Global Information Assurance Certification Paper

GIAC CERTIFIED INCIDENT HANDLER

PRACTICAL ASSIGNMENT

VERSION 3

The threat from SNMP and illustrating the need for "best practices" equipment configuration and auditing tools in equipment management systems.

By

Kenneth Baldridge

Date Submitted

August 16, 2004

Outline

Statement of Purpose 3
The Exploit 4
Name: 4
Operating Systems: 4
Protocols/Services/Applications: 4
Variants: 7
Description: 7
Signatures of the Attack: 8
The Platforms/Environments 11
Victim's Platform: 11
Source Network: 11
Target Network: 11
Network Diagram: 13
Stages of the Attack 14
Reconnaissance: 14
Scanning: 20
Exploiting the System: 22
Keeping Access: 24
Covering Tracks: 25
The Incident Handling Process 28
Preparation: 28
Identification: 31
Containment 33
Eradication 33
Recovery 33
Revised Network Diagram: 40
Extras 41
Snort Rule from signature database: 41
References 43
Works Used/Cited 44

Statement of Purpose

This paper is written to illustrate the reconnaissance use of the Simple Network Management Protocol (SNMP). At various stages of the review we will also discuss some of the hazards inherent in possession of the "read" and "write" strings by unauthorized parties. In particular we will discuss the potential for creating Denial of Service conditions using the SNMP "write" ability and how this can be mitigated by following industry accepted "best practices". For this paper we will focus on the manipulation of networking equipment however the general principles could easily be applied to most equipment utilizing SNMP.

The main scenario illustrated in this paper is as follows:

1. Company A has recently been acquired by company B.
2. The employee responsible for maintaining the network at company A (Mr. Sab A. Teur) has been told that his services will only be required for the next month at which time he will lose his job in favor of someone at the main office in company B.
3. Unfortunately Sab has become convinced that he was very ill-treated (other employees got a severance package but he didn't) and is looking for a way to "get-even".
4. Sab would like to go out in a way that leaves the company as ill-treated as he feels and with the strong feeling that perhaps centrally managing all of its networking equipment and getting rid of all the on-site support isn't a good idea.
5. Sab has discovered that the central network group uses SNMP to manage their devices and has decided to first map out the company network and then devise a strategy to take them offline using the protocol.

The Exploit

Name:

SNMP reconnaissance and the use of SNMP to create a general Denial of Service condition. Local access to the Cisco equipment will be used to bypass safeguards and gather SNMP configuration information. The ultimate goal of the person conducting this attack is not to get and keep access but rather to create a condition where the company attacked loses control of their own equipment which is then reconfigured in such a manner that all internal communication is stopped, hopefully for an extended period of time. (General Denial of Service)

A search of CVE, Bugtraq and Security Focus resources did not return any results specifically related this exploit. I have included a reference to the CERT FAQ on SNMP accompanying CERT advisory CA-2002-03 in the references section as this paper serves to at least touch upon and raise awareness of issues similar to those discussed here. **See also cve: 2002-0013, cve: 2002-0012, bugtraq: 4132, bugtraq: 4089, bugtraq: 4088 for other examples.)

Further information on the protocols, information sheets, equipment and software used can be found in the reference materials listed at the end of this paper.

Operating Systems:

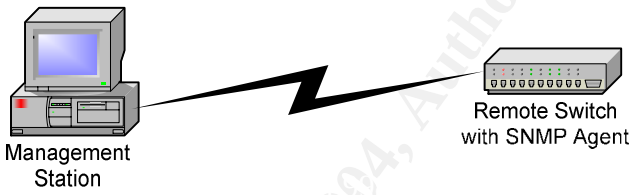
Cisco networking equipment running SNMP for management. All versions of the Cisco IOS support some type of SNMP although uses of at least the "write" functionality has been turned off by default for the last few years in recognition of the risks associated with publicly known default strings. SNMP version 1.x is the most commonly used and is available throughout the IOS line. SNMP version 2 support is available in a limited fashion based on early pre-standards in the early IOS 11 releases but was discontinued with 11.3 and reintroduced in 12.0 using the SNMPv2c information. SNMP version 3 is now supported beginning with 12.0(3) T but its actual use by the Networking and Systems administration community seems to be hampered due to already in use SNMP version 1.x implementations and the time and resource constraints around reconfiguration.

Protocols/Services/Applications:

SNMP is a protocol or instruction set defined by Internet Engineering Task force documents in the form of RFCs. These documents can be reviewed at http://www.rfc-editor.org/ however for those unfamiliar with SNMP I would suggest Thomas R. Cikoski's FAQ. The link to these articles can be found in the references section of this paper.

SNMP currently has 3 published and accepted versions 1, 2 and 3 with subversions available in each group. Version 1.x is the original and most widely used. Because version 1 was designed for use internally in a time when internal threats were not recognized as having a high level of significance it is lacking in several areas of security control centered on authentication and the protection of data in transit. It is these areas of concern that drove the development of version 2. Version three has been driven by an ever increasing need for even more security, stressing cross platform and implementation compatibility while using these enhanced controls.

SNMP works as a means of control or information gathering by using software (called a management console or management agent) running locally to communicate with counterpart software (called a remote agent) on the machine to be controlled, asking that remote agent to provide the management station with information or to perform an action.



Information gathering is done using identification provided by the management station to the remote device called a “read” string. Requests from the management station to the remote device to make changes to that device are made using the “write” string if that functionality has been enabled. In other words having the correct passwords (or Community strings as they are called in SNMP) will allow a management station to either read the configuration information from a device or write information (change) into the configuration of the device. Because SNMP operates on designated “well known ports” the communication between the management station and the remote agent can by default be found on port 161 (UDP or TCP).

SNMP version one (as dealt with in this paper) supports five basic functions.

1. The GET request or SET request. This is type of communication is originated by the management station and consists of a set of information that the management station wants (GET) or a set of information that the agent should change values to (SET). The agent will respond to the management station with a GET response.
2. The GET response is the agent's reply and will contain either the information requested by the management station, conformation of the SET values or an error.
3. The fourth basic function is the GETNEXT request. This type of request is used by the management station to ask for the next piece of information on the list and is normally used when the management station is using generic queries and doesn't know the next value's name. A set of GETNEXT requests is sometimes called "walking the MIB".
4. The final basic function is the TRAP. This is the communication that is initiated by the SNMP agent on the device and its only purpose is to notify the management station that a pre-determined event, possibly requiring attention, has occurred. Examples of a trap are things like failed connections, failed hardware or activity on the device that has exceeded a threshold like too much disk space or memory used.

There are many readily available free and commercial products for all of the major operating systems (Windows, Mac, Unix -- many with "free trial" or evaluation periods) for network analysis and SNMP management on the Internet. If you know what the equipment is (Cisco router, Mandrake server) that you are attempting to manage with SNMP (that information is normally available to you using generic quires built into the management software) then most manufactures will provide you with free to download SNMP management files tailored to their device or operating system. Using these files (called MIBs – short for Management Information Base) and the management software with the "write" string in most cases allows the user to fully control the device in a fashion similar to being logged on locally. In many cases much easier than being logged on locally for those more comfortable in the GUI world than at the command line.

In this paper I will be illustrating access and control using several pieces of software readily available to anyone for download from the publishing company's website. Links to all software referenced or used in this paper are available at the end of the paper in the references section.

In this paper SNMP will be used to transfer the original and the altered configuration files for the network equipment via the trivial file transfer protocol (TFTP). TFTP is a means of transferring files similar to FTP but transmitted over UDP and is standard on all Cisco networking equipment. A TFTP server/client is not included in windows but is readily available as either a freeware of commercial product add-on from the Internet.

Variants:

The use of the default community strings in a controllable device. Lists of the strings (as well as passwords) placed by default by manufacturers when equipment is configured are widely available on the internet. These can be retrieved from the manufactures themselves or found as precompiled lists on multiple sites using key word searches in your favorite online search engine. Search engines specializing in that sort of traffic (like http://astalavista.box.sk) can even help you find tools with these lists already supplied that will search for active devices and attempt to connect using defaults.

The network traffic analysis of SNMP related traffic could also be used in order to determine the community strings in use. Depending on the environment this method of gaining access to the strings may be more feasible however it does require access to the traffic. While it is quite common to see "read" community strings passed from monitoring stations to monitored equipment on a regular basis it may take some time to capture the use of the "write" community string.

