# *SECURE NETWORK MANAGEMENT IN A WINDOWS ENVIRONMENT*

*GSEC Practical Assignment*
*v1.4b Option 1*

Prepared by:

Steven Williams
4 December 2003

# *Contents Page*

## Abstract

This paper describes the secure implementation of some common network management concepts within a Windows environment. The intention is to provide guidance to staff that implement, manage and support network devices to practice secure methods and processes of network management. Applied successfully, this will reduce the risk of compromise to the corporate network, increase availability and reduce the time to diagnose and rectify issues.

## Introduction

The rapid growth of the internet has made available a vast wealth of information to the average person, however this has also seen a proportional growth of operating system and network device exploitations, denial of service (DOS) attacks, virus's / worms / Trojan's and even step by step guides to compromising or DOS hosts - complete with tools written to execute them.

IT staff have never been busier trying to protect IT assets from compromise or periods of non-scheduled unavailability. The increase of threats and their potential severity requires risk analysis and management, resulting in ever changing Standard Operating Environments (SOE) for device configurations, Anti Virus solutions, patch and hot fix deployment strategies and vast numbers of policies which staff struggle to adhere to.

Whilst risk analysis is conducted on our network devices (i.e. servers, routers, switches and firewalls) and services (i.e. LANs, WAN's, ISP's) to highlight points of failure, and service is improved by providing disaster recovery, high availability and implementing higher levels of support contracts etc, some organizations forget about reviewing how they manage the network.

For those who work exclusively in a Windows environment, secure network management can easily be achieved and this document briefly highlights key points in implementing some common and important features of secure network management.

## Requirements for Securing a Network

Several processes need to be implemented and maintained for effective and secure event monitoring in a network, comprising an effective event logging process, an effective time synchronisation process and an effective data collection process. Accurate and effective data gathering is only useful however, if the data can be managed easily and for this one needs an effective Network Management Service. Finally, considering the critical role of Network Management Services, it is critical to secure the services against attacks.

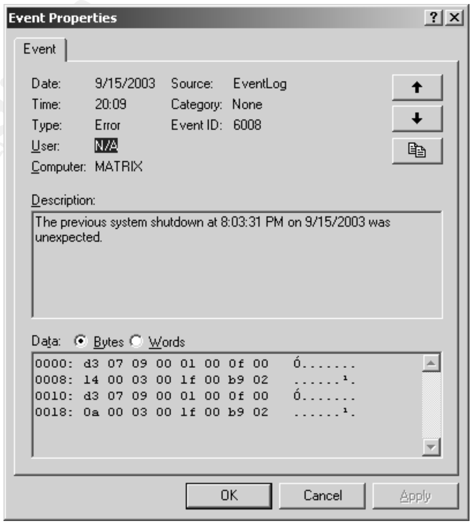
Each of these processes are explained further in the following sections.

### Event logging using SYSLOG

Log files provide administrators with the ability to record information that will assist in troubleshooting issues, log configuration changes and potentially indicate intrusions, probes and scans. As a result, logging is a very important part of network security.

On Windows platforms, there are three standard types of logs files called event logs. These are the System event log, the Application event log and the Security event log.

The System event log monitors various system events, the Application event log monitors application related events, and the Security event log monitors events such as logon, logoff, changes to access rights, and system start-up and shutdown.



Date: 9/15/2003 Source: EventLog
Time: 20:09 Category: None
Type: Error Event ID: 6008
User: N/A
Computer: MATRIX

Description:
The previous system shutdown at 8:03:31 PM on 9/15/2003 was unexpected.

Data: ● Bytes ○ Words

```
0000: d3 07 09 00 01 00 0f 00   Ó.......
0008: 14 00 03 00 1f 00 b9 02   ......¹.
0010: d3 07 09 00 01 00 0f 00   Ó.......
0018: 0a 00 03 00 1f 00 b9 02   ......¹.
```

*Figure 1. Example Microsoft Windows Event Properties Dialogue*

On a router, log files can log errors, changes in interface or routing protocol status, access list matches and configuration changes etc.

```
myrouter#sh log
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
Console logging: level critical, 0 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 123 message lines logged
Logging to 192.168.1.5, 123 message lines logged
Buffer logging: level debugging, 16 messages logged

Log Buffer (4096 bytes):

*Mar  5 12:40:15.202 UTC: %SEC-6-IPACCESSLOGDP: list Internet denied icmp 192.168.9.130
*Mar  5 12:40:15.385 UTC: %SEC-6-IPACCESSLOGDP: list Internet denied icmp 192.168.1.25
*Mar  5 12:40:15.647 UTC: %SEC-6-IPACCESSLOGDP: list Internet denied icmp 192.168.12.11
*Mar  5 12:40:15.841 UTC: %SEC-6-IPACCESSLOGP: list Internet denied udp 172.28.24.99 (137)
myrouter#
```

Reviewing individual device logs is time consuming and reviewing events across multiple devices can become inaccurate. A more efficient and effective way to handle log files is to use SYSLOG.

SYSLOG is the de-facto protocol for logging system events. It is an Internet protocol defined in RFC 3164 that allows a device to send notification messages over TCP/IP to a centralized server called a SYSLOG server using UDP 514 [1].

Applications such as Kiwi Syslog Daemon [2] can enable Windows servers or workstations to act as SYSLOG servers. Applications such as SNARE [3] allow Windows hosts to log event logs to a remote SYSLOG server.

Cisco devices support the SYSLOG protocol, which is easily implemented as shown below;

```
myrouter (config) # no logging buffered
myrouter (config) # logging console critical
myrouter (config) # logging facility local1
myrouter (config) # logging 192.168.1.5
```

Using a SYSLOG server allows centralized and consolidated collection of log files, implements log archiving, and can display, filter and forward messages based on various pattern matches such as time stamps and key words. With some time and effort, this can be turned into a form of Intrusion Detection.

