VI3 SECURING AND MONITORING

Appendix

esxcfg-firewall options

The Service Console in ESX Server 3 has a firewall **enabled** by default.

esxcfg-firewall <options>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>-q|--query</td><td>Lists current settings.</td></tr>
<tr><td>-q|--query <service></td><td>Lists setting for the specified service.</td></tr>
<tr><td>-q|--query incoming|outgoing</td><td>Lists setting for non-required incoming/outgoing ports.</td></tr>
<tr><td>-s|--services</td><td>Lists known services.</td></tr>
<tr><td>-l|--load</td><td>Loads current settings and enables the IP tables firewall.</td></tr>
<tr><td>-u|--unload</td><td>Unloads current settings and disables the IP tables firewall.</td></tr>
<tr><td>-r|--resetDefaults</td><td>Resets all options to defaults</td></tr>
<tr><td>-e|--enableService <service></td><td>Allows specified service through the firewall.</td></tr>
<tr><td>-d|--disableService <service></td><td>Blocks specified service</td></tr>
<tr><td>-o|--openPort <port,tcp|udp,in|out,name></td><td>Opens a port.</td></tr>
<tr><td>-c|--closePort <port,tcp|udp,in|out></td><td>Closes a port previously opened via --openPort.</td></tr>
<tr><td>--blockIncoming</td><td>Block all non-required incoming ports (default value).</td></tr>
<tr><td>--blockOutgoing</td><td>Block all non-required outgoing ports (default value).</td></tr>
<tr><td>--allowIncoming</td><td>Allow all incoming ports.</td></tr>
<tr><td>--allowOutgoing</td><td>Allow all outgoing ports.</td></tr>
<tr><td>-h|--help</td><td>Show this message.</td></tr>
</table>

Default Services:

Service	Description
AAMClient	Added by the vpxa RPM: Traffic between ESX Server hosts for VMware High Availability (HA) and EMC Autostart Manager – inbound and outbound TCP and UDP Ports 2050 – 5000 and 8042 – 8045
activeDirectorKerberos	Active Directory Kerberos - outbound TCPs Port 88 and 464
CIMHttpServer	First-party optional service: CIM HTTP Server - inbound TCP Port 5988
CIMHttpsServer	First-party optional service: CIM HTTPS Server - inbound TCP Port 5989
CIMSLP	First-party optional service: CIM SLP - inbound and outbound TCP and UDP Ports 427
commvaultDynamic	Backup agent: Commvault dynamic – inbound and outbound TCP Ports 8600 – 8619
commvaultStatic	Backup agent: Commvault static – inbound and outbound TCP Ports 8400 – 8403
ftpClient	FTP client - outbound TCP Port 21
ftpServer	FTP server - inbound TCP Port 21
kerberos	Kerberos - outbound TCPs Port 88 and 749
LicenseClient	FlexLM license server client - outbound TCP Ports 27000 and 27010
nfsClient	NFS client - outbound TCP and UDP Ports 111 and 2049 (0 – 65535)
nisClient	NIS client - outbound TCP and UDP Ports 111 (0 – 65535)
ntpClient	NTP client - outbound UDP Port 123
smbClient	SMB client - outbound TCP Ports 137 – 139 and 445
snmpd	SNMP services - inbound TCP Port 161 and outbound TCP Port 162
sshClient	SSH client - outbound TCP Port 22
sshServer	SSH server - inbound TCP Port 22
swISCSIClient	First-party optional service: Software iSCSI client - outbound TCP Port 3260
telnetClient	NTP client - outbound TCP Port 23

VI3 SECURING AND MONITORING

Service	Description
TSM	Backup agent: IBM Tivoli Storage Manager – inbound and outbound TCP Ports 1500
veritasBackupExec	Backup agent: Veritas BackupExec – inbound TCP Ports 10000 – 10200
veritasNetBackup	Backup agent: Veritas NetBackup – inbound TCP Ports 13720, 13732, 13734, and 13783
vncServer	VNC server - Allow VNC sessions 0-64: inbound TCP Ports 5900 – 5964
vpxHeartbeats	vpx heartbeats - outbound UDP Port 902

You can configure your own services in the file /etc/vmware/firewall/services.xml:

esxcfg-firewall examples:

Enable ssh client connections from the Service Console:

```
# esxcfg-firewall -e sshClient
```

Disable the Samba client connections:

```
# esxcfg-firewall -d smbClient
```

Allow syslog outgoing trafic:

```
# esxcfg-firewall -o 514,udp,out,syslog
```

Enabled services override the individual port settings.

Turn off the firewall

```
# /usr/sbin/esxcfg-firewall --allowIncoming
# /usr/sbin/esxcfg-firewall --allowOutgoing
```

Re-enable the firewall

```
# /usr/sbin/esxcfg-firewall --blockIncoming
# /usr/sbin/esxcfg-firewall –blockOutgoing
```

Whenever possible, use VI Client, VI Web Access, or a third-party network management tool to administer your ESX Server hosts instead of working though the command line interface as root. Using VI Client lets you limit the accounts with access to the Service Console, safely delegate responsibilities, and set up roles that prevent administrators and users from using capabilities they don't need.
Interacting directly with the iptables configurations is possible but not recommended. For configuring the firewall you should only use esxcfg-firewall or VI Client. The linux configuration tools are not supported.

Network Ports

This section lists predetermined TCP and UDP ports used for management access to your VirtualCenter Server, ESX Server hosts, and other network components. If you need to manage network components from outside a firewall, you might need to reconfigure the firewall to allow access on the appropriate ports. The ports listed in the table are connected through the Service Console interface unless otherwise indicated.

Port	Purpose	Traffic Type
80	HTTP access. The default non-secure TCP Web port typically used in conjunction with port 443 as a front end for access to ESX Server networks from the Web. Port 80 redirects traffic to an HTTPS landing page (port 443) from which you launch your virtual machine console. Use port 80 for connection to VI Web Access from the Web.	Incoming TCP
443	HTTPS access. The default SSL Web port. Use Port 443 for the following: • Connection to VI Web Access from the Web. • VI Web Access and third-party network management client connections to the VirtualCenter Server. • Direct VI Web Access and third-party network management clients' access to ESX Server hosts.	Incoming TCP
902	Authentication traffic for the ESX Server host and virtual machine configuration. Use Port 902 for the following: • VI Client access to the VirtualCenter Server. • VirtualCenter Server access to ESX Server hosts. • Direct VI Client access to ESX Server hosts. • ESX Server host access to other ESX Server hosts for migration and provisioning.	Incoming TCP Outgoing UDP
903	Remote console traffic generated by user access to virtual machines on a specific ESX Server host. Use Port 903 for the following: • VI Client access to virtual machine consoles. • VI Web Access Client access to virtual machine consoles.	Incoming TCP Outgoing TCP
2049	Transactions from your NFS storage devices. This port is used on the VMkernel interface rather than the Service Console interface.	

Port	Purpose	Traffic Type
2050 - 5000	Traffic between ESX Server hosts for VMware High Availability (HA) and EMC Autostart Manager.	Outgoing TCP Incoming UDP Outgoing UDP
3260	Transactions from your iSCSI storage devices. This port is used on the VMkernel interface and the Service Console interface.	Outgoing TCP
8000	Incoming requests from VMotion. This port is used on the VMkernel interface rather than the Service Console interface.	Incoming TCP Outgoing TCP
8042–8045	Traffic between ESX Server hosts for HA and EMC Autostart Manager.	Outgoing TCP Incoming UDP Outgoing UDP
27000	License transactions from ESX Server to the license server.	Outgoing TCP
27010	License transactions from the license server.	Incoming TCP

Note ESX Server and VirtualCenter use ports 8085, 8087, and 9080 internally. For ESX Server, ports 8085, 8087, and 9080 are protected because they don’t accept remote connections.

SWATCH

http://www.stanford.edu/~atkins/swatch — The Simple WATCHer (SWATCH) uses log files generated by syslog to alert administrators of anomalies based on user configuration files. SWATCH was designed to log any event that the user wants to add into the configuration file; however, it has been adopted widely as host-based IDS.

LIDS

http://www.lids.org — The Linux Intrusion Detection System (LIDS) is a kernel patch and administration tool that can also control file modification with access control lists (ACLs) and protect processes and files, even from the root user.

ESX Server Technical Support Commands

This appendix section lists the Service Console commands used to configure ESX Server. Most of these commands are reserved for Technical Support use and are included for your reference only. In a few cases, however, these commands provide the only means of performing a configuration task for the ESX Server host. Also, if you lose your connection to the host, executing certain of these commands through the command line interface may be your only recourse. For example, if networking becomes nonfunctional and VI Client access is therefore unavailable.