In examining CVE, Bugtraq and Security Focus resources for the Name and CVE section several issues were noted that would have a similar enough affect that they might be considered variants. These included vulnerabilities in various implementations that allow an attacker to halt the device, gain elevated privileges or access restricted information among other actions. A good summary of these vulnerabilities can be found in CERT advisory CA-2002-03 located at http://www.cert.org/advisories/CA-2002-03.html

Description:

SNMPv1.x as a management protocol relies on both the environment that it is used in and available compensating controls to provide a measure of security in its use. For most implementations SNMP can be compared to two users who have the ability to remotely log onto a system. The first user, "Read" can look at the system, how it is set up or configured, what functions it is currently performing and how well it is keeping up with them. The second user "Write" can do all of the things that "Read" can do but "Write" can also change the system so that it stops, starts or performs tasks differently than before. When used in SNMP the usernames for our users "Read" and "Write" are always the same and all of our SNMP software knows them, so to have access to the read and write functions you only need to know the passwords (community strings) and be able to communicate with the system. In this paper we will illustrate two methods of ascertaining the contents of the community strings in use. Transport or connection access from our workstation to the networking systems in question will be provided by the existing network. We will also discuss some of the recommended practices that were not followed that would have prevented this access. It is the open nature of SNMP functioning as it was designed to do and

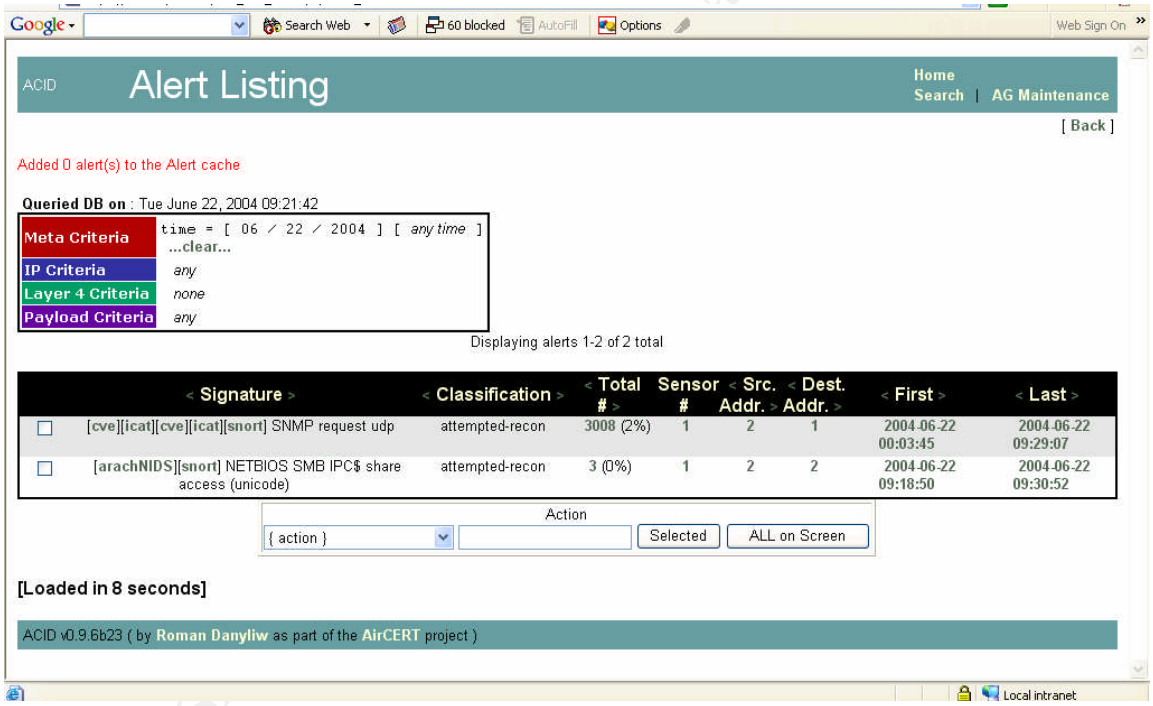
the failure of Company B to properly implement compensating controls that makes this sort of reconnaissance and attack possible.

Signatures of the Attack:

The use of SNMP from an unauthorized station will be detected by the set of SNMP signatures available in Snort. The “SNMP request” Snort signature for example will display as follows in the ACID console (similar signatures and displays are available in most network based intrusion detection systems).

See snort rule reference in the “Extras” section.

This of course requires that the sensor be located in a position relative to the workstation and equipment such that it is able to “see” the traffic and that the rule be enabled.



A typical packet capture follows, note that the traffic version is clearly marked SNMP, is UDP destined for port 161 and that the community string “private” is available in clear text. This is the method that would be used by someone who is able to capture the traffic between a management station and a managed device to discover the community strings in use.

```
Packet 1:  00:0B:DB:DE:39:49 -> 00:06:28:5A:2D:80
    Network: Ethernet,  Frame type:  ETHERTYPE,  Protocol:  0x0800 IP
```

```
    Frame network size (including 4 bytes CRC):  271
    Time:  09h:46m 04.957 142s,  Diff. time: 0.000000
    Date:  Tue Jun 22 2004
    Packet number in the original buffer: 3
    Saved partial packet size:  68
    Destination Address: 00:00:XX:XX:XX:XX
    Source Address:      00:00:XX:XX:XX:XX
    Protocol: 0x0800 IP
IP:    172.20.44.100 -> 172.16.0.200
    Status: Version = 4, IP Header Length = 20 Bytes
    0100....: Version = 4
    ....0101: IP Header Length = [5] 32 Bit Words = 20 Bytes
    Type of Service:
    000.....: Precedence = Routine
    ...0....: Delay = Normal
    ....0...: Throughput = Normal
    .....0..: Reliability = Normal
    ......0.: Cost = Normal
    .......0: Reserved
    Total IP length: 253
    ID: 0x0326
    Fragment:
    0....... ........: Reserved
    .0...... ........: Do Not Fragment = False
    ..0..... ........: More Fragments = False
    ...00000 00000000: Fragment Offset [0] * 8 = 0 Bytes
    Time to live: 128
    PROTOCOL: 17 = UDP
    Header checksum: 0x0000 (Not Present)
    IP Addresses: Source = 172.20.44.100 ,  Destination = 172.16.0.200
    Source: 172.20.44.100
    Destination: 172.16.0.200
UDP, [1044]  -> [161] SNMP
    Source port: [1044]
    Destination port: [161] SNMP
    UDP length: 233,  captured: 30; partial capture or fragmented
packet
    Checksum:  0x4BF9 (partial packet - not able to check)
SNMPv
    ASN Object Identifier: 0x30 (SNMP Message)
    SNMP Length:
    1.......: Multi-Byte Length Flag = True
    .0000001: Number of Bytes = 1
    Length  : 222 Bytes
    SNMP Version:
    ASN Type  :
    00......:  Class [0] = Universal
    ..0.....: Constructed = False
    ...00010: Tag Number = 2
    ASN Length:
    0.......: Multi-Byte Length Flag = False
    .0000001: Length = 1 Bytes
    ASN Value : 0
    SNMP Community Name:
    ASN Type:
    00......:  Class [0] = Universal
    ..0.....: Constructed = False
```

```
    ...00100: Tag Number = 4
    ASN Length:
    0.......: Multi-Byte Length Flag = False
    .0000111: Length = 7 Bytes
    ASN Value : private
    PDU:
    PDU Type: [0xA1] = Get Next Request
    PDU Length:
    1.......: Multi-Byte Length Flag = True
    .0000001: Number of Bytes = 1
    Length  : 207 Bytes
    Request ID:
    ASN Type  :
    00......:  Class [0] = Universal
    ..0.....: Constructed = False
    ...00010: Tag Number = 2
    ASN Length:
    0.......: Multi-Byte Length Flag = False
    .0000001: Length = 1 Bytes
    ASN Value : 44
    Error Status:
    ASN Type  :
    00......:  Class [0] = Universal
    ..0.....: Constructed = False
    ...00010: Tag Number = 2

                    RAW PACKET LISTING:
0000  00 06 28 5A 2D 80 00 0B  DB DE 39 49 08 00 45 00    ..(Z-
€..ÛÞ9I..E.
0010  00 FD 03 26 00 00 80 11  00 00 0A 23 21 12 0A 23
.ý.&..€....#!..#
0020  21 AF 04 14 00 A1 00 E9  4B F9 30 81 DE 02 01 00
!¯...¡.éKù0•Þ...
0030  04 07 70 72 69 76 61 74  65 A1 81 CF 02 01 2C 02
..private¡•Ï..,.
   ------------------------------------------------------------
```

The use of SNMP and TFTP as outlined in this paper to alter the configuration of the routers will also trip signatures related to the use of TFTP (The trivial file transfer protocol) and leave messages on your centralized syslog server (if used) similar to the following.

07-03-2004 14:32:52 Local7.Notice 172.16.0.200 50: 1d00h: %SYS-5-CONFIG: Configured from CentralOfficeVPNTerm.CiscoConfig by console tftp from 172.20.44.100

A power cycle and the subsequent unavailability to probes may result in someone in the network operation center being notified depending on the type of monitoring in place. In our environment a simple ICMP “ping” (rather than an SNMP “TRAP” for example) is used to determine if a device is “UP” or “DOWN” so the process is not likely to draw too much attention if performed during a time period outside of the normal business hours.

The Platforms/Environments

Victim's Platform:

The platforms in this scenario include several models of Cisco networking equipment (routers) running version 1.x of the SNMP service on IOS version 12 ((12.0(5) T1)). In this scenario it is likely that the company is also operating servers using SNMP and that these could be exploited as well but Sab is confining his interest to the networking equipment.

Source Network:

The exploit will originate from within the office network from Sab's laptop located in Remote Office 12. **See Diagram below**

Sab's laptop (attack platform) consists of a Dell C600 running Windows XP as an OS. For SNMP management and use in the exploit as described in this paper Sab has downloaded and installed the SolarWinds Network Management Tools (Professional Plus Edition) from the SolarWinds website http://solarwinds.net/Toolsets.htm . Sab has also installed Ethereal http://www.ethereal.com/download.html for packet capture and analysis.

