Interested in learning more about security?

SANS Institute InfoSec Reading Room

Securing a Windows Snort Sensor for Hostile Environments

Snort is an open-source Network Intrusion Detection System (NIDS). Originally written for UNIX, it has since been ported to the Windows platform. While Snort undoubtedly runs faster and with less packet loss on a UNIX host, many organizations lack the requisite skill sets to deploy and maintain a UNIX host within their environment. For these organizations, Snort on Windows 2000 provides a low-cost, high-quality NIDS. Deploying Snort on Windows can be a convoluted process. Michael Steele of Silicon Defense has simplifie...

Securing a Windows' Snort Sensor for Hostile Environments

By Michael Wunsch
March 22, 2003
GSEC Certification
Practical Assignment version 1.4b, Option 1

Abstract

Snort is an open-source Network Intrusion Detection System (NIDS). Originally written for UNIX, it has since been ported to the Windows platform. While Snort undoubtedly runs faster and with less packet loss on a UNIX host, many organizations lack the requisite skill sets to deploy and maintain a UNIX host within their environment. For these organizations, Snort on Windows 2000 provides a low-cost, high-quality NIDS.

Deploying Snort on Windows can be a convoluted process. Michael Steele of Silicon Defense has simplified the installation with his excellent paper, "Snort Installation Manual – Snort, MySQL, Acid & IIS – Windows NT4 Server, 2000, & XP (All Versions)[1]." His paper lays out a step-by-step procedure for the complicated build process. But it does not address the security of the Snort sensor. Indeed, a sensor built solely to his specifications will not survive on any but the most trusted of network segments. This white paper documents how to secure a Windows' Snort sensor for deployment into extremely hostile environments.

Design Goals

There are many considerations to take into account when building a Snort sensor. First are the performance requirements of the sensor itself.

Snort can be very demanding of a computer. A bottleneck in any component – the CPU, bus, memory, disk or a network interface card – will result in packets being dropped instead of being processed by the sensor. CPU utilization is directly dependent on the volume of traffic on the monitored network segment, as well as on the number and type of attack signatures that are configured within the sensor. Disk drives must be fast to support the volume of logged data without becoming a bottleneck.

The second consideration must be the security of the sensor itself. A compromised Snort sensor cannot be trusted. An attacker can erase logs and alerts to cover her tracks. She can also use the configuration files of the sensor to glean a good deal of information about the structure of a monitored network and the location of critical systems within that network.

[1] Available at http://www.silicondefense.com/support/windows/winsnortdocs/WinSnortIIS.pdf

To prevent this, the sensor must be hardened to withstand attack. It should be designed to protect itself, to issue alerts when it is under attack, and to offload copies of its alerts to a secure server. This preserves a tamper proof record for use in the event the sensor is compromised.

Finally, the rules for the Snort sensor need to be carefully tuned. This reduces the load on the sensor, protects critical systems and eliminates false alerts. Tuning of the Snort sensor is beyond the scope of this document.

Security Features

This white paper details procedures for building multi-tiered defenses into a Windows' Snort sensor. Those defenses include:

- The sensor is built with an absolute minimum of installed software and operating system components. Running services are kept to a minimum. This reduces the profile of the system, increasing performance and presenting less of a code base for an attacker to exploit.
- The operating system is installed by itself on the system partition. All other software is installed in a separate partition to reduce the potential of a successful exploit being used to compromise the OS.
- The file system is secured to prevent access to the root directory of the partitions and to potentially dangerous administrative utilities. This reduces the ability of an attacker who has compromised the sensor to move around within and expand their control of the system.
- The operating system is further secured with a security template. This security template contains all of the security configuration parameters for the sensor. It can be quickly reapplied to ensure the integrity of the sensor's configuration.
- The Snort sensor's uses the Analysis Console for Intrusion Databases (ACID) as its management console. ACID runs on Microsoft's Internet Information Services's web server. The web server is extensively hardened against attack.
- The sensor is built with two network interface cards (NICs). One NIC is placed on the monitored segment. It has no IP protocol stack bound to it, making it difficult to attack. The other NIC is installed on a protected management segment for administration and monitoring of the sensor.
- The TCP/IP protocol stack on the sensor is hardened against attack.
- A packet filter is erected around the sensor. Traffic is restricted both inbound to and outbound from the sensor. The only traffic allowed inbound is the authenticated and encrypted Remote Desktop Protocol (RDP) originating from the management workstation. The packet filter drops virtually all other incoming packets. This makes the sensor invisible to normal ping sweeps and port scans.

- The Snort sensor is configured to issues alerts on any attempt to circumvent the packet filter or manage the sensor.
- Copies of all alerts and of the Windows 2000 Event Logs are sent to a syslog server in real-time. If an attacker successfully compromises the sensor and deletes or modifies the alerts and logs on the sensor, a reliable trail will still remain on the syslog server.

