Viper IDS Sensor Release 1.0
User Documentation

Revision 1.0-03262003
(Draft – This document is subject)

Author: Joshua Jackson <jjackson@vortech.net>

Date: 02/06/2003

Table of Contents

Introduction

The Viper Intrusion Detection Sensor is a version of Embedded Coyote Linux that is designed to function as part of an intrusion detection network. The design goal for this project was to produce a system that could act as a remote intrusion sensor that relays its alert information back to a central database for logging any analysis.

The Embedded Coyote Linux project was started in December of 2000 and has progressed slowly as time permitted. Currently, the development team consists solely of the project's author Joshua Jackson (jjackson@vortech.net). Some additional suggestions and modifications have been submitted by various users over the past couple years.

To get the latest information and downloads for Embedded Coyote Linux projects, please visit the Coyote Linux project homepage at http://www.coyotelinux.com

Getting started with the Viper IDS Sensor

System Specifications

To prepare a system to run the Viper IDS Sensor, you will need to make sure you have at least the following:

Pentium 75Mhz or better processor
128Mb of RAM
32Mb IDE Drive - ATAPI Flash drives will work nicely.
At least 2 PCI network cards
CDROM Drive

The IDE storage that Viper is to be installed on to needs to be installed as the IDE primary master device.

As the network interface card (NIC) detection in Embedded Coyote Linux is intended to be automatic, only PCI interfaces are supported. This greatly simplifies the detection and configuration process for both the developers and the end users.

While many distributions of Linux will run on lesser systems, the functionality built into Viper requires at least the system specifications listed here. In particular, the attack signature detection engine (Snort) require a fair amount of processing power to keep up under heavy network loads.

If your network is under heavy utilization, you will want to greatly increase the processing power for the IDS sensor. While no exact measurements have yet been determined for Mhz per Mbps, it is recommended that a Pentium III class processor of 800Mhz or better be used on 100Mbps networks that experience frequent, heavy loads.

Installing the Viper IDS Sensor

To install Viper you will need to either download the CD image and create your own installation CD or you can order one from Vortech Consulting. Ordering information is available on the Coyote Linux web site or at the end of this document.

If you have downloaded the “viper.iso” from the Vortech Consulting download channels, you will need to create a CD using a CD mastering application. Nearly all CD mastering applications support the ISO9660 format.

Once you have booted the target machine from the installation CD, you will be asked to confirm installation of Viper. If a previous version of the sensor software is detected, you will also be given the option to perform an upgrade. Please note that all data on the primary IDE device will be erased during the installation process. The installation or upgrade process itself is fully automatic and takes less than a minute on most systems.

If the system that you are using for the IDS sensor is not capable of booting from the CDROM, you can also create boot disks from files contained in the /boot directory. You will need 2 1.44Mb floppy disks to create the boot disks from the boot.img and root.img files. These files need to be written to the floppy using the included rawrite utilities or using the unix utility “dd”. Rawrite is contained in the /utils directory of recent build. Be certain to read the README file for information on choosing the correct version of the utility for your operating system.

Upon booting the system for the first time after a new installation, you will be asked some basic questions about the desired configuration for the system. Options such as the hostname, domain name and the addresses for any network interface cards (NICs) that were detected will be automatically placed into an initial system configuration file. This configuration will then be loaded and can be edited from the main menu.

Setup Interview

When booting the system for the first time after installation, the initial configuration process will ask for the following information:

Hostname: This option specifies the name this particular firewall is to be given. Note this name should be unique throughout your network. If you have multiple IDS sensors that log to a central database, each system should have a unique hostname.

Domain Name: This should be the DNS domain name for your network. If you do not have a domain for your LAN, you can use the domain name of your ISP.

Interface Addresses: During setup, Viper will attempt to detect the network cards installed in your firewall. As mentioned in the system specifications, you need to use PCI network cards in your sensor systems. You can specify an address of "*dhcp*" first interface if it is to be configured using the DHCP.

The interface eth0 (the first detected interface) should be used as local area network connection. This interface will be used for communicating with the sensor and is used to send alert data back to the IDS database.

When specifying an IP address for an Interface, it should be in the format of *ipaddress/bitmask* (ie: 192.168.0.1/24).

Default Gateway: If you did not specify DHCP address assignment for any of the network interfaces, you will be asked to specify a default gateway address (next hop router).

