Chapter 2

Installation

Solutions in this chapter:

- Downloading the OSSEC HIDS
- Building and Installing the OSSEC HIDS
- Performing a Local Installation
- Performing Server-Agent Installations
- Streamlining the Installations

☑ Summary

☑ Solutions Fast Track

☑ Frequently Asked Questions

Introduction

Simran Singh looks at her watch in disgust as she leaves the meeting room. "I told Bob this would happen," she says calmly to Marty Feldman, her second in command and confidant. "But did they listen? Now I have to somehow try to install safeguards on all our systems with what's left of our department's budget."

Simran rose through the ranks of North America's premier defense company due to her mix of business savvy, security knowledge, and track record for fixing impossible solutions. She is known throughout the company for never having to ask for more money than her department is allocated. Simran is also the most respected security mind in the company. During her first week, she was immediately dedicated as part of the incident handling team responsible for handling a companywide worm outbreak. Her superiors were so impressed by the way she operated, before long she was leading the teams of handlers for all the critical incidents in the organization. Within two years, she was head of the department and continued to prove herself by reducing enterprise-wide incidents by 66%. It was no surprise to her employees, peers, and senior managers when she was unanimously nominated for the recently vacated Chief Information Security Officer (CISO) position. Although Simran would prefer to receive the promotion under less hostile circumstances, she completely understands why out-going CISO Bob Rogers is no longer a viable option to continue in the role. Bob spends most of his time on the golf course instead of listening to the department warnings about difficult to protect network entry points. His failure to listen to his team is his downfall. The completely preventable breach, which resulted in the theft of top-secret ballistic missile guidance software, had cost the company its largest contract in 10 years and damaged its reputation with all existing customers.

"What's the plan, boss?" Marty asked Simran, already knowing that her mind was spinning and formulating a plan of attack. "Well, we used our entire budget on those redundant perimeter firewalls and intrusion prevention systems to help mitigate denial of service attacks," mused Simran. "So we have a hard candy shell and a soft, chewy center?" laughed Marty. "And we're all out of money for nougat!" exclaimed Simran. "What about that open source HIDS tool we saw on the SANS Institute webinar a few weeks back?" asked Marty. "Do you think that would do the trick?" Simran remembered that OSSEC sounded like a very capable and feature-rich HIDS, and had jotted some notes in her notebook to follow up on at a later time. "Good idea, Marty," said Simran, thinking that this was the exact reason why you should always surround yourself with smart people. Smart people come up with creative ideas, and creative ideas must be considered. "Can you do some further investigation into this OSSEC application and get back to me by the end of the week?" Marty looked at his Smartphone and noted that it was already

Thursday. Marty didn't miss a beat and simply answered, "Can do, boss!" Marty knows that the end of this week is a hard deadline. He has worked for Simran long enough to know when something was important enough to be asked to pull an all-nighter. As Marty exited the elevator he thought, "If I can't get this done by Friday, there might be another witch hunt upstairs next week." Marty chuckled under his breath, "If I don't play my cards right, then I might be promoted next." Never had the thought of a promotion had such ominous overtones.

"Boss! Boss!!" Marty yelled as he ran across the lobby toward Simran. "Have you been here all night?" asked Simran, already knowing the answer. Marty was unshaved, wearing yesterday's clothes, and had enough caffeine in him that he could probably fly around the world a few times on his own power. "Of course I've been here all night!" raced Marty. His eyes were blinking faster than his lips were moving. Simran laughed and wondered if he was trying to use his eyes to explain his findings using Morse code at the same time he was talking to her. "I listened to the webcast again, went to the OSSEC Web site, downloaded the software, read the documentation, joined the mailing list, and then searched the mailing list archives, and you know what?" Marty said, his mouth starting to get dry, and seemingly waiting for a response. "What, Marty?" asked Simran. "Hey! It's raining out?" asked Marty, staring past Simran. Simran snapped her fingers. "Stay on target, stay on target," said Simran, knowing Marty would appreciate the Star Wars reference. "Ha! Sorry, running on fumes here!" exclaimed Marty. "There are quite a few OSSEC deployments out there and lots of people are using the deployments in an enterprise environment. Even some Telco-sized organizations have deployed OSSEC on thousands of machines and couldn't be happier with it and they say that scalability isn't a problem, which we are always worried about because we're a huge company and we're starting to grow and our number of systems is growing exponentially, am I right or what? Boy I could use a coffee." Simran handed her latte to Marty. "Cheers!" exclaimed Marty, taking a huge gulp. "Will it work in a mixed environment?" asked Simran. "Totally! It works on Windows, Linux, Unix, Solaris, OS X, and a bunch of others!" yelled Marty, oblivious to the stares he was drawing from others in the lobby. "Indoor voice, Marty," said Simran. "So you've already installed it on some test servers, I assume?" Marty took another chug of his newly acquired latte, "Fifty or so…wait…maybe sixty-five…no fifty-five…sixty, definitely sixty!" Simran couldn't believe it. "That's quite the deployment for a test bed." Marty shrugged. "I had the time." He laughed. "It only took about five minutes per machine, which gave me plenty of time to tunnel into my boxes at home and install it on them as well. I guess that makes the total count sixty-five, if we include my systems." Simran smiled. "Marty, I think we've done it again. Let's have these systems run over the weekend and I'll draft a proposal to present on Monday. If all goes well," winked Simran, "we'll be deploying on our production servers in no time at all."

Notes from the Underground …

Linux, Unix, and BSD … Oh My!

Throughout this book, we mention the various popular operating systems on which the OSSEC HIDS can be installed. Please keep in mind that when we mention a particular operating system, it typically includes all the associated derivatives, or flavors, of that branch of operating systems, unless expressly stated otherwise.

Unix

When we refer to Unix, we are referring to any Unix-like operating system that does not fall into the BSD or Linux categories described. The Unix operating system was developed by a group of AT&T employees while working at Bell Labs. Examples of popular Unix flavors are:

- Sun Solaris
- OpenSolaris
- HP-UX
- IBM AIX
- IRIX
- Etc.

BSD

When we refer to BSD, we are referring to all Berkeley Software Distributions. BSD is a Unix derivative distributed and maintained by the University of California, Berkeley. Examples of popular BSD flavors are:

- FreeBSD
- NetBSD
- OpenBSD
- DragonFlyBSD
- OpenDarwin
- Mac OS X
- And so on

Linux

When we refer to Linux, we are referring to all Unix-like operating systems that use the GNU/Linux kernel architecture. The Linux kernel, released in 1991, is one of the best examples of a free and open source development initiative. Examples of popular Linux distributions are:

- Slackware
- Debian
- Ubuntu
- Red Hat Enterprise Linux
- CentOS
- Fedore Core
- Mandriva
- openSUSE
- Gentoo
- Linspire
- And so on

If for some reason your operating system does not fall into one of the Unix-like operating system categories, please consult your operating systems documentation and the OSSEC mailing list to find out if an OSSEC installation is possible.

Downloading OSSEC HIDS

The OSSEC HIDS is most commonly downloaded, compiled, and installed from its source code form. Precompiled packages are not currently available from www.ossec.net, with the exception of the Windows agent. However, the compiling, configuring, and installation of the OSSEC HIDS software is all handled with a single and simple to use script.

On Linux- or BSD-based systems, the installation begins the same way regardless of which install type you select. For Windows, an executable installer is provided and performs the agent install type.

NOTE

On most operating systems, the OSSEC HIDS can be installed with any of the three installation types. On Windows, however, only the agent install type is available. This means that protecting Windows hosts with the OSSEC HIDS always requires a server installation on one of the other operating systems.

Getting the Files

All the OSSEC HIDS files needed for installation to any operating system are available at the www.ossec.net/files/ Web site. There are three files of interest to us: the main source tar file, the Windows agent installer, and the checksum file.

The main source tar file contains the complete source code for the OSSEC HIDS, including the Windows agent code. Because Unix- and Linux-based operating systems provide complete development tools, the main source tar file contains everything needed to install the OSSEC HIDS. For Microsoft Windows, the installation is more complex and development tools are not readily available to build the OSSEC HIDS software. Because no development tools are available, an executable, GUI-based installer is provided that installs a precompiled OSSEC HIDS service. The third file is a checksum file used to validate the integrity of the downloaded files.

From the following URLs, download the main source tar file, the Windows agent installer, and the checksum files, using a browser or command-line utility such as wget:

- www.ossec.net/files/ossec-hids-1.4.tar.gz
- www.ossec.net/files/ossec-agent-win32-1.4.exe
- www.ossec.net/files/ossec-hids-1.4_checksum.txt

The checksums are provided to ensure the integrity of the downloaded files and allow you to check for file corruption or unintentional modification. If these checks fail, you will have to try the download again. From the command line, change to the directory where you saved the downloaded files and verify the checksums.

```
# md5sum -c ossec-hids-1.4_checksum.txt
ossec-hids-1.4.tar.gz: OK
ossec-agent-win32-1.4.exe: OK
```

NOTE

On some systems, the command *md5sum* might only be available as *md5*.

Preparing the System

Because the OSSEC HIDS installer must compile the application from source code the first time it runs, a working build environment is required on your system. For most operating systems of the Linux or BSD persuasion, a C compiler and supporting files is already be installed. If not, you must install *gcc* and *development headers* before proceeding.

NOTE

Make sure you review the system requirements in Chapter 1—Getting Started; otherwise, the OSSEC HIDS software might fail to build, causing the installation to abort.

Building and Installing

Whether you are doing a *local* or *server* installation, the first stage is the same. Extract the .tar.gz file, change into the created directory, and then run the install script.

```
# gunzip -c ossec-hids-1.3.tar.gz | tar -xf -
# cd ossec-hids-1.3
# ./install.sh
```

The installation script is divided into several steps to guide you through the installation. The steps are slightly different for each install type. However, the initial screen is the same for all installations and allows you to choose your preferred language. Here we choose the default *en* for English by pressing **Enter**.