Choosing Hardware

Choose a server class machine as your Snort sensor. While it does not necessarily need to be the newest or the fastest server, bigger is obviously better. The quicker the server is, the less likely it will be to drop packets when a monitored network segment becomes busy. Ultimately, your choice of system should be driven by the amount of network traffic the sensor will be called on to handle. A single 930 Mhz PIII processor with 1Gb of RAM and a three-disk RAID 5 array should be able to handle 25Mb/s of traffic without losing packets (with a 'typical', tuned Snort rule set, if there is such a thing).

Dual network interface cards are an absolute necessity. One NIC will be placed in promiscuous mode to capture packets. It will be configured without a TCP/IP protocol stack, so it cannot send or receive TCP/IP traffic. The other NIC will be used as a management NIC.

Installing the Operating System

Before you start building the sensor, disconnect the server from any active network. It would not do to have the sensor compromised before it is completely built and secured.

Begin by installing the Windows 2000 Server operating system. The operating system should be installed with an absolute minimum set of components. This provides a smaller base of code for an attacker to exploit and use. It also improves the performance of the Snort sensor. Be sure to create the server as a stand-alone machine (not a member of Active Directory or a Windows' domain).

Plan on creating two disk partitions. The system partition that is created during the installation of the Windows 2000 Server operating system should be a minimum of 4Gb in size. This partition will only be used for the operating system and minimal software. Format all partitions with the NTFS file system.

When prompted for the Administrator password, choose a password at least 15-characters in length. Many password crackers will not properly handle passwords longer than fourteen characters in length. Use a minimum of three character sets and at least one of the following characters: []\;',./`~(){}|:"<>? These characters are not used in the faster running password cracking routines employed by popular password crackers such as L0phtCrack.

When you are prompted to install the Windows 2000 Components, install only the absolute minimum set of components – Wordpad and Terminal Services. Do

not install any other components. Do not install the Internet Information Services's Web Server at this time.

When the Terminal Services Setup screen appears, select the remote administration mode.

At the Networking Components screen, disable the Client for Microsoft Networks. (This will result in a DFS error on reboot – which will be corrected later). Uninstall File and Printer Sharing for Microsoft Networks. Do not configure TCP/IP at this time.

After the operating system is installed and the system has been rebooted, format the remaining partition with NTFS. This second partition will contain the IIS Web Server, Snort, the MySQL database, the ACID console and NTsyslog.

Configuring the Network Interface Cards

The two Network Interface Cards play different roles. One NIC is used for management and monitoring of the sensor. This NIC is connected to a more secure (or protected) network segment. It has an IP address, but a packet filter will restrict access to that address. To configure the management NIC, open Network and Dial-up Connections. Right-click on the NIC icon and select Properties. Uncheck all boxes except for the Internet Protocol (TCP/IP). This will unbind the protocols from the NIC.

Next, click the Configure button and choose the Advanced tab. Manually set the Ethernet adapter to 100 Mb full-duplex. Do not use AutoDetect, it can result in speed and duplex mismatches in the event of a server reboot. Next, configure the TCP/IP protocol stack by double-clicking on the Internet Protocol (TCP/IP) list item. Hardcode the IP address, Subnet mask, Default Gateway, Preferred DNS server and Secondary DNS server fields. Click the Advanced button, select the WINS tab and uncheck the Enable LMHOSTS lookup box. Disable NetBIOS over TCP/IP.

The other NIC is used to gather raw packets off the network for the Snort sensor. Of necessity, this NIC must be highly secured, since it will be connected to a hostile network segment. This card will not have a TCP/IP protocol stack bound to it. As a result, an attacker cannot directly address this NIC. Right-click on the icon for this NIC in the Network and Dial-up Connections window and select Properties. Uncheck all boxes to unbind ALL of the protocols (including TCP/IP) from the NIC. Click the Configure button and choose the Advanced tab. Manually set the Ethernet adapter to 100 Mb full-duplex.

Installing the Internet Information Services Web Server

Internet Information Services installs by default into the system partition of a Windows' host. Many of the most dangerous exploits of Microsoft's web server counted on this default behavior. A succession of directory transversal attacks, for example, resulted in attackers gaining access to the cmd.exe shell (and other programs) located within the system partition.

To forestall this class of attacks, install the web server into another partition. Use the unattended setup to accomplish this. First, create an answer file containing the following lines:

```
 [Components]
iis_common = on
iis_inetmgr = on
iis_www = on
iis_smtp = off
iis_nntp = off

[InternetServer]
PathWWWRoot="D:\InetPub\wwwroot"
```

Next, kick off the unattended installation of Internet Information Services using sysocmgr.exe. Assuming the answer file created above was saved as d:\answer.txt, you would enter the following command at a command prompt to install the IIS Web Server on the D: drive:

```
sysocmgr /i:%windir%\inf\sysoc.inf /u:d:\answer.txt
```

Now that all of the native operating system components are installed, apply the most current Microsoft Service Pack and all relevant Hot Fixes to the server. This eliminates many known security vulnerabilities in the code base of the Microsoft operating system.

Configuring Terminal Services

Remote management and monitoring of the sensor will use Microsoft's Remote Desktop Protocol. This is an authenticated and encrypted protocol. It will be used to access one of the two remote administration terminal server sessions built into Windows' 2000 Server.

