Rainer's Technical Tips

Installing a Network-Based Intrusion Detection

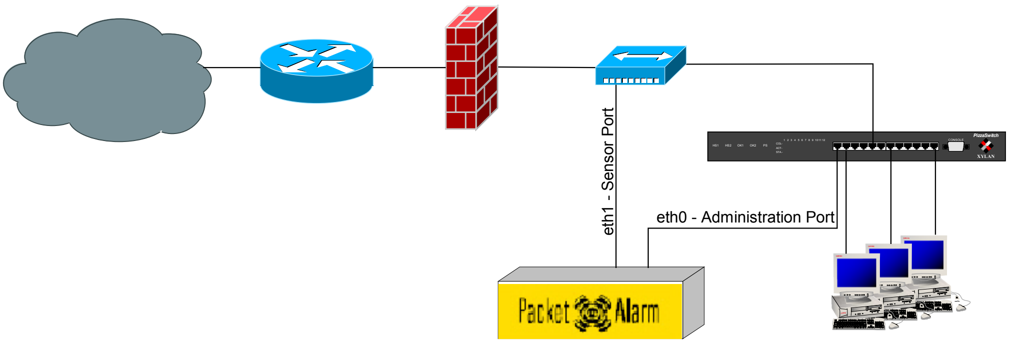
created by: Rainer Bemsel – **Version** 1.0 – **Dated:** Apr/10/2003

The purpose of this document is to help you installing a Network Based Intrusion Detection, where Manager and Network Sensor sits on a single machine. The PC is equipped with 2 Intel Pro 100 Network Interface cards, where one NIC is used for Management and the other NIC is attached to a hub for listening to all traffic. You also can use a "mirrored" port on a switch. So, for a self-starter, this might be a good start to learn about IDS.

I've used in this example Packet Alarm IDS, by VarySys Technologies

Packet Alarm

Network Drawing



Computer Specs, I've used

Intel Pentium 4
1.0 Ghz
128 MB RAM
20 GB Harddisk
CD ROM
2x Intel Pro/100 (PCI)

Rainer's Technical Tips

DISCLAIMER

This Technical Tip or TechNote is provided as information only. I cannot make any guarantee, either explicit or implied, as to its accuracy to specific system installations / configurations. Readers should consult each Vendor for further information or support.

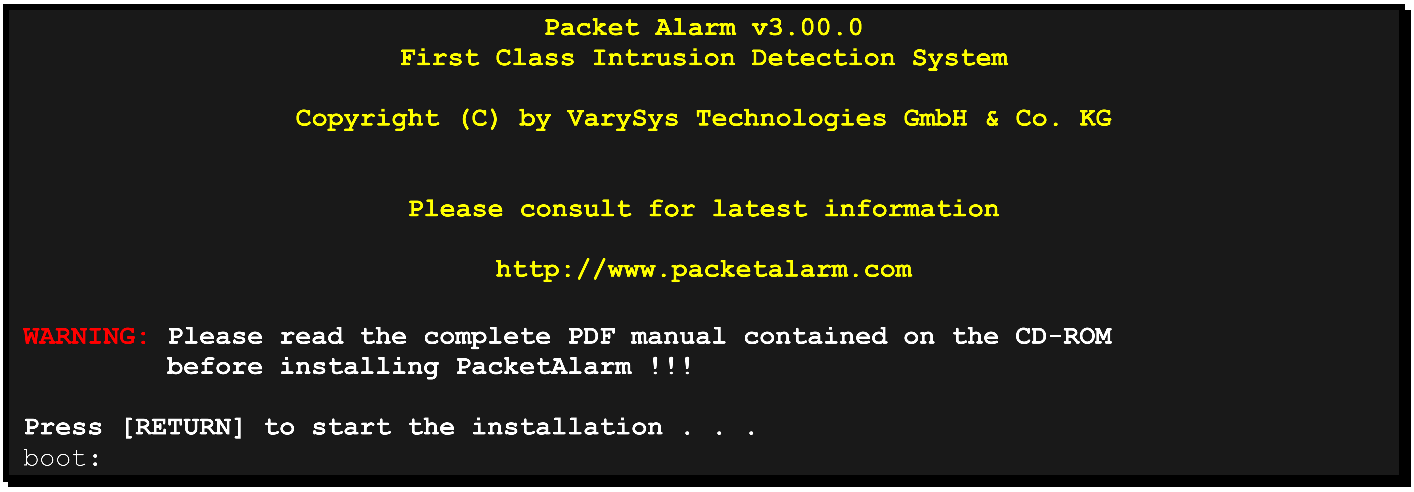
Although I believe the information provided in this document to be accurate at the time of writing, I reserve the right to modify, update, retract or otherwise change the information contained within for any reason and without notice. This technote has been created after studying the material and / or practical evaluation by myself. All liability for use of the information presented here remains with the user