NOTE

Values shown within braces, such as [en] on the installation language selection screen, are the default values for the associated installation option. Press **Enter** to confirm using the default option. Typically, the system defaults are sufficient, but please adjust the values as required by your installation requirements.

```
** Para instalação em português, escolha [br].
** 要使用中文进行安装, 请选择 [cn].
** Fur eine deutsche Installation wohlen Sie [de].
** For installation in English, choose [en].
** Para instalar en Español , eliga [es].
** Pour une installation en français, choisissez [fr].
** Per l’installazione in Italiano, scegli [it].
** 日本語でインストールします．選択して下さい [jp].
** Aby instalowa w jzyku Polskim, wybierz [pl].
** Для инструкций по устаноВке на русскоМ ,ВВеДите [ru].
```

```
  ** Za instalaciju na srpskom, izaberi [sr].
  ** Türkçe kurulum için seçin [tr].

(en/br/cn/de/es/fr/it/jp/pl/ru/sr/tr) [en]:

OSSEC HIDS v1.4 Installation Script - http://www.ossec.net
You are about to start the installation process of the OSSEC HIDS.
You must have a C compiler pre-installed in your system.
If you have any questions or comments, please send an e-mail
to dcid@ossec.net (or daniel.cid@gmail.com).

- System: Linux earth 2.6.20-16-generic
- User: root
- Host: earth

-- Press ENTER to continue or Ctrl-C to abort. --
```

Next, we press **Enter** to move to the selection of install type. At this point, you must decide which install type you require. You might now decide to jump ahead in the chapter to a specific install, but be sure to review all installation types because each type provides useful information about OSSEC HIDS components and features.

TIP

If you still have not decided which installation types you need, refer back to the section in Chapter 1 titled *Which Type Is Right for Me?*

Performing Local Installation

Local installations can only be done on Linux- and BSD-based operating systems, including Mac OS X. Start by choosing **local** installation in step 1 and then a directory location in step 2. The defaults are shown in square braces and can be accepted by pressing **Enter** or customized as in the case where we have chosen /opt/ossec instead of /var/ossec.

NOTE

The default location for the OSSEC HIDS is the /var/ossec directory. The location is not important as long as it is made to a directory where only the root user has write permissions. Wherever there is a reference to /var/ossec, you can substitute your preference.

```
1- What kind of installation do you want (server, agent, local or help)? local
   - Local installation chosen.
2- Setting up the installation environment.
  - Choose where to install the OSSEC HIDS [/var/ossec]: /var/ossec
    Installation will be made at /var/ossec .
```

Step 3, and the corresponding substeps, deal with notifications and alerts. At this point, you must decide which features you want to enable. You can alter any of the choices later in the ossec.conf file or by reinstalling the OSSEC HIDS.

The OSSEC HIDS communicates alert conditions that require your attention through email. You should specify an email address you check frequently. The sooner you are aware of a new threat, the sooner you can respond before it becomes a major problem.

WARNING

Use caution when choosing an SMTP server for *local* and *server* installations. You must be sure that SMTP relaying is permitted from the host running the OSSEC HIDS. Repeated denials on the SMTP server are likely to annoy your mail administrator. When in doubt, choose 127.0.0.1 and then alter the configuration after the installation, after you are certain of the correct address to use.

```
3- Configuring the OSSEC HIDS.
  3.1- Do you want e-mail notification? (y/n) [y]: y
   - What's your e-mail address? earth@localhost
   - We found your SMTP server as: 127.0.0.1
   - Do you want to use it? (y/n) [y]: y
   --- Using SMTP server: 127.0.0.1
```

The integrity check daemon is responsible for monitoring and reporting changes in system files. The rootkit detection engine regularly performs tests looking for evidence of an installed rootkit. Careful configuration of both services provides granular protection or notification of illicit file modifications, hidden network port activity, and other evidence of intrusion. The details of configuration and rule-tuning are addressed in later chapters. These features are very important for most HIDS solutions and should be enabled.

```
3.2- Do you want to run the integrity check daemon? (y/n) [y]: y
  - Running syscheck (integrity check daemon).
3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
  - Running rootcheck (rootkit detection).
```

Active response is a very powerful tool for taking automated actions to prevent intrusion or to reduce the extent of an intrusion. Often, an active response will block invasive activity much more quickly than you or your attacker can respond. If misconfigured, however, the active response can also lock you out of your system or interrupt vital services. By default, the OSSEC HIDS active response is quite safe and we recommend enabling it. Be sure, however, to have at least one or two well-trusted IP addresses in the white list so you can always access the system.

```
  3.4- Active response allows you to execute a specific
        command based on the events received. For example,
        you can block an IP address or disable access for
        a specific user.
        More information at:
        http://www.ossec.net/en/manual.html#active-response
   - Do you want to enable active response? (y/n) [y]: y
     - Active response enabled.
   - By default, we can enable the host-deny and the
     firewall-drop responses. The first one will add
     a host to the /etc/hosts.deny and the second one
     will block the host on iptables (if linux) or on
     ipfilter (if Solaris, FreeBSD or NetBSD).
   - They can be used to stop SSHD brute force scans,
     portscans and some other forms of attacks. You can
     also add them to block on snort events, for example.
   - Do you want to enable the firewall-drop response? (y/n) [y]: y
     - firewall-drop enabled (local) for levels >= 6
   - Default white list for the active response:
       - 192.168.65.2
   - Do you want to add more IPs to the white list? (y/n)? [n]: n
  3.6- Setting the configuration to analyze the following logs:
     -- /var/log/messages
     -- /var/log/auth.log
     -- /var/log/syslog
     -- /var/log/mail.info
- If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .
   --- Press ENTER to continue ---
```

After you press **Enter**, the OSSEC HIDS is compiled, installed, and configured with the options you specified. When the installation is complete, the installer script provides you with some final information. You should make note of the information and take any recommended actions. Typically, any platform-specific steps needed to make the OSSEC HIDS operate fully are provided. For example, for the OSSEC HIDS to use the OpenBSD pf firewall, some lines must be added to the /etc/pf.conf script. The lines and instructions are provided in the final information.

TIP

If the compilation of the OSSEC HIDS application fails, you do not get the informational screen indicating how to stop and start the OSSEC HIDS. Instead, you will see the line “Building error. Unable to finish the installation.” at the end of the compiler output.

This is typically related to a missing prerequisite. If this occurs, revisit Chapter 1 for tips on installing the correct build environment.

Now that the install is complete, we can start the OSSEC HIDS service by running the following command:

```
# /opt/ossec/bin/ossec-control start
```

Of course, with the initial configuration created by the installation script, the OSSEC HIDS might not do much for you just yet. In the next chapter, we cover altering the configuration to better suit your environment. With just a little more work, the OSSEC HIDS will become a powerful defensive tool against the invading hordes.

Tools & Traps…

Init Scripts—A Question of Timing

Depending on your platform, the OSSEC HIDS installer adds initialization scripts to start the OSSEC HIDS on your system. For systems that use SysV style initialization, primarily Linux, the script is added so that it starts for all common run levels. For BSD-style initializations, the script is added to the end of your /etc/rc.local script. In any case, but especially for BSD, you should review your system initialization to understand when the OSSEC HIDS starts compared with other services.

It is important with any security measure to make sure it is applied at the right point to avoid any unnecessary exposure or lapse in coverage. By ensuring that the OSSEC HIDS starts before network services, such as remote access or Web servers, you can be sure there are few momentary exposures.

With Linux, and other SysV style systems, the OSSEC HIDS has a start order that places it before most common network services for a *local* installation. For a *server* or *agent* installation, the OSSEC HIDS starts after all other network services, which is typically fine. In BSD, because the start is appended to the end of the /etc/rc.local script, the OSSEC HIDS starts after most network services, regardless of the install type. Depending on your system configuration, you might consider starting the OSSEC HIDS earlier, particularly if any other services take a long time to start.

Performing Server-Agent Installations

Server-agent installations are meant for a central controller with multiple agents, which is ideal for providing protection among networked hosts. It provides some advantages over simply having *local* installations on each host. This is because the server performs all log analysis for agents connected to it. Active responses are initiated from the server, but can be executed on an agent or all agents simultaneously.

Because Windows hosts can only be agents, a server is always required prior to installing the OSSEC HIDS on Microsoft Windows. Windows installations are covered separately in this chapter, after a Unix *server-agent* setup.

The *server* and *agent* installations proceed similar to the *local* installation, except that the server is configured to listen for communication from the agents.

Installing the Server

As with the *local* install type, *server* installations can only be done on Linux- and BSD-based operating systems, including Mac OS X. After the initial screen and language selection, we start by choosing ***server*** installation in step 1 and then a directory location in step 2. Defaults are shown in square braces and can be accepted by pressing **Enter**, or customized similar to the following:

```
1- What kind of installation do you want (server, agent, local or help)? server

  - Server installation chosen.

2- Setting up the installation environment.

  - Choose where to install the OSSEC HIDS [/var/ossec]: /var/ossec

    - Installation will be made at /var/ossec .
```

Step 3, and the corresponding sub steps, deal with notifications and alerts. At this point, you must decide which features you want to enable. You can alter any of the choices later in the ossec.conf file or by reinstalling the OSSEC HIDS.