Below is the SYSLOG output from a server and router exporting to SYSLOG that was scanned by NESSUS [4]. This clearly shows login attempts from illegitimate accounts on the server and RSHELL connection attempts to the router.

```
2003-09-21 07:57:51     Local7.Debug        SERVER     Sep 21 07:52:15 server.Home.local <009>Security<009>23849<009>Sun Sep 21
07:52:15 2003<009>529<00 9>Security<009>SYSTEM<009>User<009>Failure Audit<009>SERVER<009><009>  Logon Failure:    Reason: Unknown user
name or bad password    User Name: NULL    Domain: HOME     Logon Type: 2    Logon Process: IIS       Auth  entication Package:
MICROSOFT_AUTHE NTICATION_PACKAGE_V1_0    Workstation Name: SERVER

2003-09-21 07:58:27     Local7.Debug        SERVER     Sep 21 07:52:51 server.Home.local <009>Security<009>23853<009>Sun Sep 21
07:52:49 2003<009>529<009>Security<009>SYSTEM<009>User<009>Failure Audit<009>SERVER<009>    <009>Logon Failure:    Reason: Unknown user
name or bad password    User Name: BOGUS    Domain: HOME     Logon Type: 2    Logon Process: IIS       Authentication Package:
MICROSOFT_AUTHENTICATION_PACKAGE_V1_0    Workstation Name: SERVER

2003-09-21 07:58:27     Local7.Debug        SERVER     Sep 21 07:52:51  Server  MSWinEventLog<009>1<009>Security<009>23853<009>Sun
Sep 21 07:52:49 2003<009>529<009>Security<009>SYSTEM<009>User<009>Failure Audit<009>SERVER<009>Logon/Logoff  <009><009>    Logon
Failure:    Reason: Unk nown user name or bad password    User Name: BOGUS    Domain: HOME     Logon Type: 2    Logon Process: IIS
Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0    Workstation Name: SERVER

21-09-2003 11:43:21 Local1.Info 172.28.24.99  %SEC-6-IPACCESSLOGP:  list Internet denied tcp  192.168.1.1(35643) (Serial0.1 DLCI 500)  ->
172.28.24.99(23), 1 packet
```

```
21-09-2003 11:43:24 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied tcp 192.168.1.1(35699) (Serial0.1 DLCI 500) ->
172.28.24.99(79), 1 packet

21-09-2003 11:43:37 Local1.Warning 192.168.1.5 %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.1.1

21-09-2003 11:43:37 Local1.Warning 192.168.1.5 %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.1.1

21-09-2003 11:48:11 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied tcp 192.168.1.1(43657) (Serial0.1 DLCI 500) ->
172.28.24.99(23), 1 packet

21-09-2003 11:48:13 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied tcp 192.168.1.1(43713) (Serial0.1 DLCI 500) ->
172.28.24.99(79), 1 packet

21-09-2003 11:48:21 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied tcp 192.168.1.1(43875) (Serial0.1 DLCI 500) ->
172.28.24.99(79), 1 packet

21-09-2003 11:48:28 Local1.Warning 192.168.1.5 %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.1.1

21-09-2003 11:48:28 Local1.Warning 192.168.1.5 %RCMD-4-RSHPORTATTEMPT: Attempted to connect to RSHELL from 192.168.1.1

21-09-2003 11:49:27 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied tcp 192.168.1.1(46795) (Serial0.1 DLCI 500) ->
172.28.24.99(79), 1 packet

21-09-2003 11:49:58 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGDP: list Internet denied icmp 192.168.1.1 (Serial0.1 DLCI 500) -> 172.28.24.99 (8/0),
1 packet

21-09-2003 11:51:36 Local1.Info 192.168.1.5 %SEC-6-IPACCESSLOGP: list Internet denied udp 192.168.1.1(51792) (Serial0.1 DLCI 500) ->
172.28.24.99(161), 1 packet
```

*Figure 2. Server and Router SYSLOG messages*

Whilst the advantages of using SYSLOG are clear, the protocol itself is poorly implemented and suffers from some major problems;

- Being a UDP based protocol, there is no connection establishment or congestion control. This reduces network delay however there is no guarantee that the SYSLOG data will be delivered and therefore requires a reliable network. TCP is typically used for robust and reliable communications.
- It does not have any mechanisms for sending or receiving host authentication.
- It does not have any mechanisms for providing message integrity
- Data is transmitted in clear text.

```
2003-11-11 21:59:32     Local1.Warning      192.168.1.5 4923: *Apr 6 01:09:15.868 UTC: %RCMD -4-RSHPORTATTEMPT: Attempted to connect
to RSHELL from 192.168.1.106
```

*Figure 3. Network analyser summary decode of a SYSLOG message*

```
IP: ----- IP Header -----
    IP:
    IP: Version = 4, header length = 20 bytes
    IP: Type of service = 00
    IP:       000. ....   = routine
    IP:       ...0 .... = normal delay
    IP:       .... 0... = normal throughput
    IP:       .... .0..  = normal reliability
    IP:       .... ..0. = ECT bit  - transport protocol will ignore the CE bit
    IP:       .... ...0 = CE bit  - no congestion
    IP: Total length    = 138 bytes
    IP: Identification  = 4922
    IP: Flags           = 0X
    IP:       .0.. .... = may fragment
    IP:       ..0. .... = last fragment
    IP: Fragment offset = 0 bytes
    IP: Time to live    = 255 seconds/hops
    IP: Protocol        = 17 (UDP)
    IP: Header check sum = 246D (correct)
    IP: Source address      = [ 192.168.1.6], SERVER
    IP: Destination address = [192.168.1.5], MATRIX
    IP: No options
    IP:
UDP: ----- UDP Header -----
    UDP:
    UDP: Source port      =  7100
    UDP: Destination port =   514 (Syslog)
    UDP: Length           = 118
    UDP: Checksum         = 68BC (correct)
    UDP: [110 byte(s) of data]
    UDP:
```

```
UNK: ----- Unknown Protocol  -----
ADDR  HEX                                                        ASCII
0000: 00 00 f8 08 26 0a 00 d0 bb e0 b8 b6 08 00   45 00 | ..ø.&..Ð»à¸¶..E.
0010: 00 8a 13 3a 00 00 ff 11 24 6d c0 a8 01 66 c0 a8 | .Š.:..ÿ.$mÀ¨.fÀ¨
0020: 01 05 1b bc 02 02 00 76 68 bc 3c 31 34 30 3e 34 | ...¼...vh¼<140>4
0030: 39 32 33 3a 20 2a 41 70 72 20 20 36 20   30 31 3a | 923: *Apr  6 01:
0040: 30 39 3a 31 35 2e 38 36 38 20 55 54 43 3a 20 25 | 09:15.868 UTC: %
0050: 52 43 4d 44 2d 34 2d 52 53 48 50 4f 52 54 41 54 | RCMD  -4-RSHPORTAT
0060: 54 45 4d 50 54 3a 20 41 74 74 65 6d 70 74 65 64 | TEMPT: Attempted
0070: 20 74 6f 20 63 6f 6e 6e 65 63 74 20 74 6f 20 52 |  to connect to R
0080: 53 48 45 4c 4c 20 66 72 6f 6d 20 31 39 32 2e 31 | SHELL from 192.1
0090: 36 38 2e 31 2e 31 30 36                          | 68.1.106
```

