RAPID7

Nexpose

Hardening Guide

Product version: 6.0

Table of contents

Revision history

Revision date	Description
November 30, 2015	Created document.

File System

The Rapid7 appliance file system consists of a *bootable ext3 partition* and an *LVM volume*.

The *LVM volume* contains the root partition */* and a LUKS encrypted */opt* partition that contains all the Nexpose data.

Installation

The Rapid7 appliance base OS is a minimal install of Ubuntu 14.04. A minimal install provides the following benefits:

- Approximately 270 packages, where a full server install typically consists of over 750 package
- Reduced attack surface (i.e. fewer packages to exploit)
- Faster patching (meaning fewer packages to upgrade)
- Improved performance (fewer services for the OS to manage)

Configuration

Users

The Rapid7 appliance is only configured with a single user account.

The username is *administrator* and the default password is *rapid7*.

The default password will expire by default upon first login. The user will then be required to set a complex password.

The password must be more than 8 characters and include at least three of the four options below:

- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character (!@#$%^&*())

The new password cannot be a simple dictionary word.

Note: The root account has no password set to allow password recovery via single-user mode.

Also, Rapid7 does not provide any other method for password recovery other than booting to single-user mode. Therefore, if a root password is set and subsequently forgotten, there is no way to recover the password.

Services

The Rapid7 appliance is configured with only 2 services that listen on the network.

- Nexpose: Listens for HTTPS requests on port 3780
- SSH: Listens for connections on port 22

Kernel Settings

The Rapid7 appliance configures several kernel parameter via sysctl settings.

The following files configure specific sysctl settings.

- 60-r7-cis.conf: CIS Benchmark specific settings
- 60-r7-nexpose.conf: Nexpose specific optimizations
- 60-r7-security.conf: Security settings not covered by CIS Benchmarks

For more details, see the corresponding *60-r7-*.conf* file in the */etc/sysctl.d/* folder on the appliance.

CIS Benchmarks

The Rapid7 appliance includes most of the CIS Benchmarks for Ubuntu 14.04.

For more details, see the CIS Ubuntu 14.04 LTS Server Benchmark.

See */root/cisBenchmark.log* on the appliance for more details about which CIS benchmarks are configured.

Not Configured

Some of the CIS benchmarks were not implemented by default.

The reason why some CIS benchmarks were not implemented varies depending on the benchmark. Some reasons include:

- Reduced functionality: Some recommended CIS benchmarks make remote management difficult
  For example, setting a boot password for grub. This would require a user to have physical access to the appliance and enter the password at the boot prompt.
- Unnecessary complexity: Some recommended CIS benchmarks for the file system introduce unnecessary complexity
  For example, creating separate partitions for /var, /var/log, and /home. There is only one user configured on the appliance and Nexpose saves all logs to the /opt partition.
- Impact Nexpose functionality: Some recommended CIS benchmarks may reduce or break Nexpose functionality
  For example, it is NOT recommended to run AppArmor or AIDE. It is also NOT recommended to run restrictive firewall rules as they can negatively impact scan performance.

Customer Configured

Some CIS benchmarks must be configured by the end user in accordance with their organization's security policies. It is recommended that customers configure the following services in accordance with their organization's security policies.

- SSH for remote management
- rsyslog for remote logging
- logrotate for log rotation
- auditd for auditing

It is also recommended that customers configure password policies in accordance with their organization's security policies

Updates

The Rapid7 appliance is shipped with all the latest Ubuntu 14.04 updates. All Ubuntu update repositories remain intact. Customers are responsible for applying all future Ubuntu updates.

A script is included on the appliance to facilitate unattended updates. Run */root/postinstall/tools/updateAppliance.sh* to apply Ubuntu updates.

Automatic Updates

The Rapid7 appliance can be configured to perform automatic updates of the Ubuntu OS.

See *etc/apt/apt.conf.d/30r7applaptupdate* for more details.

Offline Updates

The Rapid7 appliance supports performing offline OS updates in accordance with Ubuntu's recommendations.

See Ubuntu's AptGet/Offline/Repository page for complete details on offline updates.