WARNING

Use caution when choosing an SMTP server. You must be sure the SMTP server permits email to be relayed from the host running the OSSEC HIDS. Repeated denials on the SMTP server might annoy your mail administrator. When in doubt, choose 127.0.0.1 and then alter the configuration after you are certain of the correct address to use.

```
3- Configuring the OSSEC HIDS.

  3.1- Do you want e-mail notification? (y/n) [y]: y

    - What's your e-mail address? root@localhost

    - We found your SMTP server as: 127.0.0.1
    - Do you want to use it? (y/n) [y]: y
--- Using SMTP server: 127.0.0.1
```

The integrity check daemon is responsible for monitoring and reporting changes in system files. The rootkit detection engine regularly performs tests looking for evidence of an installed rootkit. These features are very important on most HIDS solutions and should be enabled. As with the local installation, these services, after being tuned, provide fine-grained protections.

```
3.2- Do you want to run the integrity check daemon? (y/n) [y]: y
  - Running syscheck (integrity check daemon).
3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y
  - Running rootcheck (rootkit detection).
```

Active response is a very powerful tool for taking automated actions to prevent intrusion or reduce the extent of an intrusion. Often, an active response can block invasive activity much more quickly than you or your attacker can respond. If misconfigured, however, active response can also lock you out of your system or interrupt vital services. By default, the OSSEC HIDS active response is quite safe and we recommend enabling it. Be sure, however, to have at least one or two well-trusted IP addresses in the white list so that you can always access the system.

```
3.4- Active response allows you to execute a specific
        command based on the events received. For example,
        you can block an IP address or disable access for
        a specific user.
        More information at:
        http://www.ossec.net/en/manual.html#active-response
  - Do you want to enable active response? (y/n) [y]: y
    - Active response enabled.
  - By default, we can enable the host-deny and the
    firewall-drop responses. The first one will add
    a host to the /etc/hosts.deny and the second one
    will block the host on iptables (if linux) or on
    ipfilter (if Solaris, FreeBSD or NetBSD).
  - They can be used to stop SSHD brute force scans,
    portscans and some other forms of attacks. You can
    also add them to block on snort events, for example.
  - Do you want to enable the firewall-drop response? (y/n) [y]: y
    - firewall-drop enabled (local) for levels >= 6
  - Default white list for the active response:
      - 192.168.65.2
  - Do you want to add more IPs to the white list? (y/n)? [n]: n
```

With a server installation, the OSSEC HIDS can receive alerts through an encrypted channel (port 1514) or through syslog (port 514). Enabling remote syslog allows the OSSEC

HIDS to receive alerts using syslog. Typically, it is better to use encryption for the transport of any security related information; you can choose to disable remote syslog for this reason. Remote syslog can be enabled or disabled at any time in the main configuration file. For the moment, leave it enabled. The significance of providing remote syslog becomes clear after the rule-tuning and log analysis sections of this book.

```
3.5- Do you want to enable remote syslog (port 514 udp)? (y/n) [y]: y
  - Remote syslog enabled.
3.6- Setting the configuration to analyze the following logs:
    -- /var/log/messages
    -- /var/log/auth.log
    -- /var/log/syslog
    -- /var/log/mail.info
  - If you want to monitor any other file, just change
    the ossec.conf and add a new localfile entry.
    Any questions about the configuration can be answered
    by visiting us online at http://www.ossec.net .
--- Press ENTER to continue ---
```

After you press **Enter**, the OSSEC HIDS is compiled, installed, and configured with the options you specified. When the installation is complete, the installer script provides you with some final information. You should make note of the information and take any recommended actions. For example, for the OSSEC HIDS to use the OpenBSD pf firewall, a few lines must be added to the /etc/pf.conf.

TIP

If the compile of the OSSEC HIDS application fails, you do not get the informational screen indicating how to stop and start OSSEC HIDS. Instead, you will see the line "Building error. Unable to finish the installation." at the end of the compiler output.

This is typically always related to a missing prerequisite. If this occurs, revisit Chapter 1 for tips on installing the correct build environment.

You now have a working *server* installation of the OSSEC HIDS. All binaries, scripts, and configurations for the OSSEC HIDS are in the installation directory you specified. To verify that everything is ok, start the OSSEC HIDS and complete the installation.

```
# /opt/ossec/bin/ossec-control start
```

Before moving on to setting up agents, remember that the OSSEC HIDS server needs to receive communication from agents on port 1514 and possibly 514. You must ensure that the firewall or packet filter on the server host machine allows this traffic. Each operating system and software distribution provides a way to do this. You must enable inbound UDP traffic on ports 1514 and 514 from any subnets where agents are installed. The firewall rule must maintain connection state because the agent expects responses from the server.

Managing Agents

Before moving on to another install type, let's review the key management in the OSSEC HIDS. Agents must be able to identify themselves to the server, and the server must be able to validate the identity of the agent. This ensures that illicit messages aren't processed by the server when sent from non-agent hosts.

The server-agent traffic is encrypted and validated using pre-shared keys. These keys must be generated on the server and then *imported* on the agent side. The procedure is the same regardless of the agent platform. All agent key management is done using the *manage_agents* utility in the OSSEC HIDS bin directory.

You must create a key for each agent by adding the agent using the *manage_agents* utility. Run the utility and then choose *Add an agent* by entering **A**.

```
# /opt/ossec/bin/manage_agents
****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
  (A)dd an agent (A).
  (E)xtract key for an agent (E).
  (L)ist already added agents (L).
  (R)emove an agent (R).
  (Q)uit.
Choose your action: A,E,L,R or Q: A
```

You are prompted for host details and an identifier for the agent. The IP address, not the hostname, of the agent host must be provided. The ID can be any number you choose, but it must be numeric. The name can be any identifying text that is meaningful to you, without spaces, but typically it makes most sense to use the hostname.

```
- Adding a new agent (use '\q' to return to the main menu).
  Please provide the following:
    * A name for the new agent: mars
    * The IP Address of the new agent: 192.168.65.40
    * An ID for the new agent[001]: 001
Agent information:
   ID:001
   Name:mars
   IP Address:192.168.65.40
Confirm adding it?(y/n): y
Agent added.
```

Repeat this procedure for each agent you must install. After you are done creating keys, restart the OSSEC HIDS service, using /var/ossec/bin/ossec-control, so that the OSSEC HIDS can read the updated keys and permitted agent IP addresses. Failure to restart the OSSEC HIDS server might result in connection failures for the agents. After the OSSEC HIDS software is installed on the agents, you will return to the server to retrieve the keys for each agent using the same *manage_agents* utility.

Installing Agents

Agent installation on Unix/Linux/BSD platforms is performed similar to the other install types. The only notable difference is that you must provide the server IP address. After installation, the agent does not start properly until the key, which is generated on the server, is imported.

For Microsoft Windows, the installation is also simple, but it is performed using a graphical installer. Importing the key from the server to the agent typically requires Secure Shell (SSH) access to the server, so make sure the Windows host has an SSH client.

TIP

After the install.sh script is successfully run once, the files are compiled. The install.sh script has a *binary-install* option that allows you to reinstall without recompiling every time. Also, by copying the install files to another host, you can perform the installation on multiple hosts without recompiling every time. This assumes, of course, that all hosts are of the same operating system.

The hosts still require some build tools, such as *make*, to be installed, but do not require a full build environment.

Installing the Unix Agent

The same installation procedure used for *local* and *server* installations is used for an *agent* installation on Unix- and Linux-based hosts. Start by choosing ***agent*** installation in step 1 and then a directory location in step 2. The defaults are shown in square brackets and can be accepted by pressing **Enter**, or customized as in this case. You will notice that the agent install has fewer options to configure. This is because the server does much of the work.

```
1- What kind of installation do you want (server, agent, local or help)? agent

     - Agent(client) installation chosen.

2- Setting up the installation environment.

 - Choose where to install the OSSEC HIDS [/var/ossec]: /opt/ossec

     - Installation will be made at /opt/ossec .

3- Configuring the OSSEC HIDS.

   3.1- What's the IP Address of the OSSEC HIDS server?: 192.168.65.20

     - Adding Server IP 192.168.65.20

   3.2- Do you want to run the integrity check daemon? (y/n) [y]: y

     - Running syscheck (integrity check daemon).

   3.3- Do you want to run the rootkit detection engine? (y/n) [y]: y

     - Running rootcheck (rootkit detection).
```

On the agent installation, notice that the only options for active response are enable or disable. Enabling active response on an agent allows the server to initiate responses that are executed on this agent. We recommend enabling for all agents.

```
 3.4 - Do you want to enable active response? (y/n) [y]: y

 3.5- Setting the configuration to analyze the following logs:
     -- /var/log/messages
     -- /var/log/authlog
     -- /var/log/secure
     -- /var/log/xferlog
     -- /var/log/maillog

- If you want to monitor any other file, just change
   the ossec.conf and add a new localfile entry.
   Any questions about the configuration can be answered
   by visiting us online at http://www.ossec.net .

--- Press ENTER to continue ---
```

After you press **Enter**, the OSSEC HIDS is compiled, installed, and configured with the options you specified. When the installation is complete, the installer script provides you with some final information. You should make note of the information and take any recommended actions. For example, for the OSSEC HIDS to use the OpenBSD pf firewall, a few lines must be added to the /etc/pf.conf script.

TIP

If the compilation of the OSSEC HIDS application fails, you do not get the informational screen indicating how to stop and start the OSSEC HIDS. Instead, you will see the line "Building error. Unable to finish the installation." at the end of the compiler output.

This is typically always related to a missing prerequisite. If this occurs, revisit Chapter 1 for tips on installing the correct build environment.

Before starting the OSSEC HIDS agent, the key generated on the server must be imported. The *manage_agents* utility is used to import the keys. Because the keys are on the server, the normal method for retrieving the keys is to connect to the server using SSH and run the *manage_agents* utility.