NOTE: If you use the commands in this appendix, you must execute the service mgmt-vmware restart command to restart the vmware-hostd process and alert the VI Client and other management tools that the configuration has changed. In general, avoid executing the commands in this appendix if the host is currently under the VI Client or VirtualCenter Server management. The VI Client graphical user interface provides the preferred means of performing the configuration tasks described in this appendix. You can use this appendix to learn which VI Client commands to use in place of the Service Console commands. This appendix provides a summary of the actions you take in VI Client but does not give complete instructions. For details on using commands and performing configuration tasks through VI Client, see the online help.

You can find additional information on a number of ESX Server commands by logging on to the Service Console and using the man <esxcfg_command_name> command to display man pages.

esxcfg-advcfg

Configures advanced options for ESX Server. To configure advanced options in VI Client, click **Advanced Settings**. When the **Advanced Settings** dialog box opens, use the list on the left to select the device type or activity you want to work with and then enter the appropriate settings.

VI3 SECURING AND MONITORING

esxcfg-auth

Configures authentication. You can use this command to switch between the pam_cracklib.so and pam_passwdqc.so plugins for password change rule enforcement. You also use this command to reset options for these two plugins. There is no means of configuring these functions in VI Client.

esxcfg-boot

Configures bootstrap settings. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no means of configuring these functions in VI Client.

esxcfg-dumppart

Configures a diagnostic partition or searches for existing diagnostic partitions. When you install ESX Server, a diagnostic partition is created to store debugging information in the event of a system fault. You don't need to create this partition manually unless you determine that there is no diagnostic partition for the host. You can perform the following management activities for diagnostic partitions in VI Client:
* **Determine whether there is a diagnostic partition.** Click **Storage** > **Add** and check the first page of the **Add Storage** Wizard to see whether it includes the **Diagnostic** option. If **Diagnostic** is not one of the options, ESX Server already has a diagnostic partition.
* **Configure a diagnostic partition.** Click **Storage** > **Add** > **Diagnostic** and step through the wizard.

esxcfg-firewall

Configures the Service Console firewall ports. To configure firewall ports for supported services and agents in VI Client, you select the Internet services that will be allowed to access the ESX Server host. Click **Security Profile** > **Firewall** > **Properties** and use the **Firewall Properties** dialog box to add services. You cannot configure unsupported services through the VI Client.

esxcfg-info

Prints information about the state of the Service Console, VMkernel, various subsystems in the virtual network, and storage resource hardware. VI Client does not provide a method for printing this information, but you can obtain much of it through different tabs and functions in the user interface. For example, you can check the status of your virtual machines by reviewing the information on the **Virtual Machines** tab.

esxcfg-linuxnet

Converts vswif to eth when booting ESX Server into service□console□only mode rather than into ESX Server mode. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no VI Client equivalent for this command.

esxcfg-module

Sets driver parameters and modifies which drivers are loaded during startup. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no VI Client equivalent for this command.

esxcfg-mpath

Configures multipath settings for your Fibre Channel or iSCSI disks. To configure multipath settings for your storage in VI Client, click **Storage**. Select a datastore or mapped LUN and click **Properties**. When the **Properties** dialog box opens, select the desired extent if necessary. Then, click **Extent Device** > **Manage Paths** and use the **Manage Path** dialog box to configure the paths.

esxcfg-nas

Manages NAS mounts. You use this command to add, delete, list, and change the attributes of NAS devices. To view NAS devices in VI Client, click **Storage** and scroll through the storage list. You can also perform the following activities from the **Storage** view:
* **Display the attributes of a NAS device.** Click the device and review the information under **Details**.
* **Add a NAS device.** Click **Add Storage**.

* **Delete a NAS device.** Click **Remove**.
* **Change the attributes of a NAS device.** Click the device and click **Details** > **Properties**.

esxcfg-nics
Prints a list of physical network adapters along with information on the driver, PCI device, and link state of each NIC. You can also use this command to control a physical network adapters speed and duplexing.
To view information on the physical network adapters for the host in VI Client, click **Network Adapters**.
To change the speed and duplexing for a physical network adapter in the VI Client, click **Networking** > **Properties** for any of the virtual switches associated with the physical network adapter. In the **Properties** dialog box, click **Network Adapters** > **Edit** and select the speed and duplex combination.

esxcfg-resgrp
Restores resource group settings and lets you perform basic resource group management. Select a resource pool from the inventory panel and click **Edit Settings** on the **Summary** tab to change the resource group settings.

esxcfg-route
Sets or retrieves the default VMkernel gateway route. To view the default VMkernel gateway route in VI Client, click **DNS and Routing**. To change the default routing, click **Properties** and update the information in both tabs of the **DNS and Routing Configuration** dialog box.

esxcfg-swiscsi
Configures your software iSCSI software adapter. To configure your software iSCSI system in VI Client, click **Storage Adapters**, select the iSCSI adapter you want to configure, and click **Properties**. Use the **iSCSI Initiator Properties** dialog box to configure the adapter.

esxcfg-vmhbadevs
Prints a map of VMkernel storage devices to Service Console devices. There is no VI Client equivalent for this command.

esxcfg-vmknic
Creates and updates VMkernel TCP/IP settings for VMotion, NAS, and iSCSI. To set up VMotion, NFS, or iSCSI network connections in VI Client, click **Networking > Add Networking**. Select **VMkernel** and step through the **Add Network Wizard**. Define the IP address subnet mask and VMkernel default gateway in the **Connection Settings** step.
To review your settings, click the blue icon to the left of the VMotion, iSCSI, or NFS port. To edit any of these settings, click **Properties** for the switch. Select the port from the list on the switch **Properties** dialog box and click **Edit** to open the port **Properties** dialog box and change the settings for the port.

Additional Linux Configuration Commands

esxcfg-vswif
Creates and updates Service Console network settings. This command is used if you cannot manage the ESX Server host through the VI Client because of network configuration issues.
To set up connections for the Service Console in VI Client, click **Networking > Add Networking**. Select **Service Console** and step through the **Add Network Wizard**. Define the IP address subnet mask and the Service Console default gateway in the **Connection Settings** step.
To review your settings, click the blue icon to the left of the service console port. To edit any of these settings, click **Properties** for the switch. Select the Service Console port from the list on the switch **Properties** dialog box. Click **Edit** to open the port **Properties** dialog box and change the settings for the port.

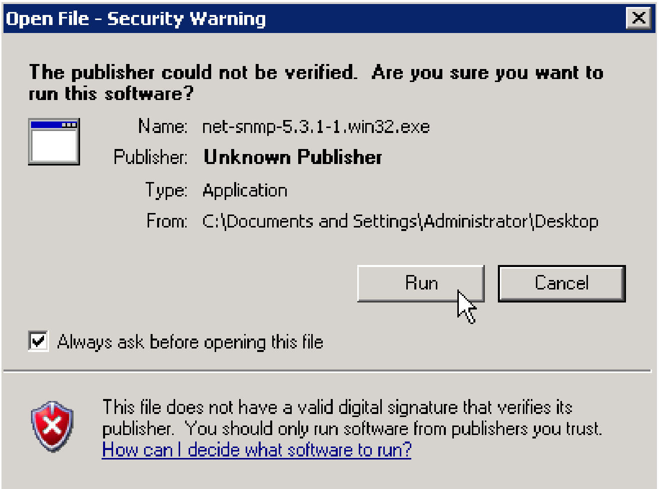
VI3 SECURING AND MONITORING

esxcfg-vswitch
Creates and updates virtual machine network settings. To set up connections for a virtual machine in VI Client, click **Networking > Add Networking**. Select **Virtual Machine** and step through the **Add Network Wizard**.
To review your settings, click the speech bubble icon to the left of the virtual machine port group. To edit any of these settings, click **Properties** for the switch. Select the virtual machine port from the list on the switch **Properties** dialog box, then click **Edit** to open the port **Properties** dialog box and change the settings for the port.

