

NetDiff Guide

NetDiff Guide

Revision History

Revision \$Revision: 1.1 \$ \$Date: 2006/01/03 17:18:31 \$ Revised by: pd

Table of Contents

1. Introduction	1
2. Installation	3
2.1. Prerequisites	3
2.2. RPM Installation	3
2.3. Manual Installation	3
3. Configuration	5
3.1. MySQL Database Table Creation	5
3.2. Manual NetDiff Configuration	5
4. Usage	7
4.1. Command Line	7
4.2. EnGarde Secure Linux WebTool Module	7
A. Resources	11

List of Figures

- 4-1. Example of NetDiff Usage7
- 4-2. NetDiff WebTool module.....7
- 4-3. NetDiff options.....8
- 4-4. NetDiff report.....9
- 4-5. NetDiff network.....9

Chapter 1. Introduction

NetDiff is a network reporting tool written in perl that runs nmap portscans of a specified network or networks and stores the results to a MySQL database. It can then report the differences between successive scans, giving administrators a snapshot view of recent changes on their network.

This report is very useful for network maintenance and monitoring, it will automatically let you know when:

- A new host is added to the network.
- A host is shut down or disconnected from the network.
- A service has stopped running.
- A new service port has been opened.

Additionally, if version and OS scanning is enabled, the report will list those differences as well, telling you if:

- A server daemon was upgraded or patched.
- The host's operating system was upgraded or changed.

Chapter 2. Installation

An rpm package is available for installation on EnGarde Secure Linux. Alternatively, NetDiff can be manually installed.

2.1. Prerequisites

NetDiff depends on several other software packages that must be installed for proper operation.

- Perl v5.6.0 or greater
- Perl DBI module for MySQL
- Perl XML::Parser module
- Perl XML::Simple module
- MySQL 3.23 or greater
- Nmap 3.81 or greater

See Appendix A for web links to these required packages.

2.2. RPM Installation

Simply copy the NetDiff and NetDiff WebTool RPMs to your EnGarde Secure Linux server and run the following command:

```
# rpm -Uvh netdiff-*.rpm
```

The NetDiff files will be installed automatically.

2.3. Manual Installation

Extract the NetDiff files from the archive and install them by running the following commands:

```
# tar xvfz netdiff-<version>.tar.gz
# cd netdiff-<version>
# cp netdiff /usr/sbin
# mkdir /etc/netdiff
# cp netdiff.conf /etc/netdiff
# cp netdiff-create-tables.sql /etc/netdiff
# cp netdiff.cron /etc/cron.d
```


Chapter 3. Configuration

Before you begin using NetDiff, it must be configured. The MySQL tables must be created, and the configuration file must be edited to add the target networks you wish to scan.

Follow the steps below to configure NetDiff. Alternatively, if you are using EnGarde Secure Linux, you may install the NetDiff WebTool module which will automatically create the MySQL tables if they do not exist and will allow you to configure NetDiff using the WebTool's browser based interface.

3.1. MySQL Database Table Creation

Create a new MySQL database and user for NetDiff's use. If you're unsure how to do this, refer to the online MySQL documentation (<http://dev.mysql.com/doc/mysql/en/>). Then run the following command:

```
# mysql -u mysql-user -p mysql-db-name < /etc/netdiff-create-tables.sql
```

If you are using the EnGarde Secure Linux WebTool module for NetDiff, you do not need to set up the database, the WebTool will do this for you automatically the first time it is run.

3.2. Manual NetDiff Configuration

Edit the file `/etc/netdiff/netdiff.conf` and provide the following information.

- Set the `db_name`, `db_user`, and `db_pass` lines to the appropriate database name, database user and password that you set up when you created the MySQL database.
- Set the `report_to` line to an email address you would like the NetDiff reports sent to.
- Add a `networks` line specifying the network or networks you would like to scan, in `192.168.1.0/24` format.

Again, if you are using the WebTool module for NetDiff, these options can be configured within the module. See Section 4.2 for details on how to use the NetDiff WebTool module.

Chapter 4. Usage

There are two distinct methods of interacting with the NetDiff application. It can be invoked from the command line as with any standard Unix command. Alternatively for those running EnGarde Secure Linux, it can be administered via a web browser using the NetDiff WebTool module.