From the manage agents menu, enter **e** to extract a key. You are provided with a list of already configured agents. Choose your agent by entering the correct ID. The key is displayed so you can copy it to your clipboard.

```
# /opt/ossec/bin/manage_agents

***************************************
* OSSEC HIDS v1.3 Agent manager.      *
* The following options are available:*
***************************************
  (A)dd an agent (A).
  (E)xtract key for an agent (E).
  (L)ist already added agents (L).
  (R)emove an agent (R).
  (Q)uit.
Choose your action: A,E,L,R or Q: e
Available agents:
  ID: 001, Name: mars, IP: 192.168.65.40
Provide the ID of the agent to extract the key (or '\q' to quit): 001
Agent key information for '001' is:
MDAxIG1hcnMgMTkyLjE2OC42NS40MCBmY2UzMjM4OTc1ODgzYTU4ZWM3YTRkYWJiZTJmMjQ2Y2ViODhmMzl
mYjE3MmI4OGUzMTE0MDczMzVhYjk2OTRh
** Press ENTER to return to the main menu.
```

Exit from the *manage_agents* utility on the server by entering **q** from the menu, exit the SSH session, and return to the agent host. To import the key, run the *manage_agents* utility on the agent host. The menu for agents is much simpler, because importing keys is the only option. Enter **i** to import and then paste the key value previously saved to your clipboard.

```
# /opt/ossec/bin/manage_agents
***************************************
* OSSEC HIDS v1.3 Agent manager.      *
* The following options are available:*
***************************************
  (I)mport key from the server (I).
  (Q)uit.
```

```
Choose your action: I or Q: i

* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDAxIG1hcnMgMTkyLjE2OC42NS40MCBmY2UzMjM4OTc1ODgzYTU4ZWM3YTRkYWJiZTJmMjQ2Y2ViODhmMzl
mYjE3MmI4OGUzMTE0MDczMzVhYjk2OTRh

Agent information:
  ID:001
  Name:mars
  IP Address:192.168.65.40
Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
***************************************
* OSSEC HIDS v1.3 Agent manager.      *
* The following options are available: *
***************************************
  (I)mport key from the server (I).
  (Q)uit.
Choose your action: I or Q: q

** You must restart the server for your changes to have effect.

manage_agents: Exiting ..
```

Now that the agent installation is complete, we can start the OSSEC HIDS service by running the following command:

```
# /opt/ossec/bin/ossec-control start
```

The agent starts and connects to the server. You can verify this by checking the agent logs (/var/ossec/logs/ossec.log) and finding messages similar to the following near the end of the file:

```
2007/10/10 23:25:48 ossec-agentd: Connecting to server (192.168.65.20:1514).
2007/10/10 23:25:48 ossec-agentd(4102): Connected to the server.
```

Installing the Windows Agent

As you have already seen, performing the local, server, and agent installations on Unix-based operating systems is similar and relatively easy. The Windows installation, however, is different. This is because Windows environments do not typically have development tools included. Even when these tools are available, they often require more preparation before use compared with Unix and Linux systems.

Because of these issues, the Windows agent comes precompiled and packaged in a graphical installation wizard. The text menu procedure seen with the other installations is replaced with

GUI screens. Similarly, after the software is installed, there is a GUI version of the manage agents utility.

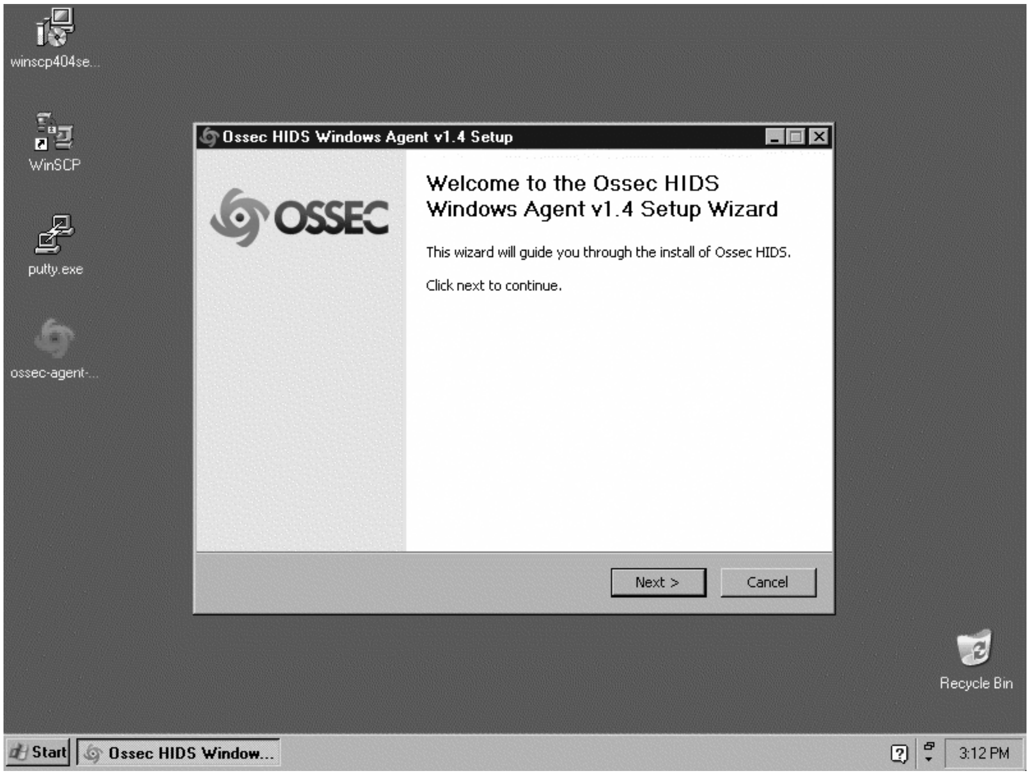
TIP

Windows operating systems do not come with SSH utilities for remote access to Unix hosts. SSH access to the server host is required to complete the agent install. Fortunately, there is a freely available SSH utility for Windows called PuTTY, which has become exceedingly popular.

PuTTY is an SSH and telnet terminal emulator that can be downloaded from www.chiark.greenend.org.uk/~sgtatham/putty/. You should install an SSH client before installing the OSSEC HIDS just to make the process easier.

Begin by running the installation executable ossec-agent-win32-1.4.exe as seen in Figure 2.1, to open the wizard.

Figure 2.1 Launching the Installer



Ossec HIDS Windows Agent v1.4 Setup

Welcome to the Ossec HIDS Windows Agent v1.4 Setup Wizard

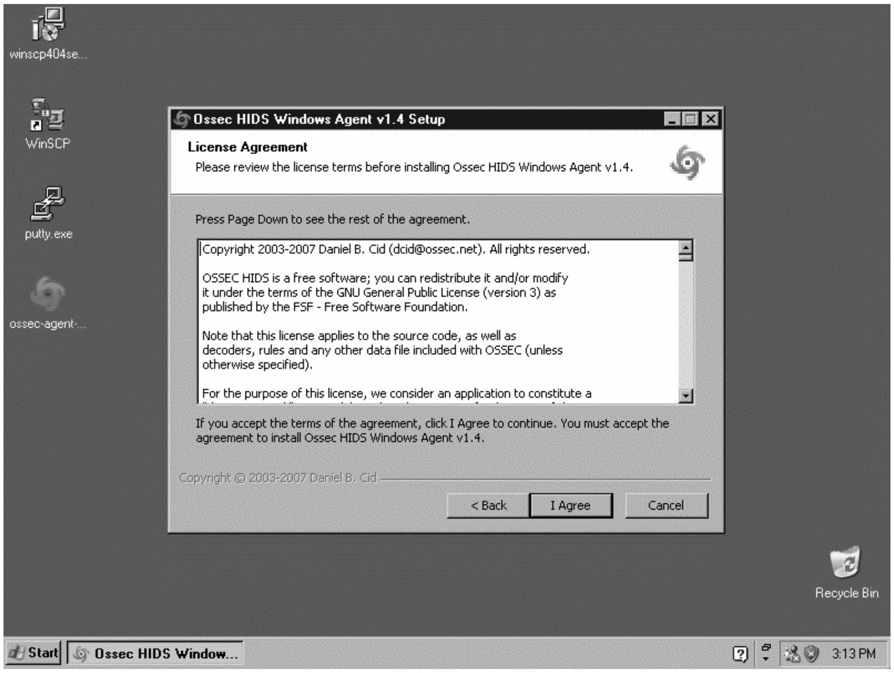
This wizard will guide you through the install of Ossec HIDS.

Click next to continue.

Click **Next** to start the installation.

Review the license agreement and then click **I Agree** to continue (Figure 2.2).

Figure 2.2 Accepting the License Text



Ossec HIDS Windows Agent v1.4 Setup

License Agreement

Please review the license terms before installing Ossec HIDS Windows Agent v1.4.

Press Page Down to see the rest of the agreement.

Copyright 2003-2007 Daniel B. Cid (dcid@ossec.net). All rights reserved.

OSSEC HIDS is a free software; you can redistribute it and/or modify
it under the terms of the GNU General Public License (version 3) as
published by the FSF - Free Software Foundation.

Note that this license applies to the source code, as well as
decoders, rules and any other data file included with OSSEC (unless
otherwise specified).

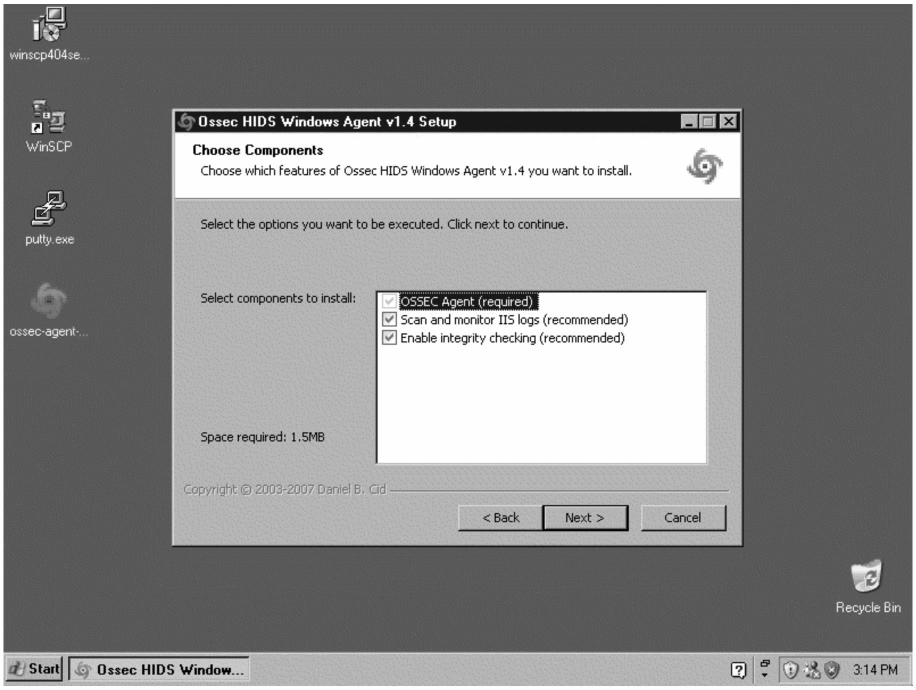
For the purpose of this license, we consider an application to constitute a

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Ossec HIDS Windows Agent v1.4.