Installation Process:

Note: If you do not have a Packet Alarm product available, you can download a demo version from their website at: http://www.packetalarm.com

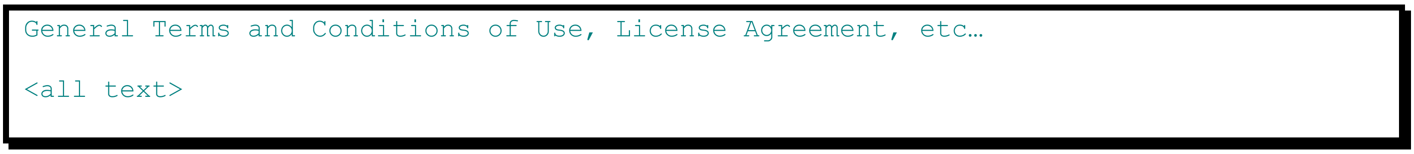
Insert Packet Alarm CD Rom into the CD Drive and perform a cold-boot, to be sure, that Computer starts from CD ROM. *(If CD ROM does not start, you may have to change boot-order at BIOS setup)*

This is the first initial Setup Screen, you will get.



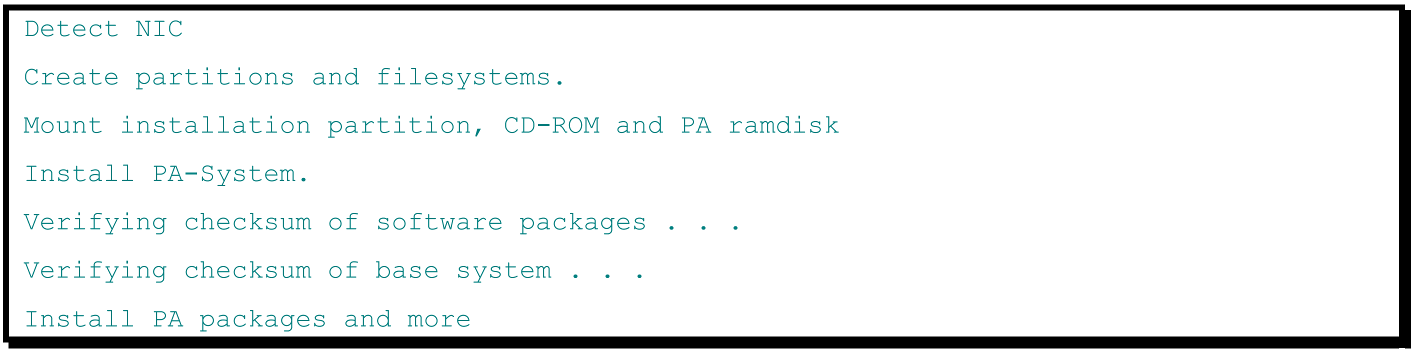
```
                        Packet Alarm v3.00.0
               First Class Intrusion Detection System

          Copyright (C) by VarySys Technologies GmbH & Co. KG


                 Please consult for latest information

                       http://www.packetalarm.com

WARNING: Please read the complete PDF manual contained on the CD-ROM
         before installing PacketAlarm !!!

Press [RETURN] to start the installation . . .
boot:
```

There will be a couple of scripts running, until it comes up to



```
General Terms and Conditions of Use, License Agreement, etc…

<all text>
```

With Arrow-Down, you can browse the complete agreement. You have to accept, to be able to continue. Again, some automatic scripts are running.



```
Detect NIC
Create partitions and filesystems.
Mount installation partition, CD-ROM and PA ramdisk
Install PA-System.
Verifying checksum of software packages . . .
Verifying checksum of base system . . .
Install PA packages and more
```

```
Please select kernel image

Single Processor Kernel (   )
Multi Processor Kernel (  )


[OK]
```

You can jump between toggle fields with TAB and space bar will change toggle. I've select Single Processor Kernel. On the next screen you will be asked for administration interface:

```
Please select the network interface, which should be used to administrate the system.
The IP Address will be bound to this interface.

If       Vendor              Card                           Supported  Admin

Eth0     Intel Corp          82557/8/9 [Ethernet Pro 100]   yes        ( X )
Eth1     Intel Corp          82557/8/9 [Ethernet Pro 100]   yes        (   )
Eth2     Silicon Integrat    SiS900 10/100 Ethernet         yes        (   )


[OK]
```

You can jump between toggle fields with TAB and space bar will change toggle. The next step will be an automatic process.

```
Creating recovery image . . .
```

You can jump between toggle fields with TAB and space bar will change toggle. The next step will be an automatic process. Finally, you will be notified that installation has been finished (if everything worked properly)

```
         ==================================================================
                 The installation has been finished successfully
         ==================================================================


Please remove the CD ROM from the drive and press RETURN. The system will be rebooted
to finish the installation of the software

When the system has booted you will see the login prompt

      pa login:

You have to login with the username 'admin' and no password to complete the basic
configuration of the system.

<more text>
```