DNS Server: This will allow you to specify a DNS server for name resolution on your network. If you do not have an internal DNS server configured, you can use the DNS servers for your ISP.

Administrator Password: This password will be stored for use with the users "admin", "root", and "debug". When logging into the sensor through the console or remote SSH/Telnet, the use of "admin" or "root" will place you directly into the administration menu. If you log in as "debug", you will be given an ASH shell prompt instead. Unless you are familiar with the command line and Linux in general, the use of the "debug" login is not recommended.

Remote SSH Address: This option will allow you to specify an address or network of addresses which will be allowed to connect to the firewall remotely using the telnet or SSH protocols. This address is in the same format as the *Interface Addresses*, specified above.

Remote MySQL Database: When an alert is generated by the sensor, it will be sent to a remote MySQL database for storage. The layout for this database can be found in the /docs directory on the Viper IDS Sensor CD. You will need to supply the name of the remote server, database, username, and password. Failure to supply a valid database configuration for logging will result in a non-functional sensor.

Update username and Password*: You will need to enter the username and password for the account you created when you purchased Wolverine. This account is the same as the one you use to log into the Coyote Linux (www.coyotelinux.com) or Vortech Customer Service (https://secure.vortech.net/login.php) web sites. If you do not currently have an account, you can sign up for one at the following location:

- https://secure.vortech.net/signup.php

* Commercial editions only

Once you have an account established, you can purchase a download subscription to the Viper IDS subscription channel. For more information on ordering a download subscription, please see the “Ordering Viper” section at the end of this manual.

Once the initial configuration has been loaded, your sensor should have network connectivity and can now be fine-tuned to meet the specific needs of the network it is protecting.

Using the Viper IDS Sensor

System Boot-up

During boot up, Viper will display various messages about the actions it is performing. If your sensor is not performing as expected, be sure to take note of any error messages that are displayed during the boot-up process.

System Shutdown

Unlike most Linux systems, you do not have to prepare a Viper IDS Sensor for shutdown. The boot filesystem is kept read-only during normal system operation. This allows for a cold power-down without risk of damaging the filesystem. The exceptions to this are during the editing of the system configuration or during a system image update. You should not power-down the firewall during these events.

Logging into the IDS sensor

Once the firewall has booted, you will be given a login prompt that will appear as follows:

```
Viper system login
testids login:_
```

The above example shows the hostname which was assigned to this firewall was "testfw". From here you can log in using the username "admin" with the password you assigned during system setup. You will then be presented with the system configuration main menu. From this menu you can reconfigure and control nearly all aspects of the sensor.

If you are familiar with Linux and want to access the underlying system, you can log in as the user "debug". This will give you a shell prompt instead of the main menu. Note that the use of the debug login is not recommended or supported.

System Console

If you are using a monitor and keyboard on the sensor, you can log in on any of three virtual terminals (TTY) with logging output available on a fourth. To switch between these terminals, hold down the ALT key and press F1 through F4.

While viewing output on any of the given TTYs, you can scroll back through the last several screens by holding down the CTRL key and using Page-Up and Page-Down.

If you have a hardware firewall from Vortech Consulting, you should refer to the firewall documentation for additional information on connecting to the console and logging ports.

System Main Menu

Once you have logged into Viper, you will be presented with the main system menu. From here you can save/restore your system configuration, edit the master config file, reboot or reload the system, or enter the system information menus.

Configuration backup and restore

The first two options on the main menu are used to save and restore your system configuration to a floppy disk. The disk that you use to store your configuration files on should be pre-formatted with an DOS FAT filesystem (these include factory pre-formatted floppies or those formatted in any version of Microsoft Windows or DOS). If you need to format a floppy disk in Linux, you can do so with the following commands:

```
fdformat /dev/fd0h1440
```

The above command will low level format the floppy to 1.44Mb capacity. If this completes without errors, you can create the FAT filesystem using either of the following commands:

```
mformat a:
mkdosfs /dev/fd0
```

If the first command does not work on your Linux system, try the second one. The use of the “mformat” command requires that the “mtools” package be installed; some distributions do not install this package by default.

Once you have a properly formatted floppy disk, you can back up your configuration using option 2 form the main menu. This will copy your system configuration and encryption identification keys to the disk. This floppy can be used to configure another, identical sensor using option 1 from the main menu.