Open the Administrative Tools icon within the Control Panel. Click on the Terminal Services Configuration tool to configure the security of these remote administration sessions. When the tool launches, double-click on RDP-Tcp in the right-hand pane to display the property tabs. Set the Encryption Level to High on the General tab. Click on the Sessions tab and check both of the Override user settings boxes. Set End a disconnected session to 30 minutes, then set both the Active and Idle session limits to Never. This will allow the remote management workstation to remain permanently connected to the Snort sensor. Select the Client Settings tab and uncheck the Use connection settings from user settings box. Uncheck the Connect client printers at logon and Default to main client printer boxes.

Installing the Snort NIDS

Snort was written for UNIX. While Snort will work on a Windows' host, installing it is an involved process. As mentioned earlier, Michael Steele of Silicon Defense has written an excellent, step-by-step procedure for installing Snort on Windows.

The procedures he outlines in the document detail the installation of Snort with the MySQL database and the ACID console. It also requires the installation of the WinPcap driver, PHP, ADODB, PHPLot and JPGraph.

Mr. Steele focused on creating an easy-to-follow procedure for installing the Snort sensor and ACID console on Windows. And in that he did admirably well, which is why I will not try to improve on his installation procedures here.

What his procedure 'lacks' is a process for securing the sensor. (And quite frankly, since this was not the focus of his paper, 'lacks' is perhaps not the correct term). If you follow his install procedure meticulously, you will end up with a Snort sensor that is subject to all of the vulnerabilities of the base Windows' operating system – NetBIOS null sessions, WebDAV vulnerabilities, etc. Such a system will not survive for long outside of a firewall, and may not survive long inside of a DMZ.

Eliminating those vulnerabilities will be the focus of the remainder of this white paper.

But first, I recommend you refer to Michael Steele's document to install the various components of a Windows' Snort sensor. It is available at:

http://www.silicondefense.com/support/windows/winsnortdocs/WinSnortIIS.pdf

Follow the instructions carefully, with the following exceptions. Do not perform the steps outlined in the sections titled Installing Internet Information Services (IIS) Webserver and IIS Lockdown[2]. The procedures for installing the IIS Web Server were discussed previously within this white paper. The steps for securing the Web Server are immediately following this section.

Securing the Internet Information Services Web Server

After testing the installation of the Snort IDS and ensuring that it is functioning correctly, it is time to secure the web server. Start by running the IIS Lockdown tool (IISLockd.exe) available for download from Microsoft. This tool performs 95% of the work required to secure the web server. Just double-click on the executable to launch the application. Accept the license when prompted. When the Select Server Template dialog box appears, choose the Static Web Server option. Accept the defaults to complete the lockdown of the web server. IIS Lockdown has just removed a number of unneeded script mappings, restricted access to administrative tools and removed the sample web site, turned off WebDAV and implemented various other security settings.

One of those configuration changes involved the installation of the URLScan ISAPI filter. This filter validates incoming URLs and rejects HTTP request if it includes Unicode (used in various directory transversal attacks), accesses .bat, .cmd or .exe files, or uses restricted verbs. This filter must be modified to work with the ACID console.

---

[2] Steele, pp. 11 – 12.

To modify URLScan, open the UrlScan.ini file located in the C:\WINNT\system32\inetsrv\urlscan folder with a text editor. Scroll down to the RemoveServerHeader line and set RemoveServerHeader=1. This removes IP address information from the HTTP headers that are sent back to a web browser. This will prevent the internal address of the Snort sensor from being divulged in the event it is behind a firewall or router that is performing Network Address Translation.

Now scroll down to the [AllowVerbs] section and add POST to the verb list. This will allow the ACID console to query the MySQL database. Save the URLScan.ini file. Stop and restart the World Wide Web Publishing service to activate the new UrlScan filters.

Next move the web server logs off of the system partition. This will prevent them from consuming space on the partition and potentially crashing the server if it runs out of free space. Move the C:\WINNT\system32\logfiles folder to d:\logfiles. Open the Computer Management tool in the Administrative Tools folder, then double-click on Services and Applications. Right-click on Internet Information Services and choose Properties. Within the Master Properties dialog box, verify that the WWW Service is in the drop down box and click on the Edit button. Under the General Properties tab, set the Log file directory to d:\logfiles. Close the window and click on the Home Directory tab. Uncheck the Index this resource option. Click on the Configuration button and choose the App Options tab Uncheck the Enable Parent Paths. This will prevent directory transversal attacks. Close the WWW Service Master Properties window.

Configuring a Packet Filter

The Snort sensor as it is now configured has two network interfaces. One has no protocol stack bound to it, and is not subject to direct attack. The other interface, however, has an IP address. Steps must be taken to protect this interface from attack.

A packet filter can be created to protect this interface. This packet filter needs to allow some outbound traffic: queries to a Domain Name Server, syslog messages destined for a syslog server and web browsing to allow links contained in the ACID console to work correctly and to allow research on Snort alerts.

In addition, Remote Desktop Protocol should be allowed inbound from a management workstation. The IP packet filter will be configured to drop all other traffic inbound or outbound.