When system has been booted up you should be prompted with ‘pa login:’

```
Basic Configuration - Please select the system type

Sensor/Manager ( X )
Manager      (   )
Sensor (   )
```

```
Basic Configuration - Hostname and IP Settings

Hostname                 N-IDS
IP Address               192.168.10.150
Netmask                  255.255.255.0
Default Gateway          192.168.10.1

Primary DNS              212.185.252.201
Secondary DNS            212.185.253.9
```

```
Basic Configuration - Admin Password

Attention: US keyboard layout is used. If you are using a non-US keyboard watch the
different location of some keys:

Password
Retype Password
```

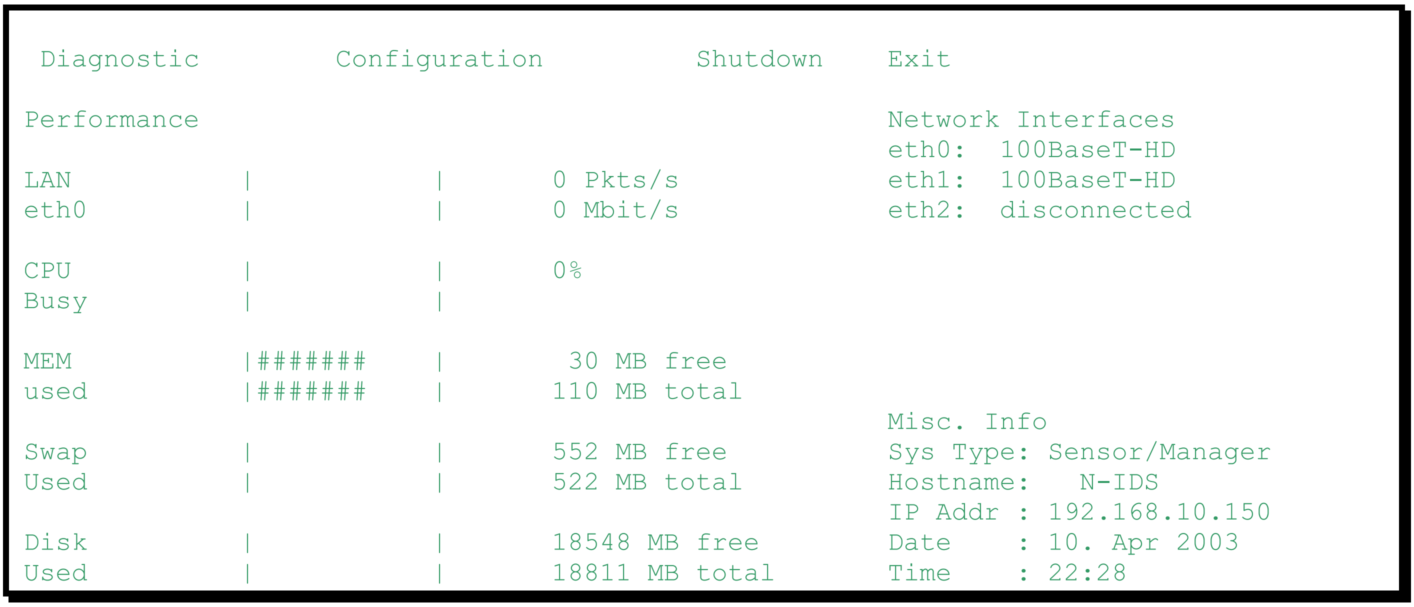
```
System successfully configured

             [OK]
```

Note: You can change keyboard layout, at Status Screen under CONFIGURATION

The system will reboot for the last time, during this setup.

You will be prompted with:
N-IDS login: **admin** *(or the hostname, you have defined)*
Password: *(type the password, you have defined)*

You will get into the System Overview Screen



```
 Diagnostic         Configuration          Shutdown    Exit

Performance                                            Network Interfaces
                                                       eth0:  100BaseT-HD
LAN           |           |      0 Pkts/s              eth1:  100BaseT-HD
eth0          |           |      0 Mbit/s              eth2:  disconnected

CPU           |           |      0%
Busy          |           |

MEM           |#######    |       30 MB free
used          |#######    |      110 MB total
                                                       Misc. Info
Swap          |           |      552 MB free           Sys Type: Sensor/Manager
Used          |           |      522 MB total          Hostname:   N-IDS
                                                       IP Addr : 192.168.10.150
Disk          |           |      18548 MB free         Date    : 10. Apr 2003
Used          |           |      18811 MB total        Time    : 22:28
```

Well, that's pretty much the initial setup of a Network-Based Intrusion Detection System. There is another document available, where I've described the basic configuration of the System.

It 's available on Rainer's TechTips at www.bemsel.com/TechTip