Interested in learning more about security?

SANS Institute InfoSec Reading Room

Intrusion Detection with MOM - Going Above the Wire

There are several areas, or layers, where intrusions into a system can occur. At the "wire" or network layer, there are several tools that can successfully discern the nature of traffic for most commercial protocols. But how do you respond to the challenge of knowing what happens when you need to analyze "above the wire", at the operating system and application layers? What about when traffic is properly formed and does not trigger IDS rules? By focusing on the WAN/LAN layer traffic and looking for "exception traffic" ...

Assignment One: Intrusion Detection with MOM - Going Above the Wire

By Don Murdoch – June 11th 2003

Introduction

There are several areas, or layers, where intrusions into a system can occur. At the "wire" or network layer, there are several tools that can successfully discern the nature of traffic for most commercial protocols. But how do you respond to the challenge of knowing what happens when you need to analyze "above the wire", at the operating system and application layers? What about when traffic is properly formed and does not trigger IDS rules? By focusing on the WAN/LAN layer traffic and looking for "exception traffic" – signatures within packets that are indicative of malicious intent - properly formed, legal traffic is virtually ignored. With attackers getting more sophisticated, the analyst needs to respond with tools that can be used above the wire at the application and operating system level.

In this paper, Microsoft Operations Manager 2000 (hence, MOM) will be discussed as a tool to aid the analyst in understanding what occurs within the operating system and the application level.

Recent Statistics

Over the past several years, a variety of studies have revealed that while attacks from outside an organization have increased, greater financial loss has occurred from deliberate actions by staff within an organization. Some studies conducted during 2001 indicated that as much as 80% of the identified financial loss is from insiders, not outsiders[1], while others clearly indicate that their Internet connection is responsible for 2/3 of attacks[2]. Unauthorized insider access has varied between 15% and 25% over 1997 to 2002, with losses ranging from a low of $1000 to $50M for the same period[3]. These statistics emphasize the point that an organization needs to look both within and without for intrusions, anomalies, and violations of computer usage policy.

Introducing Microsoft Operations Manager 2000

Microsoft Operations Manager 2000 (hence MOM[4]) is Microsoft's solution for event management, centralized reporting, and automated event response for the Windows NT/2000/2003 operating system and most of Microsoft's BackOffice product line. There are many capabilities of MOM that are beyond the scope of this paper; emphasis here is on features that aid and assist the intrusion analyst in identification and examination of Events Of Interest (EOI) particular to the Windows environment.

---

[1] Source URL: http://www.all.net/journal/netsec/2001-05.html

[2] Source URL: http://www.gocsi.com/press/20020407.html

[3] Computer Security Institute. "2002 Computer Security Institute/FBI Computer Crime & Security Survey", p. 10. URL: http://www.gocsi.com/press/20020407.html

[4] MOM2000, for the purposes of this paper, is running on Windows 2000 Service Pack 3, with Active Directory. MOM's features URL: http://www.microsoft.com/mom/evaluation/features/default.asp

MOM Architecture

The major components of MOM reside in one of three tiers (following Microsoft's three tier component architecture model) as illustrated in the figure.