Microsofts's IP Security Policy Editor will be used to create the packet filter. This packet filter permits or denies traffic based on protocol type, source and destination address and source or destination port. It drops all packets that are not allowed through the filter.

You can use a GUI tool to configure the packet filter, or you may use ipsecpol.exe, which is a batch version of the tool. Ipsecpol will be used here and is available for download from Microsoft. After ipsecpol.exe is downloaded and installed on the sensor, the following commands can be entered at a command

prompt to create a packet filter. Just replace s.s.s.s with the IP address of the Snort sensor, d.d.d.d with the IP address of a DNS server, m.m.m.m with the address of a management workstation and x.x.x.x with the address of the syslog server:

```
ipsecpol -w REG -p "Snort Sensor" -r "Inbound RDP Traffic"
    -f m.m.m.m+ s.s.s.s:3389:TCP -n PASS
ipsecpol -w REG -p "Snort Sensor" -r "Outbound DNS Traffic"
    -f s.s.s.s+d.d.d.d:53:UDP -n PASS
ipsecpol -w REG -p "Snort Sensor" -r "Outbound Web Traffic"
    -f s.s.s.s+*:80:TCP -f s.s.s.s+*:443:TCP -n PASS
ipsecpol -w REG -p "Snort Sensor" -r "Outbound Syslog Traffic"
    -f s.s.s.s+x.x.x.x:514:UDP -n PASS
ipsecpol -w REG -p "Snort Sensor" -r "Deny All Other Traffic"
    -f *+* -n BLOCK
ipsecpol -w REG -p "Snort Sensor" -x
```

This is a very tightly defined packet filter. The first command only allows point-to-point Remote Desktop Protocol traffic from the management workstation to the sensor. The second allows point-to-point DNS queries from the sensor to a DNS server. The third allows allows all HTTP and HTTPS web browsing traffic outbound from the sensor. The fourth command allows point-to-point syslog traffic from the sensor to the syslog server. The next command prevents all other types of traffic. And the last command applies the filter.

It's a pretty tightly defined packet filter, but Microsoft will try to sneak a few other types of traffic through without telling you. By design Microsoft allows certain types of traffic through its IP Security packet filters by default. Broadcast and multicast traffic is always allowed though the filter, there is not way to prevent it. In addition, several other protocols are allowed through the filter. They are:

- Resource Reservation Protocol (RSVP – IP protocol 46)
- Internet Key Exchange Protocol (IKE – UDP packets with source and destination port 500)
- Kerberos (TCP or UDP packets with a source or destination port of 88)

This behavior can be partially modified by adding a value to the Windows 2000 registry. Both RSVP and Kerberos traffic can be prevented from leaking through the packet filter. Multicast, broadcast and IKE traffic will always traverse the packet filter. See the section "Modifying a Security Template" below.

Customizing Snort Rules to Protect the Sensor

Microsoft's IP Security packet filter is a very simple packet filter. It is not aware of session state or of TCP flags. As a result, the above packet filter may still allow an attacker to gain access to the sensor. For example, the web-browsing rule allows the Snort sensor to access any web server on the Internet using HTTP (TCP 80) or HTTPS (TCP 443). A hacker can turn this around to attack the

sensor. All they have to do is alter a packet destined for the Snort sensor to use TCP port 80 or 443 as its source port. The packet filter will treat these incoming packets as replies from a web server. It will act as if they are responses to web requests that originated on the sensor and will allow them to pass through to the sensor. In this fashion an attacker can connect to any open TCP port on the Snort sensor. In essence, the packet filter ceases to exist when the source port of an incoming packet is correctly modified.

The Snort sensor can be configured to monitor for attacks that bypass the packet filter. Use a text editor to open the local.rules file in the D:\Applications\snort\rules folder. Insert the following three attack signatures into the file, replacing s.s.s.s with the IP address of the Snort sensor.

```
alert tcp $EXTERNAL_NET any -> s.s.s.s 3389 (msg:"LOCAL RDP
    Connection to Snort"; flags: S; classtype:bad-unknown; sid:1000002;
    rev:5;)
alert tcp s.s.s.s !3389 -> $EXTERNAL_NET any (msg:"LOCAL TCP
    Session to Snort"; flags: SA; classtype:bad-unknown; sid:1000001;
    rev:5;)
alert udp $EXTERNAL_NET !53 -> s.s.s.s any (msg:"LOCAL UDP Packet
    to Snort"; classtype:bad-unknown; sid:1000003; rev:5;)
```

The first signature alerts when a connection is made to the RDP port on the Snort sensor. It is triggered by TCP SYN packet from port 3389 indicating an attempt to connect to the Snort sensor to manage or monitor it. The only source address that should ever appear in this message is the IP address of the designated management station. Any other source address indicates a conscious attempt by someone to circumvent the IP packet filter. This is a positive indication of an attack on the sensor.

The second signature alerts when a connection is made to any other open TCP port on the Snort sensor. It alerts when the sensor responds to the attempt with a TCP SYN/ACK packet. A SYN/ACK response is used instead of the original SYN request to eliminate false positives that would be generated by a user on the sensor browsing out to a web site on the Internet. If this alert is triggered it indicates an attack on the sensor. There are no false positives.