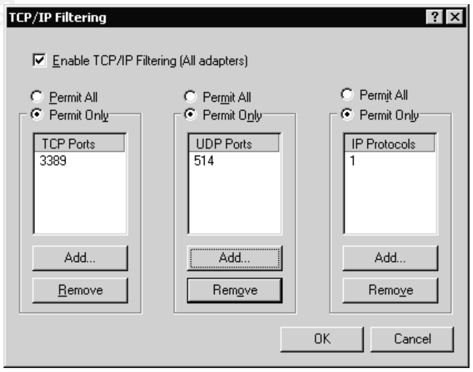
*Figure 4. Network analyser detailed decode of a plai n text SYSLOG message*

These problems expose the SYSLOG protocol, servers and hosts to the following vulnerabilities;

- Attackers may flood the server with messages with the intention of performing a Denial of Service by filling disk space or overwhelming the server. This can hide evidence of a security event amongst other events which could be false to mislead administrators.
- Source address's can be spoofed.
- Attackers could capture, view, modify and retransmit messages to modify event times, insert false events, view the status of applications and devices or hide activities.
- Attackers could send invalid messages to network devices SYSLOG ports exploiting known vendor vulnerabilities and performing a Denial of Service by crashing the device.

These problems could be resolved by;

- Encrypting network traffic via SSL or IPSEC
- Implement message authentication
- Monitor and alert on disk space utilisation
- Use file encryption
- Use TCP/IP Filtering on the SYSLOG server to authorise message source IP address's



TCP/IP Filtering

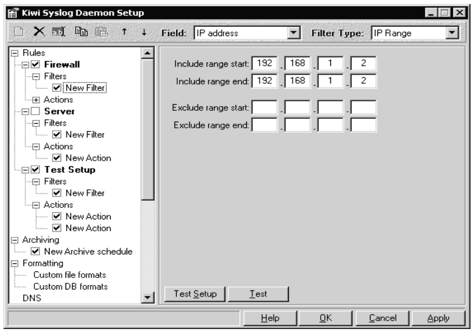
☑ Enable TCP/IP Filtering (All adapters)

○ Permit All ● Permit Only — TCP Ports: 3389

○ Permit All ● Permit Only — UDP Ports: 514

○ Permit All ● Permit Only — IP Protocols: 1

*Figure 5. W2K Network Interface TCP/ IP Filtering allowing RDP, SYSLOG and ICMP*



Field: IP address
Filter Type: IP Range

Include range start: 192 . 168 . 1 . 2
Include range end: 192 . 168 . 1 . 2

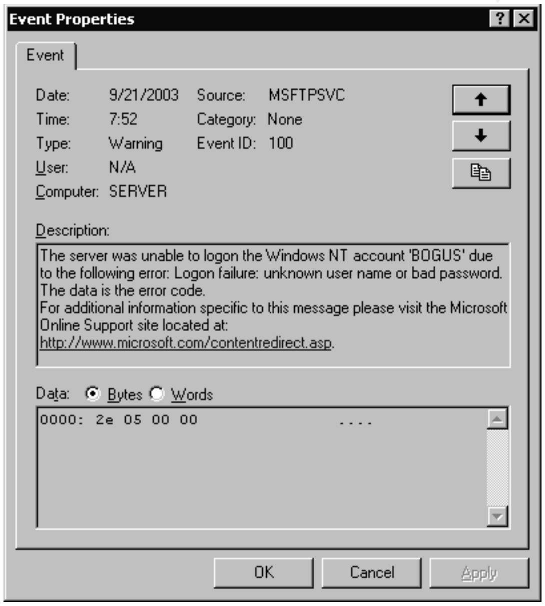
Exclude range start: . . .
Exclude range end: . . .

*Figure 6. Kiwi Syslog Daemon IP address filtering*

## *Time Synchronisation using NTP*

The ability to successfully audit a network can depend on the accuracy of the time stamps applied to the various device log entries. Most network devices have the ability to set the date and time however these can drift apart from each other and lose accuracy over time. Manually adjusting the clocks is a time consuming and unreliable method of maintaining time synchronization.

Take a look at the following logs from a server and router. These events are generated from a single NESSUS scan across both hosts within a few minutes of each other however inaccurate timestamps on the logs don't indicate this.



Date: 9/21/2003 Source: MSFTPSVC
Time: 7:52 Category: None
Type: Warning Event ID: 100
User: N/A
Computer: SERVER

Description:
The server was unable to logon the Windows NT account 'BOGUS' due to the following error: Logon failure: unknown user name or bad password. The data is the error code.
For additional information specific to this message please visit the Microsoft Online Support site located at: http://www.microsoft.com/contentredirect.asp.