Copyright © 2003-2007 Daniel B. Cid

Choose the components you want to install, and click **Next** (Figure 2.3).

Figure 2.3 Selecting Components



Ossec HIDS Windows Agent v1.4 Setup

Choose Components

Choose which features of Ossec HIDS Windows Agent v1.4 you want to install.

Select the options you want to be executed. Click next to continue.

Select components to install:

☑ OSSEC Agent (required)
☑ Scan and monitor IIS logs (recommended)
☑ Enable integrity checking (recommended)

Space required: 1.5MB

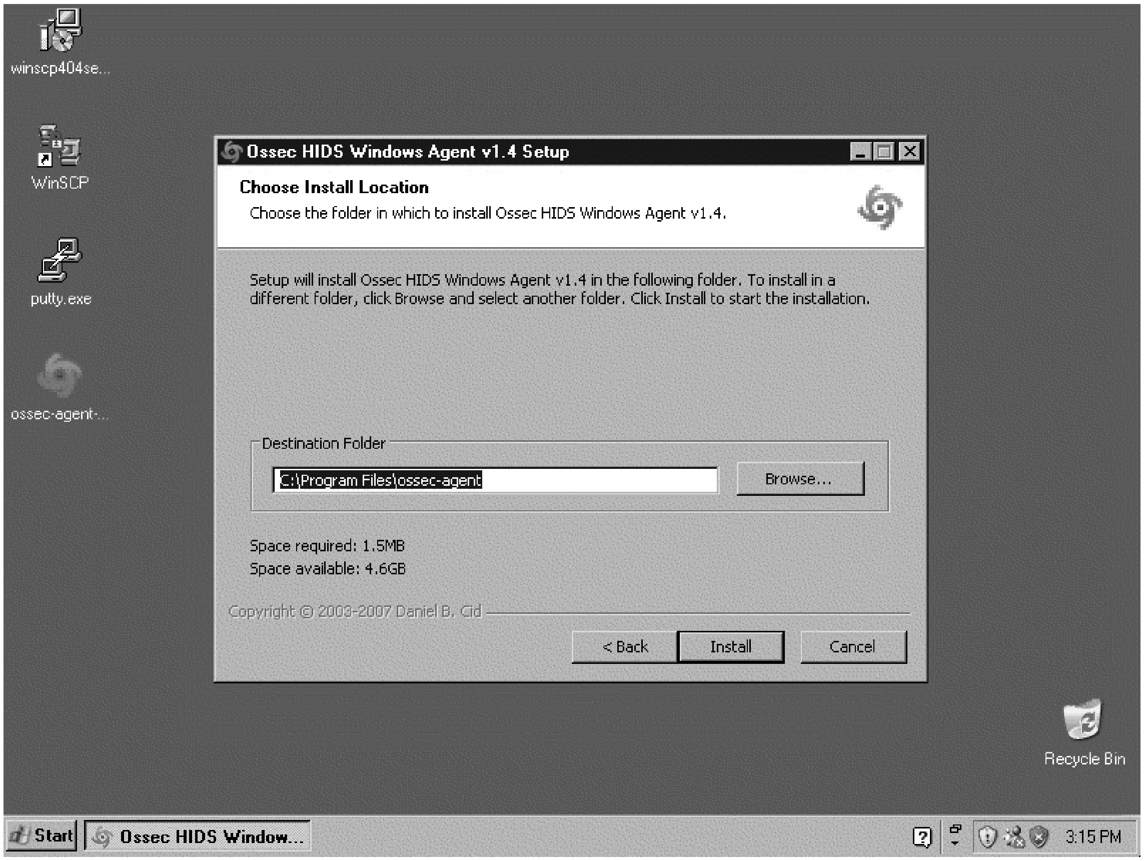
Copyright © 2003-2007 Daniel B. Cid

NOTE

The default installation options work in most cases.

Accept the default installation folder, or click **Browse** to specify a new location. Click **Install** to continue (Figure 2.4).

Figure 2.4 Specifying the Location



Ossec HIDS Windows Agent v1.4 Setup

Choose Install Location

Choose the folder in which to install Ossec HIDS Windows Agent v1.4.

Setup will install Ossec HIDS Windows Agent v1.4 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

Destination Folder: C:\Program Files\ossec-agent

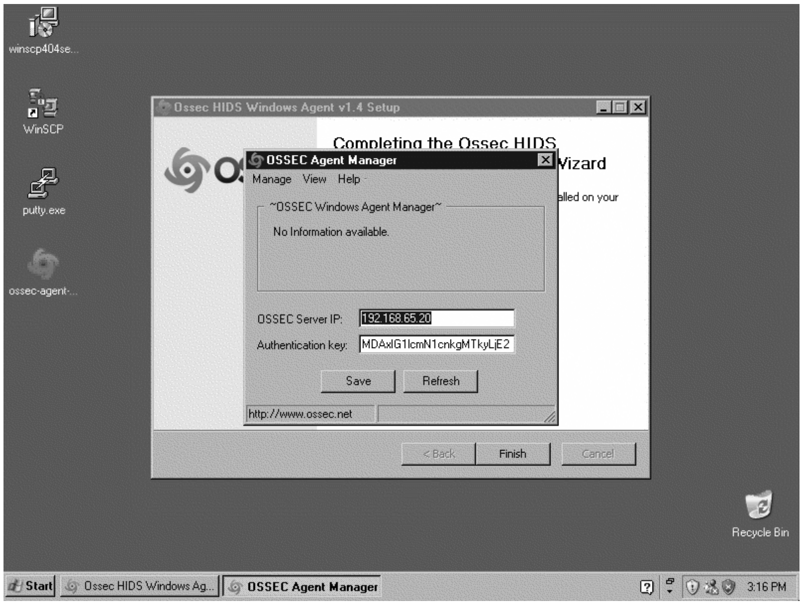
Space required: 1.5MB
Space available: 4.6GB

Copyright © 2003-2007 Daniel B. Cid

Because this is an agent installation, there are very few questions to answer as part of the installation. Apart from picking the location in Figure 2.3 and importing the agent key in Figures 2.5 through 2.9, the installation on Windows is very simple.

Launch the SSH client on your Windows host and connect to the OSSEC HIDS server. We must use SSH to connect to the OSSEC HIDS server, *Extract* the key for this agent, and then paste the key in the Authentication key field (Figure 2.5).

Figure 2.5 Managing the Agent



~OSSEC Windows Agent Manager~

No Information available.

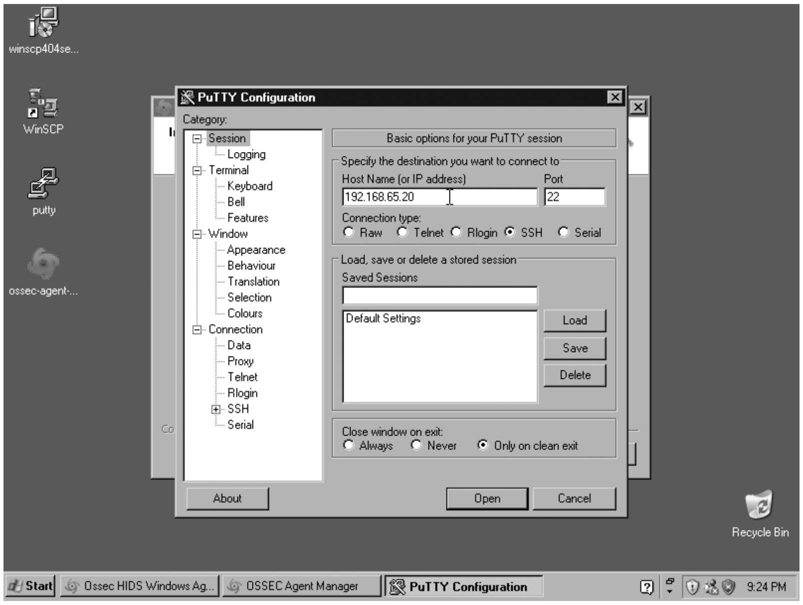
OSSEC Server IP: 192.168.65.20

Authentication key: MDAxIG1lcmN1cnkgMTkyLjE2

http://www.ossec.net

PuTTY is an ideal SSH client and is shown in Figure 2.6. In the Host Name field, type the IP address or hostname of your OSSEC HIDS server and then click **Open**. If this is your first time connecting to the server from this Windows host, you are asked to accept the server SSH identity. Accept the server identity, log in to the server, and then execute the *manage_agents* utility.