4.1. Command Line

Normally NetDiff is set up as a cron job to be run nightly, scanning the network and sending a report to the email addresses specified in the configuration file. It can be run manually from the command line, accepting one of four options.

Figure 4-1. Example of NetDiff Usage

```
Usage: netdiff [OPTION] [FILE]

-a, --all      Perform full scan and report
-s, --scan    Scan but do not report
-r, --report   Report results of last scan
-i, --import   Import FILE where FILE is an nmap XML report
```

4.2. EnGarde Secure Linux WebTool Module

Users of EnGarde Secure Linux are recommended to use the WebTool module available for NetDiff. The WebTool module will create the database automatically if it is not found, and will allow you to set scanning options, configure report recipients, and edit your list of networks to scan, as well as view all of your past reports in a browser based interface.

The main page of the NetDiff WebTool module contains a configuration link, a list of your past generated reports, and a list of your networks to scan.

Figure 4-2. NetDiff WebTool module

GUARDIAN™
DIGITAL

EnGarde™
Secure Linux

Go Back | Main Index | Logout | Custom WebTool Modules

NetDiff Network Scan Reports

NetDiff is a reporting tool that runs network scans of specified networks and can report the differences between successive scans, giving administrators a snapshot view of recent changes on their network.

[\[Configure \]](#)

Recent Reports

[05/23/2005](#) [06/01/2005](#)

Networks to Scan

[67.111.153.128/25](#) [67.111.153.64/26](#) [67.111.153.0/26](#)
[67.110.173.224/28](#)

[\[Add Network \]](#)

Guardian Digital Secure Network | Guardian Digital.com | Support | Guardian Digital Store

Clicking the configuration link launches the configuration popup, where you can set your nmap scanning options and your email report recipients. See the nmap documentation (http://www.insecure.org/nmap/nmap_documentation.html) for details on the nmap scanning options. Multiple recipient email addresses may be included if separated by commas.

Figure 4-3. NetDiff options

NetDiff Options

Here you may change the options passed to the nmap command line. It's recommended that you not change these unless you know what you're doing, see the nmap documentation for details.

Nmap Options

Here you may set the email addresses to send NetDiff reports to. Multiple addresses should be separated by commas.

Report Recipients

[Update Options](#)

Selecting a report from the list opens a window where the report's contents can be viewed and optionally deleted from the database if it is no longer needed. The report prefixes lines added since the previous scan with a + and lines removed since the previous scan with a -. For example, the report below shows that since the last scan, ports 22 and 1023 were closed and ports 25 and 53 were opened on 67.111.153.5.

Figure 4-4. NetDiff report

```

NetDiff Report for 06/01/2005
#
# Guardian Digital NetDiff Report
#
# Networks scanned:
# 67.111.153.128/25 67.111.153.64/26 67.111.153.0/26
# 67.110.173.224/28
#
# Last scan completed: 2005-06-01 15:35:24
# Scan started: 2005-06-01 15:54:16
# Scan completed: 2005-06-01 15:57:23
# Hosts Scanned/Found: 272/272
#
67.111.153.5          ** CHANGED **
ns.guardiandigital.com
-67.111.153.5        Port 22             ssh open table 3
-67.111.153.5        Port 1023          netvenuechat open table 3
+67.111.153.5        Port 25            smtp open table 3
+67.111.153.5        Port 53            domain open table 3
-----

```

Choosing a network or clicking the *Add Network* link opens a window where you may edit or delete a specified network from the scanning list. Networks must be entered in a *192.168.1.0/24* style format.

Figure 4-5. NetDiff network

Edit Network

Network

Appendix A. Resources

This section provides links where you may obtain the most recent version of NetDiff and its required software prerequisites, as well as more information about EnGarde Secure Linux and scanning networks with nmap.

- **NetDiff**

<ftp://ftp.engardelinux.org/pub/engarde/people/pax/netdiff/>

- **Perl**

<http://www.perl.com/download.csp>

- **Perl Modules (DBI, XML::Parser, and XML::Simple)**

<http://www.cpan.org>

- **MySQL**

<http://www.mysql.com>

- **Nmap Network Scanner**

<http://www.insecure.org/nmap/>

- **EnGarde Secure Linux**

<http://www.engardelinux.com/>