The third signature alerts when the sensor receives any UDP packet other than a response to a DNS query. This alert also indicates an attack on the sensor. There are no false positives.

These three attack signatures, together with active monitoring of the Snort sensor, compensate for the deficiencies of Microsoft's IP Security packet filter. For this solution to work, however, network traffic to and from the management NIC must be 'mirrored' to the NIC the Snort sensor is listening on.

Modifying a Security Template

Several registry modifications need to be made to close holes in the IP packet filter and to harden the TCP/IP protocol stack, among other things. While those

changes could be entered directly to the Windows' Registry using a registry editor, it is better to modify the Microsoft Management Console (MMC) Security Template interface to include the registry options.

Security Templates are used in conjunction with the MMC Security Analysis and Configuration editor to apply security settings to a Windows 2000 host. Adding the registry entries to the Security Template interface makes it easy to reapply security settings in the event the settings may have been changed – for instance, after the application of a Service Pack or Hot Fix.

To modify the template, open C:\WINNT\INF\SCEREGVL.INF with Notepad. Page down to the [Register Registry Values] section and add the following lines to this section:

```
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\EnableICMPRedirect,4,%noredirect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DeadGWDetectDefault,4,%nogwdetect%,0
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\DisableIPSourceRouting,4,%srcroute%,3,0|%SrcRoute0%,1|%SrcRoute1%,2|%SrcRoute2%
MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect,4,%synattack%,3,0|%SynAttack0%,1|%SynAttack1%,2|%SynAttack2%
MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters\AutoShareServer,4,%noadminshares%,0
MACHINE\System\CurrentControlSet\Services\DnsCache\Parameters\QueryIpMatching,4,%ipmatching%,0
MACHINE\System\CurrentControlSet\Services\IPSEC\NoDefaultExempt,4,%IpFilters%,0
```

Now scroll down to the [Strings] section and add the following lines to the section:

```
noredirect = # IP Protection - Enable ICMP redirection
nogwdetect = # IP Protection - Enable dead gateway detection
srcroute = # IP Protection - Source Routing
SrcRoute0 = Forward all packets
SrcRoute1 = Do not forward packets
SrcRoute2 = Drop all packets
synattack = # IP Protection - SYN Attack Protection
SynAttack0 = No protection
SynAttack1 = Reduced retries and delayed route cache entry
SynAttack2 = Reduced retries and delayed RCE and WinSock
noadminshares = # Shares - Enable administrator sharepoints
ipmatching = # DNS - Accept DNS responses only from queried hosts
ipfilters = # IP Filters – Close RSVP and Kerberos holes in IP Filters
```

Save and close the SCEREGVL.INF file. Now go to a command prompt and type:

```
REGSVR32 SCECLI.DLL
```

This command adds entries to the MMC Security Template GUI. The purpose of the additional entries will be discussed in the next section.

Configuring a Security Template

Open the Microsoft Management Console by typing "mmc" at a command prompt. Click on the File menu and select Add/Remove Snapin… When the dialog box appears, click on the Add button and add the Security Configuration and Analysis and Security Templates snapins. Click the Close button, then the OK button to return the main MMC console.

Click on Security Templates in the left-hand pane to expand the tree. Now click on the "securews" policy to expand it. This template will be used as the basis for securing the Snort sensor.

Make the following alterations to the policy.

Open the Local Policies\Security Options section of the template. At the top of this portion of the template are the values that were just added to the Security Template GUI. The values start with a pound sign (#). Set these new values to the following:

```
# IP Protection - Enable ICMP redirection = Disabled
# IP Protection - Enable dead gateway detection = Disabled
# IP Protection - Source Routing = Drop all packets
# IP Protection - SYN Attack Protection = Reduced retries and delayed
  RCE and WinSock
# Shares - Enable administrator sharepoints = Disabled
# DNS - Accept DNS responses only from queried hosts = Enabled
# IP Filters – Close RSVP and Kerberos holes in IP Filters = Enabled
```

What do these new values do? The first four (identified by "# IP Protection") are used to harden the TCP/IP protocol stack from attack. The first disables ICMP redirection. An attacker can use redirection to modify the internal routing tables of the sensor. The second disables dead gateway detection, which potentially allows an attacker to redirect traffic flows to and from the server. The third drops all source-routed packets. The host sending a source-routed packet determines the path the packet takes through a network. This potentially allows an attacker to push packets into a network. The fourth value delays the point at which the system reserves TCP session resources – helping protect the sensor from SYN flood attacks (a type of denial of service attack).

The fifth value disables the administrator sharepoints – IPC$, ADMIN$, C$, etc.

The next value ensures that DNS responses will be entered into the Windows' DNS cache only if the server first queried DNS for the address. By default Windows' 2000 will accept responses for DNS queries that it never made. An attacker can use this behavior to poisoning the sensor's DNS cache, redirecting traffic to a server under the attacker's control.

The last value closes the RSVP and Kerberos holes in the IP Security Policy filters (discussed above).