Figure 2.6 Connecting to the Server



Specify the destination you want to connect to

Host Name (or IP address): 192.168.65.20 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

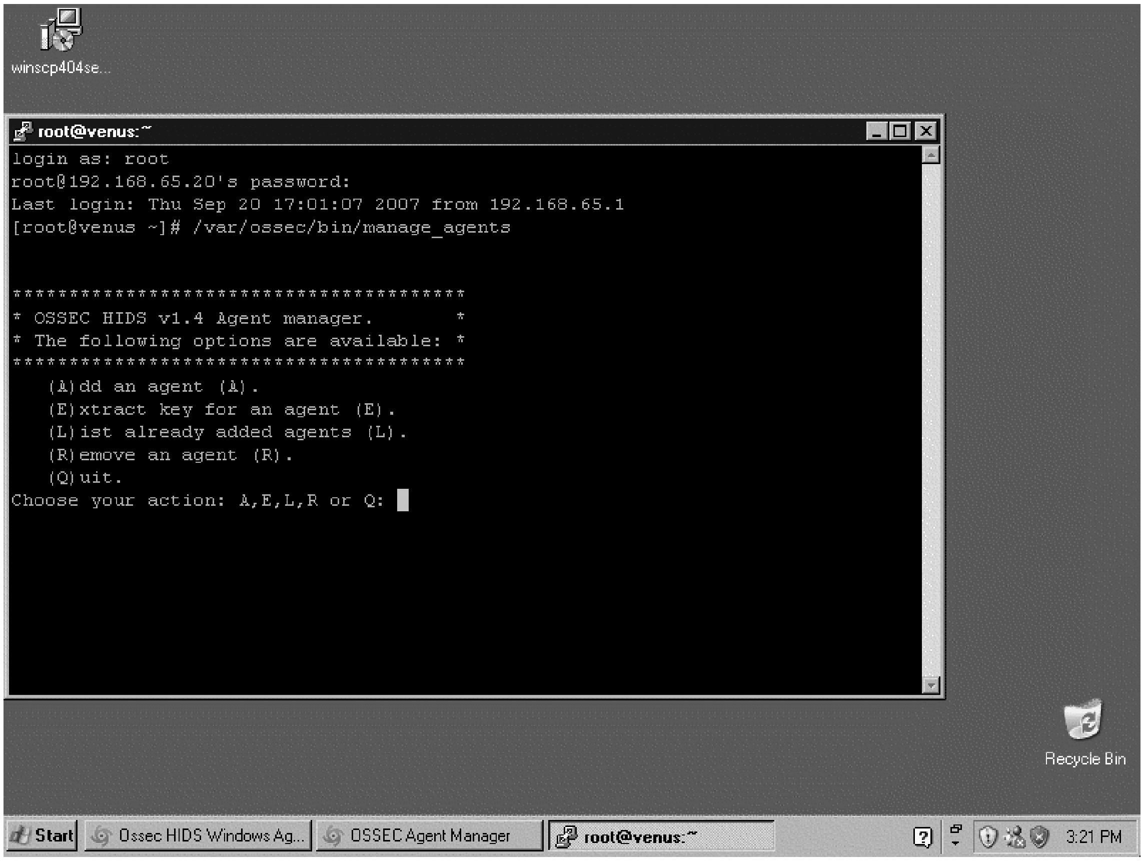
Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Enter **E** to extract the agent key for the current Windows host (Figure 2.7).

Figure 2.7 Running manage_agents



```
login as: root
root@192.168.65.20's password:
Last login: Thu Sep 20 17:01:07 2007 from 192.168.65.1
[root@venus ~]# /var/ossec/bin/manage_agents


****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:
```

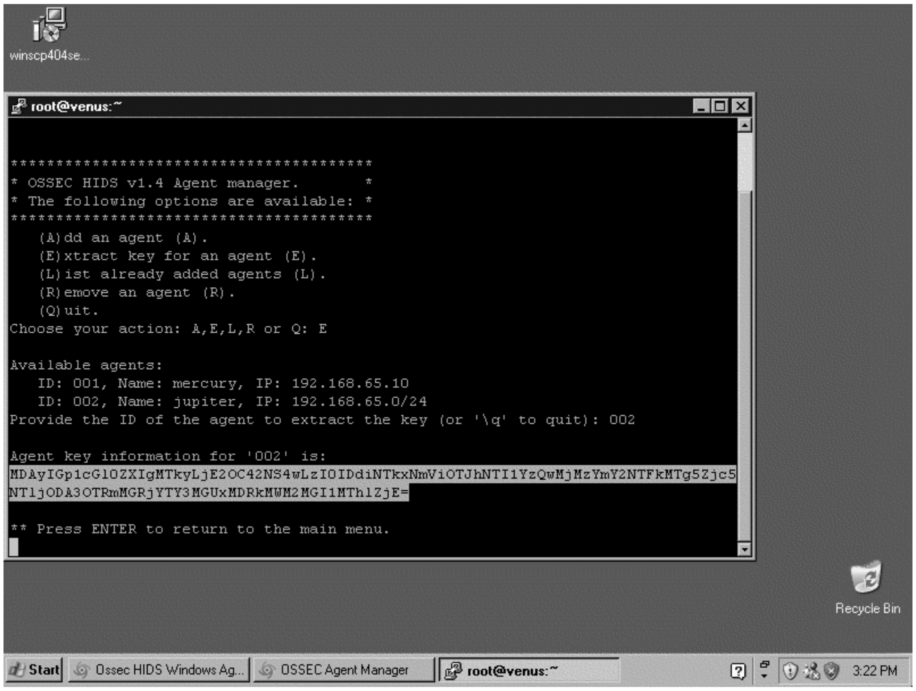
In this case, the host is *mercury*, which has ID 002. Enter **002**, select the key information, and copy it to the clipboard (Figure 2.8).

Now return to the OSSEC HIDS installer.

Type the OSSEC HIDS server IP address and paste the agent key information into the appropriate fields. Click **Save** (Figure 2.9).

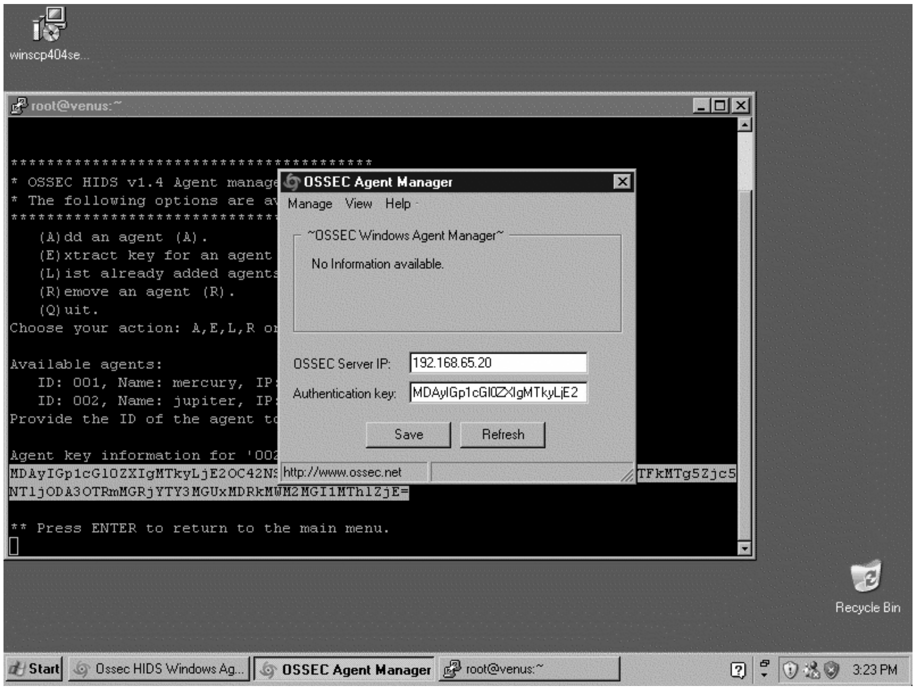
You are asked to confirm the values by clicking **OK**. After the values have been confirmed, exit the Agent Manager by clicking the **X** at the top-right corner of the window (Figure 2.10).

Figure 2.8 Copying the Key to the Clipboard



```
****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: mercury, IP: 192.168.65.10
   ID: 002, Name: jupiter, IP: 192.168.65.0/24
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIGp1cGl0ZXIgMTkyLjE2OC42NS4wLzI0IDdiNTkxNmViOTJhNTI1YzQwMjMzYmY2NTFkMTg5Zjc5
NTljODA3OTRmMGRjYTY3MGUxMDRkMWM2MGI1MTh1ZjE=

** Press ENTER to return to the main menu.
```

Figure 2.9 Pasting the Key



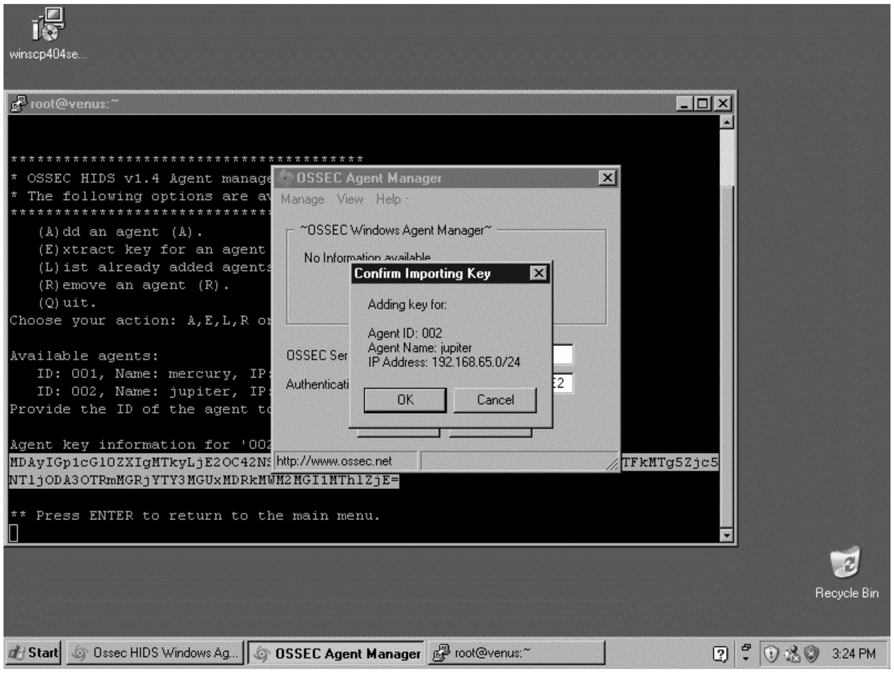
~OSSEC Windows Agent Manager~

No Information available.