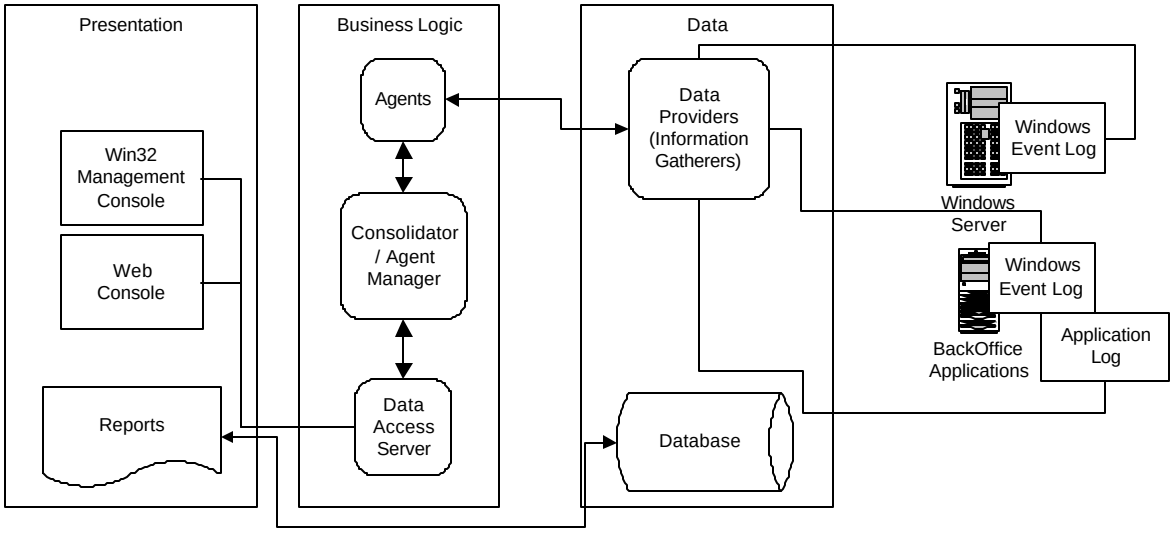


Figure 1: Basic MOM Architecture

The presentation tier is composed of user interface applications – whether via the web through a browser or with the Win32 MOM console. At the business logic layer, the agents monitor the systems and take action based on processing rules defined using the console. The consolidator is the focal point for all reported information and it provides data confidentiality by using encrypted channels. It collects and processes all data from agents. MOM's agents run on managed servers in the enterprise, and are configured with processing rules. These agents read the Windows event log and process data. There are a variety of other data providers designed to appeal to the enterprise. These include a syslog interface for receiving information from UNIX systems, a generic log file provider for applications that write single line log files, SNMP traps, and performance counters embedded within Windows.

MOM2000 Processing Rules

MOM has three classes of processing rules. These rules define how MOM collects and responds to information generated by monitored systems. The three processing rule classes are event, alert, and performance.

Within the event processing rule category, there are five distinct actions that MOM performs as its agents report information. First, it can either alert or respond to a specific event. Second, it can search for missing events for a given time period. This is an example of process by exception – if a specific event is not seen, then something deserves some attention. Third, MOM can also consolidate and summarize events. Fourth, MOM can filter out insignificant events, essentially discarding events that are reported from monitored systems. This feature allows you to audit for events on a computer, but not present them for reporting and alerting within MOM. Last, MOM the system can specify that specific data should be collected from specific sources.

Alert processing rules are the second set of processing rules. MOM can take a variety of actions based on the collected data. It can perform a variety of actions in order to communicate with operations staff, such as paging and email notification.

The last group of processing rules is performance counter monitoring rules. These are based on Windows Management Instrumentation (WMI), which is Microsoft's implementation of the DTMF standards. Here, MOM monitors for specific measurement statistics on system and application performance. MOM can also generate an alert if a specific performance counter passes a threshold - say a disk reaches 90% capacity.

Windows Events of Interest

There are numerous Events of Interest (EOI's) that the Windows OS will record in the various event logs and application log files. MOM monitors the Windows event logs and takes action based on events or event characteristics posted to the event logs (System, Security, Application, DNS, File Replication, and Directory Service). MOM is delivered with several Management Packs designed to monitor event logs. Depending on how auditing configured throughout Windows, highly granular information can be reported to the event logs. Event monitoring can be enabled or disabled as needed. Below are some representative Management Packs provided with MOM that relate to intrusion detection.

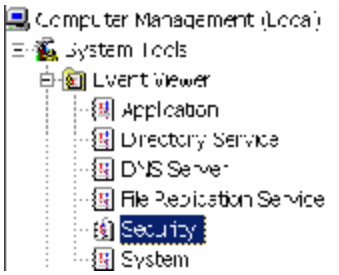


Figure 2: Domain Controller Event Logs

Sample Management Pack	EOI's and Area of Functionality
Default Event Collector	Monitors all event logs and provides comprehensive monitoring.
Domain Name Service	All DNS events.
Internet Information Service	Monitors IIS (web server), FTP, SMTP, and NNTP services. There are also sample scripts to determine server responsiveness.
Routing and Remote Access	Monitor dial up devices, VPN client access failures and bad logon attempts, and capacity issues.
Active Directory	Access to the directory service, replication, and security if auditing is configured within the directory service.

Microsoft also supplies Application Packs that monitor specific products such as Exchange, SQL Server, and Systems Management Server. These contain additional rules configured to monitor for events specific to the monitored application.