Data: ● Bytes ○ Words

```
0000: 2e 05 00 00          ....
```

```
myrouter#sh log
Syslog logging: enabled (0 messages dropped, 0 flushes, 0
overruns)
Console logging: level critical, 0 messages logged
Monitor logging: level debugging, 0 messages logged
Trap logging: level informational, 123 message lines logged
Logg ing to 192.168.1.5, 123 message lines logged
Buffer logging: level debugging, 16 messages logged

Log Buffer (4096 bytes):

*Mar  5 12:40:15.202 UTC:  %SEC-6-IPACCESSLOGP: list Internet
denied tcp  172.28.24.99(35643) (Serial0.1 DLCI 500)  ->
192.168.1.254 (23)
*Mar  5 12:40:15.385 UTC:  %SEC-6-IPACCESSLOGP: list Internet
denied tcp  172.28.24.99(35699) (Serial0.1 DLCI 500)  ->
192.168.1.254 (79)
*Mar  5 12:40:15.647 UTC:  %SEC-6-IPACCESSLOGP: list Internet
denied udp  172.28.24.99 (51792) (Serial0.1 DLCI 500)  ->
192.168.1.254 (161)
*Mar  5 12:40:15.841 UTC:  %SEC-6-IPACCESSLOGP: list Internet
denied udp  172.28.24.99 (51942) (Serial0.1 DLCI 500)  ->
192.168.1.254 (69)
*Mar  5 12:40:16.151 UTC: %RCMD -4-RSHPORTATTEMPT:
Attempted to conn ect to RSHELL from  172.28.24.99
myrouter#
```

*Figure 7. Example Event Log entry with corresponding Router log alongside*

Note the server timestamp was 07:52 21st of Sept, whilst the router was 12:40 5th of March. If time was synchronized on both of these hosts, this would have clearly highlighted to the administrator that source address 172.28.24.99 had attempted connections to the router and most likely the server. This information could then be used to audit firewall and IDS logs for further information.

Most network devices today support Network Time Protocol (NTP) which is a protocol designed to automatically distribute and maintain time synchronization.

NTP is a TCP/IP protocol specified in RFC 1305 which synchronizes time on hosts and devices using UDP port 123. Devices are typically synchronized to a reference source such as an atomic clock provided via satellite / GPS, Radio or the Internet [5]. Public servers are provided by Universities and Government Research facilities via the Internet.

The Simple Network Time Protocol (SNTP) is a simplified version of NTP specified in RFC 1769. This version is less complex and accurate however it can maintain accuracy to within milliseconds. The two versions are interoperable [6].

Time synchronization is important within a Windows 2000 environment because Windows 2000 uses Kerberos V5 as the primary authentication protocol for users and hosts within a domain. Kerberos V5 is defined in RFC 1510, and requires time synchronization because time stamping is a critical part of the authentication process [7]. Time synchronization is also important for event log file analysis and performance monitoring.

A domain’s time synchronization can be achieved by configuring an authoritative time server on the Domain controllers using the following command.

```
C:\>net time ?
The syntax of this command is:

NET TIME
[\\computername | /DOMAIN[:domainname] | /RTSDOMAIN[:domainname]] [/SET]
        [\\computername] /QUERYSNTP
        [\\computername] /SETSNTP[:ntp server list]

C:\>net time /setsntp:192.168.1.5,192.168.1.6
The command completed successfully.
```

Member servers or workstations follow the Active Directory hierarchy and synchronise their time against the Domain controller during startup, and some companies include the NET TIME command within logon scripts to update time with every user login.

Time synchronization is also important to other network devices such as routers, switches and firewalls for log file analysis in troubleshooting, incident analysis or debugging.

Cisco routers can form two types of NTP associations, being peer (this device is able to synchronize to other hosts or allow other devices to synchronize from it) or server (this device is only able to synchronize to the NTP server)

[8]. This is done by sending broadcast packets or listening to them on a specific interface.

```
myrouter (config) # clock timezone PST -8
myrouter (config) # clock summer-time PDT recurring
myrouter (config) # ntp update-calendar
myrouter (config) # ntp peer 192.168.1.5
myrouter (config) # ntp peer 192.168.1.6
myrouter (config) # interface Ethernet 0/0
myrouter (config-if) # ntp broadcast
```

NTP operation can be confirmed by showing the NTP associations and NTP status.

```
myrouter#sh ntp assoc

    address        ref clock     st  when  poll reach  delay  offset    dis  p
 ~192.168.1.5    192.168.4.3      14    13    64  377     2.0  130.50   122.0
*~192.168.1.6     172.28.47.37     2     0    64  100     3.4   19.03  16000.
 * master (synced), # master (unsynced), + selected,  - candidate, ~ configured


myrouter#sh ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 249.5901 Hz, actual freq is 249.5811 Hz, precision is 2**18
reference time is C309850F.4DBE6DE0 (21:10:07.303 EST Wed Sep 10 2003)
clock offset is 19.0339 msec, root delay is 3.4 3 msec
root dispersion is 16230.12 msec, peer dispersion is 15958.60 msec
```

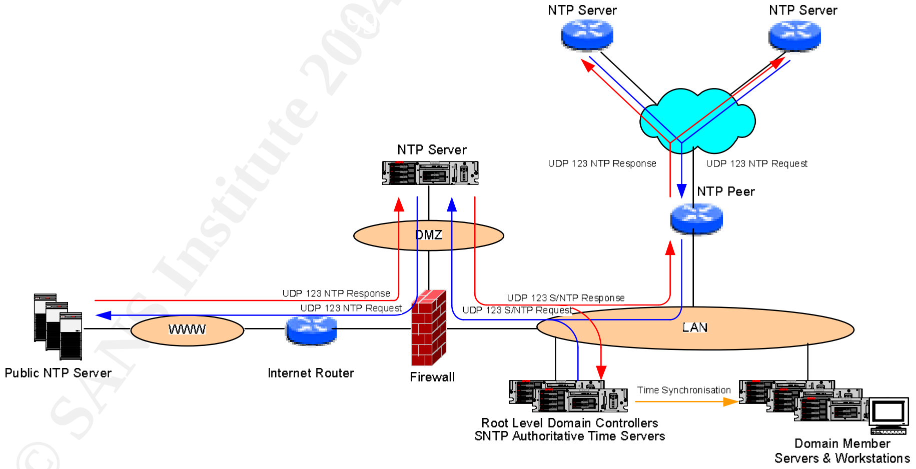


*Figure 8. NTP traffic flows*

NTP as a protocol is poorly implemented and suffers from some major problems;