Set up an SNMP Trap Receiver (Example of a Windows based SNMP Trap Reciever)

We will use net-snmp as an SNMP trap receiver. The software can be downloaded here:
http://prdownloads.sourceforge.net/net-snmp/net-snmp-5.3.1-1.win32.exe?download
Start the net-snmp Installer by double clicking the desktop icon "net-snmp-5.3.1-1.win32.exe:

In the Security Warning window click "Run":



Open File - Security Warning

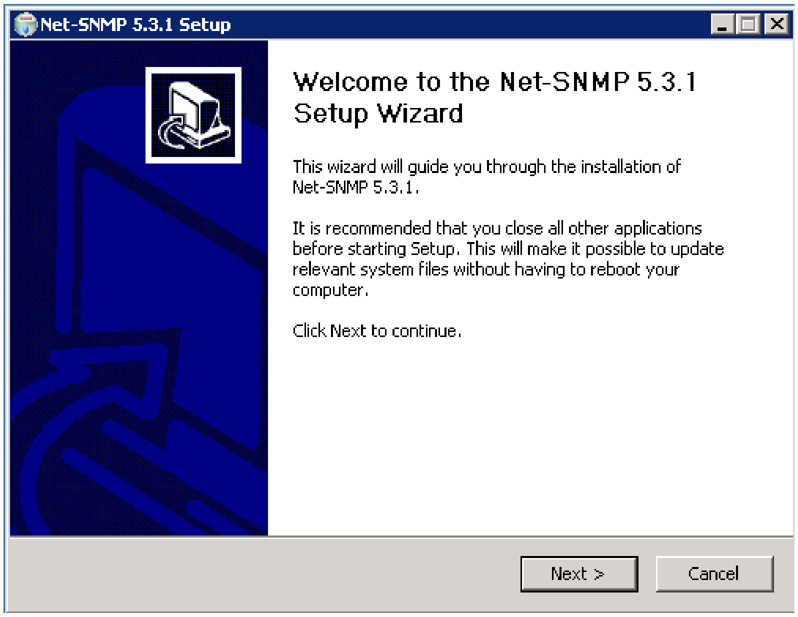
The publisher could not be verified. Are you sure you want to run this software?

Name: net-snmp-5.3.1-1.win32.exe
Publisher: Unknown Publisher
Type: Application
From: C:\Documents and Settings\Administrator\Desktop

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

In the Welcome window click "Next":



Net-SNMP 5.3.1 Setup

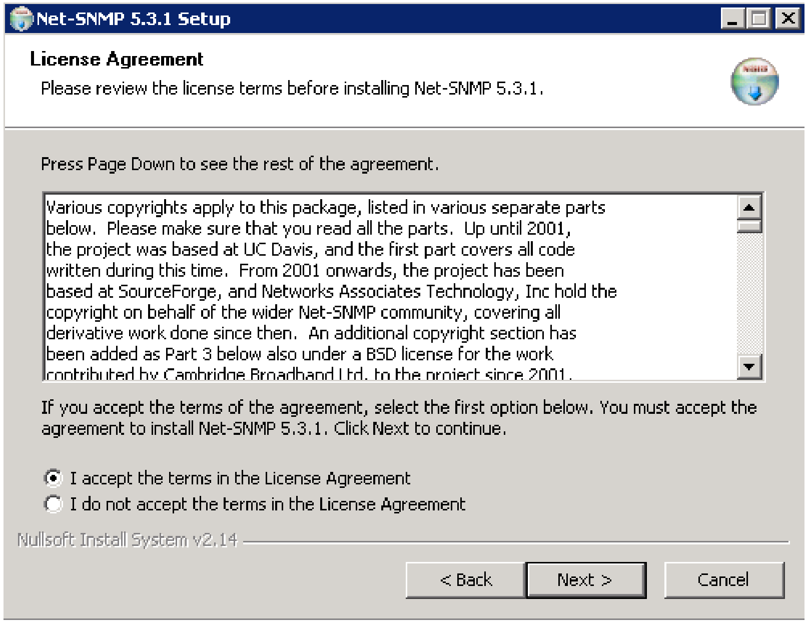
Welcome to the Net-SNMP 5.3.1 Setup Wizard

This wizard will guide you through the installation of Net-SNMP 5.3.1.

It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.

Click Next to continue.

In the License window select "I accept the terms in the License Agreement" and click "Next":



License Agreement

Please review the license terms before installing Net-SNMP 5.3.1.

Press Page Down to see the rest of the agreement.

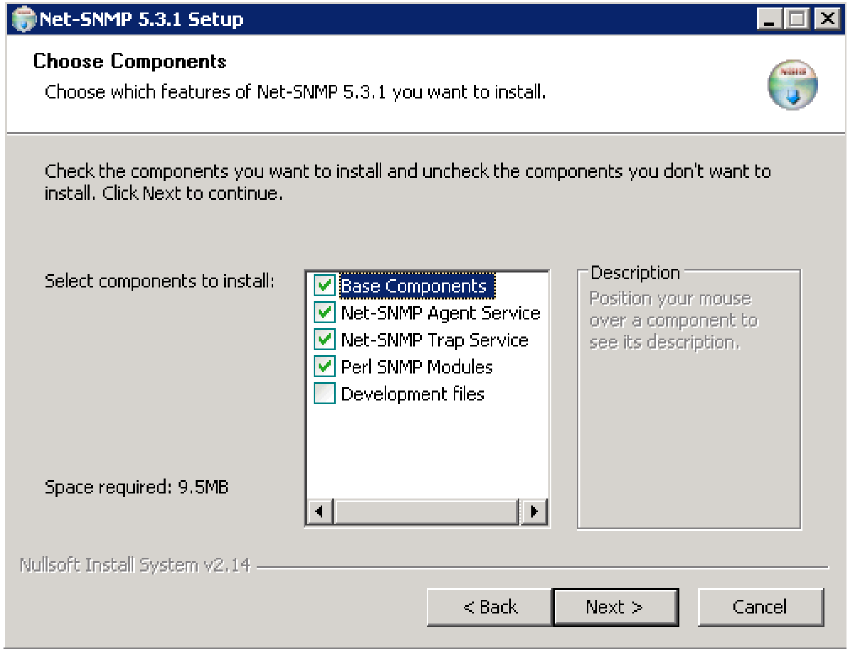
Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001.

If you accept the terms of the agreement, select the first option below. You must accept the agreement to install Net-SNMP 5.3.1. Click Next to continue.

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

In the Components window click "Next":



Choose Components

Choose which features of Net-SNMP 5.3.1 you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

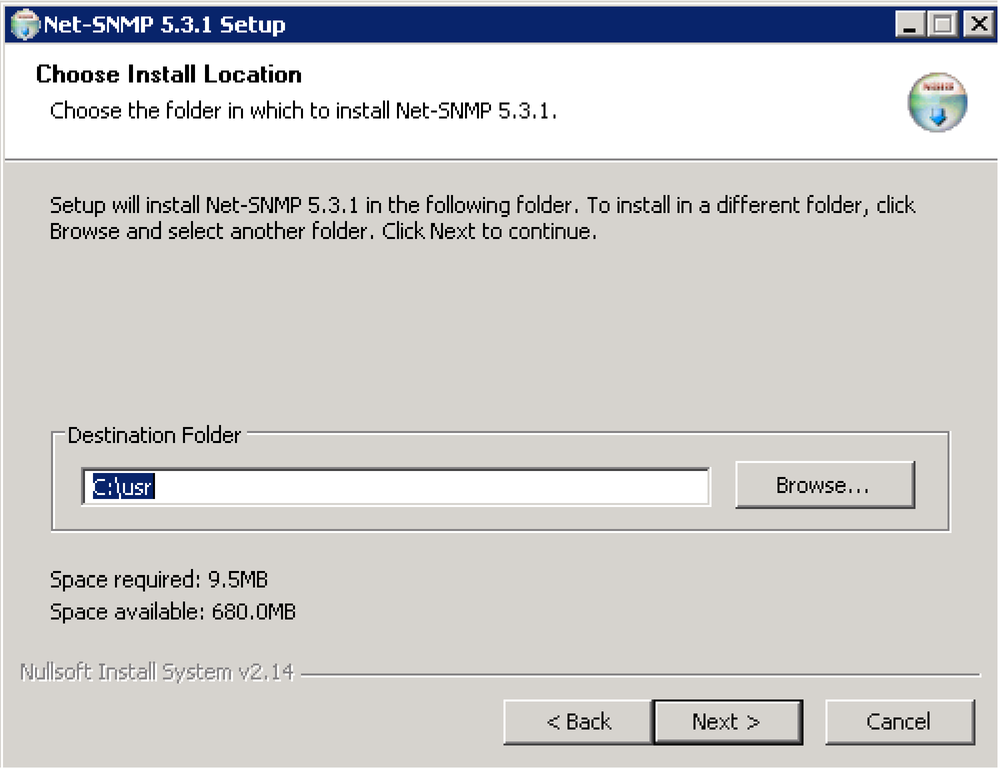
☑ Base Components
☑ Net-SNMP Agent Service
☑ Net-SNMP Trap Service
☑ Perl SNMP Modules
□ Development files

Description

Position your mouse over a component to see its description.