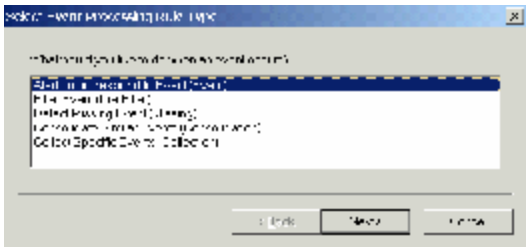
Event Processing Rule Setup and Example

In this example, a rule will be configured to monitor for failed logon attempts. Failed logon attempts qualify as an EOI, since they indicate an access was attempted without knowing proper authentication credentials.

First, open the MOM console and survey the list of Processing Rule Groups under the Rules node. Note that there are a variety of groups, which have logically associated processing rules. Also, if a processing rule group is not assigned to a particular computer group type, the defined rules will not be processed. Therefore, in order to activate a processing rule group, one must right click on the processing rule group, select Properties, the Computer Group tab, and add the appropriate computer group. Servers that are in this group type will process these rules.

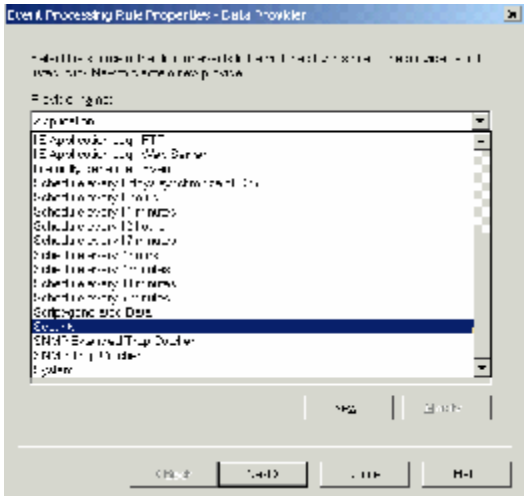
Step One: Determine rule type, and choose "Alert on or Respond to Event (Event)".

Then press Next.



Step Two: Chose the "Security" provider from the list.

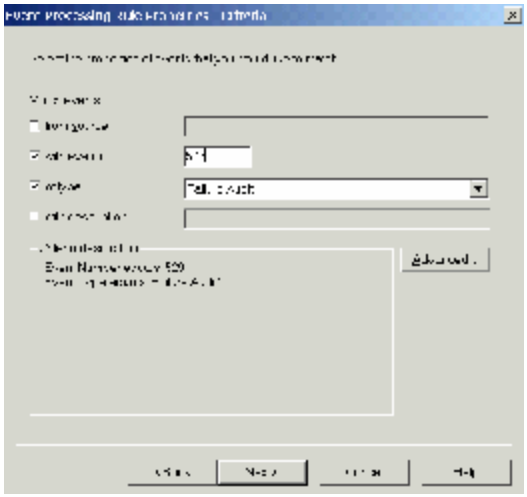
Then press Next.



Step Three: Enter in the specific criteria that this rule needs to match against.

Here, the Event ID 529 corresponds a Logon/Logoff audited event from the Security subsystem. The criteria are further limited to Failure Audits, because the alert should not fire for successful logon events. Note that this event is not generated unless auditing is enabled.

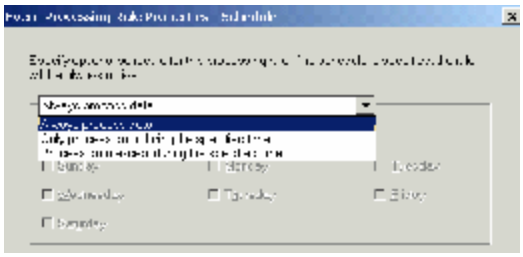
Then press Next.



Step Four: Select "Always process data" from the menu.

This type of event monitoring should be round the clock.

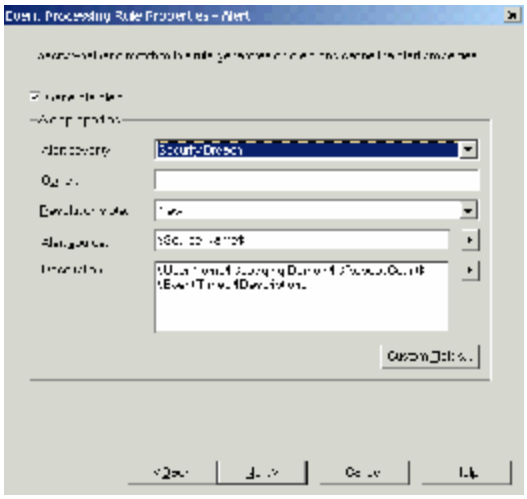
Then press Next.



Step Five: Check the Generate Alert Checkbox. Then, for this alert, select Security Breach for the Severity.