- Being a UDP based protocol, there is no connection establishment or congestion control. This reduces network delay however there is no guarantee that the NTP data will be delivered and therefore requires a reliable network. TCP is typically used for robust and reliable communications.
- It does not have any mechanisms for sending or receiving host authentication.
- It does not have any mechanisms for providing message integrity
- Data is transmitted in clear text

```
          Frame Status Source                 Destination             Byte   s Rel Time     Delta Time   Abs time            Summary
 ----------------------------------------------------------------------------------------------------------------------------------------------------
 348      [1 92.168.1.101]          [1 72.28.24.99]           90 0:00:21.910  0.010.189    11/11/2003 10:56:59 PM NTP/SNTP: V  ersion 2
 349      [172.28.24.99 ]           [192 .168.1.101]          90 0:00:21.985  0.074.451    11/11/2003 10:57:00 PM NTP/SNTP: V  ersion 2
```

*Figure 9. Network analyser summary decode of NTP messages*

```
UDP: ----- UDP Header  -----
    UDP:
    UDP: Source port      =   123 (NTP)
    UDP: Destination port =  1641
    UDP: Length           = 56
    UDP: Checksum         = 3AD3 (correct)
    UDP: [48  byte(s) of data]
    UDP:
NTP: ----- NTP/SNTP header  -----
    NTP:
    NTP: LI, VN, Mode:       = 14
    NTP:          00.. .... = Lea  p Indicator 0(no warning)
    NTP:          ..01 0... = Version Number 2
    NTP:          ... .. .100 = Mode 4(server)
    NTP: Stratum           = 2 (secondary reference (via NTP))
    NTP: Poll              = 11 (2048 seconds)
    NTP: Precision         =  -17 (2** -17 seconds)
    NTP: Root Delay        = 0.021453857421875 seconds
    NTP: Root Dispersion   = 0.03009033203125 seconds
    NTP: Reference Clock ID  = [130.155.101.122]
    NTP: Reference Timestamp = Tue Nov 11 11:47:33 2003
    NTP:   Fraction        = 0.02796506096922057952880859375
    NTP: Originate Tim esta mp = Tue Nov 11 11:55:57 2003
    NTP:   Fraction        = 0.52  100061033795321018829345703125
    NTP: Receive Timestamp   = Tue Nov 11 11:55:57 2003
    NTP:   Fraction        = 0.55  763912318664523608245849609375
    NTP: Transmit Timestam p  = Tue Nov 11  11:55:57 2003
    NTP:   Fraction        = 0.55  765023275985716282501220703125
    NTP:
    NTP: [Normal end of "NTP  /SNTP header".]
    NTP:
```

*Figure 10. Network analyser detailed decode of a NTP message*

The NTP protocol, servers and hosts are exposed to the following vulnerabilities;

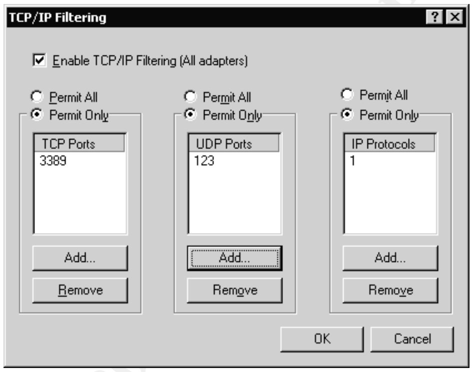
- Attackers may flood the server with messages with the intention of performing a Denial of Service producing excessive time resynchronisation traffic.
- Specially crafted poison or malformed NTP packets can crash NTP services or exploit vulnerabilities in the vendors implementation.
- Source address’s can be spoofed.

These problems could be resolved by;

- Encrypting network traffic via SSL or IPSEC.
- Use access-lists on servers and routers to authorise sending and receiving IP addresses.
- Prevent using public internet servers by obtaining GPS or Satellite based time services.
- Patch or upgrade vendors operating systems / firmware

```
myrouter (config) # access-list 99 permit host 192.168.1.5
myrouter (config) # access-list 99 permit host 192.168.1.6
myrouter (config) # access-list 99 deny any
myrouter (config) # ntp access-group peer 21
```

*Figure 11. Cisco NTP Peer Access List*



TCP/IP Filtering

☑ Enable TCP/IP Filtering (All adapters)

| ○ Permit All<br>● Permit Only | ○ Permit All<br>● Permit Only | ○ Permit All<br>● Permit Only |
|---|---|---|
| TCP Ports | UDP Ports | IP Protocols |
| 3389 | 123 | 1 |

*Figure 12. W2K Network Interface TCP/IP Filtering*

## *Network Management using SNMP*

Simple Network Management Protocol (SNMP) is a TCP/IP protocol specified in RFC 1157 which provides a connection between a “manager” and a managed host called an “agent” via UDP 161. It also supports another TCP/IP protocol called SNMP Trap, specified in RFC 1215, which allows an agent to send alert messages to the SNMP Management Station indicating various conditions via UDP 161.

The agent maintains a hierarchical structure or database of every bit of data, called objects, which are made available to the manager. This structure is called the Management Information Base (MIB) objects within which are referenced by an object identifier (OID).

Typical SNMP management applications include HP Openview Network Node Manager and Whatsup Gold. There are also great freeware tools such as Getif [9] for viewing and graphing MIB information and MRTG [10] for graphing counter type data.

SNMP on a Windows server is configured and run as a service. This allows the administrator to define contact and location information, as well as SNMP trap destination hosts and the community string. Microsoft's implementation of SNMP wasn't implemented very well, however third party add-ons such as SNMP4W2K [11] increase the number of available performance counters.

Typical information obtained from Microsoft servers can include Percentage CPU Utilization, Available Disk Space and application specific information from applications such as ISA, Exchange and IIS.