Most of the default Security Option settings of the "securews" template can be accepted as is. Make just the following alterations to the template:

Additional restrictions for anonymous connections – No access without explicit anonymous permissions
Allow system to be shut down without having to log on – Disabled
Clear virual memory pagefile when system shuts down – Enabled
Do not display last user name in logon screen – Enabled
LAN Manager Authentication Level – Send NTLMv2 response only \ refuse LM & NTLM
Message text for users attempting to log on - <legal banner of your choice>
Message title for users attempting to log on - <legal banner of your choice>
Number of previous logons to cache (in case domain controller is not available) – 0 logons
Rename administrator account - <account name of your choice>
Rename guest account - <account name of your choice>
Unsigned non-driver installation behavior – Warn but allow installation

Next, open the Local Policies\Audit Policy section of the template. Set the following options for the type of events that will be logged:

Audit account logon events – Success, Failure
Audit account management – Success, Failure
Audit directory service access – No auditing
Audit logon events – Success, Failure
Audit object access – No auditing
Audit policy change – Success, Failure
Audit privilege use – Failure
Audit process tracking – No auditing
Audit system events – Success, Failure

Now open the Event Log\Settings for Event Logs section of the template and set the following options. The event logs are set to rollover as needed with a 16Mb log file size:

Maximum application log size – 16384 kilobytes
Maximum security log size – 16384 kilobytes
Maximum system log size – 16384 kilobytes
Restrict guest access to application log – Enabled

Restrict guest access to security log – Enabled
Restrict guest access to system log – Enabled
Retain application log – Not defined
Retain security log – Not defined
Retain system log – Not defined
Retention method for application log – As needed
Retention method for security log – As needed
Retention method for system log – As needed
Shut down the computer when the security audit log is full – Disabled

Open the System Services section of the template. All services except those in the following list should be disabled. All of the services in the following list should be set to start automatically (with the exception of the two listed as Manual). The permissions for managing these services should be set to the Administrators group/Full Control. While a Windows 2000 Snort sensor can be run with fewer services, this sets a good balance between the security and the manageability of the sensor:

COM+ Event System
DNS Client
Event Log
IIS Admin Service
IPSEC Policy Agent
Logical Disk Manager
MySql
Network Connections – Manual
NTsyslog
Plug and Play
Protected Storage
Remote Procedure Call (RPC)
Security Accounts Manager
Snort
System Event Notification
Terminal Services
Windows Management Instrumentation
Windows Management Instrumentation Driver Extensions – Manual
World Wide Web Publishing

Finally, open the File System portion of the template. Some portions of the NTFS file system should be more secured to prevent their use by any attacker that is able to compromise the sensor. Add entries for the following folders and restrict them to Full Control access for the Administrators group and the System account only. Be sure that you do not allow these permissions to propagate down into the child folders. These settings will prevent access for non-administrators to the root of the system drives:

C:\ D:\

Next, add entries for the following files and set their permissions to access by the local Administrators group only (Full Control). Unless otherwise specified, the files are located in the C:\WINNT\system32\ folder:

append.exe	at.exe	attrib.exe	cacls.exe
cmd.exe	command.com	cscript.exe	debug.exe
exe2bin.exe	finger.exe	ftp.exe	hostname.exe
mmc.exe	mountvol.exe	nbtstat.exe	net.exe
net1.exe	netsh.exe	netstat.exe	nslookup.exe
ntsd.exe	pathping.exe	ping.exe	rcp.exe
regedt32.exe	regini.exe	regsvr32.exe	rexec.exe
route.exe	rsh.exe	runas.exe	runonce.exe
secedit.exe	share.exe	telnet.exe	termsrv.exe
tftp.exe	tracert.exe	tsadmin.exe	tscon.exe
tskill.exe	tsprof.exe	tsshutdn.exe	wscript.exe
xcopy.exe	arp.exe	change.exe	chglogon.exe
chgport.exe	chguser.exe	chkdsk.exe	chkntfs.exe
cipher.exe	cluster.exe	compact.exe	convert.exe
dfscmd.exe	doskey.exe	edlin.exe	expand.exe
fc.exe	find.exe	findstr.exe	forcedos.exe
iisreset.exe	ipxroute.exe	label.exe	logoff.exe
lpq.exe	lpr.exe	makecab.exe	mem.exe
msg.exe	ntbackup.exe	print.exe	query.exe
rasdial.exe	recover.exe	register.exe	replace.exe
reset.exe	setpwd.exe	shadow.exe	snmp.exe
snmptrap.exe	subst.exe	tsdiscon.exe	chcp.com
diskcomp.com	diskcopy.com	format.com	mode.com
more.com	tree.com	usrmgr.com	
C:\WINNT\regedit.exe			

An easy way to set these file permissions is to add a single entry for one of the files and then save the “securews” template. Now open the template using Notepad and locate the line setting the file permissions. Copy the line and repeatedly paste the line back into the template, changing the file names as you go. Save the file.

Applying the Security Template

Now that the template is built, right-click on Security Configuration and Analysis tool in the left-hand portion of the Microsoft Management Console. Select Open Database and type “security.sdb” as the database name. Then browse to the template file that was just modified and select it. Click the Open button.