In order to get the additional data fields to be reported in the Description, press the arrow button and select the fields from the popup list. MOM will retrieve additional data from the reported event.

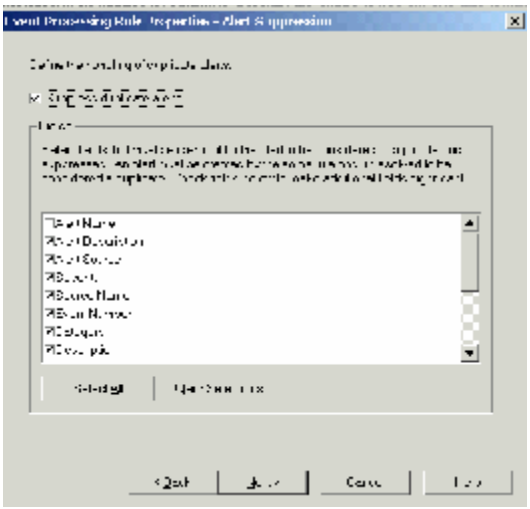
Then press Next.



Step Six: Check the Suppress duplicate alerts box.

By default, MOM will attempt to roll up multiple matching alerts into one alert. This prevents an alert storm from occurring. Duplicate suppression is based on matching fields, as shown in the dialog.

Then press Next.

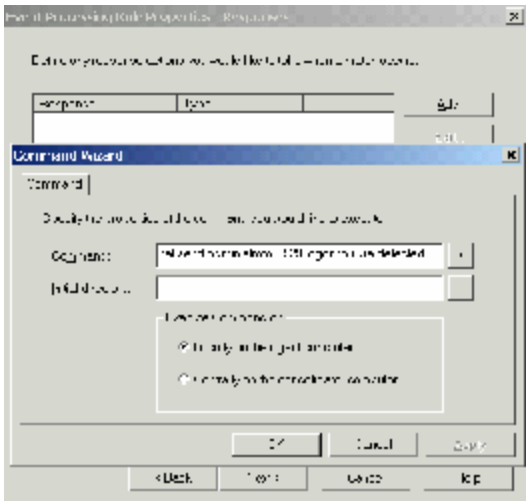


Step Seven: If desired, define an automated response (as shown here) by pressing the Add button.
There are five types of responses.

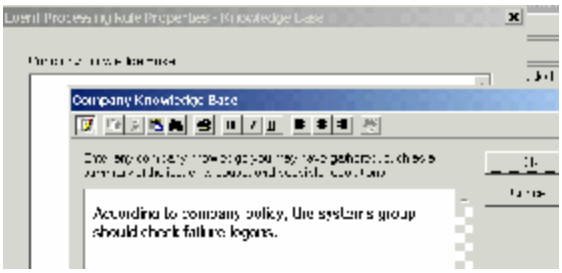
- Launch a Script
- Send an SNMP Trap
- Send a notification to a notification group
- Execute a command or batch file
- Update state variable

The response here is to execute the "net send" command (windows popup on the console).

Then press Next.



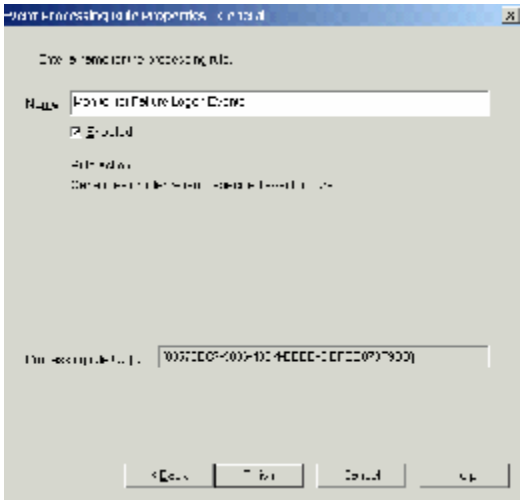
Step Eight: If desired, text can be entered in the Knowledge base tab (the Edit button is covered).



This area can be used for a variety of purposes, and is editable when responding to an alert - useful for site-specific information.

Then press Next.

Step Nine: Enter in an appropriate name for the event-processing rule.