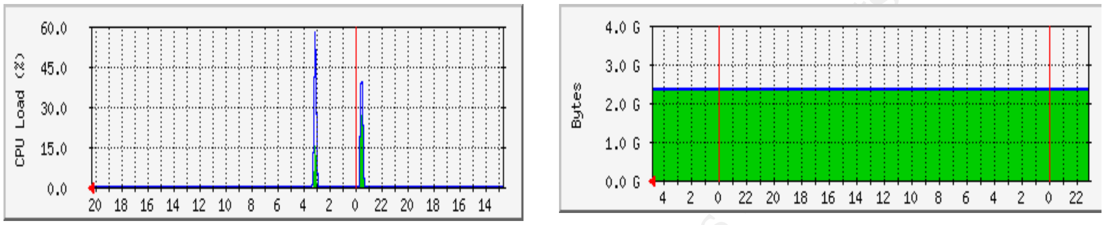
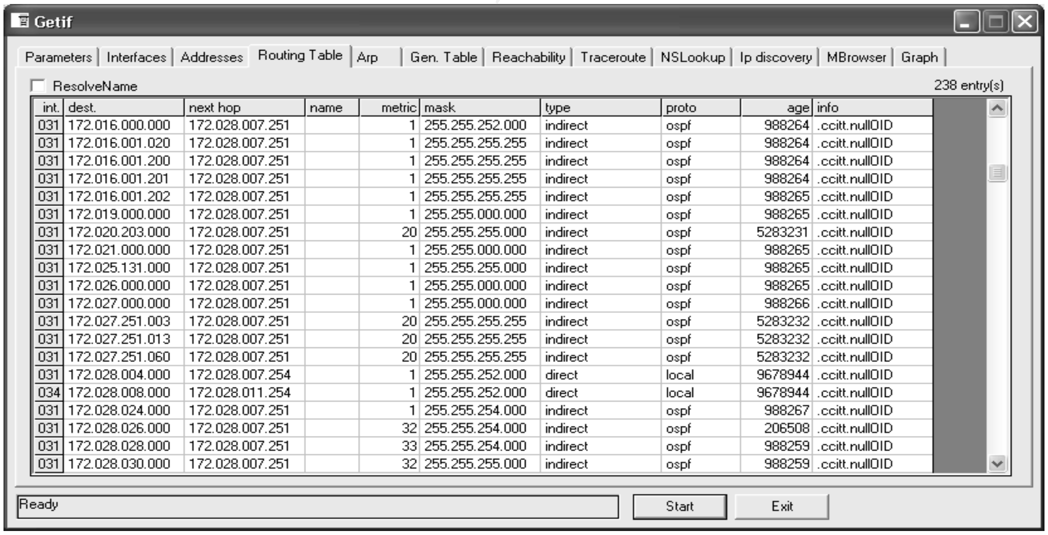


*Figure 13: Graphic representation of SNMP output for CPU Utilisation and Disk Space*

Network devices such as Cisco routers provide detailed information such as route tables, configurations and traffic utilization via SNMP, as well as providing an ability to remotely manage the device with Read Write (RW) strings. Using specific sequences of SNMP Gets and Sets, administrators can perform tasks such as automating configuration backups remotely via TFTP or obtain latency between routers using the Cisco Ping MIB.



□ ResolveName

238 entry(s)

| int. | dest. | next hop | name | metric | mask | type | proto | age | info |
|---|---|---|---|---|---|---|---|---|---|
| 031 | 172.016.000.000 | 172.028.007.251 | | 1 | 255.255.252.000 | indirect | ospf | 988264 | .ccitt.nullOID |
| 031 | 172.016.001.020 | 172.028.007.251 | | 1 | 255.255.255.255 | indirect | ospf | 988264 | .ccitt.nullOID |
| 031 | 172.016.001.200 | 172.028.007.251 | | 1 | 255.255.255.255 | indirect | ospf | 988264 | .ccitt.nullOID |
| 031 | 172.016.001.201 | 172.028.007.251 | | 1 | 255.255.255.255 | indirect | ospf | 988264 | .ccitt.nullOID |
| 031 | 172.016.001.202 | 172.028.007.251 | | 1 | 255.255.255.255 | indirect | ospf | 988265 | .ccitt.nullOID |
| 031 | 172.019.000.000 | 172.028.007.251 | | 1 | 255.255.000.000 | indirect | ospf | 988265 | .ccitt.nullOID |
| 031 | 172.020.203.000 | 172.028.007.251 | | 20 | 255.255.255.000 | indirect | ospf | 5283231 | .ccitt.nullOID |
| 031 | 172.021.000.000 | 172.028.007.251 | | 1 | 255.255.000.000 | indirect | ospf | 988265 | .ccitt.nullOID |
| 031 | 172.025.131.000 | 172.028.007.251 | | 1 | 255.255.255.000 | indirect | ospf | 988265 | .ccitt.nullOID |
| 031 | 172.026.000.000 | 172.028.007.251 | | 1 | 255.255.000.000 | indirect | ospf | 988265 | .ccitt.nullOID |
| 031 | 172.027.000.000 | 172.028.007.251 | | 1 | 255.255.000.000 | indirect | ospf | 988266 | .ccitt.nullOID |
| 031 | 172.027.251.003 | 172.028.007.251 | | 20 | 255.255.255.255 | indirect | ospf | 5283232 | .ccitt.nullOID |
| 031 | 172.027.251.013 | 172.028.007.251 | | 20 | 255.255.255.255 | indirect | ospf | 5283232 | .ccitt.nullOID |
| 031 | 172.027.251.060 | 172.028.007.251 | | 20 | 255.255.255.255 | indirect | ospf | 5283232 | .ccitt.nullOID |
| 031 | 172.028.004.000 | 172.028.007.254 | | 1 | 255.255.252.000 | direct | local | 9678944 | .ccitt.nullOID |
| 034 | 172.028.008.000 | 172.028.011.254 | | 1 | 255.255.252.000 | direct | local | 9678944 | .ccitt.nullOID |
| 031 | 172.028.024.000 | 172.028.007.251 | | 1 | 255.255.254.000 | indirect | ospf | 988267 | .ccitt.nullOID |
| 031 | 172.028.026.000 | 172.028.007.251 | | 32 | 255.255.254.000 | indirect | ospf | 206508 | .ccitt.nullOID |
| 031 | 172.028.028.000 | 172.028.007.251 | | 33 | 255.255.254.000 | indirect | ospf | 988259 | .ccitt.nullOID |
| 031 | 172.028.030.000 | 172.028.007.251 | | 32 | 255.255.255.000 | indirect | ospf | 988259 | .ccitt.nullOID |

Ready

*Figure 14: Getif dialogue showing routing table entries*

SNMPV1 and V2 are still widely used by agents, vendors and management applications however this suffers from some major problems;