The main MMC console will appear again. Right-click on Security Configuration and Analysis tool and select Configure Computer Now to apply the settings in the security template.

Syslog Monitoring

Syslog monitoring is implemented on the sensor to offload both Snort alerts and the Windows' Event Logs to a backend syslog server. In the event that an attacker successfully compromises the Snort sensor, the alerts and logs on the sensor can no longer be trusted. An attacker can easily alter both to cover their tracks. However, the copies of the logs that are on the syslog server can be used to provide a reliable audit trail of the attacker's activities.

Snort is configured for syslogging by editing the snort.conf file in the D:\Applications\snort\etc directory. Michael Steele's directions for installing Snort actually includes the required edits to this file:

> There are several other settings that will need to be changed, and these MUST be copied EXACTLY as they are described here. Do a search and replace the like same lines….
>
> Original: # output alert_syslog: LOG_AUTH LOG_ALERT
> Change: output alert_syslog: LOG_AUTH LOG_ALERT[3]

However, by itself this is not sufficient. Snort was originally written to use the syslog daemon of a UNIX operating system. Windows 2000 Server comes with no such daemon. A syslog forwarder must be installed on the Windows' host to forward logs to a remote syslog server.

NTsyslog is a capable, freeware syslog client for Microsoft hosts. It acts as a syslog forwarder and can also be configured to forward all events in the Application, System, Security and other Windows' Event Logs to a syslog server. The software can be downloaded from:

http://sourceforge.net/projects/ntsyslog/

NTsyslog is very easy to install. Unzip the download into D:\. It will create a D:\ntsyslog-1.13 folder with all of the required software. Open a command window and change to this directory. Run the following command to install Ntsyslog as a service:

```
ntsyslog –install
```

Ntsyslog can be configured either with the NTSyslogCrtl.exe GUI tool located in the D:\ntsyslog-1.13 folder or by editing the Windows' registry. I find it easier to install with registry edits and use NTSyslogCrtl to only manage the service after the original installation. Ntsyslog.reg can be used as a template for a registry file. It is located in D:\ntsyslog-1.13\ntsyslog folder. Open it with a text editor and make the following alterations (replacing sss.sss.sss.sss with the IP address of the syslog server):

---

[3] Steele, p. 5.

```
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet]
"Syslog"="sss.sss.sss.sss"

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet\Syslog\System]
"Information"=dword:00000001
"Information Priority"=dword:0000000d
"Warning"=dword:00000001
"Warning Priority"=dword:0000000c
"Error"=dword:00000001
"Error Priority"=dword:00000009
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:0000000e
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:0000000b

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet\Syslog\Security]
"Information"=dword:00000001
"Information Priority"=dword:0000000d
"Warning"=dword:00000001
"Warning Priority"=dword:0000000c
"Error"=dword:00000001
"Error Priority"=dword:00000009
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:0000000e
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:0000000b

[HKEY_LOCAL_MACHINE\SOFTWARE\SaberNet\Syslog\Application]
"Information"=dword:00000001
"Information Priority"=dword:0000000d
"Warning"=dword:00000001
"Warning Priority"=dword:0000000c
"Error"=dword:00000001
"Error Priority"=dword:00000009
"Audit Success"=dword:00000001
"Audit Success Priority"=dword:0000000e
"Audit Failure"=dword:00000001
"Audit Failure Priority"=dword:0000000b
```

These settings forward all Windows' Event Logs to the syslog server using the "user" facility. Audit Success events are configured with "information" severity. Both Audit Failure and Information events have "notice" severity. Warning events carry "warning" severity. Error events are logged as "alert" severity.

Save and close the file, then double-click on it to install the changes in the Windows' registry. Open NTSyslogCrtl and use it to start the Ntsyslog service. All Snort alerts and Windows' Event Log entries will now be forwarded to the syslog server.

Finishing Up

Anti-virus software can be installed on the Snort sensor, but real-time protection should only be enabled when you are using the ACID console to research alerts on the Internet. Disable real-time protection for normal sensor use, it consumes too much processing power.

The Snort sensor is now ready for deployment. It is hardened against attack and will alert on any attempt to connect to the sensor. Reboot the computer to ensure that all of the security modifications take effect and connect the sensor to your production network. You now need to tune the sensor to protect your critical servers and to remove 'false positive' alerts.