OSSEC Server IP: 192.168.65.20

Authentication key: MDAyIGp1cGl0ZXIgMTkyLjE2

Figure 2.10 Confirming the Import



```
****************************************
* OSSEC HIDS v1.4 Agent manage
* The following options are av
********************************
   (A)dd an agent (A).
   (E)xtract key for an agent
   (L)ist already added agents
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or

Available agents:
   ID: 001, Name: mercury, IP:
   ID: 002, Name: jupiter, IP:
Provide the ID of the agent to

Agent key information for '002
MDAyIGp1cGl0ZXIgMTkyLjE2OC42NS                                                TFkMTg5Zjc5
NTljODA3OTRmMGRjYTY3MGUxMDRkMWM2MGI1MThlZjE=

** Press ENTER to return to the main menu.
```

OSSEC Agent Manager

~OSSEC Windows Agent Manager~

No Information available

OSSEC Ser

Authenticati

http://www.ossec.net

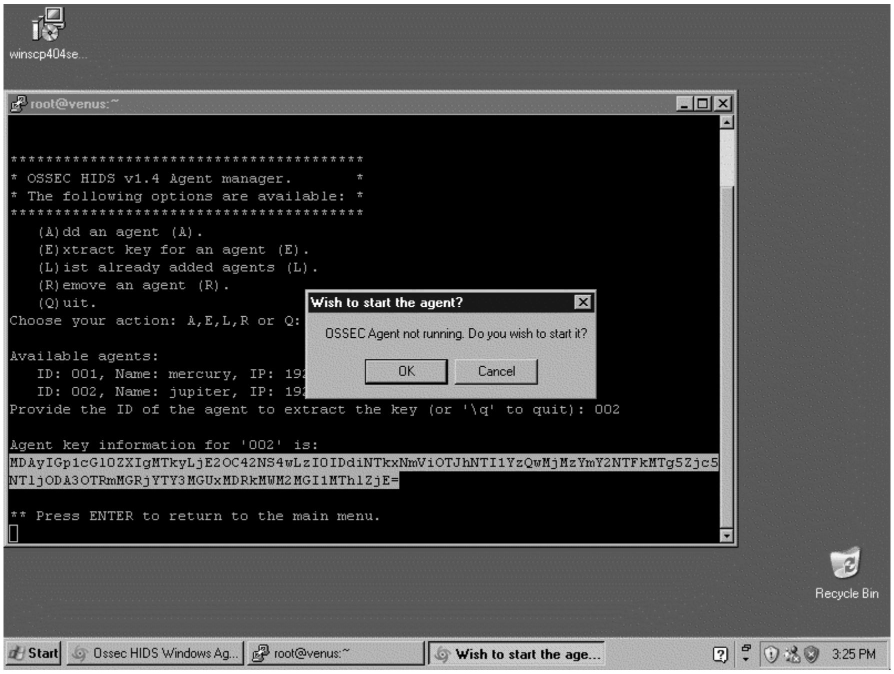
Confirm Importing Key

Adding key for:

Agent ID: 002
Agent Name: jupiter
IP Address: 192.168.65.0/24

The installer asks if you want to start OSSEC HIDS; click **OK** (Figure 2.11).

Figure 2.11 Starting the OSSEC HIDS



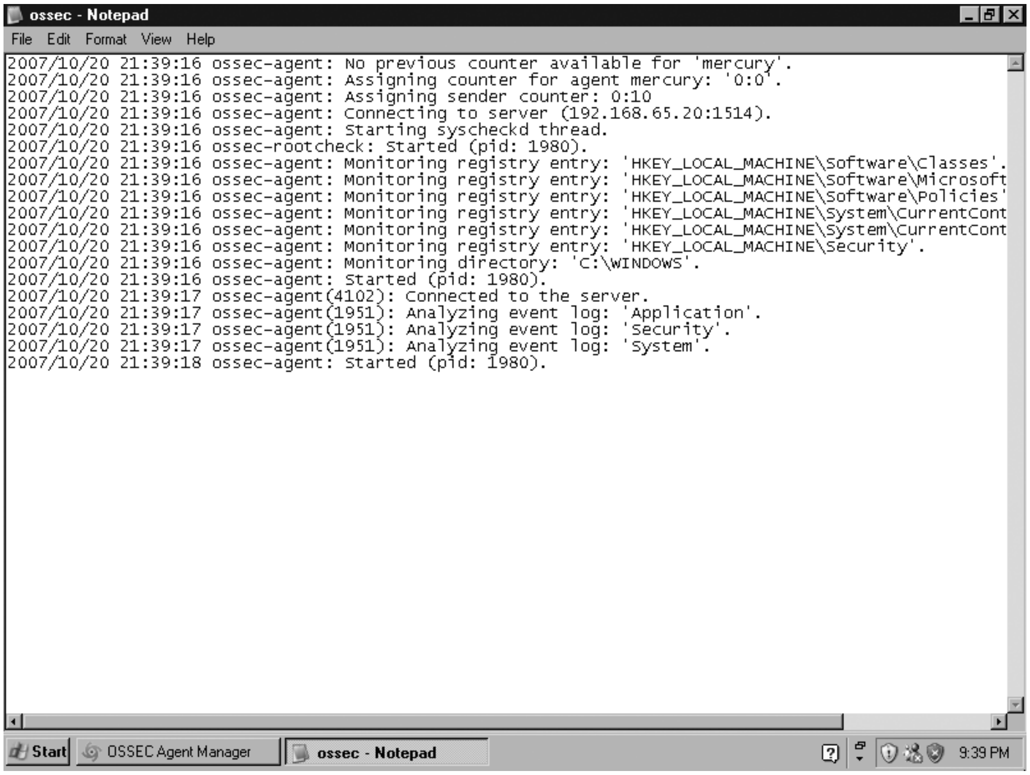
```
****************************************
* OSSEC HIDS v1.4 Agent manager.       *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q:

Available agents:
   ID: 001, Name: mercury, IP: 19
   ID: 002, Name: jupiter, IP: 19
Provide the ID of the agent to extract the key (or '\q' to quit): 002

Agent key information for '002' is:
MDAyIGp1cGl0ZXIgMTkyLjE2OC42NS4wLzI0IDdiNTkxNmViOTJhNTI1YzQwMjMzYmY2NTFkMTg5Zjc5
NTljODA3OTRmMGRjYTY3MGUxMDRkMWM2MGI1MThlZjE=

** Press ENTER to return to the main menu.
```

Wish to start the agent?

OSSEC Agent not running. Do you wish to start it?

The Windows agent is now installed and running. To confirm that the agent is connected to the server, let's look at the logs for the Windows agent. In Figure 2.12, the two messages *Connecting to server* and *Connected to server* confirm that the agent key is properly imported and the agent is able to connect to UDP port 1514. The Windows agent is successfully installed and communicating with the server.

Figure 2.12 Confirming the Server Connection



```
2007/10/20 21:39:16 ossec-agent: No previous counter available for 'mercury'.
2007/10/20 21:39:16 ossec-agent: Assigning counter for agent mercury: '0:0'.
2007/10/20 21:39:16 ossec-agent: Assigning sender counter: 0:10
2007/10/20 21:39:16 ossec-agent: Connecting to server (192.168.65.20:1514).
2007/10/20 21:39:16 ossec-agent: Starting syscheckd thread.
2007/10/20 21:39:16 ossec-rootcheck: Started (pid: 1980).
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Classes'.
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Microsoft
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Software\Policies'
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\System\CurrentCont
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\System\CurrentCont
2007/10/20 21:39:16 ossec-agent: Monitoring registry entry: 'HKEY_LOCAL_MACHINE\Security'.
2007/10/20 21:39:16 ossec-agent: Monitoring directory: 'C:\WINDOWS'.
2007/10/20 21:39:16 ossec-agent: Started (pid: 1980).
2007/10/20 21:39:17 ossec-agent(4102): Connected to the server.
2007/10/20 21:39:17 ossec-agent(1951): Analyzing event log: 'Application'.
2007/10/20 21:39:17 ossec-agent(1951): Analyzing event log: 'Security'.
2007/10/20 21:39:17 ossec-agent(1951): Analyzing event log: 'System'.
2007/10/20 21:39:18 ossec-agent: Started (pid: 1980).
```

Streamlining the Installations

Because the installation script is menu-driven, it does not lend itself well to an automated installation. On the server side, this is not a significant issue because there are fewer servers. On the agent side, however, this can be cumbersome. Fortunately, the OSSEC HIDS file structure and configuration is reasonably simple, and therefore there are a few tricks we can play.

Install Once, Copy Everywhere

With the agents in particular, almost all the files are identical for every agent. The one significant exception is the *client.keys* file, which must be unique for each host. Assuming a mass installation is required and that the host operating system is virtually identical for all agents, we can install to one agent and then replicate the files to all agents.

Similarly, if you or your organization has a standard system image, the files can be added to the image and therefore automatically installed on each host. This is a common strategy for many organizations or enterprises, and works well for the OSSEC HIDS. The only customization required is to properly import the agent key on each host. This, too, can be done more directly than with the cut-and-paste method, which is difficult to automate.

In the case of Unix-based hosts, SSH is used for file transfers and remote access. Virtually every Unix administrator is familiar with its use and utility.

Unix, Linux, and BSD

Because all of the OSSEC HIDS files (excluding the initialization scripts) are contained the directory where it is installed, we can copy this entire directory structure (excluding etc/client.keys) to each host using whichever file transfer method is most convenient. It is important, however, to preserve file permissions and ownership during the transfer. Typically, this means using tar to package the files, transferring the tar file to the destination host, and then extracting on the host. Assuming the OSSEC HIDS is installed at /var/ossec and the agent hosts are all Linux, the tar file can be created using:

```
# cd /; tar –exclude client.keys -cf /tmp/ossec.tar var/ossec \
etc/init.d/ossec ‘find etc -name “S[0-9][0-9]ossec”’ \
‘find etc -name “K[0-9][0-9]ossec”’
```

Now, assuming that the target host is 192.168.65.30, we can transfer the full OSSEC HIDS install in one long line. The *ossec* user must be created on the target to preserve permission so this is included:

```
# cat /tmp/ossec.tar | ssh root@192.168.65.30 \
“groupadd ossec; useradd -g ossec -d /var/ossec ossec; cd / ; tar -xf - ”
```

The full OSSEC HIDS installation, configuration, and rules have been transferred to the remote agent, including initialization scripts and proper permissions. These commands also work similarly with any Unix-based operating system that has SSH installed. All that remains now is to import the keys to each agent.