- Being a UDP based protocol, there is no connection establishment or congestion control. This reduces network delay however there is no guarantee that the SNMP data will be delivered and therefore requires a reliable network. TCP is typically used for robust and reliable communications.
- It poorly implements mechanisms for sending or receiving host authentication using clear text community strings
- It does not have any mechanisms for providing message integrity
- Data is transmitted in clear text
- Most vendors implement a default read only and read write community string unique to the vendor ie “cisco”, or use “public / private”.

```
Frame Status Source                 Destination             Byte  s Rel Time Delta Time   Abs time            Summary
------------------------------------------------------------------------------------------------------------------------------------------------------------------    --------
   348    [192.168.1 .101]           [192.168.1.254 ]              90 0:00:21.910  0.010.189    11/11/20 03 10:56:59 PM SNMP  GetNext  sysDescr
  349     [192.168.1.254 ]              [192 .168.1.101]             90 0:00:21.985  0.074.451    11/11/2003 10:57:00 PM  SNMP  GetReply sysDescr = Cisco Internetwork
                                                     Operating System Software <0D0A>IOS (tm) 1600 Software (C1600  -Y-L), Ve
```

*Figure 15. Network analyser summary decode of SNMP  messages*

```
UDP:  ----- UDP Header  -----
     UDP:
     UDP: Source port      =   161 (SNMP)
     UDP: Destination port =  2003
     UDP: Length           = 268
     UDP: Checksum         = 4397 (correct)
     UDP: [260 byte(s) of data]
     UDP:
SNMP: ----- Simple Network Management Protocol (Version 1  ) -----
     SNMP:
     SNMP: SNMP Version = 1
     SNMP: Community    = public
     SNMP: Command      = Get response
     SNMP: Request ID   = 7164
     SNMP: Error status = 0 (No error)
     SNMP: Error index  = 0
     SNMP:
     SNMP: Object  = {1.3.6.1.2.1.1.1.0} (sys  Descr.0)
     SNMP: Value   = Cisco Internetwork Operating System Software <0D0A>I  OS (tm)  1600 Software (C1600 -Y-L), Version 11.3(11a), RELEASE
SOFTWARE (fc1)<0D0A>Copyright (c) 1986  -1999 by cisco Syst ems, Inc.<0D0A>Compiled Mon  20-Sep-99 09:46 by jjgreen
     SNMP:
ADDR  HEX                                          ASCII
0000: 00 00 f8 1a 1e a6 00 d0 bb e0 b8 b6 08 00   45 00 | ..ø..¦.Ð»à¸¶..E.
0010: 01 20 00 26 00 00 ff 11 36 87 c0 a8 01 66 c0 a8 | . .&..ÿ.6‡À¨.fÀ¨
0020: 01  69 00 a1 07 d3 01 0c 43 97 30 82 01 00 02 01 | .i.¡.Ó..C  —0‚....
0030: 00 04 06 70 75 62 6c 69 63 a2 81 f2 02 02 1b fc | ...public¢    ò...ü
0040: 02 01 00 02 01 00 30 81 e5 30 81 e2 06 08 2b 06 | ......0    å0   â..+.
0050: 01 02 01 01 01 00 04 81 d5 43 69 73 63   6f 20 49 | .......   ÕCisco I
0060: 6e 74 65 72 6e 65 74 77 6f 72 6b 20 4f 70 65 72 | nternetwork Oper
0070: 61 74 69 6e 67 20 53 79 73 74 65 6d 20 53 6f 66 | ating System Sof
0080: 74 77 61 72 65 20 0d 0a 49 4f 53 20 28 74 6d 29 | tware ..IOS (tm)
0090: 20 31 36 30 30 20 53 6f 66 74 77 61 72 65 20 28 |  1600 Software (
00a0: 43 31 36 30 30 2d 59 2d 4c 29 2c 20 56 65 72 73 | C1600  -Y-L), Vers
00b0: 69 6f 6e 20 31 31 2e 33 28 31 31 61 29 2c 20 52 | ion 11.3(11a), R
00c0: 45 4c 45 41 53 45 20 53 4f 46 54 57 41 5  2 45 20 | ELEASE SOFTWARE
00d0: 28 66 63 31 29 0d 0a 43 6f 70 79 72 69 67 68 74 | (fc1)..Copyright
00e0: 20 28 63 29 20 31 39 38 36 2d 31 39 39 39 20 62 |  (c) 1986  -1999 b
00f0: 79 20 63 69 73 63 6f 20 53 79 73 74 65 6d 73 2c | y cisco Systems,
0100: 20 49 6e 63 2e 0d 0a 43 6f 6d 70 69 6c 65 64 20 |  Inc...Compiled
0110: 4d 6f 6e 20 32 30 2d 53 65 70 2d 39 39 20 30 39 | Mon 20   -Sep-99 09
0120: 3a 34 36 20 62 79 20 6a 6a 67 72 65 65 6e       | :46 by jjgreen
```

*Figure 16. Network analyser summary decode of S NMP messages*

The SNMP protocol, servers and hosts are exposed to the following vulnerabilities;

- Eavesdropping via network analysis tools and compromise via brute force or dictionary attacks
- Specially crafted poison or malformed SNMP packets can crash SNMP services or exploit vulnerabilities in the vendors implementation.
- Source address's can be spoofed.

These problems could be resolved by;

- Encrypting network traffic via SSL or IPSEC.
- Use access-lists on servers and routers to authorise sending and receiving IP addresses.
- implement SNMPv3
- Patch or upgrade vendors operating systems / firmware
- Change vendor default community strings to strong passwords and change regularly.

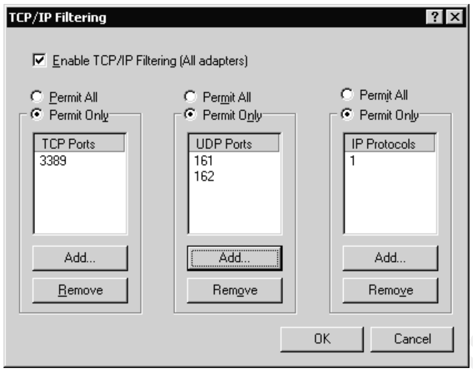
SNMP is unique as compared to SYSLOG and NTP as the protocol has evolved and recently addressed some security issues. SNMPV3 has been recently released but not yet widespread which supports MD5 or SHA authentication and uses DES encryption.