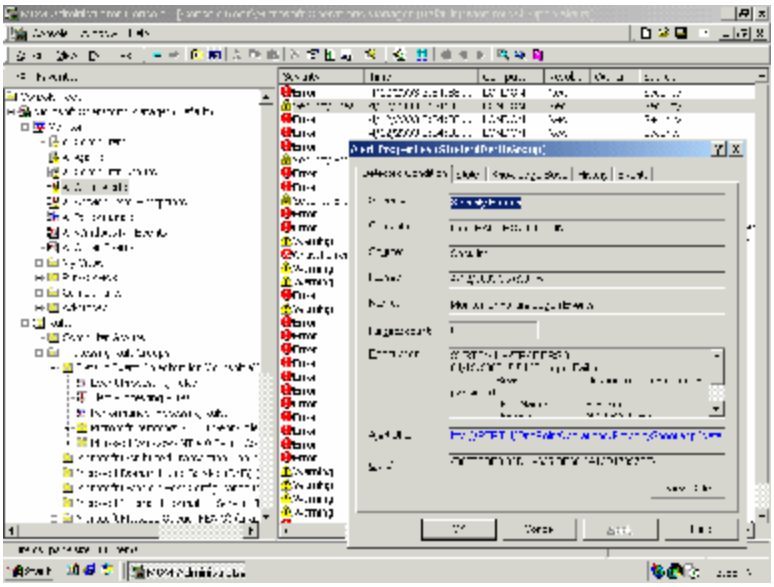


Then press Finish, and MOM will save the event definition.

Once the event-processing rule is defined, the changes will need to be committed to the MOM agents. In the MOM console, right click on the Rules node and select "Commit Configuration Change". MOM will inform agents that there are new rules, and this update will occur in a few minutes. Changes are committed to the MOM server when Event 21241 appears in the Application log, and Event ID 21240 appears on the agents.

Note in this screen capture the details on the alert. There are also other alerts from the domain, and a variety of tabs in the alert dialog.

This screen capture shows the MOM console responding to the alert configured above.



Considerations in Deployment

There are several considerations one should consider when deploying MOM in a manner that can best support an Information Security role within the organization. In particular, the needs of an intrusion analyst – having a reference point for EOI correlation from an IDS – require quite a bit of planning for MOM deployment.

Events to Monitor

Microsoft has documented about 6500 events that Windows produces. Below is a non-exhaustive list of some examples of security events to monitor for intrusion detection on systems or across the enterprise (candidates for Windows EoI's).

Event	Description
517	The audit log was cleared by a specific user.
528/529	Successful/unsuccessful logon by specified user.
531	Logon attempted to disabled account
532	Logon attempted to expired account (accounts can be time limited)
538	Logon attempted to a locked out account
546	Internet Key Exchange (IKE) session establishment failed
547	Internet Key Exchange (IKE) session negotiation failed
564	Object deleted by process
576	Special privileges applied to user
612-615	Events for IPSec policy changes
1309	Impersonation attempted on a thread not associated with a client
1317,1319	Specified user, group does not exist
1326-1331	Logon failures for specific events relating to account status

As can be seen from this representative list, there are a variety of highly granular events that Windows can be configured to produce which help the intrusion analyst. Note that often auditing is not enabled for a specific service by default – so if monitoring is desired, then auditing will need to be configured using the specific management tool for that service.

Example Usage of MOM for Intrusion Detection

Exploring MalWare: There are several worms and viruses that attempt to explore and make use of network shares. If specific systems are configured to audit for "failure" events when a Windows share is accessed, MOM can inform an operator within a few minutes. Recent examples of this behavior include the SoBigB (May 2003) and Nimda (2001) virus's which explore network drives on all possible machines.

Repeated Administrator Logon Attempts: Since the "Administrator" account cannot be locked out by default in Windows NT4 and Windows 2000, an operator can be informed in a few minutes about a dictionary or brute force password attack attempt.

Anomalous Disk Usage: One of the malicious uses of compromised systems is to use them as file servers for movies, MP3's, and pirated software. An attacker may be smart enough to not fill up a disk, but the performance monitor counters can be configured to monitor for logical disk space (as opposed to physical) usage and if it reaches a threshold inform an operator.

Providing Event Correlation

One of the more difficult challenges in intrusion analysis is event correlation. It is highly valuable to be able to correlate EOI's raised by a network Intrusion detection system with events raised in an enterprise from its managed servers. By using an authoritative centralized timeserver for all servers, correlation between the networks' IDS and MOM can reliably be made. Since MOM cam use UNIX syslog data, an IDS or other UNIX processes can post information to MOM, improving event correlation chances[5].