Target Network:

The target network is a business network set up in a general hub and spoke arrangement. Each remote office connects directly to the main office via a VPN connection between the Cisco routers located in their office and the Cisco router located in the main office. Each remote office is a "trusted" extension of the main office internal corporate network and is tied directly onto the internal network at the main office. Each remote office can communicate with all of the other remote offices with the routing for this traffic occurring on the VPN endpoint router located in the main office. Traffic (other than the carrier for the VPN tunnel) destined for the Internet is routed into the main office and then out the firewall to the final destination. The firewall itself is configured with the following rules:

1. Allow incoming traffic to specific machines on the DMZ designed to service public requests using FTP, HTTP and HTTPS.
    a. Allow – Any – (FTP Server address) – FTP
    b. Allow – Any – (Web Server address) – HTTP, HTTPS

2. Allow incoming VPN traffic from each of the remote offices to the central office VPN endpoint router.

3. Allow outgoing VPN traffic from the central office VPN endpoint router to each of the remote office routers.

4. Allow ICMP traffic from/to company routers.

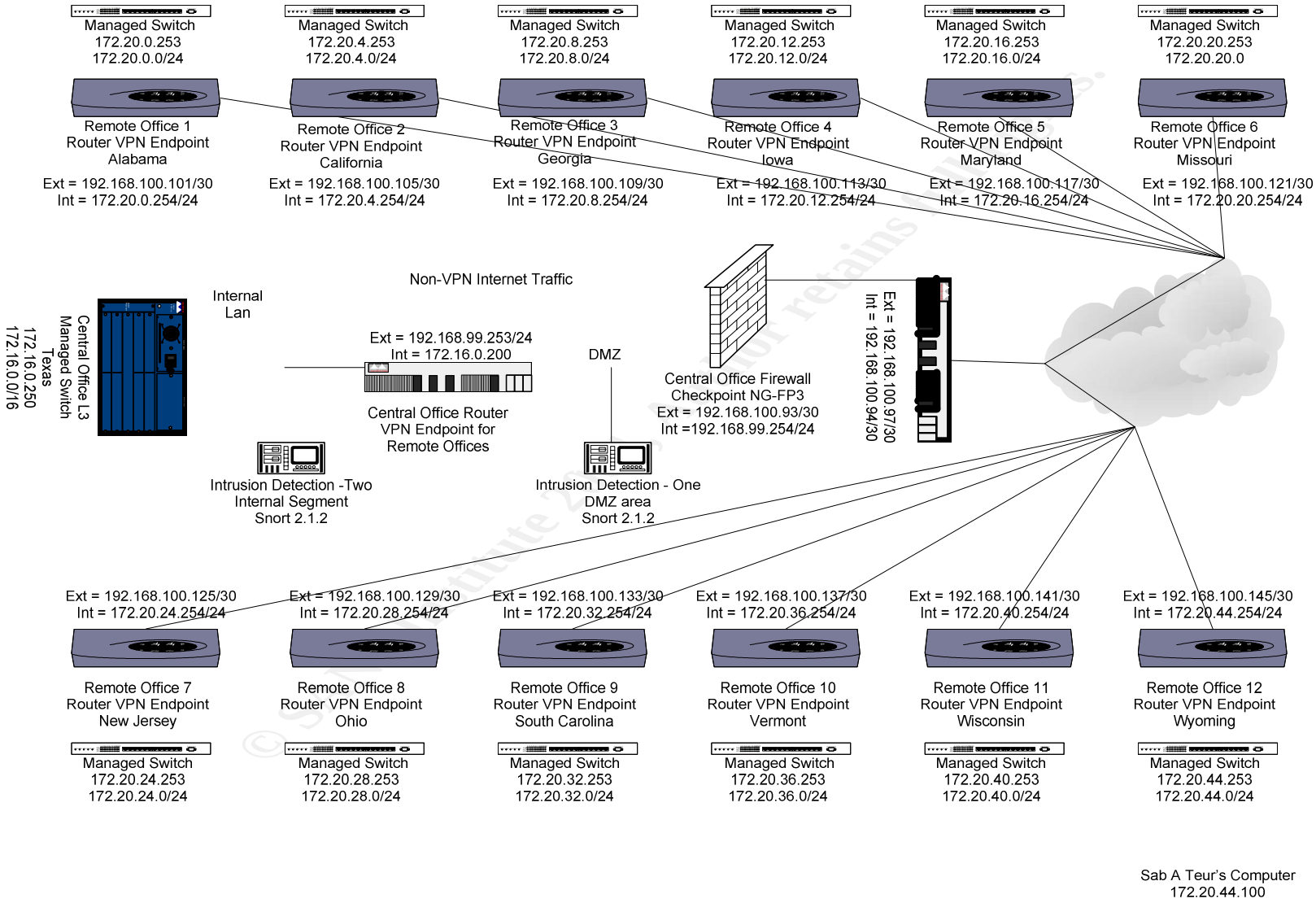
5. Allow traffic from the internal LAN ranges out.
    a. Traffic from the internal LAN addresses are hidden behind an external address on the firewall using many to one NAT.

6. Allow established.

It was thought that this configuration would save the company money on Firewall and IDS costs since all of the remote offices would be protected from Internet traffic intrusion by the Firewall and IDS systems located in the Central office.

For the purposes of this paper the address ranges expressed as 192.168.*.* are considered to be in a valid externally routable address space. All 172.*.*.* address ranges are considered to be internal private address space.

Network Diagram:



Stages of the Attack

Reconnaissance:

Sab A Teur is an employee of the company with legitimate physical access to the premises. This exploit could, however, be used by anyone able to gain access to the equipment. Some examples of this would be an unsecured data center or wiring closet. In many cases a company will spend a great deal of time and effort in placing firewalls and erecting perimeter defenses while placing networking equipment in a closet without a locking door. I personally have witnessed a company where the data center door was propped open at night with a fan in order to improve air circulation.

The pre-targeting for this attack would therefore consist of a physical inspection of the premises for equipment access and a time period in which the equipment could be rebooted without attracting immediate attention.

In our case Sab has found that the wiring closet housing the remote office router and switch is not locked and can be accessed from the office suite at any time. Sab has planned on being in the office on a holiday morning when no one else is there both so that the loss of the connection will not be noticed by the local employees and so that if anyone in the main office is notified it will take them some time to receive the notification and respond to it. Sab hopes to complete his initial review of the equipment configuration and have the equipment back online with no changes prior to that response if it occurs. This would likely cause the responder to conclude that there was a temporary network or power issue since at this point there would be no discernable change to the system. If done quickly enough it is possible that a typical administrator on a holiday would see that the equipment was up and functioning normally and not investigate any further. At worst the administrator would find that the system had rebooted a couple of times and examine the equipment for issues that would not be found.

Sab's initial review of the system is generally conducted as outlined in the "Cisco password recovery procedures" (available from the Cisco web site – see reference) however the purpose at this stage is only to examine the configuration and no changes will be made.

Sab begins by connecting his laptop to the router using a console cable These cables are available for purchase or instructions can be found for making one by performing a search on Google using the keywords "make cisco console cable". The specifications for Cisco cables can also be found on Cisco's public web site at:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/cis2500/2509/acsvrug/cables.pdf .

He then starts the HyperTerminal application which is listening on the port to which the console cable is attached (com 1 in our example). Following the instructions contained in the password recovery procedures (see reference section for download information) Sab is able to view the configuration of the router and then restart the router without change. The entire process takes less than 5 minutes and is captured to a file by the terminal application. It is important to note that the period of time that the router would not be responding to pings is less than 3 minutes and may not be noticed at all by the central office. Since this router is configured to send SNMP notices to a monitoring station it may create a note in the log but again given the timing and duration it is unlikely to cause further action to be taken by the staff.

The file from this process is shown below. Note that despite the running password encryption service the read string (public) and the write string (private) are in clear text.

```
System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 32768 Kbytes of main memory

PC = 0xfff0a530, Vector = 0x500, SP = 0x80004864

monitor: command "boot" aborted due to user interrupt
rommon 1 > PC = 0xfff0a0e4, Vector = 0x500, SP = 0x80004ddc

rommon 1 > confreg 0x2142


You must reset or power cycle for new config to take effect
rommon 2 > reset

System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)
Copyright (c) 1999 by cisco Systems, Inc.
TAC:Home:SW:IOS:Specials for info
C2600 platform with 32768 Kbytes of main memory

program load complete, entry point: 0x80008000, size: 0x6a82d8
Self decompressing the image :
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################################################################
################################## [OK]

        Restricted Rights Legend
```

Use, duplication, or disclosure by the Government is
subject to restrictions as set forth in subparagraph
(c) of the Commercial Computer Software - Restricted
Rights clause at FAR sec. 52.227-19 and subparagraph
(c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3S56I-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 14:28 by cmong
Image text-base: 0x80008088, data-base: 0x80C72114

Compliance with U.S. Export Laws and Regulations - Encryption

This product performs encryption and is regulated for export
by the U.S. Government.

This product is not authorized for use by persons located
outside the United States and Canada that do not have prior
approval from Cisco Systems, Inc. or the U.S. Government.

This product may not be exported outside the U.S. and Canada
either by physical or electronic means without PRIOR approval
of Cisco Systems, Inc. or the U.S. Government.

Persons outside the U.S. and Canada may not re-export, resell,
or transfer this product by either physical or electronic means
without prior approval of Cisco Systems, Inc. or the U.S.
Government.

cisco 2611 (MPC860) processor (revision 0x203) with 26624K/6144K bytes of memory.
Processor board ID JAD051809X9 (4011857168)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
1 Channelized T1/PRI port(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