On Cisco routers, access-lists can be used to restrict SNMP requests to only the Network Management station.

```
myrouter# config t
Enter configuration command, one per line. End with CNTL/Z
myrouter (config) # access-list 20 permit 192.168.1.5
myrouter (config) # access-list 20 permit 192.168.1.6
myrouter (config) # access-list 20 deny any log
myrouter (config) # no snmp-server community public ro
myrouter (config) # no snmp-server community public rw
myrouter (config) # snmp-server community MyCoMmUnItYsTrInGrO ro  20
myrouter (config) # snmp-server community MyCoMmUnItYsTrInGrW rw  20
myrouter (config) # exit
```

```
myrouter#sh snmp
Chassis: 13930226
0 SNMP packets input
   0 Bad SNMP version errors
   0 Unknown community name
   0 Illegal operation for community name supplied
   0 Encoding errors
   0 Number of requested variables
   0 Number of altered variables
   0 Get-request PDUs
   0 Get-next PDUs
   0 Set-request PDUs
0 SNMP packets output
   0 Too big errors (Maximum packet size 1500)
   0 No such name errors
   0 Bad values errors
```

```
0 General errors
0 Get-response PDUs
0 SNMP trap PDUs
```


TCP/IP Filtering

☑ Enable TCP/IP Filtering (All adapters)

○ Permit All
● Permit Only
TCP Ports
3389

○ Permit All
● Permit Only
UDP Ports
161
162

○ Permit All
● Permit Only
IP Protocols
1

*Figure 12. W2K Network Interface TCP/IP Filtering*

## *IPSEC*

The use of IPSEC between a Windows 2000 Host server and Management Server overcomes many of the vulnerabilities previously discussed with SYSLOG, NTP and SNMP. IPSEC provides authentication by the use of Digital Certificates or Pre-shared keys, and also provides encryption of data in transit. Other traffic such as remote management, ie Terminal Services via RDP or telnet can also be protected. This is done by creating protocol and source / destination IP address based filters for the hosts of interest.

Because IPSEC is a group of standards based protocols for securing packet transportation within IP, it is possible to tunnel network management traffic between a Windows 2000 Server and Cisco devices if using the correct IOS versions and meet the hardware requirements for these versions.

It is outside the scope of this document to discuss the implementation of IPSEC on W2K Servers and Cisco devices, however further information can be obtained from the following sources;

IPSEC between two W2K hosts
http://www.microsoft.com/windows2000/techinfo/planning/security/ipsecsteps.asp

IPSEC between a W2K host and Cisco Device
http://www.cisco.com/warp/public/707/2000.html#cfg_3640
http://nsa2.www.conxion.com/cisc o/guides/cis-2.pdf

## *Secure NMS Configuration*

The network management server is the server that hosts the network management applications. These applications vary in role from monitoring and alerting, collecting SYSLOG's and traffic statistics or could act as the central IDS server.

The NMS itself is typically deployed as an authorized host able to connect to devices and collect information. As a result, these servers should be hardened to prevent compromise or exposure to known vulnerabilities.

Microsoft has made available details for implementing and securing its server range, however the NSA has produced Security Recommendation Guides [12] which are very thorough and are considered independent of Microsoft. If your company doesn't have a policy on building and securing these devices, this site provides more than enough information to implement and maintain a reasonably secure server or workstation. The NSA also provides example security policies via .INF files ready to import into and apply to the server.

Microsoft also has provided tools such as the Microsoft Baseline Analyser which identifies basic configuration errors and missing security updates and Windows Update service or Software Update Services to identify and update missing security hotfixes.

## *Conclusion*

There are many other network management features that could have been discussed in this document, however in my experience, SYSLOG, NTP and SNMP are the three most commonly used.

Implementing the use of these securely is a good first step, however these tools do not replace the necessity for maintaining other security concepts such as implementing and maintaining strict security policies, regularly auditing all aspects of the network, strict authentication policies, employing effective encryption techniques and establishing a well devised and documented intrusion detection system. Only by means of a combination of tools and procedures will your overall network security be effectively maintained.

Network management applications and servers are attractive to attackers as they can remove or mask evidence of intrusion, obtain system and network information, perform Denial of services or possibly obtain access to network hosts.

Unix and Linux based systems have typically led the way in securing network management communications via SSH, and are usually the first to implement improvements to network management applications, such as the SDSC Secure Syslog project.

However, this document has explained issues and provided solutions showing that Windows based secure network management can be implemented and provide a very secure network management infrastructure.

## *References*

1. The Internet Engineering Task Force RFC 3164 Syslog
   URL: http://www.ietf.org/rfc/rfc3164.txt (Aug 2001)
2. Kiwi Syslog Daemon
   URL: http://www.kiwisyslog.com (23 Sept 2003)
3. SNARE
   URL: www.intersectalliance.com (23 Sept 2003)
4. NESSUS
   URL: http://www.nessus.org/ (2 Feb 2003)
5. Understanding and using the Network Time Protocol URL:
   URL: http://www.ntp.org/ntpfaq/NTP-s-def.htm  (17 July 2003)
6. The Internet Engineering Task Force RFC 1769 SNTP
   URL: http://www.ietf.org/rfc/rfc1769.txt
7. Microsoft, “The Windows Time Service”,
   URL: http://www.microsoft.com/windows2000/docs/wintimeserv.doc
   (6 March 2003)
8. Cisco CCO, ”Performing Basic System Management”
   URL:http://www.cisco.com/en/US/partner/products/sw/iosswrel/ps1831/products_configuration_guide_chapter09186a00800ca66f.html#1001395 (10 Sept 2003) (Requires CCO access)
9. SNMP4tPC, “GETIF”
   URL: http://www.wtcs.org/snmp4tpc/getif.htm  (18 Sept 2003)
10. MRTG Homepage, “MRTG:
    URL http://people.ee.ethz.ch/~oetiker/webtools/mrtg/ (Sept 2003)
11. SNMP4tPC, “SNMP4W2k”
    URL: http://www.wtcs.org/snmp4tpc/implemen.htm (18 Sept 2003)
12. NSA, ”Security Recommendation Guides”
    URL: http://nsa2.www.conxion.com/win2k/ (24 Oct 2001)