Space required: 9.5MB

In the Location window click "Next":



Net-SNMP 5.3.1 Setup

Choose Install Location

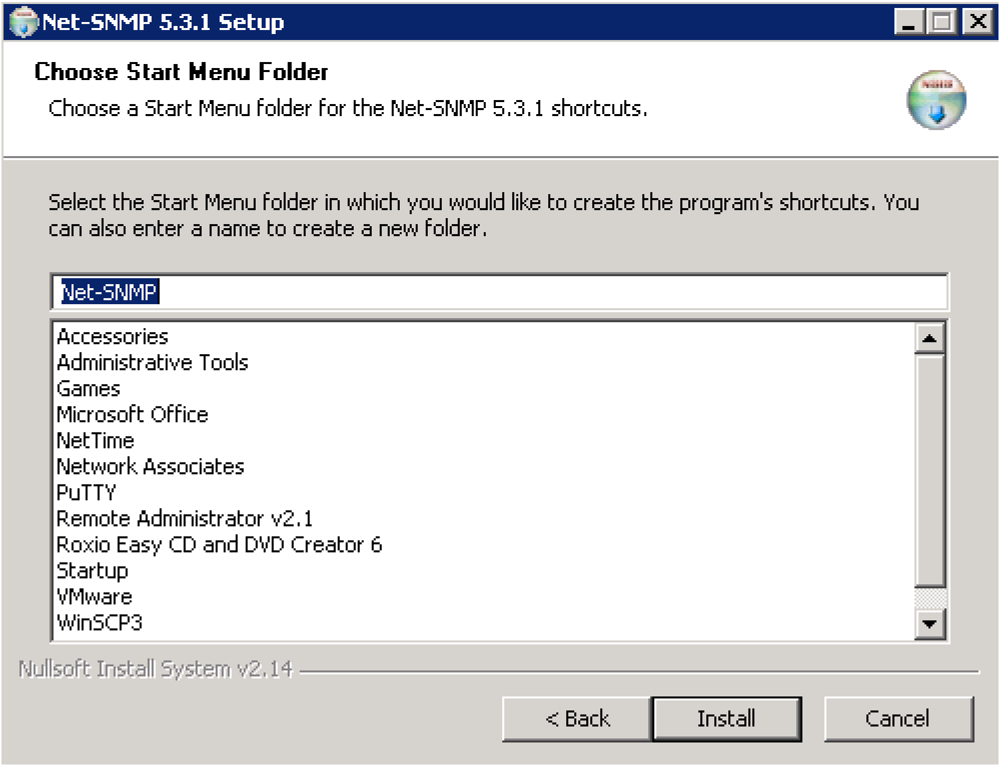
Choose the folder in which to install Net-SNMP 5.3.1.

Setup will install Net-SNMP 5.3.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Next to continue.

Destination Folder: C:\usr

Space required: 9.5MB
Space available: 680.0MB

In the Start Menu Folder window click "Install":



Net-SNMP 5.3.1 Setup

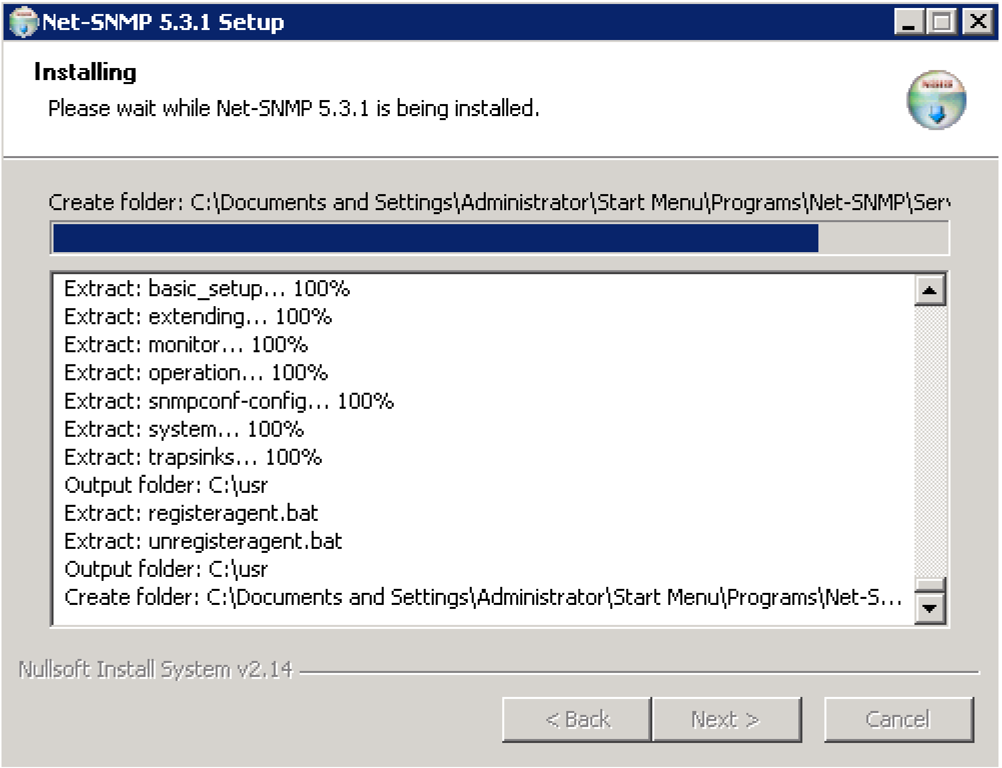
Choose Start Menu Folder

Choose a Start Menu folder for the Net-SNMP 5.3.1 shortcuts.

Select the Start Menu folder in which you would like to create the program's shortcuts. You can also enter a name to create a new folder.

Net-SNMP

The installation progress is showing:



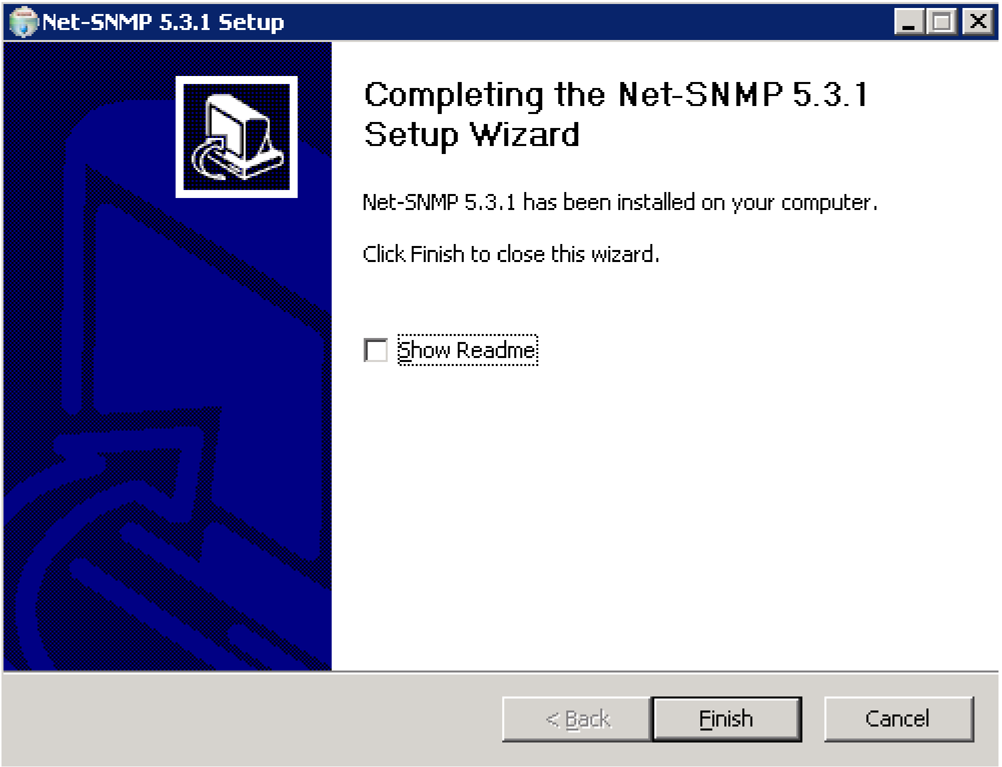
Installing

Please wait while Net-SNMP 5.3.1 is being installed.

Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Net-SNMP\Serv

```
Extract: basic_setup... 100%
Extract: extending... 100%
Extract: monitor... 100%
Extract: operation... 100%
Extract: snmpconf-config... 100%
Extract: system... 100%
Extract: trapsinks... 100%
Output folder: C:\usr
Extract: registeragent.bat
Extract: unregisteragent.bat
Output folder: C:\usr
Create folder: C:\Documents and Settings\Administrator\Start Menu\Programs\Net-S...
```

In the Completing window deselect "Show Readme" and click "Finish":



Completing the Net-SNMP 5.3.1 Setup Wizard

Net-SNMP 5.3.1 has been installed on your computer.

Click Finish to close this wizard.