Push the Keys

With all the files in place on the agents, each agent needs a key. The only difference between the client.keys file on the server and the file on an agent host is the number of lines. The server copy of the client.keys file has all agent keys, with one per line. The agent client.keys file has only the one line belonging to that agent.

Configuring the keys on the agent simply requires you to extract the single line for that agent to a file and then copy that file to the agent host. On the server side, because it is always Unix or Linux based, extracting the key for a single agent is the first step. Assuming the agent name provided when creating the key is *mars* and that the OSSEC HIDS is installed at /var/ossec:

```
# grep 192.168.65.30 /var/ossec/etc/client.keys > /tmp/agent.key
```

Unix, Linux, and BSD

Pushing the key to a Unix- or Linux-based host is also a one-line command. Assuming the OSSEC HIDS is installed to /var/ossec on the agent:

```
# scp /tmp/agent.key root@192.168.65.30:/var/ossec/etc/client.keys
```

Alternatively, if the agent is accessible using a networked file system, a file copy can be performed. While this approach does not provide a complete solution, you can see that the steps required to perform a remote installation and configuration of the OSSEC HIDS are easy.

Summary

The OSSEC HIDS is an easily accessible HIDS solution, offering a simple, menu-driven installation. It can be downloaded from the OSSEC Web site as uncompiled source code, allowing you to build and compile the application for any operating system, or as a binary executable file specifically for Windows agent deployments.

To build and compile the OSSEC source code you must first ensure that the necessary development tools are installed. The two modes of installation, *local* and *server-agent*, provide the flexibility to plan complex deployments. While the *server-agent* installation requires minor extra effort, getting the agents connected to the servers is a simple task.

The OSSEC HIDS server must receive communication from agents on port 1514 and possibly 514. You must ensure that the firewall or packet filter on the OSSEC server allows this traffic. Each operating system and software distribution provides a way to do this, so please consult your operating system documentation.

Installing the OSSEC HIDS on multiple hosts can be automated using a combination of the SSH protocol and some Unix commands. This allows you to deploy OSSEC HIDS agents to multiple hosts without having to physically sit at every computer you must configure.

At this point, you have seen that performing an OSSEC HIDS installation takes minimal time and effort. Local installations are effortless and a great way to get functioning with the OSSEC HIDS quickly. With this introduction to the accessibility of the OSSEC HIDS, you are now ready to examine more information about this remarkable security solution.

Solutions Fast Track

Downloading the OSSEC HIDS

☑ The OSSEC HIDS is most commonly downloaded, compiled, and installed from the source code available on the OSSEC Web site (www.ossec.net).

☑ Because Unix- and Linux-based operating systems provide complete development tools, the main OSSEC source tar file contains everything needed to install the OSSEC HIDS.

☑ Because the OSSEC HIDS installer must compile the application from source code the first time it runs, a working build environment is required on your system. For most Linux and BSD operating systems, a C compiler and supporting files are already installed. If the files are not installed, you must install gcc and development headers before proceeding.

☑ Because development tools are not typically installed on most Microsoft Windows systems, an executable, GUI-based installer is provided that installs a precompiled OSSEC HIDS service.

Building and Installing the OSSEC HIDS

☑ The installation script is divided into several easy steps to guide you through the installation.

☑ The steps are slightly different for each of the install types, however; the initial screen is the same for all installations.

☑ The OSSEC HIDS installer allows you to choose your installation language of choice from one of 12 supported languages, including English, Brazilian Portuguese, Chinese, German, Spanish, French, Italian, Japanese, Polish, Russian, Serbian, and Turkish.

Performing a Local Installation

☑ Local installations can only be done on Linux-, Unix-, and BSD-based operating systems.

☑ The integrity check daemon is responsible for monitoring and reporting changes in system files.

☑ The rootkit detection engine regularly performs tests looking for evidence of an installed rootkit.

☑ Careful configuration of both services provides fine-grained protection or notification of illicit file modifications, hidden network port activity, and other evidence of intrusion.

☑ Depending on your platform, the OSSEC HIDS installer adds initialization scripts to start the OSSEC HIDS on your system.

Performing Server-Agent Installations

☑ Server-agent installations are meant for a central controller with multiple agents.

☑ Because Microsoft Windows hosts can only be agents, a server is always required prior to installing the OSSEC HIDS on Windows.

☑ The OSSEC HIDS server must receive communication from agents on port 1514 and possibly 514, so firewall rules might need to be adjusted in your environment to allow this communication.

☑ Agents must be able to identify themselves to the server, and the server must be able to validate the identity of the agent. This ensures that illicit messages are not processed by the server when sent from non-agent hosts.

☑ Importing the key from the server to the agent typically requires SSH access to the server.

☑ The OSSEC HIDS Windows agent comes precompiled and packaged in a graphical installation wizard. The text menu procedure seen with the other installations is replaced with GUI screens. Similarly, after the software is installed, there is a GUI version of the *manage_agents* utility.

Streamlining Installation

☑ Using SSH and some simple Unix commands, you can install and configure multiple OSSEC HIDS agents from one central location.

☑ The *ossec* user must be created on every remote host to ensure file permissions are synchronized across your deployment.

☑ If the agent is accessible using a networked file system, the *client.keys* file can be copied from one file system to the networked file system.

Frequently Asked Questions

Q: Where can I download the OSSEC HIDS files I need?

A: All files needed for your OSSEC HIDS installation can be found at the OSSEC Web site at www.ossec.net.

Q: What files do I need to install the OSSEC HIDS?

A: If you plan to install the OSSEC HIDS on a Unix, Linux, or BSD operating system, you need the source code tar.gz archive. If you plan to install the OSSEC HIDS on a Microsoft Windows system, you can download the precompiled Windows agent installation executable. Regardless of the file you download, it is strongly reccomended that you also download the checksum text file to validate the integrity of your downloads prior to installation.

Q: I don't have development tools installed on my Unix, Linux, or BSD machine. Is there a precompiled OSSEC HIDS executable for Unix, Linux, or BSD operating systems?

A: At the time of this writing, there were no officially supported OSSEC HIDS packages available for download. The OSSEC HIDS team, however, is investigating packages for Debian/Ubuntu, Mac OS X, and Red Hat based operating systems as a future roadmap item.

Q: What languages does the OSSEC HIDS installer support?

A: The OSSEC HIDS installer allows you to choose your installation language of choice from one of 12 supported languages, including English, Brazilian Portuguese, Chinese, German, Spanish, French, Italian, Japanese, Polish, Russian, Serbian, and Turkish.

Q: I don't see my native language listed. How can I get support for my language into the OSSEC HIDS?

A: The OSSEC HIDS team is always looking for translators for documentation and the user interface. If you, or someone you know, is capable of translating from one of the currently supported languages, please contact the OSSEC HIDS development team.

Q: The installer wants me to install the OSSEC HIDS in the /var/ossec directory, but I want to put it somewhere else. Does it matter what directory I install to?

A: You can install the OSSEC HIDS to any directory on your system as long as the root user has write access to that directory.

Q: If I did not enable one of the features during installation, can I enable that feature later?

A: Yes, you can run the installer script as many times as you like to make changes to the current configuration or edit the existing configuration. The configuration of the OSSEC HIDS is covered in greater depth later in this book.

Q: Active response sounds potentially dangerous. Should I still enable it?

A: Even though active response could be potentially dangerous, we still recommend that you enable it. It is a very powerful feature of the OSSEC HIDS and its configuration is discussed in greater detail later in this book.

Q: When the installation completed there was a message indicating that a startup script could not be created. What do I do now?

A: The OSSEC HIDS installer is able to create a startup script on most operating systems, but if one is not created, you can create your own initialization script to launch the OSSEC HIDS on system boot.

Q: How do I manually start the OSSEC HIDS processes?

A: If you want to start the OSSEC HIDS manually, you can run *ossec-control start* from the bin directory where your OSSEC HIDS installation is located. Please note that the OSSEC HIDS might need to be started as the root user, so you might have to log in as a user with root permissions or leverage *sudo* to run the command.

Q: When should I install my OSSEC HIDS server—before or after my agents?

A: When installing your OSSEC HIDS agents, you are asked to supply the IP address for your OSSEC HIDS server. It is always recommended that your OSSEC HIDS server be installed prior to deploying your agents.

Q: How do I manage my agents?

A: On Unix, Linux, and BSD operating systems you can run the *manage_agents* utility to add new agents, extract keys for agents, list agents, and remove existing agents. On a Windows agent, you can click on the Manage Agents icon where your *ossec* start menu group is located.

Q: The agent is not able to connect to the server, what's wrong?

A: There are two common issues. If there are no messages in the server log regarding the agent, chances are there is a firewall blocking port 1514 between the server and agent. If you see a message similar to:

```
2007/05/23 09:27:35 ossec-remoted(1403): Incorrectly formated message from
'xxx.xxx.xxx.xxx'.
```

there is an issue with the key on the agent. Either the key is used by another agent or the IP address configured in the key is incorrect.

Q: When copying the OSSEC HIDS files from one system to another, are there any files I shouldn't copy?

A: Because each OSSEC HIDS agent requires its own generated *client.keys* file, and the OSSEC HIDS server copy of *client.keys* contains all agent keys, it is recommended that you exclude this file from your copy.

Q: How can I get the OSSEC HIDS files to the remote systems?

A: Depending on your environment, you might be able to use SSH to securely transfer the files from one system to the other. If you have a networked file system, you can copy the files from one file system to the other. Alternately, if no connection is available, you can simply copy the files to a floppy, CD-ROM, or DVD, and then copy the files to the system.

Q: Which command can I use to securely copy the key from the OSSEC HIDS server to the remote agent?

A: You can use the *grep* command to extract the OSSEC HIDS agent key from the OSSEC HIDS server *client.keys* file, and use SCP to copy it to the other system.