NOTE: The files contained on the system backup floppy contain security sensitive information about your sensor. This floppy must be kept secure or your IDS sensor security may be compromised.

Updating the sensor software

* NOTE: Not active yet!!

From the main menu, you can download an update to your firewall software using option 3. This option can be used to download updates from the official Coyote Linux update server or from an FTP server of your choice (handy if you have the developer's kit and have made custom modifications to the sensor software).

If you are updating from a server other than update.coyotelinux.com, you will be asked to specify the source directory and authentication information for the server you have selected. The files on the source FTP server are expected to match those that would be present on the official server (a kernel image, ramdrive image, image version information file, IDS signature rule definitions, and a checksum file).

Before downloading the update, Viper will attempt to determine the build number of the update files. If your system is up to date or running a newer build than the one present on the update server, you will be asked to confirm the download action before it is carried out.

After the new files are downloaded, the integrity of the downloaded files will be checked using the MD5 hashes present in the checksum file downloaded during the update. If the files do not pass the integrity check, the update will not be performed.

Editing the main configuration file

From the main menu, you can edit the main system configuration file using option 4. The editor that is opened by default is GNU “nano”. This editor is very similar to “pico” on other Linux or BSD based systems. If you are not familiar with either of these editors, some keyboard shortcuts that you may find handy:

Ctrl-o - Save the current file
Ctrl-x - Exit the editor
Ctrl-v - Page Down
Ctrl-y - Page Up
Ctrl-^ - Set Mark
Ctrl-k - Cut Line / Marked text
Ctrl-u - Paste text

When you edit the master configuration file, your changes do not go into affect immediately. For this, you will need to reload or reboot the system.

Rebooting or Reloading the system

Options 5 and 6 on the main menu allow you to reboot or reload the system. Most changes to the sensor configuration will not require you to reboot. The exception to this would be downloading a system update; you must reboot for the system update to to take affect.

Viper IDS Sensor System Configuration

Network Interface Configuration

As of this writing, only PCI Ethernet network interfaces are supported by Embedded Coyote Linux. Support for USB and dial-up serial modems are being considered but ISA and PCMCIA types will not likely be supported by this product.

Viper uses the standard Linux naming scheme for any network interface adapters present in the system. The first interface in the firewall will be listed as "eth0", the second as "eth1" and so on.

LAN Interface

The Viper configuration system normally assumes that the first interface in the system is connected to the local network segment. This interface is used for remote access to the sensor and to send alert and logging data to a LAN host. This interface should not be connected to an untrusted network segment that may be subject to packet sniffing by a malicious party.

Address Assignment

The Viper IDS Sensort allows for DHCP and static address assignment for the local network interface. If your LAN connection uses a DHCP configured address, you can enable DHCP address assignment with the following statement:

```
interface eth0 address dhcp
```

Controlling ICMP Responses

A frequently asked question is how to get the system to respond to ICMP requests. This can be accomplished using the "icmp" directive. Care should be taken when enabling ICMP responses to the Internet or other untrusted networks. A commonly used denial of service (DoS) relies on ICMP responses from a network host. Enabling ICMP responses from the sensor itself can lead to problems if you come under such an attack.

To get the sensor to respond to the typical "ping" request, the following command can be used:

```
icmp permit any echo-request eth0
```

If you want to enable all ICMP message types (should only be performed on a trusted segment), you could use a command such as:

```
icmp permit 192.168.0.0/24 all eth0
```

Configuring external logging

By using the "logging" directive, it is possible to send Wolverine's system logging information to a remote host. This requires a syslog server to be running on the remote host which is configured to accept external logging information. To enable remote logging on Wolverine, use the following statement:

```
logging host 192.168.0.3
```

Where 192.168.0.3 is the host running the syslog server. With most Unix implementations, enabling the syslogd daemon to accept external logging information is accomplished by adding a "-r" to the command line. On Red Hat Linux, you can enable this feature by editing the /etc/sysconfig/syslog file and editing the line that reads:

```
SYSLOGD_OPTIONS="-m 0"
```

to

```
SYSLOGD_OPTIONS="-m 0 -r"
```

You will also need to restart the system loggers with the command:

```
service syslog restart
```

You should not enable remote logging on a host which can be logged to (uncontrolled) from the Internet. This can lead to a DoS attack against your server. If your logging server is publicly accessible, be sure to at least set the firewall rules to only permit logging data from authorized hosts.