--- System Configuration Dialog ---

Would you like to enter the initial configuration dialog? [yes/no]: n

Press RETURN to get started!

```
00:00:20: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
00:00:20: %LINK-3-UPDOWN: Interface Ethernet0/1, changed state to up
00:00:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to
up
00:00:21: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to
up
00:00:51: %SYS-5-RESTART: System restarted --
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3S56I-M), Version 12.0(5)T1,  RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 14:28 by cmong
00:00:53: %LINK-5-CHANGED: Interface Ethernet0/0, changed state to administratively down
00:00:53: %LINK-5-CHANGED: Interface Ethernet0/1, changed state to administratively down
00:00:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to
down
00:00:54: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/1, changed state to
down
.

Router>en
Router#copy startup-config running-config
Destination filename [running-config]?
788 bytes copied in 1.78 secs (788 bytes/sec)
RemoteOffice#
00:02:24: %SYS-5-CONFIG: Configured from  by
RemoteOffice#sh run
Building configuration...

Current configuration : 2732 bytes
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname RemoteOffice12
!
enable secret 5 $1$qvuD$8YvrJ9TGQ3adHKZjpyLZMO
!
!
!
!
!
ip subnet-zero
!
!
!
crypto isakmp policy 10
 authentication pre-share
 group 2
 lifetime 3600
crypto isakmp key VPNcentral0ffice address 192.168.99.253
!
!
```

```
crypto ipsec transform-set tunnelset esp-des esp-md5-hmac
!
crypto map toCentralOffice local-address FastEthernet0/1
crypto map toCentralOffice 10 ipsec-isakmp
 set peer 192.168.99.253
 set transform-set tunnelset
 match address 101
!
!
!
!
!
!
interface Tunnel0
 bandwidth 1544
 ip address 172.16.0.200 255.255.255.252
 ip mtu 1476
 no ip route-cache
 no ip mroute-cache
 tunnel source FastEthernet0/1
 tunnel destination 192.168.99.253
 crypto map toCentralOffice
!
interface FastEthernet0/0
 description Inside LAN Interface
 ip address 172.20.44.254 255.255.255.0
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.100.145 255.255.255.252
 no ip route-cache
 no ip mroute-cache
 duplex auto
 speed auto
 crypto map toCentralOffice
!
ip classless
ip route 0.0.0.0 0.0.0.0 192.168.100.146
ip route 192.168.99.253 255.255.255.255 192.168.100.146
ip route 172.16.0.0 255.255.0.0 Tunnel0 name CentralOffice
ip route 172.20.0.0 255.255.255.0 Tunnel0 name RemoteOffice1
ip route 172.20.4.0 255.255.255.0 Tunnel0 name RemoteOffice2
ip route 172.20.8.0 255.255.255.0 Tunnel0 name RemoteOffice3
ip route 172.20.12.0 255.255.255.0 Tunnel0 name RemoteOffice4
ip route 172.20.16.0 255.255.255.0 Tunnel0 name RemoteOffice5
ip route 172.20.20.0 255.255.255.0 Tunnel0 name RemoteOffice6
ip route 172.20.24.0 255.255.255.0 Tunnel0 name RemoteOffice7
ip route 172.20.28.0 255.255.255.0 Tunnel0 name RemoteOffice8
ip route 172.20.32.0 255.255.255.0 Tunnel0 name RemoteOffice9
ip route 172.20.36.0 255.255.255.0 Tunnel0 name RemoteOffice10
ip route 172.20.40.0 255.255.255.0 Tunnel0 name RemoteOffice11
```

```
no ip http server
!
access-list 101 permit gre host 192.168.100.146 host 192.168.100.145
!
snmp-server engineID local 0000000902000004C1A21611
snmp-server community public RO
snmp-server community private RW
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps hsrp
snmp-server enable traps entity
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server enable traps rsvp
snmp-server enable traps frame-relay
snmp-server enable traps rtr
snmp-server enable traps dlsw
snmp-server enable traps dial
snmp-server enable traps voice poor-qov
snmp-server host 172.16.0.25 public

snmp-server manager
!
!
line con 0
 password 7 082243401A160912
line aux 0
line vty 0 4
 password 7  0519091A35495C
 login
!
end

RemoteOffice#config t
Enter configuration commands, one per line.  End with CNTL/Z.
RemoteOffice(config)#config-r
RemoteOffice(config)#config-register 0x2102
RemoteOffice(config)#exit


RemoteOffice#reload

System configuration has been modified. Save? [yes/no]: no

Proceed with reload? [confirm]y
```

At this point Sab would take this information and leave to study it at his leisure.

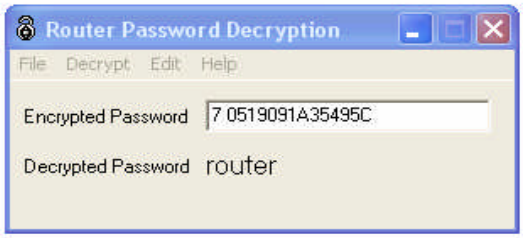
In studying the configuration file that we obtained from the local office we are able to gather a number of pieces of interesting information.

1. That SNMP is in use

2. That there is both a read and write string and what those strings are (public, private)
3. The routing to the main and other remote offices and the use of the VPN.
4. We can also see the encrypted versions of the enable, console and terminal passwords.

Since the enable password is a type 5 (illustrated by the 5 in “enable secret 5 1qvuD$8YvrJ9TGQ3adHKZjpyLZMO”) We can’t do much with it but there are many tools available to reverse type 7 passwords like we find on the console and terminal ports. Examples are the “Router Password Decryption” tool published by SolarWinds (http://www.solarwinds.net/Tools/Cisco_Networking/Password_Decryptor/) and the “GetPass” tool published by Boson (http://www.boson.com/promo/utilities/getpass/getpass_utility.htm)

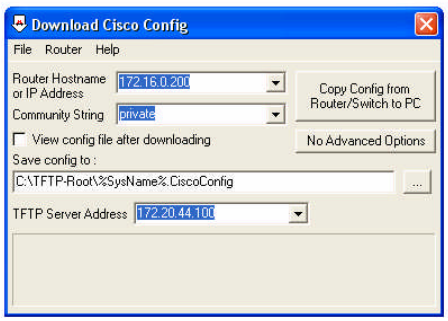
Using the router password decryption tool we are able to cut and paste the encrypted console and terminal passwords from the configuration file to see that the passwords they are using are “console” and “router”.



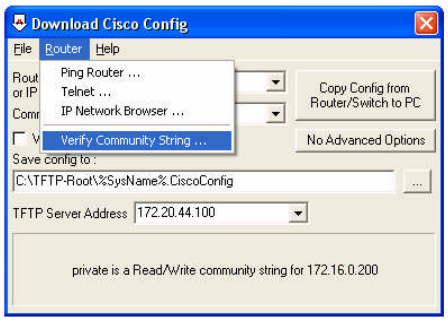
Scanning:

Using the information that we gathered from the local router configuration file we will now use our SNMP management program (in this case the SolarWinds Cisco Download Config tool) to test our SNMP strings and retrieve the configuration of the Central Office VPN router at 172.16.0.200.

First we open the tool and paste the address we want to contact into the destination field with the community string we want to use.



Then from the router menu we choose “verify community string” to confirm that the write string on the Central Office router is the same as the one on our local router.



We can see that the string is the same so we will continue by downloading the central office configuration file to our local computer for review. (Since we’ve successfully connected with the download tool getting a copy of the configuration file is as simple as pressing the button marked “Copy configuration from Router/Switch to PC) Note that this requires a TFTP server. We will be using the one that is included in the SolarWinds package that we downloaded since it is setup and started for us by the package installation program.

After receiving the configuration file we examine it in the same way we looked at the file from our local router and find the following:

1. The central router has VPN tunnels to all of the remote offices.
2. It appears that the other remote offices are set up in a similar fashion to ours and that the router is located on .254 of the class C associated with that office.
3. The central office is using the same community strings as our local router.
4. The central office is using the same console and terminal passwords as our local router.

From the information contained in the two configuration files we are now able to construct an initial diagram of the path that traffic will flow in getting from our office to the local office and from there to the other remote offices. It appears that the network team is using a standard template for each of the offices and one set of SNMP strings for all of their routing equipment.

We’ll confirm our assumptions and continue our mapping of the network by connecting to and downloading the configuration file from each of the routers located at the other remote offices. We’ll do this using the same procedures we used for the central office. In order to avoid drawing attention to our activity we’ll perform this process over several days at off hours.

Sab has now downloaded a copy of the running configuration on all of the Remote office routers and the Central office VPN endpoint router. Each of the other remote offices are configured in a manner similar to the router located in Sab's office. A test connection to the local managed switch in Remote office 12 shows that the switch is using SNMP but that the community strings are different. Because time is running short and he wants to stay within the encrypted environment Sab decides he has all of the information that he needs and he won't worry about anything beyond the VPN connections environment.

At this point given our current network configuration only the initial reboots used to gain a copy of the configuration from the RemoteOffice12 router may have been noticed. Since no changes have been made to any router and no centralized syslog server is in use in the environment none of Sab's activities to this point should have been noticed.

There are two network based IDS devices located on the network that were supposed to catch this type of activity however they never saw the traffic and therefore never alerted anyone. The IDS located in the DMZ would only have seen the VPN tunnel and not the traffic contained therein. The IDS located on the internal LAN would never have seen the traffic because it never left the VPN network. Traffic from the Remote Office 12 segment to the Central Office VPN router would stop at the router before reaching the internal LAN. Traffic from one remote office to another would be routed at the Central Office VPN router and never leave the VPN connections environment to be detected.

The firewall would also never "see" the SNMP or TFTP traffic since they are contained within the VPN tunnel that is allowed to pass by the VPN connections rules.