Configuring Auditing

In order to actually receive audit events, auditing must be configured – it is not enabled by default for Windows NT/2000. The best place to configure domain-wide auditing policies is by using the "Default Domain Group Policy", and enable auditing. By doing this, a system administrator would not have to modify each server's local security policy.

At an absolute minimum, the domain should be configured to monitor for Failure evens for account logon, logon events, and system events. Windows 2000 and Active Directory differentiates local interactive logon from over the network logon - thus two different of logon event types. As show in the accompanying figure, Failure auditing for everything, and Success auditing for *at least logon*, *account logon* and *system* events[6] should be configured.

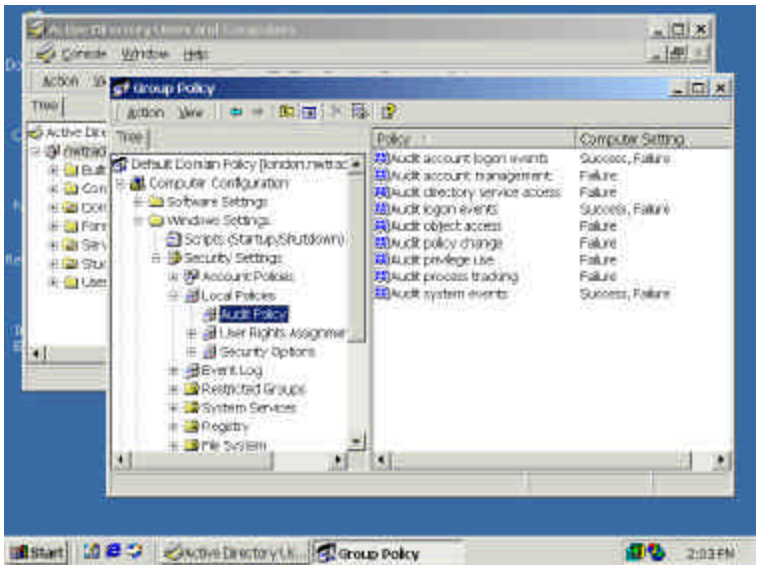


Figure 3 : Windows Auditing with Group Policy

As mentioned earlier, most services under Windows have their own management tool. Using service specific tools is required in order to configure auditing related to a specific service. For example, if auditing Active Directory is required, the container nodes need to have specific auditing configured.

Deploying MOM may impact operating system performance and the network in general. MOM must be deployed in stages in order to make sure that each managed node functions properly and reports what it needs to report. Not all of MOM event reporting is enabled by default. Site-specific event categories for processing rule groups can (and should) be set for individual or groups of systems as needed. DCAM reporting of events across a firewall boundary also require special deployment

[5] For details on setting up MOM to use UNIX syslogs, see Microsoft Support article 297443. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;297443

[6] Current consensus guidelines on auditing can be found in the SANS "Securing Windows 2000 Professional – Using the Gold Template Standard" and "Securing Windows 2000 Step by Step" books.

considerations and don't "just work" by default, as explained in the Installation Guide [7].

Summary

The intrusion analyst needs to be better armed and informed about what is occurring on the network. By concentrating on the packet layer, the analyst can miss valuable EoI's at the operating system and application level. MOM can be brought to bear on this space, thus increasing the quality of "above the wire" data which can help to detect intrusion, misuse, and violations of security policy within an organization and help better respond to incidents.

References: Assignment One

Microsoft Corporation. "Microsoft Operations Manager 2000 Product Information". 7 June 2003. URL: http://www.microsoft.com/mom/evaluation/default.asp

Microsoft Corporation. "Microsoft Operations Manager 2000 Deployment and Migration", 7 June 2003. URL: http://www.microsoft.com/mom/techinfo/deployment/default.asp

Microsoft Corporation. "Microsoft Operations Manager 2000 Product Documentation", 7 June 2003. URL: http://www.microsoft.com/mom/techinfo/productdoc/default.asp (the Users Guide, Installation Guide, and online Help are all available).

Jeff Shawgo, ed. "Securing Windows 2000 Step by Step (Ver 1.5)". The SANS Institute, July 1, 2001. Chapter 3.

Ben Bower, Dean Farrimgton, Chris Weber. "Security Windows 2000 Professional Using the Gold Standard Security Template". SANS Press, 2002.

[7] Deployment of MOM through a firewall for servers on a DMZ or perimeter network is beyond the scope. See the MOM Installation Guide, Ch. 5 and Ch. 8 for more details. URL: http://www.microsoft.com/mom/docs/installg.pdf

Last Updated: June 23rd, 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