Configuration Reference

This is a list of directives that can be used in the Viper IDS Sensor configuration file. If you are familiar with the Cisco PIX firewalls, this configuration system will seem very familiar to you.

This configuration file is loaded and parsed during system boot-up or when a reload is forced. The location of this file is /etc/coyote/sysconfig (which is symlinked to /coyote/config on the parent, boot filesystem). When this file is parsed, it is also sorted and invalid directives are removed before it is passed to the system config script. The parsed and sorted version of this file that is actually loaded can be found in /tmp/running-config.

clock

clock timezone <zone>

Sets the timezone for the firewall.

zone - Timezone name. Valid entires are:

CST, GMT, GMT+1, GMT+2, GMT+3, GMT+4, GMT+5, GMT+6, GMT+7, GMT+8. GMT+9, GMT+10, GMT+11, GMT+12, GMT-1, GMT-2, GMT-3, GMT-4, GMT-5, GMT-6, GMT-7, GMT-8. GMT-9, GMT-10, GMT-11, GMT-12, UTC, CST, EDT, EST, MST, PST

Note: The timezone names should be specified in upper case (just as listed above).

clock server <host>

host - The host to sync the firewall time to.

Examples:

```
clock timezone EST
clock server time.nist.gov
```

config

config version <xx.xx>

Specifies the configuration version number. This directive will eventually be auto-generated by the configuration editor and should not be altered directly.

domain-name

domain-name <domain>

Set the default domain name for the firewall.

domain - The domain name to use

hostname

hostname <hostname>

Sets the hostname of the firewall

hostname - The hostname to use for the firewall.

icmp

icmp deny <interface>

This command technically does nothing. The denial of ICMP packets is the default behavior for Wolverine. This command is included simply to more closely mimic the PIX config structure.

icmp permit <ip_address/netmask> <icmp-type> <interface>

Allows ICMP requests on a given interface.

ip_address/netmask - Specifies the host or network that ICMP packets should be accepted from.
icmp-type - The numeric or text (see text type list below) ICMP message type to permit
interface - The interface name or alias

Examples:

```
icmp permit 192.168.0.0/24 echo-request eth0
icmp permit any all eth1
```

ICMP text types that are permitted:

```
echo-reply
destination-unreachable
  network-unreachable
  host-unreachable
  protocol-unreachable
```

port-unreachable
fragmentation-needed
source-route-failed
network-unknown
host-unknown
network-prohibited
host-prohibited
TOS-network-unreachable
TOS-host-unreachable
communication-prohibited
host-precedence-violation
precedence-cutoff
source-quench
redirect
network-redirect
host-redirect
TOS-network-redirect
TOS-host-redirect
echo-request
router-advertisement
router-solicitation
time-exceeded
ttl-zero-during-transit
ttl-zero-during-reassembly
parameter-problem
ip-header-bad
required-option-missing
timestamp-request
timestamp-reply
address-mask-request
address-mask-reply

Note: The use of "any" for the IP address will permit ICMP from any host on the given interface

Note 2: The use of "all" will permit all ICMP types

interface

interface <ifname> <**module** | **address** | **public** | **mtu**> <mod_name | ip_address/netmask | **dhcp** | mtu_size> [**down** | **secondary**]

Sets various parameters about the network interfaces that are present in the firewall.

ifname - Specifies the name (eth0, eth1, etc) of a given interface. With the exception of the "module" directive, this can also be an alias specified by a "nameif" statement.
module - Used to indicate the module (driver) needed by the interface
address - Used to indicate the IP address or method of obtaining an IP address for the interface

public - Defines a given interface as "public". This is typically used to indicate the interface that is attached to the Internet.
mtu - Used to specify the MTU size of an interface.
mod_name - Used in conjunction with the "module" directive. Specifies the actual module name (less the .o).
ip_address/netmask - Used in conjunction with the "address" directive. Specifies the ipv4 address and number of subnet bits for the interface
dhcp - Used in conjunction with the "address" directive. Indicates that the interface should obtain its address using DHCP.
down - Indicates that the specified interface should be kept offline.
secondary - Used in conjunction with the "address" directive. Indicates that this address is in addition to the "primary" address and should not overwrite any address information that is currently configured. Do not attempt to assign secondary addresses to an interface that was configured using DHCP or PPPoE as the processes responsible for these types of address assignments do not honor the fact that a secondary address has been assigned during address negotiation (in short, the secondary addresses will get wiped out).