Exploiting the System:

To implement our denial of service we will create a new configuration file that we will upload to all of the routers. This will be a very simple file consisting of the following 14 lines:

```
!
service password-encryption
!
enable secret nobodyknowsme
!
no logging on
no logging console
no logging monitor
no logging trap
!
line vty 0 4
```

password mypassword
!
end

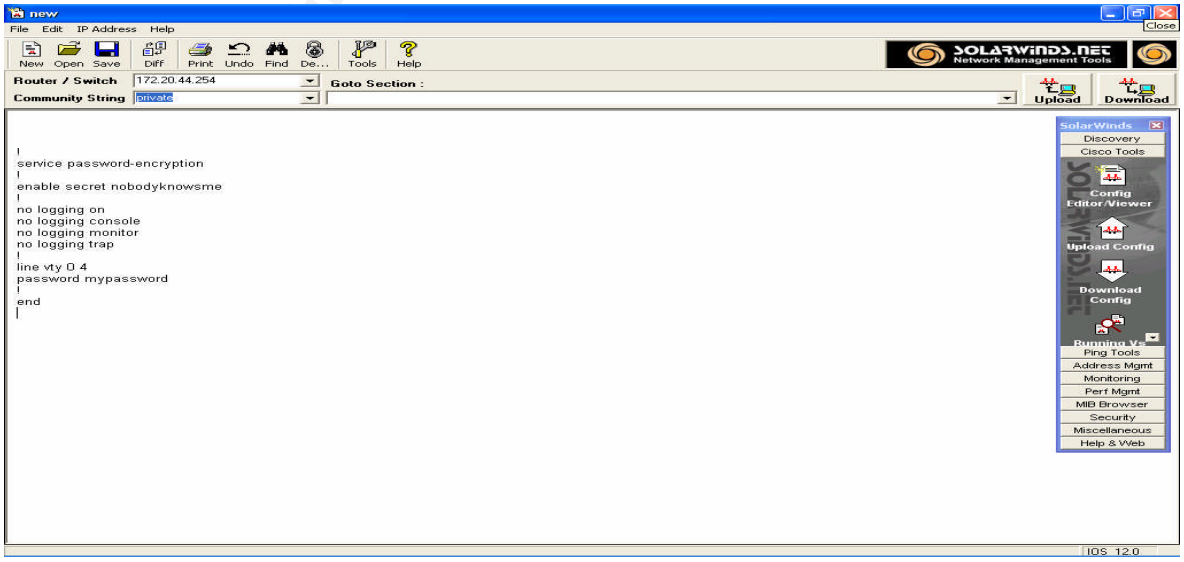
This file will have the effect of turning off all logging, setting the enable secret password to “nobodyknowsme”, setting the terminal password to “mypassword” and making sure the password encryption service is running.

It will also, since there are no values present, disable all of the interfaces on the device. By performing the change with blank, rather than specific, values we do not have to worry about formatting our file to fit the various interface configurations or IOS versions that may be out there. Greatly simplifying our work.

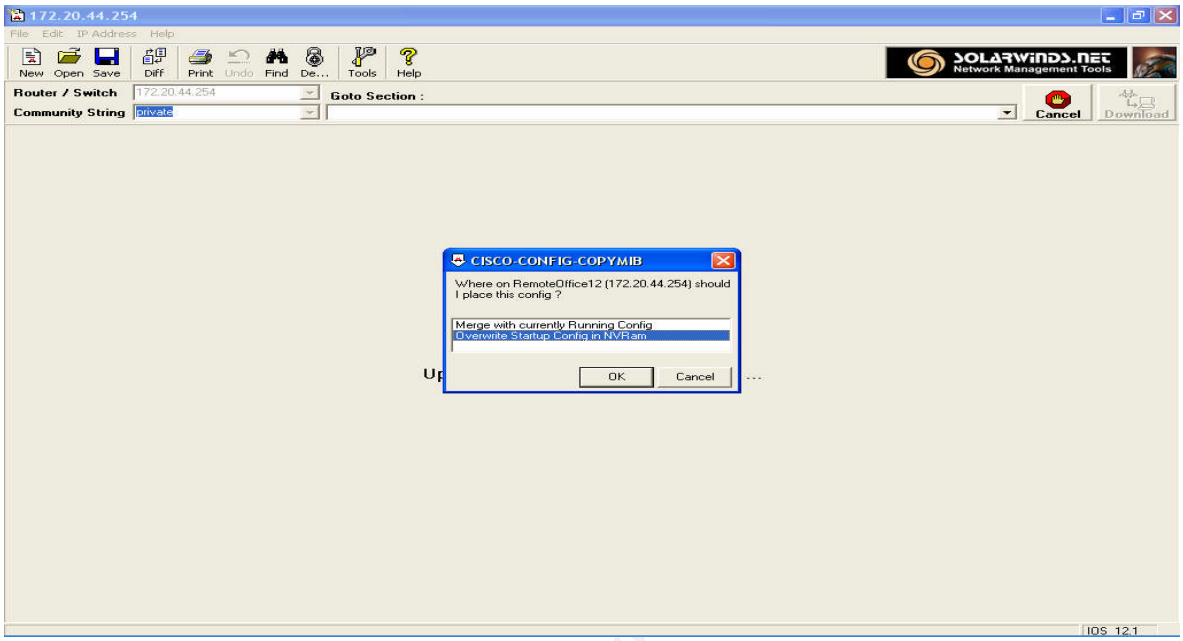
When we are ready to create the denial of service condition we will upload the changed configuration file to the startup-config of each router. This will leave the router functioning as it has been until rebooted at which time our altered configuration will be installed as the running configuration cutting off all outside access. Recovery from this condition will require someone to access the router locally (as we did at the reconnaissance stage of this attack) and reinstall the previous configuration (hopefully for them someone still at the company made a recent copy). If there is no copy of the previous configuration available then the local person will have to reset the passwords and rebuild the configuration from scratch.

The upload of the altered configuration file is very easy and again we will turn to our evaluation toolset that we downloaded to accomplish this task as illustrated below.

First, open the configuration file that you have created within the Config Editor tool:



Then upload the configuration, selecting to overwrite the nvram.



That's all there is to it. The router is now running with the original configuration and will run the new configuration you uploaded when rebooted.

Keeping Access:

Since the point of this exercise is to cripple the network we will not be making plans to attempt to keep the access that we've gotten. However had we wanted to maintain access there are a few points to consider.

The first is that if Sab is still employed by the company and still has access to the equipment he can simply repeat the exercise. If the company doesn't figure out what has taken place they will likely reuse the same community strings and it will simply be a matter of connecting to the network and using the same process.

The second method of maintaining access would be to alter the configuration of the edge routers to allow access from the Internet. (This would simply be a matter of downloading the configuration files, making the needed changes to the ACL's and then uploading. The routers would continue to function as the business expects with the added functionality of accepting outside connections.) As a side note, this kind of alteration would enable Sab to conduct the attack from outside of the network, possibly further obscuring the trail by using remote zombie connections.

Third Sab could explore further into the network and attempt to corrupt the main office internet router or an internal server running SNMP to install a backdoor there. Note however that if Sab did go beyond the bounds of the VPN structure the traffic would have been noted by the IDS Sensors.

Covering Tracks:

We are now ready to execute our plan. First we will again choose an off hour (taking into account time zones since we will be working across the US) so that we have the longest period of time before someone notices something is wrong.

Beginning with the remote offices and ending with the Central Office VPN device we'll follow the following steps. (Remember, the order is important! If you alter the Central office router before completing the remote offices you will lose your connection.)

1. Merge the new file with the running-config.
    a. This is done in the same manor outlined above under "exploiting the system" except here we will choose to merge the changes with the running config. (For example, the following telnet output shows the change on the router at 172.20.44.254 after the upload)

```
RemoteOffice12#sh logging
Syslog logging: disabled (0 messages dropped, 20 flushes, 0 overruns)
   Console logging: disabled
   Monitor logging: disabled
   Buffer logging: disabled
   Trap logging: disabled
RemoteOffice12#
```

We have now disabled all logging and locked everyone out of the terminal and enable prompts of the routers. If we have timed things right then no one is noticing anything because they are not trying to log in and the routers are still functioning. But we need to work fairly quickly just in case.

2. Upload the file again, this time overwriting the startup-config (NVRAM)
    a. We will complete these two steps for all of the equipment before moving on to step three.

3. In step three we will open 13 telnet sessions to the enable prompt of each router at the same time. This will enable us to issue the reload command within a few seconds to all of the routers.

a. Issue the reload command to each router, again starting with Remote offices 1 to 11, then the Central office and finally our local router RemoteOffice12.
b. Since we previously altered the running-config you will be prompted to save the file. Be sure to choose no so that you do not overwrite the startup-config you just uploaded and leave a functioning router behind.

Microsoft Telnet> open 172.20.44.254
Connecting To 172.20.44.254...

User Access Verification
Password:
Router>en
Password:
Router#reload

System configuration has been modified. Save? [yes/no]: no
Proceed with reload? [confirm]y
Connection to host lost.

Press any key to continue...

All of the remote offices are now offline. The configuration on the routers is wiped except for the passwords of your choosing and the interfaces are all down. There should be no logs or records left behind for anyone to trace the incident back to Sab. Recovery of the routers will require on-site support and it is likely the business will be offline for some time.

In this scenario a number of “best practices” were not followed that would have helped either prevent the incident or to provide evidence of the cause.

A hostile work environment was created for the employee and precautions were not taken to eliminate or restrict the terminated employee’s access.

The equipment was not secured. Although this would seem to be a basic step, many businesses fail to realize that no software firewall will protect the systems if someone has physical access.

Although SNMP was in use configuration changes were not set to cause an alert using the “snmp-server enable traps config” command.

There was no centralized syslog server to gather and maintain records generated by the various pieces of equipment.

Access lists were not in place to control SNMP traffic to the routers

Access lists were not in place to control TFTP traffic to the routers

No IDS sensors were in use outside of the central office

Routing of the VPN connections took place on the Central Router thus shielding all of the remote office to remote office traffic within the VPN.