Bibliography

Steele, Michael E. "Snort Installation Manual – Snort, MySQL, Acid & IIS – Windows NT4 Server, 2000, & XP (All Versions)." v1.2. March 5, 2003. URL: http://www.silicondefense.com/support/windows/winsnortdocs/WinSnortIIS.pdf (March 19, 2003)

Roesch, Martin and Green, Chris. "Snort Users Manual – Snort Release: 1.9.1." November 11, 2002. URL: http://www.snort.org/docs/SnortUsersManual.pdf (March 15, 2003)

Microsoft Corporation. "How to Add Custom Registry Settings to Security Configuration Editor." January 17, 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;214752 (March 7, 2003)

Riley, Steve. "Using IPSec to Lock Down a Server." v1.2. January 15, 2003. URL: http://www.microsoft.com/serviceproviders/columns/using_ipsec.asp (March 10, 2003)

Microsoft Corporation. "IPSec Does Not Secure Kerberos Traffic Between Domain Controllers." October 16, 2002. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;254728 (March 20, 2003)

"Ntsyslog – Windows NT/2000/XP syslog service." URL: http://ntsyslog.sourceforge.net (March 6, 2003)

"Update: Winpcap support on Multiprocessor (MP) Machines." URL: http://www.ntop.org/winpcap.html (March 12, 2003)

Microsoft Corporation. "IIS Lockdown Tool 2.1." URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=dde9efc0-bb30-47eb-9a61-fd755d23cdec&displaylang=en (March 20, 2003)

Microsoft Corporation. “ipsecpol.exe: IPSEC Policy Configuration Tool.” URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=7d40460c-a069-412e-a015-a2ab904b7361&DisplayLang=en (March 17, 2003)

Scambray, Joel and McClure, Stuart. Hacking Windows 2000 Exposed. Berkeley: Osborne / McGraw-Hill, 2001.

Goins, Bonnie, Witt, Benn and Wunsch, Michael. Hardening a Windows Host, Madison: Integrated Information Systems, 2002. 123 – 176.

Norberg, Stefan. Securing Windows NT/2000 Servers for the Internet. Sebastopol: O’Reilly & Associates, 2001.

Last Updated: June 21st, 2018

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Paris June 2018	Paris, FR	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Minneapolis 2018	Minneapolis, MNUS	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS Vancouver 2018	Vancouver, BCCA	Jun 25, 2018 - Jun 30, 2018	Live Event
SANS London July 2018	London, GB	Jul 02, 2018 - Jul 07, 2018	Live Event
SANS Cyber Defence Singapore 2018	Singapore, SG	Jul 09, 2018 - Jul 14, 2018	Live Event
SANS Charlotte 2018	Charlotte, NCUS	Jul 09, 2018 - Jul 14, 2018	Live Event
SANSFIRE 2018	Washington, DCUS	Jul 14, 2018 - Jul 21, 2018	Live Event
SANS Cyber Defence Bangalore 2018	Bangalore, IN	Jul 16, 2018 - Jul 28, 2018	Live Event
SANS Pen Test Berlin 2018	Berlin, DE	Jul 23, 2018 - Jul 28, 2018	Live Event
SANS Riyadh July 2018	Riyadh, SA	Jul 28, 2018 - Aug 02, 2018	Live Event
Security Operations Summit & Training 2018	New Orleans, LAUS	Jul 30, 2018 - Aug 06, 2018	Live Event
SANS Pittsburgh 2018	Pittsburgh, PAUS	Jul 30, 2018 - Aug 04, 2018	Live Event
SANS San Antonio 2018	San Antonio, TXUS	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS August Sydney 2018	Sydney, AU	Aug 06, 2018 - Aug 25, 2018	Live Event
SANS Boston Summer 2018	Boston, MAUS	Aug 06, 2018 - Aug 11, 2018	Live Event
Security Awareness Summit & Training 2018	Charleston, SCUS	Aug 06, 2018 - Aug 15, 2018	Live Event
SANS Hyderabad 2018	Hyderabad, IN	Aug 06, 2018 - Aug 11, 2018	Live Event
SANS New York City Summer 2018	New York City, NYUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Northern Virginia- Alexandria 2018	Alexandria, VAUS	Aug 13, 2018 - Aug 18, 2018	Live Event
SANS Krakow 2018	Krakow, PL	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Chicago 2018	Chicago, ILUS	Aug 20, 2018 - Aug 25, 2018	Live Event
Data Breach Summit & Training 2018	New York City, NYUS	Aug 20, 2018 - Aug 27, 2018	Live Event
SANS Prague 2018	Prague, CZ	Aug 20, 2018 - Aug 25, 2018	Live Event
SANS Virginia Beach 2018	Virginia Beach, VAUS	Aug 20, 2018 - Aug 31, 2018	Live Event
SANS San Francisco Summer 2018	San Francisco, CAUS	Aug 26, 2018 - Aug 31, 2018	Live Event
SANS Copenhagen August 2018	Copenhagen, DK	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS SEC504 @ Bangalore 2018	Bangalore, IN	Aug 27, 2018 - Sep 01, 2018	Live Event
SANS Wellington 2018	Wellington, NZ	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Amsterdam September 2018	Amsterdam, NL	Sep 03, 2018 - Sep 08, 2018	Live Event
SANS Tokyo Autumn 2018	Tokyo, JP	Sep 03, 2018 - Sep 15, 2018	Live Event
SANS Tampa-Clearwater 2018	Tampa, FLUS	Sep 04, 2018 - Sep 09, 2018	Live Event
SANS MGT516 Beta One 2018	Arlington, VAUS	Sep 04, 2018 - Sep 08, 2018	Live Event
SANS Cyber Defence Canberra 2018	OnlineAU	Jun 25, 2018 - Jul 07, 2018	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced