down the port if malicious activity starts up again or you may immediately shutdown the port if you believe it will prevent a virus from spreading. Make a decision then take action. If the port is shutdown, make sure your network is back to normal. Do not assume that fixing one problem means all is well. There may be other infected workstations affecting the network. Keep querying the MSFCs observing cpu utilization and ICMP echo request traffic flow.

12. Paying a friendly but quick visit

A quick visit is imperative. After locating and verifying the suspect workstation, you'll typically uncover an infected machine. This may occur if its antivirus definition files are not current and self scanning is not being accomplished according to the enterprise's schedule.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Workstations that are only powered on when needed, will typically fall behind in 1) obtaining current definition files and 2) performing its self scanning routine. These could be training lab workstations or shared workstations that are only used (powered on) when needed.

An infected workstation must be scanned and cleaned before it is reconnected to the network. Be sure dispatched staff are well trained in detecting viruses and completing the cleanup process. The worst situation is to have a repeat denial of service incident from the same workstation. Remember, denial of service attacks are disruptive not only to the network but more so to the enterprise's business operation.

13. Closing the incident

Once the workstation has been cleaned and stabilized, notify all concerned parties, especially those responsible for antivirus software. They must be made aware of the incident to ensure enterprise virus detection and protection practices are being followed and truly safeguarding the enterprise's computer resources. Notify the help desk that the incident is closed. This will ensure any subsequent disruptions will be reported as new problems. Finally brief your supervisor and co-workers on the outcome.

14. Summary

This paper explained the trouble shooting process and provided the necessary step-by-step instructions to detect and stop an internal attack. Initially, the effort begins with a trouble call and eventually leads to suspecting malicious activity from one or more workstations.

The key steps were 1) identifying the workstation 2) learning its ip address 3) using the ip address to determine its MAC address 4) using the MAC address to locate the physical Cisco edge switch port number 5) shutting down the port and 6) locating the workstation by tracing cable or relying on hostname information. Lastly, the suspect workstation must be visited immediately to resolve the malicious activity.

In closing, this paper provides useful information to all network personel seeking to locate workstations and stopping an internal attack. The steps may have appeared complicated however they do work and become easier after using them a few times. Hopefully though, your network remains virus free and these command line tools will be used for other purposes.

15. References:

Symantec's Security Response – W32.Welchia.Worm (Nachi Virus). Oct. 8, 2003. Technical Details, items 6 and 7.
http://securityresponse.symantec.com/avcenter/venc/data/w32.welchia.worm.html

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Cole, Eric; Fossen, Jason; Northcutt, Stephen; Pomeranz, Hal. SANS Security Essentials with CISSP CBK version 2.1. SANS Press; April 2003; pgs. 84,138-140.

Cisco's NetFlow on Logical Interfaces
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800ad046.shtml

Catalyst 6500 Series Cisco IOS Command Reference, 12.1 E
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/comref/index.htm

Catalyst 6000 Family Switch and ROM Monitor Commands
http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_6_3/cmd_ref/sh_a_c.htm#18219

Cisco Catalyst 3500 Series XL Switches – Cisco IOS Commands
http://www.cisco.com/en/US/products/hw/switches/ps637/products_command_reference_chapter09186a00800d85e5.html#xtocid113

Microsoft Technet - Nbtstat
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/proddocs/nbtstat.asp

Windows 2000 Server – Displaying DHCP server Information
http://www.wown.com/j_helmig/w2kdhcpd.htm

Negus, Christopher. Red Hat Linux 7.2 Bible. New York: Hungry Minds Inc., 2002. 875.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.