The Incident Handling Process

Preparation:

1. As part of the change control process the configuration of each piece of Network equipment is backed up before and after any change. These configuration files are kept for a minimum period of 3 months with the last set kept indefinitely.
2. Policies and procedures for system security, backup and change control are published to all employees.
3. On call information for all systems and security personnel are published to all employees.
4. Maintenance and service agreements are in place on all equipment required for day to day operation with a 4 hour response window.
5. The incident handling process is loosely defined in policy as follows:
    a. Any person with reason to believe an incident or event has occurred that compromises the security of the data or systems of the company must report that information to the designated information security officer immediately by contacting the published on call numbers.
    b. Upon becoming aware of a possible incident or event the designated Information Security Officer will immediately conduct research to determine if such incident or event has in fact occurred.
    c. In the event that an incident occurs that is of a significance to warrant such, the designated Information Security Officer shall inform the Chief Security Officer of the decision to activate the Incident Response Team.
    d. The Chief Security Officer shall inform the Information Security Steering Committee of this decision as soon as is practical for the situation.
    e. The Incident response team shall be comprised of the following permanent members:
        i. A designated Information Security officer
        ii. A designated member of the Internal Audit Team
        iii. A designated member of the Systems and Networking staffs.
        iv. A designated member of the Legal department staff.
        v. A designated member of the Human Resources staff.
    f. The designated Information Security Officer shall act as the Manager of the Incident Response team and shall be responsible for directing the activities of the team during the time of the active incident response.
    g. In addition to the permanent members of the Incident Response Team already identified the team shall contain such other persons as designated by the Chief Security Officer whose specialized

knowledge or position is needed to address a then-current situation.

h. Upon activation of the Incident Response Team all members will meet as quickly as possible to review the situation. Each member is expected to participate on a full time basis during the time of activation unless released by the team manager to perform other non-related tasks.
i. In the event that an Incident results in the loss of critical services for the company it is the priority of the team to first restore service in a safe manner and then attempt to identify the chain of events that establish cause and effect.
j. If it is possible to restore services in a time frame satisfactory to the Information Security Steering committee while preserving conditions or evidence needed to reconstruct events then every effort should be made to do so.
k. Any situation which poses a threat to the integrity of the Corporation's other systems or data should be contained in a manner and timeframe appropriate for the threat posed by the situation.

6. The Incident Handling team is made up of a group of individuals with expertise and in-depth knowledge of Security, Company Policy, Procedure and the corporate systems. If needed other individuals may be added to the team to assist in addressing specific situations. These individuals can be other members of staff (for example a member of a product development team or database analyst) or a contractor hired for their specialized knowledge of an operating system or equipment type.

Some sections of Policy supporting the resolution of an incident, the incident handling process and the preparation status are:

<u>A statement of responsibilities for the Information Security Department:</u>

While all Workers are responsible for following these policies and safeguarding the information under their care, the Information Security Department (ISD) has primary responsibility for carrying out the mission of protecting the company's Information Assets. The ISD will fulfill its mission through the performance of the following duties:
· Performing regular risk assessments and implementing an Information Security Plan to address appropriate threats and vulnerabilities identified in this assessment
· Developing and managing Information Security Policies, Guidelines, Standards and Procedures, including this document
· Initiating and ensuring the implementation of projects to strengthen the company's information security controls and to meet client and legislative requirements

· Providing security information and advice to all areas of the corporation, and responding to all security information requests and audits from clients
· Reviewing new and pending legislation, and on request, client contracts, to ensure that the company is compliant with information security provisions
· Assessing on a regular basis our information security controls, as well as those of appropriate third parties, to ensure their adequacy and use
· Developing a Security Incident Response Program and managing its use in the event of a security incident
· Ensuring that all Workers receive ongoing training in information security appropriate to their position
· Monitoring threat and vulnerability information sources and alerting appropriate parties to take action as needed

A statement of support and responsibilities for Senior Management in guiding Information Security policies:

In order to provide top management support and direction for Information Security, an Information Security Steering Committee (ISSC) comprised of a cross section of the company's executives will meet on a regular basis to:
· Review and approve information security policy changes
· Monitor significant changes in the exposure of Information Assets to major
· Review and monitor information security incidents
· Approve and monitor major initiatives to enhance information security

A statement requiring policy compliance by employees:

All Workers are expected to understand and follow the policies detailed in this document and in referenced guidelines, standards and procedures. Failure to follow these policies may result in implementation of the company's performance improvement process which could lead to disciplinary action, up to and including termination of employment or contract. Additionally, violators could be subject to civil suit and/or criminal prosecution.

Business Continuity policy:

Operations shall be responsible for preparing, managing and testing Business Continuity and Disaster Recovery plans, and coordinating the implementation of supporting infrastructure, in order to meet the requirements for availability of the Information Assets defined by its Data Owner. These plans must be fully tested in an active scenario on at least an annual basis.

Patch Management:

Each platform team is responsible for ensuring that their platform is current with appropriate software patches and updates. The ISD will monitor appropriate advisory services for alerts concerning patches and vulnerabilities and will notify

the appropriate platform teams whenever a critical patch or work-around needs to be applied in order to protect against a known vulnerability in the platform.

Security Requirements in Product Development:

Security should be considered in development projects during the design stage, and also preferably during the requirements specification by the development team. In addition, all regulations governing the data intended to be processed by the application system will be identified and addressed during the requirements definition. The Company Legal Department shall be contacted on all questions regarding applicable regulations.

Internal Audits:

The Information Security Department will periodically audit all internal systems, networks and ASP applications to insure compliance with the Company's Information Security policies, standards and procedures.

Currently the company uses a standard "jump kit" for incident response consisting of a camera, two laptop computers (one windows, one Red Hat Fedora), a hub, standard and crossover cables, external USB/Firewire hard drives, and an assortment of software including Encase Forensic edition, Knoppix V3.4, Knoppix the security tools distribution, the systernals and foundstone tools on CD and the winternals administrator's pack.

Identification:

Monday morning – 2 am
The problem was first noticed by workers in the Network Operations Center when they became aware that they were unable to reach any of the remote offices to perform their regular Windows Server reboots. The secondary on call member of the network staff was notified of the problem after the primary on call failed to respond to a page. The secondary on call network administrator proceeded to come into the office after being unable to connect to the Central office VPN router remotely. Priority is considered low at this point.

Monday morning – 3:30 am
The network administrator on-site can only connect to the VPN router at the console user prompt and does not have the password to enter enable mode on the router. More time passes as the other network administrators are contacted to see if anyone knows the password. Priority is still not considered high.

Monday morning – 5:00 am
The decision is made to reset the password and access is gained to the router. A review of the running and startup configuration files indicates that there has

been some sort of problem with the router and a decision is made to restore the configuration from backup. At this point the issue is considered to have a medium-high priority but the Administrators consider the issue to be confined to this one router.

Monday morning - 6:30 am
The central office VPN router is back up and functioning however no tunnel is being established with the remote offices. A series of connection attempts (ICMP Pings and Traceroutes) indicates that the remote office routers may be down as well. Pages and phone calls go out to personnel normally located in the remote offices to try and find out if the equipment in those offices is turned on.

Monday morning - 7:30 am
It has been established that the routers in the remote offices appear to have some kind of problem as well. The routers in office 3 and 4 have been power-cycled several times with no effect.

Monday morning - 8:00 am
An emergency meeting of the networking staff and several members of senior management is called to discuss the situation. It is decided to call in support staff in the various cities affected under the company's service agreements to help in diagnosing the problems.

Monday morning - 11:30 am
Reports coming in from remote offices 3, 4 and 7 where the contractors have arrived make the situation in the field sound very similar to the situation reported to have been found in the central office. At this point the similarity between the experiences in the remote offices and the central office is noticed and notification is given to the Information Security Department that this may be some sort of Denial of Service attack.

More than 9 and a half hours have passed before the Information Security Department is notified that there may be an Incident in progress. No evidence is left of the conditions encountered on the Central Office VPN router as the network administrator did not save the contents of his console session, the running and startup configs on the router itself have been overwritten, and the router has been rebooted multiple times. We have also lost the chance to recover much of the evidence in offices 3, 4 and 7 due to the work that has already been done in those facilities. However the general conditions indicate that the VPN routers have been the subject of some type of attack and that the damage appears to have been confined to this area of equipment.

Containment

Monday afternoon - 12:00 pm
All remote office routers and the Central Office VPN endpoint router are isolated by disconnecting their internal and external network connections. The central office firewall rules are verified as to content and the logs are examined for unusual traffic as are the IDS logs.

Eradication

No determination has been made at this time on if this was an internally or externally based attack. The Networking department is under a tremendous amount of pressure to get the network back up and running so permission is given to reset the passwords and configurations on the various routers to the contractors. Archived configuration files for each router are retrieved from the Central Office storage area and carefully examined for known-good content. Strict ACLs are included in the configurations to control any type of management connection to the routers as well as limiting the destination addresses for any traffic originating from the remote office. These new configurations are then encrypted with PGP and emailed to the person on site responsible for conducting the restore along with the incident response forms downloaded from the SANS website. Each contractor is directed to capture their entire session while connected to the router and to include that printout along with a narrative of events and their operations. Each contractor is also told to examine and capture via console printout each router's configuration and version information before rebooting the router as well as backing up the existing configuration file once the enable password is reset in an attempt to capture as much information on conditions as they can. All information/documentation is to be forwarded via PGP signed and encrypted email to the Information Security Department immediately upon completion.

Recovery

In accessing and restoring the routers each contractor uses essentially the same techniques as Sab originally used to access the routers. Following Cisco's instructions for recovering the enable password (see works cited section for a link to these instructions.) Once the enable password is recovered the contractor the contractor first issues the "Show Run" and "Show Ver" commands to preserve a copy of the configuration to their console session and then issues the "setup" command at the enable prompt. This command executes a script on the router that will walk the issuer through a set of questions that establish a management interface with an IP address. The contractor is then able to TFTP the updated configuration that was emailed to them onto the router and reboot. After completing the reload the external connection is restored and the VPN tunnels

are reestablished. After verifying that the tunnels are up and functioning the internal office connections are restored.

Monday afternoon – 1:30 pm
All routers are functional and communication is restored. Soft copy printouts from the various contractors that worked on the routers are forwarded to the Information Security Department for review. Reports on each contractor's actions taken during the course of events will follow as soon as possible.

Review of available information is begun in an attempt to determine cause and possible countermeasures. A quick review of the files provided by the contractors of their console sessions at the routers quickly reveals that the configuration on each router is the same. This indicates that whatever occurred was apparently the same on all routers.

Each session capture is then compared with the others in an attempt to find any difference or similarity. All appear to be the same except for some slight differences in uptime as displayed in the "show ver" command. Examples of the output are shown below. It was also noted that each router was restarted by reload.

RemoteOffice1>sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3S56I-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 14:28 by cmong
Image text-base: 0x80008088, data-base: 0x80C72114

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

RemoteOffice1 uptime is 9 hours, 46 minutes
System returned to ROM by reload
System image file is "flash:c2600-io3s56i-mz.120-5.T1.bin"

cisco 2611 (MPC860) processor (revision 0x203) with 26624K/6144K bytes of memory.
Processor board ID JAD051809X9 (4011857168)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
1 Channelized T1/PRI port(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

RemoteOffice5>sh ver
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IO3S56I-M), Version 12.0(5)T1, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Tue 17-Aug-99 14:28 by cmong
Image text-base: 0x80008088, data-base: 0x80C72114

ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

RemoteOffice5 uptime is 10 hours, 26 minutes
System returned to ROM by reload
System image file is "flash:c2600-io3s56i-mz.120-5.T1.bin"

cisco 2611 (MPC860) processor (revision 0x203) with 26624K/6144K bytes of memory.
Processor board ID JAD051809X9 (4011857168)
M860 processor: part number 0, mask 49
Bridging software.
X.25 software, Version 3.0.0.
Primary Rate ISDN software, Version 1.1.
2 Ethernet/IEEE 802.3 interface(s)
1 Channelized T1/PRI port(s)
32K bytes of non-volatile configuration memory.
16384K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

After comparing the amount of uptime displayed for each router and making adjustments for when each router was examined it quickly became apparent that the outages began first with the lower numbered offices and went upward to the higher numbered offices. It appeared as best we were able to determine that office 12 went down at least two minutes later than router 11 and was the last router to reload.

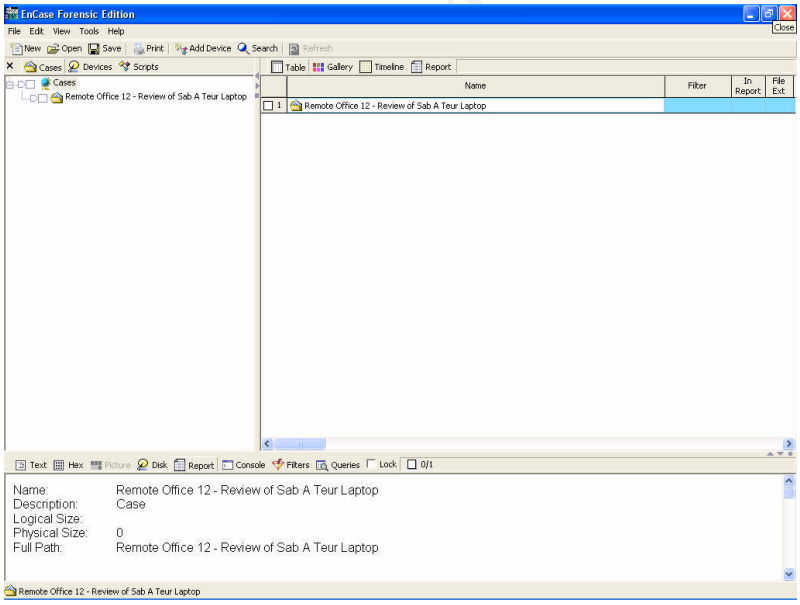
This raised the suspicion that the attack may have originated from this office and attention was focused on reviewing access records and equipment located in this office. The front door for this building has an electronic card access system and a review of the office showed that Mr. Sab A Teur's passcard was used to enter the building at approximately 1 am. While no passcard was required to exit the building use of the exit door is recorded in the log. No exits were shown to have

occurred between 1 am and 2:30 am. One exit was shown at 2:31 am and no other door events occurred until the doors unlocked for the day at 7 am.

When asked into the manager's office for questioning Mr. Sab A Teur was observed to be wearing his employee access card (indicating that it was likely him that entered and left the building at the times reflected in the logs). While Mr. Teur was in the manager's office his company supplied laptop was examined. The presence of a number of prohibited types of software were noted on the computer including password reversal (contained in the SolarWinds tools) and packet capture (ethereal). Further use of the computer was halted pending imaging of the hard drive.

Two copies of the hard drive were made. The first was performed by connecting a second hard drive to the laptop expansion bay while it was powered off. The laptop was then booted to a static CD version of Linux (Knoppix 3.4, www.knoppix.org) and the DD command was issued from a root prompt in a terminal window. (dd if=/dev/hda of=/dev/hdb) This disk copy was then placed in an identical laptop for live examination.

The second copy of the hard drive was made using the Encase forensic edition (V4.19a) boot CD and an external USB hard drive (This procedure is as simple as connecting the USB hard drive, booting the laptop with the Encase Boot CD, selecting USB support and following the prompts). Checksums were calculated and recorded for the images created to be used in the event that materials needed to be presented as evidence in a legal proceeding.



The original laptop was then sealed shut with evidence tape and placed in a laptop bag which was also sealed shut with evidence tape. The laptop and case

remained in the possession of the on-site Information Security Officer and returned to the evidence storage area at the main office.

Upon examination of the hard drive image using Encase forensic edition software (http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm) the drive was found to contain deleted configuration images from all of the corporate VPN routers.

To copy or unerase a file from within the encase image explorer you simply select the file, folder or drive, right click and select copy/unerase from the pop-up menu. In this case a simple browse of the available files revealed the router configuration files. There are a number of supplied Encase script files and queries that could have been used had a more in-depth review been needed.

Confronted with this evidence Mr. Teur confessed to his involvement in the outage and the methodology that had been used. As a result of this admission his employment was terminated with the case being turned over to law enforcement for prosecution.

Lessons Learned

A recap and examination session was held with Information Security, the networking team and senior management including a representative of the Human Resources department where the following items were discussed and an action plan agreed to.

A review of gathered materials revealed that:

The outage period lasted approximately 11.5 hours. With business hours beginning at 8 am there was a loss of at least:

1. 6.5 hours for the offices (5) in the Eastern Time zone. As very little work was possible these offices were closed resulting in the loss of an entire day.
2. 5.5 hours for the offices (5) in the Central time zone. These offices were also closed after 4 hours resulting in the loss of an entire day.
3. 4.5 hours for the offices (1) in the Mountain Time zone.
4. 3.5 hours for the offices (1) in the Pacific Time zone.

Functionality and productivity for those employees in the Central office was only mildly impacted during the outage period. Functionality for those employees in the remote offices was severely impacted during the outage period. Due to the hub and spoke arrangement all of the remote offices lost access to network file servers, Exchange, the corporate intranet and the public Internet.

The average amount of lost time was 7 hours for 832 employees at an average cost to the company of $54.00 per hour for a total minimum cost in lost time of (7x832=5824 x 54 =314,496) $314, 496. There were also costs associated with the contractors and follow up activities resulting in further costs in the amount of $19,652.00. Lost income was not factored. Costs related to a loss of public confidence were not factored.

Based on the review and recommendations from staff It was decided to implement those changes to address the issues outlined earlier on page 23 (copied below) and a new network diagram reflecting those changes follows this section. In addition each router will be reviewed using the Center for Internet Security's Router Audit Tool (RAT) from http://www.cisecurity.org/bench_cisco.html.

A hostile work environment was created for the employee and precautions were not taken to eliminate or restrict the terminated employee's access.

New Human Resource Policies were put in place governing dismissal and employee access.

The equipment was not secured. Although this would seem to be a basic step, many businesses fail to realize that no software firewall will protect the systems if someone has physical access.

All equipment is now required to be located in a secured area.

Although SNMP was in use configuration changes were not set to cause an alert using the "snmp-server enable traps config" command.

SNMP traps are now sent on any config event to a central server that will automatically notify network operations center employees.

There was no centralized syslog server to gather and maintain records generated by the various pieces of equipment.

All routers now send syslog messages at the "informational" level to a central syslog server for records retention.