Examples:

```
interface eth0 module eepro100
interface eth1 module 3c59x
interface eth0 public
interface eth0 address 192.168.0.1/24
interface eth1 address dhcp
interface eth0 mtu 576
```

Note: The use of the "module" directive must always precede the use of any other interface directives.

Note 2: When specifying a static IP address, be sure to include the /## prefix-style netmask. If this is not specified, the default IP class mask will be assigned.

logging

logging host <ip_address>

Specifies a remote host to send syslog data to. If no logging host is specified, all data will be logged to the console.

name-server

name-server <server_address>

Adds a DNS server address to the list of servers to use for name resolution.

server_address - The IP address of a server to use for name resolution

password

password <**user** | **monitor** | **admin** | **debug**> <data> [encrypted]

Specifies the various passwords for the user, monitor, and admin level security. Currently, only the "admin" and "debug" levels are actually supported.

When logging into Wolverine, the "admin" login will give you the main menu immediately after logging in, while the "debug" login will give a BASH shell prompt.

When using the main menu option to edit the system configuration, any passwords specified with this command will be automatically encrypted when you leave the editor.

Note: When logging is as the admin user, you can also use the login name of "root".

route

route <source/mask> <gateway> [**dev** ifname] [**metric** metric_num]

Establishes static routing information.

source/mask - The source network number and bit mask.
gateway - The remote IP address to route traffic through
ifname - Specifies the network interface to use for this route. "ifname" should be the interface identifier (eth0, eth1, etc).
metric_num - Specifies a metric for this route.

snmp

snmp <contact | location | host> <data>

Sets various parameters which are passed to the internal SNMP service.

contact - Specifies the contact name for the firewall.
location - Specifies the system location
host - Indicates a host IP address that is allowed to query the SNMP service.
data - A string containing the text data for the above directives

NOTE: In order to use the SNMP server, the domain name and DNS servers must be specified or the SNMP service will fail to start properly. These can either be specified via the "domain-name" and "name-server" directives, or from the automatic specifications provided by using a DHCP assigned Internet address.

ssh

ssh <address[/mask]>

Sets allowed hosts for ssh access to the firewall

Example Configurations

This section contains some diagrams and sample configurations for typical Viper IDS Sensor applications. For these examples, some assumptions are:

192.168.x.x are used to indicate private address ranges
172.20.x.x are used to indicate public, Internet routeable addresses.

Even though 172.20.x.x is defined for private use, they represent what would normally be Internet routeable addresses for the purpose of these examples.

General IDS Sensor configuration

Configuration:

```
# Viper IDS Sensor Configuration File
config version 1.0
hostname testids
domain-name testdomain.com
clock timezone EST
clock server time-b.nist.gov
name-server 172.20.0.100
password admin xxxxxxxxxxxx encrypted
password debug xxxxxxxxxxxx encrypted
interface eth0 module ne2k-pci
interface eth1 module 3c59x
interface eth0 address dhcp
database 192.168.0.25 idsdb idsuser idspassword
ssh 0.0.0.0/0
```

This configuration shows a typical sensor setup with the LAN connection being assigned an address by a DHCP server. The sensor alert data is sent to a remote MySQL database server at 192.168.0.25 with a database name of *idsbd*, a database username of *idsuser*, and the database password of *idspassword*.

Ordering Viper

While Viper is in its initial development stages, it is publicly available for download. Once it is complete, a commercial version will be made to provide additional support and update options to paying customers. Additional details about commercial products and services will be made available at a later date.

Educational or Reseller licensing

If you would like to use an Embedded Coyote Linux product in an educational facility or would like to become an authorized reseller, please contact Joshua Jackson at Vortech Consulting (jjackson@vortech.net) for further information. Educational facilities may qualify for a free site license and resellers can obtain quantity discounts.

Ordering media kits

If you would like the CD-ROM and manual for Embedded Coyote Linux products, you can order these directly from the Vortech Consulting online store. The store is linked from the Vortech homepage at http://www.vortech.net.