□ Show Readme

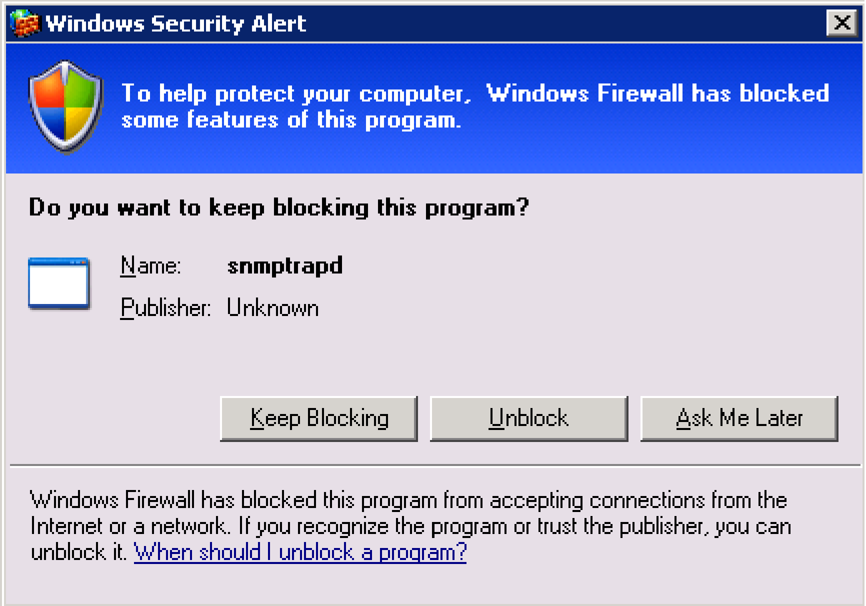
Configure the SNMP Trap receiver to accept all incoming data from the vmworld06 community. Open a command prompt window and go to the directory C:\usr\etc\snmp. Create a snmptrapd.conf file and specify the community name "vmworld06":

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>cd \usr\etc\snmp

C:\usr\etc\snmp>echo authCommunity log,execute,net vmworld06 > snmptrapd.conf
```

Start the SNMP Trap Receiver and display any received traps on the command line:

```
C:\usr\etc\snmp>cd \usr\bin

C:\usr\bin>snmptrapd -Lo
NET-SNMP version 5.3.1
```

When you see a warning from the Windows Firewall after you started snmptrapd click on "Unblock":



Windows Security Alert

To help protect your computer, Windows Firewall has blocked some features of this program.

Do you want to keep blocking this program?

Name: snmptrapd

Publisher: Unknown

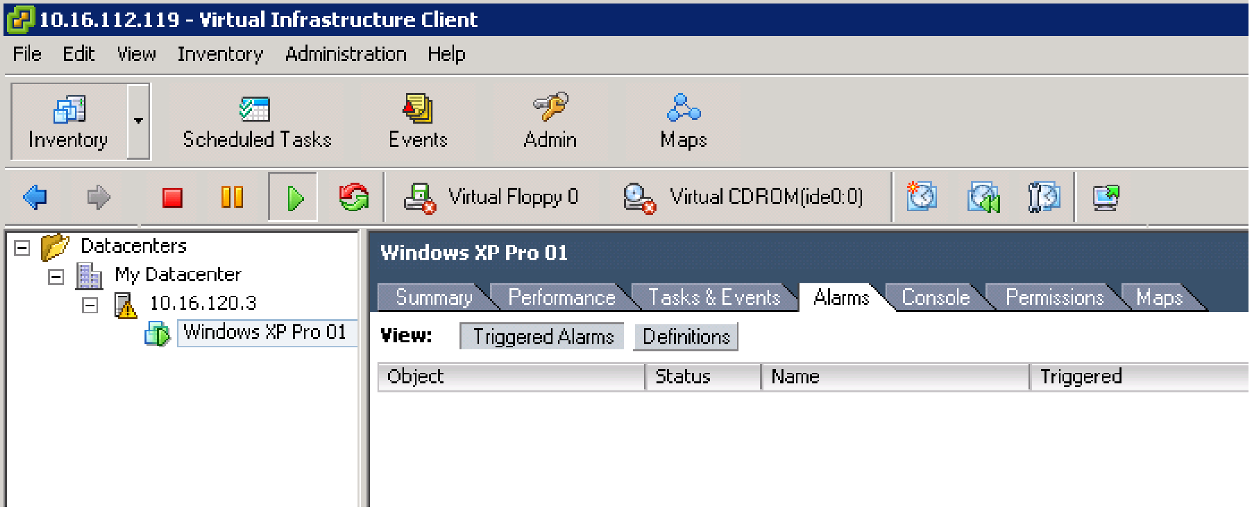
Windows Firewall has blocked this program from accepting connections from the Internet or a network. If you recognize the program or trust the publisher, you can unblock it. When should I unblock a program?

Create and View SNMP Traps

We will generate CPU load to trigger the "Virtual Machine CPU Usage" alarm:

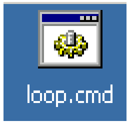
1. Step

In your VI Client select the VM to monitor, click on the "Alarms" tab and select "Triggered Alarms" to see if any alarms are fired:



2. Step

On the desktop double click on the loop.cmd icon to generate CPU load:

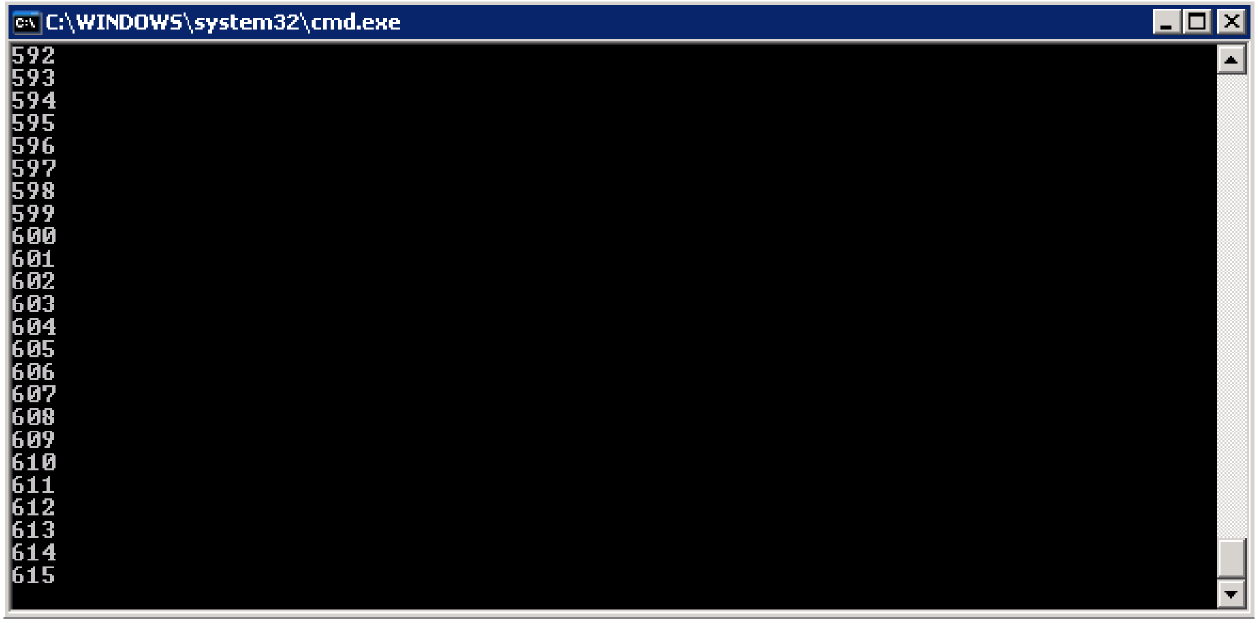


Note: The content of this file is:

```
@echo off

:loop
for /l %%n in (1,1,10000) do echo %%n
goto loop
```

3. Step

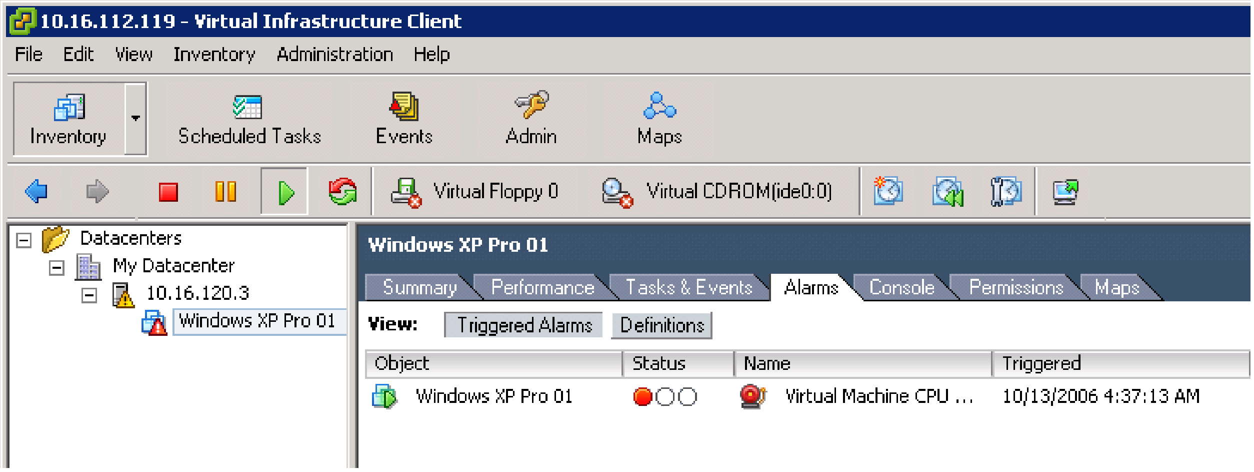
A command line window opens and displays numbers – this window can be minimized, it is not needed for other purposes. Close the window if you want to stop generating load later:



```
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
```

4. Step

After a few minutes a CPU Load Alarm will show up in the VI Client:



Object	Status	Name	Triggered
Windows XP Pro 01	●○○	Virtual Machine CPU ...	10/13/2006 4:37:13 AM

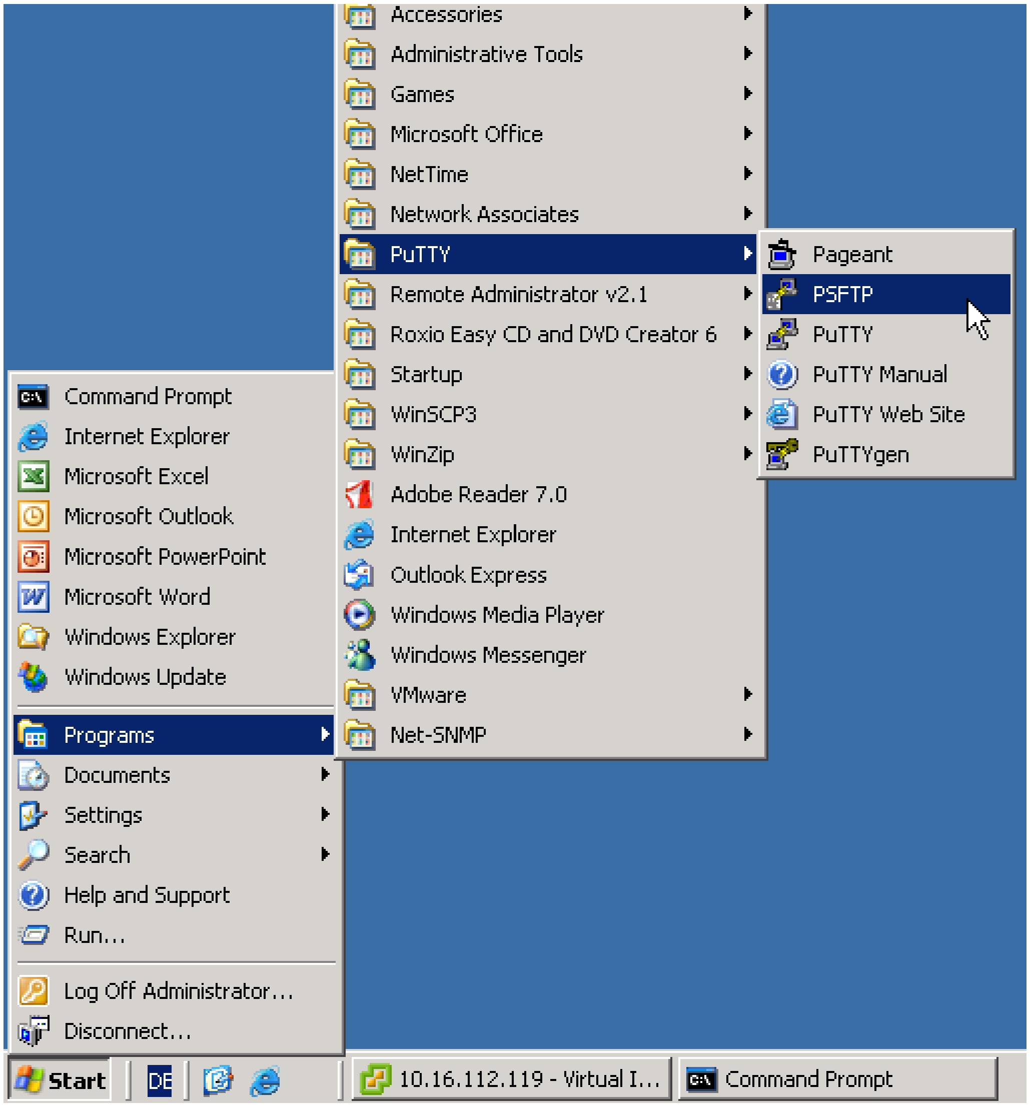
5. Step

Output will be in NST VMAt the same time the command line output of snmptrapd will show this text:

```
NET-SNMP version 5.3.1
2006-10-13 04:41:17 VMWARE-20E6C784.eng.vmware.com [10.16.112.119] (via UDP:
[10.16.112.119]:4236) TRAP, SNMP v1, community vmworld06
  SNMPv2-SMI::enterprises.6876.50 Enterprise Specific Trap (201) Uptime: 2 days,
23:08:49.48
  SNMPv2-SMI::enterprises.6876.50.301 = STRING: "vm"
  SNMPv2-SMI::enterprises.6876.50.302 = ""
  SNMPv2-SMI::enterprises.6876.50.303 = STRING: "Windows XP Pro 01"
  SNMPv2-SMI::enterprises.6876.50.304 = STRING: "Green"
  SNMPv2-SMI::enterprises.6876.50.305 = STRING: "Red"
  SNMPv2-SMI::enterprises.6876.50.306 = STRING: "Virtual Machine CPU Usage - (Metric CPU
Usage (Average/Rate) = 99%)"
```

SNMP MIBs

The snmptrapd output contained strings like "enterprises.6876.50.301". We can get a clear text representation of these strings to understand their meaning by installing the VMware MIBs on this system. Copy all *.mib files from the directory /usr/lib/vmware/snmp/mibs on the ESX Server host to the directory C:\usr\share\snmp\mibs on your laptop using PSFTP:



```
psftp: no hostname specified; use "open host.name" to connect
psftp> open 10.16.120.3
login as: alpha
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 6f:6f:b6:d7:69:77:64:eb:84:18:b8:7a:d0:d2:30:cc
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) y
Using username "alpha".
alpha@10.16.120.3's password: *****
Remote working directory is /home/alpha
psftp> cd /usr/lib/vmware/snmp/mibs
Remote directory is now /usr/lib/vmware/snmp/mibs
psftp> lcd /usr/share/snmp/mibs
New local directory is C:\usr\share\snmp\mibs
psftp> mget *.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-RESOURCES-MIB.mib => local:VMWARE-RESOURCES-
MIB.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-ESX-MIB.mib => local:VMWARE-ESX-MIB.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-SYSTEM-MIB.mib => local:VMWARE-SYSTEM-MIB.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-ROOT-MIB.mib => local:VMWARE-ROOT-MIB.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-TRAPS-MIB.mib => local:VMWARE-TRAPS-MIB.mib
remote:/usr/lib/vmware/snmp/mibs/VMWARE-VMINFO-MIB.mib => local:VMWARE-VMINFO-MIB.mib
psftp>quit
```

Edit the file C:\usr\etc\snmp\snmpd.conf and add the lines in bold font:

```
mibdirs C:/usr/share/snmp/mibs
persistentDir C:/usr/snmp/persist
tempFilePattern C:/usr/temp/snmpdXXXXXX
mibs +VMWARE-RESOURCES-MIB
mibs +VMWARE-ESX-MIB
mibs +VMWARE-SYSTEM-MIB
mibs +VMWARE-ROOT-MIB
mibs +VMWARE-TRAPS-MIB
mibs +VMWARE-VMINFO-MIB
```

Stop the SNMP Trap Receiver by hitting Ctrl-C in the window. You may also need to hit the Return key and Ctrl-C again:

```
C:\usr\etc\snmp>cd \usr\bin

C:\usr\bin>snmptrapd -Lo
NET-SNMP version 5.3.1
^C
C:\usr\bin>
```

Start the snmptrapd again to read the MIBs:

```
C:\usr\bin>snmptrapd -Lo
NET-SNMP version 5.3.1
```

Close the loop.cmd window, wait some time, and start it again to trigger the CPU Load Alarm. The next time an SNMP trap is received the text is more descriptive:

```
NET-SNMP version 5.3.1
2006-10-13 05:10:21 VMWARE-20E6C784.eng.vmware.com [10.16.112.119] (via UDP:
[10.16.112.119]:4264) TRAP, SNMP v1, community vmworld06
  VMWARE-ROOT-MIB::vmwTraps Enterprise Specific Trap (VMWARE-TRAPS-MIB::vpxdTrap) Uptime:
2 days, 23:37:53.23
  VMWARE-TRAPS-MIB::vpxdTrapType = STRING: "vm"
  VMWARE-TRAPS-MIB::vpxdHostName = ""
  VMWARE-TRAPS-MIB::vpxdVMName = STRING: "Windows XP Pro 01"
  VMWARE-TRAPS-MIB::vpxdOldStatus = STRING: "Green"
  VMWARE-TRAPS-MIB::vpxdNewStatus = STRING: "Red"
  VMWARE-TRAPS-MIB::vpxdObjValue = STRING: "Virtual Machine CPU Usage - (Metric CPU Usage
(Average/Rate) = 87%)"
```

You can find some explanations about the meaning of these fields if you open the file C:\usr\share\snmp\mibs\VMWARE-TRAPS-MIB.mib in a text editor and search for "vpxdVMName":

```
vpxdVMName OBJECT-TYPE
   SYNTAX     DisplayString
   ACCESS     read-only
   STATUS     mandatory
   DESCRIPTION
      "This is the name of the VM in the preceding traps."
   ::= { vmwTraps 303 }

vpxdOldStatus OBJECT-TYPE
   SYNTAX     DisplayString
   ACCESS     read-only
   STATUS     mandatory
   DESCRIPTION
      "This is the old status in the preceding traps."
   ::= { vmwTraps 304 }

vpxdNewStatus OBJECT-TYPE
   SYNTAX     DisplayString
   ACCESS     read-only
   STATUS     mandatory
   DESCRIPTION
      "This is the new status in the preceding traps."
   ::= { vmwTraps 305 }

vpxdObjValue OBJECT-TYPE
   SYNTAX     DisplayString
   ACCESS     read-only
   STATUS     mandatory
   DESCRIPTION
      "This is the current object value in the preceding traps."
```

SNMP Traps from ESX Server

Start the SNMP Trap Receiver to display any received traps on the command line:

```
C:\usr\etc\snmp>cd \usr\bin

C:\usr\bin>snmptrapd -Lo
NET-SNMP version 5.3.1
```

Configure SNMP on the ESX Server host:

```
login as: alpha
alpha@10.16.120.3's password: *****
Last login: Wed Oct 11 21:33:20 2006 from fwegnerxp.vmware.com
[alpha@wpavm-001 alpha]$ su -
Password: *****
[root@wpavm-001 root]# vi /etc/snmp/snmpd.conf
```

Specify the correct communities and trap receiver in the file /etc/snmp/snmpd.conf (as shown in bold font). Also add a line at the end with "disk / 30%". This will be used later for monitoring disk space:

```
# Sample snmpd.conf containing VMware MIB module entries.

# This is a simple snmpd.conf that may help you test SNMP.
# It is not recommended for production use. Consult the
# snmpd.conf(5) man pages to set up a secure installation.

syscontact root@localhost (edit snmpd.conf)
syslocation room1 (edit snmpd.conf)
rocommunity vmworld06
trapcommunity vmworld06
trapsink 10.16.112.119

# VMware MIB modules. To enable/disable VMware MIB items
# add/remove the following entries.
dlmod SNMPESX            /usr/lib/vmware/snmp/libSNMPESX.so
disk /vmimages 30%
~
```

Make sure the SNMP agents are started automatically when you reboot by running this command as root:

```
[root@wpavm-001 root]# chkconfig snmpd on
```

Start the SNMP agent manually:

```
[root@wpavm-001 root]# /etc/rc.d/init.d/snmpd start
Starting snmpd:                                            [  OK  ]
```

As soon as the SNMP agent is started on the ESX Server host an SNMP Trap is received on our snmptrapd window:

```
NET-SNMP version 5.3.1
2006-10-13 05:43:08 wpavm-001.vmware.com [10.16.120.3] (via UDP: [10.16.120.3]:32770)
TRAP, SNMP v1, community vmworld06
  NET-SNMP-MIB::netSnmpAgentOIDs.10 Cold Start Trap (0) Uptime: 0:00:01.20
```

Query SNMP Data from ESX Server

Find the ESX Server product name by running.

```
C:\usr\bin>snmpwalk -v 1 -c vmworld06 10.16.120.3 vmwProdName
VMWARE-SYSTEM-MIB::vmwProdName.0 = STRING: "VMware ESX Server"
```

Query shares and utilization of all virtual machines:

```
C:\usr\bin>snmpwalk -v 1 -c vmworld06 10.16.120.3 CpuEntry
VMWARE-RESOURCES-MIB::cpuVMID.16 = INTEGER: 16
VMWARE-RESOURCES-MIB::cpuShares.16 = INTEGER: 1000
VMWARE-RESOURCES-MIB::cpuUtil.16 = INTEGER: 11022617
```

This describes a VM with the ID 16. The VM has 1000 CPU shares, and the CPU utilization is 11022617. CPU utilization is the time the virtual machine has been running on the CPU in seconds.

Query the disk space status using the following command on your local system:

```
C:\usr\bin>snmpwalk -v 1 -c vmworld06 10.16.120.3 DskEntry
C:\usr\bin>snmpwalk -v 1 -c vmworld06 10.16.120.3 DskEntry
UCD-SNMP-MIB::dskIndex.1 = INTEGER: 1
UCD-SNMP-MIB::dskPath.1 = STRING: /vmimages
UCD-SNMP-MIB::dskDevice.1 = STRING: /dev/sda3
UCD-SNMP-MIB::dskMinimum.1 = INTEGER: -1
UCD-SNMP-MIB::dskMinPercent.1 = INTEGER: 30
UCD-SNMP-MIB::dskTotal.1 = INTEGER: 15116868
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 12202756
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 2146208
UCD-SNMP-MIB::dskPercent.1 = INTEGER: 15
UCD-SNMP-MIB::dskPercentNode.1 = INTEGER: 0
UCD-SNMP-MIB::dskErrorFlag.1 = INTEGER: 0
UCD-SNMP-MIB::dskErrorMsg.1 = STRING:
```

Optional - Disk Error Flag

To simulate the Disk Error Flag do this:

Change value in the last line of the file /etc/snmp/snmpd.conf to 90%. This will trigger an error as soon as less than 90% of this partition are free:

```
disk /vmimages 90%
```

Restart the snmpd process to activate the changed configuration:

```
[root@wpavm-001 root]# /etc/rc.d/init.d/snmpd restart
Stopping snmpd:                                            [  OK  ]
Starting snmpd:                                            [  OK  ]
```

Query the disk space status using the following command on your local system:

```
C:\usr\bin>snmpwalk -v 1 -c vmworld06 10.16.120.3 DskEntry
UCD-SNMP-MIB::dskIndex.1 = INTEGER: 1
UCD-SNMP-MIB::dskPath.1 = STRING: /vmimages
UCD-SNMP-MIB::dskDevice.1 = STRING: /dev/sda3
UCD-SNMP-MIB::dskMinimum.1 = INTEGER: -1
UCD-SNMP-MIB::dskMinPercent.1 = INTEGER: 90
UCD-SNMP-MIB::dskTotal.1 = INTEGER: 15116868
UCD-SNMP-MIB::dskAvail.1 = INTEGER: 12202756
UCD-SNMP-MIB::dskUsed.1 = INTEGER: 2146208
UCD-SNMP-MIB::dskPercent.1 = INTEGER: 15
UCD-SNMP-MIB::dskPercentNode.1 = INTEGER: 0
UCD-SNMP-MIB::dskErrorFlag.1 = INTEGER: 1
UCD-SNMP-MIB::dskErrorMsg.1 = STRING: /vmimages: less than 90% free (= 15%)
```

The last two lines show the error condition we created due to the changed configuration.

Command line primer

usermod - System administration command. Modify *user* account information.

usermod [**-c** comment] **-G** group,[...]] *user*

DESCRIPTION
The **usermod** command modifies the system account files to reflect the changes that are specified on the command line. The options which apply to the **usermod** command are:
-c *comment*

The new value of the user's password file comment field. It is normally modified using the **chfn**(1) utility.

-G *group,[...]*

A list of supplementary groups which the user is also a member of. Each group is separated from the next by a comma, with no intervening whitespace. The groups are subject to the same restrictions as the group given with the **-g** option. If the user is currently a member of a group which is not listed, the user will be removed from the group

ls

ls [*options*] [*names*]

List contents of directories. If no *names* are given, list the files in the current directory. With one or more *names*, list files contained in a directory *name* or that match a file *name*. *names* can include filename metacharacters.

vi [*options*] [*files*]

A screen-oriented text editor based on **ex**. **vi** is bi-modal, with a command mode and an insert mode

su

su [*option*] [*user*] [*shell_args*]

Create a shell with the effective user ID *user*. If no *user* is specified, create a shell for a privileged user (i.e., become a superuser). Enter EOF to terminate. You can run the shell with particular options by passing them as *shell_args* (e.g., if the shell runs **bash**, you can specify **-c** *command* to execute *command* via **bash**, or **-r** to create a restricted shell).

If you want to save your changes, type :w

Use the ex command :q to quit from vi.
If you want to save your changes, type :w.
If you want to save your changes to another file, type :w filename.txt to save as filename.txt. If you want to save and quit, type :x or :wq.

sudo

The sudo utility allows users defined in the /etc/sudoers configuration file to have temporary access to run commands they would not normally be able to due to file permission restrictions. The commands can be run as user "root" or as any other user defined in the /etc/sudoers configuration file.

groupadd

groupadd [*options*] *group* System administration command. Create new group of accounts for the system.

NMAP Command Line Descriptions:

Arguments Cheat Sheet

The following are the most useful uses of nmap. Use nmap –v to view additional information.

-sT TCP connect() port scan (default)
This option is the most simple and straightforward. It performs a simple connect() system call on any interesting port on the target machine. This type of scan is easily detected by intrusion detection software.

*** -sS TCP SYN stealth port scan (best all-around TCP scan)**
This technique is often referred to as "half-open" scanning, because you don't open a full TCP connection. You send a SYN packet, as if you are going to open a real connection and you wait for a response. A SYN|ACK indicates the port is listening. A RST is indicative of a non-listener. If a SYN|ACK is received, a RST is immediately sent to tear down the connection. The primary advantage to this scanning technique is that fewer sites will log it. Unfortunately you need root privileges to build these custom SYN packets.

*** -sU UDP port scan**
UDP scans: This method is used to determine which UDP (User Datagram Protocol, RFC 768) ports are open on a host. The technique is to send 0 byte udp packets to each port on the target machine. If we receive an ICMP port unreachable message, then the port is closed. Otherwise we assume it is open.

-sP ping scan (Find any reachable machines)
This option will simply attempt to ping any machine or range of machines listed. * -O Use TCP/IP fingerprinting to guess remote operating system This option activates remote host identification via TCP/IP fingerprinting. In other words, it uses a bunch of techniques to detect subtleties in the underlying operating system network stack of the computers you are scanning. It uses this information to create a 'fingerprint' which it compares with its database of known OS fingerprints (the nmap-os-fingerprints file) to decide what type of system you are scanning.

-p ports to scan. Example range: '1-1024,1080,6666,31337'
Specify a range of ports to scan

-F Only scans ports listed in nmap-services
Pretty self explainatory!

-v Verbose. Its use is recommended. Use twice for greater effect.
Print more useful information to stdout.

-P0 Don't ping hosts (needed to scan www.microsoft.com and others)
Some hosts don’t respond to ICMP Ping requests, even though they are still alive. You will need to use this option for this type of host.

-T General timing policy
General timing policy is basically the rate at which packets are sent out. Main question here, is do you care if the network administrator for the IP or block you are scanning knows you are scanning it?

-oN/-oX/-oG Output normal/XML/grepable scan logs to

-iL Get targets from file; Use '-' for stdin

*** -S /-e Specify source address or network interface**
--interactive Go into interactive mode (then press h for help)

Usage Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'

Options Summary

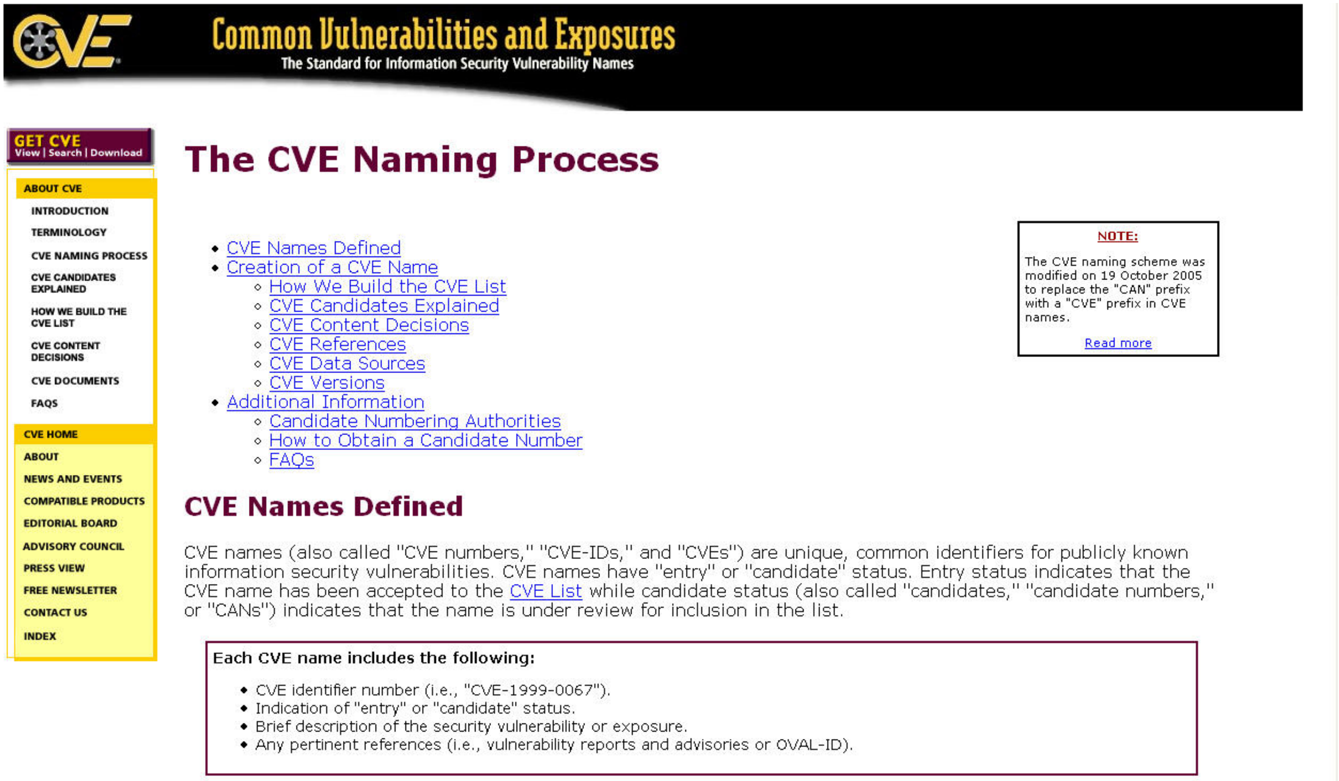
This options summary is printed when Nmap is run with no arguments, and the latest version is always available at http://insecure.org/nmap/data/nmap.usage.txt. It helps people remember the most common options, but is no substitute for the in-depth documentation in the rest of this manual. Some obscure options aren't even included here.

```
Nmap 4.20ALPHA11 ( http://insecure.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sP: Ping Scan - go no further than determining if host is online
  -P0: Treat all hosts as online -- skip host discovery
  -PS/PA/PU [portlist]: TCP SYN/ACK or UDP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idlescan
  -sO: IP protocol scan
  -b <ftp relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080
  -F: Fast - Scan only the ports listed in the nmap-services file)
  -r: Scan ports consecutively - don't randomize
```

```
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
OS DETECTION:
  -O: Enable OS detection (try 2nd generation w/fallback to 1st)
  -O2: Only use the new OS detection system (no fallback)
  -O1: Only use the old (1st generation) OS detection system
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in milliseconds, unless you append 's'
  (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T[0-5]: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <time>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use twice for more effect)
  -d[level]: Set or increase debugging level (Up to 9 is meaningful)
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Insecure.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enables OS detection and Version detection
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sP 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -P0 -p 80
```

Credits and Information

MITRE
Mitre.com
For use of their CVE resources



The CVE Naming Process

- CVE Names Defined
- Creation of a CVE Name
  - How We Build the CVE List
  - CVE Candidates Explained
  - CVE Content Decisions
  - CVE References
  - CVE Data Sources
  - CVE Versions
- Additional Information
  - Candidate Numbering Authorities
  - How to Obtain a Candidate Number
  - FAQs

NOTE:

The CVE naming scheme was modified on 19 October 2005 to replace the "CAN" prefix with a "CVE" prefix in CVE names.

Read more

CVE Names Defined

CVE names (also called "CVE numbers," "CVE-IDs," and "CVEs") are unique, common identifiers for publicly known information security vulnerabilities. CVE names have "entry" or "candidate" status. Entry status indicates that the CVE name has been accepted to the CVE List while candidate status (also called "candidates," "candidate numbers," or "CANs") indicates that the name is under review for inclusion in the list.

Each CVE name includes the following:

- CVE identifier number (i.e., "CVE-1999-0067").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).

PuTTY 0.56

www.chiark.greenend.org.uk

SnagIt software from TechSmith
http://www.techsmith.com

Reference source materials included:
http://www.oreillynet.com

Firefox
Mozilla.org

VMware resources
http://www.vmware.com/pdf/vi3_systems_guide.pdf