Access lists were not in place to control SNMP traffic to the routers

All SNMP traffic to the routers is now restricted by ACL's

Access lists were not in place to control TFTP traffic to the routers

All TFTP traffic to the routers is now restricted by ACL's

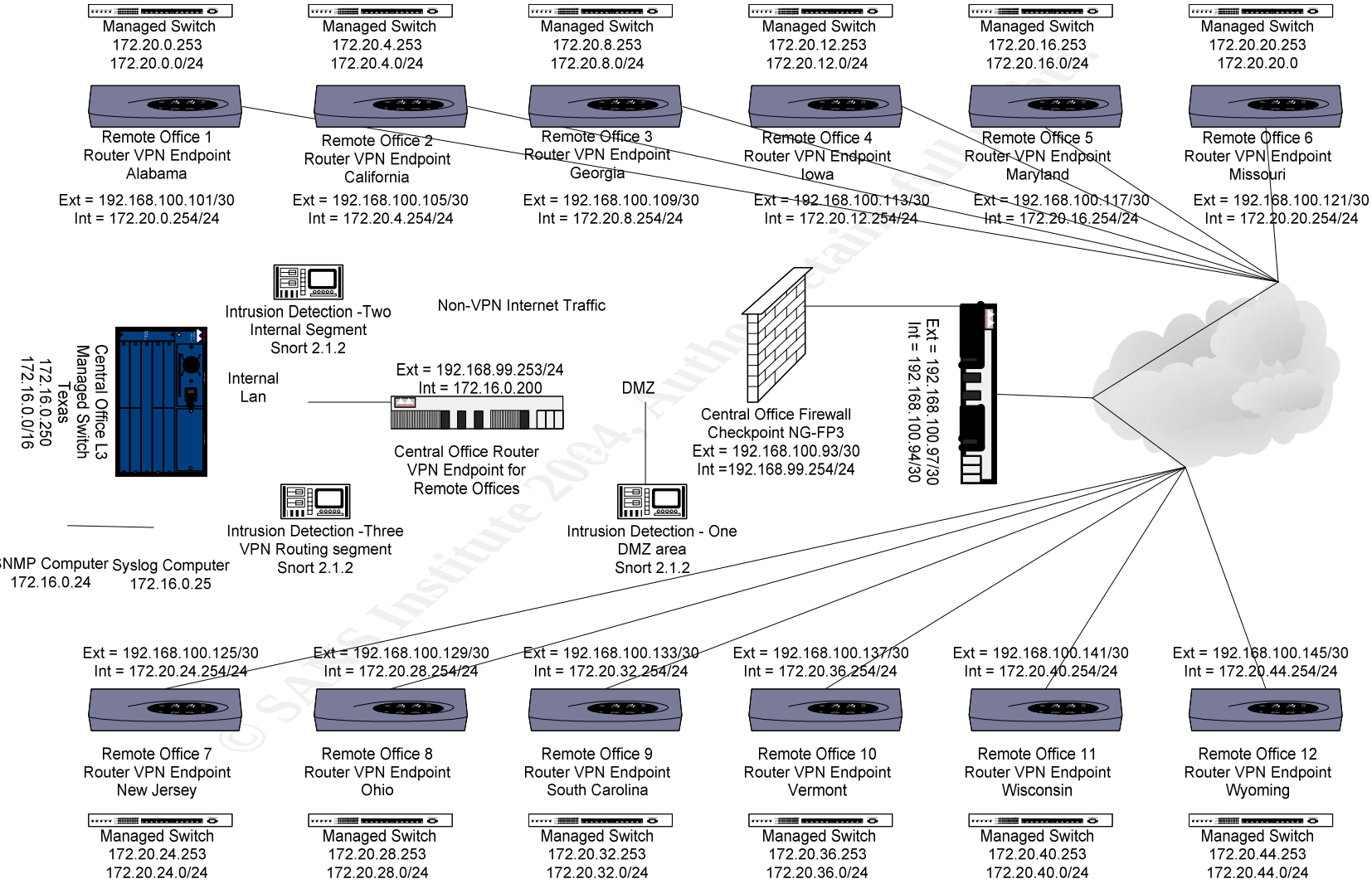
No IDS sensors were in use outside of the central office

Routing of the VPN connections took place on the Central Router thus shielding all of the remote office to remote office traffic within the VPN.

An additional snort sensor has been added and the routing to and from the remote offices now takes place off of the main office VPN router and "in the clear" so that it can be viewed by the IDS systems.

An incident report was prepared containing the timeline, findings, individuals and locations affected and recommendations listed above. This report was included in the file records along with the configurations, evidence reports, Human Resources reports and contractor and staff reports.

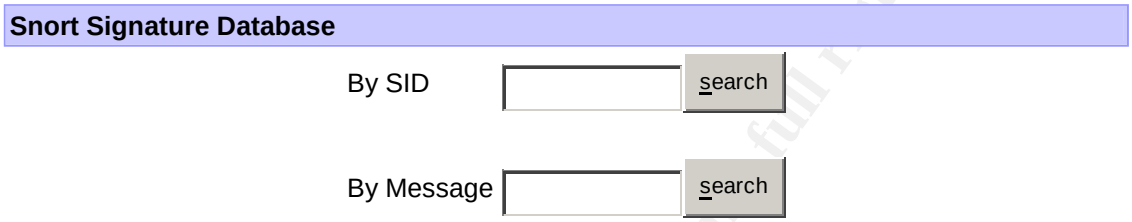
Revised Network Diagram:



Extras

Snort Rule from signature database:

Snort rule 1417 from the snort signature database page. (www.snort.org/snort-db) This is the rule that is presented in the ACID console print screen under the "Signatures of the Attack" section. As you can see below, the snort database allows you to search for related rules by SID or by words from the message like "SNMP".



SID	1417
Message	SNMP request udp
Signature	alert udp $EXTERNAL_NET any -> $HOME_NET 161 (msg:"SNMP request udp"; reference:bugtraq,4088; reference:bugtraq,4089; reference:bugtraq,4132; reference:cve,2002-0012; reference:cve,2002-0013; classtype:attempted-recon; sid:1417; rev:9;)
Summary	This event is generated when an SNMP-Trap connection over UDP to an SNMP daemon is made.
Impact	Information gathering
Detailed Information	The SNMP (Simple Network Management Protocol) Trap daemon usually listens on port 161, tcp or udp. An attacker may attempt to send this request to determine if a device is using SNMP.
Affected Systems	Devices running SNMP daemons on well known ports.
Attack Scenarios	An attacker sends a packet directed to udp port

	161, if sucessful a reply is generated and the attacker may then launch further attacks against the SNMP daemon.
Ease of Attack	Simple.
False Positives	None known. If you think this rule has a false positives, please help fill it out.
False Negatives	None known. If you think this rule has a false negatives, please help fill it out.
Corrective Action	Use a packet filtering firewall to protect devices using the SNMP protocol and only allow connections from well-known hosts.
Contributors	Sourcefire Research Team Brian Caswell <bmc@sourcefire.com> Nigel Houghton <nigel.houghton@sourcefire.com> Snort documentation contributed by Chaos <c@aufbix.org>
References	cve: 2002-0013 cve: 2002-0012 bugtraq: 4132 bugtraq: 4089 bugtraq: 4088

References

CERT. "Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQ)" 13 Feb 2002.
URL: http://www.cert.org/tech_tips/snmp_faq.html

Cikoski, Thomas R. "snmp-faq/part1" Anthology Edition. 2 Jul 2003
URL: http://www.faqs.org/faqs/snmp-faq/part1/

Cikoski, Thomas R. "snmp-faq/part1" Anthology Edition. 2 Jul 2003
URL: http://www.faqs.org/faqs/snmp-faq/part2/

Cisco, Inc. "Network Security Policy: Best Practices White Paper" 4 May 2004
URL: http://www.cisco.com/warp/public/126/secpol.pdf

Cisco, Inc. "Password recovery procedure for the Cisco 2600 series router" Multiple versions of this document for other Cisco platforms are available by searching for "password recovery" on the public Cisco web site.
URL: http://www.cisco.com/warp/public/474/pswdrec_2600.pdf

Works Used/Cited

CERT. "Simple Network Management Protocol (SNMP) Vulnerabilities Frequently Asked Questions (FAQ)" 13 Feb 2002.
URL: http://www.cert.org/tech_tips/snmp_faq.html

CERT. "Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)" 13 Feb 2002.
URL: http://www.cert.org/advisories/CA-2002-03.html

Common Vulnerabilities and Exposures "CAN-2002-0013" 15 March 2002.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0013

Common Vulnerabilities and Exposures "CAN-2002-0012" 15 March 2002.
URL: http://cve.mitre.org/cgi-bin/cvename.cgi?name=2002-0012

Security Focus – BugTraq **–** "Cisco Malformed SNMP Message Denial of Service Vulnerabilities" 1 March 2004.
URL: http://www.securityfocus.com/bid/4132

Security Focus – BugTraq **–** "Multiple Vendor SNMP Trap Handling Vulnerabilities" 25 July 2003.
URL: http://www.securityfocus.com/bid/4089

Security Focus – BugTraq **–** "Multiple Vendor SNMP Trap Handling Vulnerabilities" 11 April 2003.
URL: http://www.securityfocus.com/bid/4088

Cikoski, Thomas R. "snmp-faq/part1" Anthology Edition. 2 Jul 2003
URL: http://www.faqs.org/faqs/snmp-faq/part1/

Cikoski, Thomas R. "snmp-faq/part1" Anthology Edition. 2 Jul 2003
URL: http://www.faqs.org/faqs/snmp-faq/part2/

Cisco, Inc. "Network Security Policy: Best Practices White Paper" 4 May 2004
URL: http://www.cisco.com/warp/public/126/secpol.pdf

Cisco, Inc. "Password recovery procedure for the Cisco 2600 series router" Multiple versions of this document for other Cisco platforms are available by searching for "password recovery" on the public Cisco web site.
URL: http://www.cisco.com/warp/public/474/pswdrec_2600.pdf

Cisco, Inc. "Cable specifications guide"

URL:
http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/cis2500/2509/acsvrug/cables.pdf

National Security Agency. “Cisco Router Guides”
URL: http://nsa1.www.conxion.com/cisco/

Center for Internet Security. “Benchmarks/tools for the Cisco IOS” October 2003
URL: http://www.cisecurity.org/bench_cisco.html

Fluke Networks. “Lan MapShot – Free trial”
URL:
http://www.flukenetworks.com/us/LAN/Monitoring+Analysis+Diagramming/LAN+MapShot/_free+trial.htm

Castle Rock. “SNMPc7 – Free Trial”
URL: http://www.castlerock.com/products/download/evaluation.htm

Solarwinds. “Network Management Toolsets”
URL: http://solarwinds.net/Toolsets.htm

Observer by Network Instruments (Free trail available under product links)
URL: http://www.networkinstruments.com/index.html

WinPcap – Packet capture architecture for Windows
URL: http://winpcap.polito.it

Ethereal – Protocol analyzer (Windows version)
URL: http://www.ethereal.com/download.html

Snort Intrusion Detection System
URL: www.snort.org

Snort IDS rules database
URL: www.snort.org/snort-db/

Guidance Software, Encase Forensic Edition
URL: http://www.guidancesoftware.com/products/EnCaseForensic/index.shtm

Knoppix, A CD based static Linux distribution
URL: http://www.knoppix.org