Security By Default

A Comparative Security Evaluation of Default Configurations

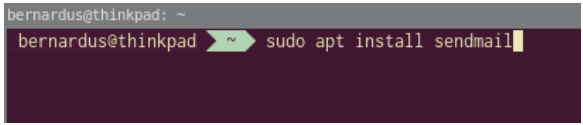
Bernardus A. Jansen, BSc

MSc System and Network Engineering
Universiteit van Amsterdam

July 3, 2018

Introduction

- Installing software from repositories is easy and accessible
- Software typically requires configuration in order to run



Introduction

- Software often ships with defaults to get up and running quickly
- Not always with security in mind

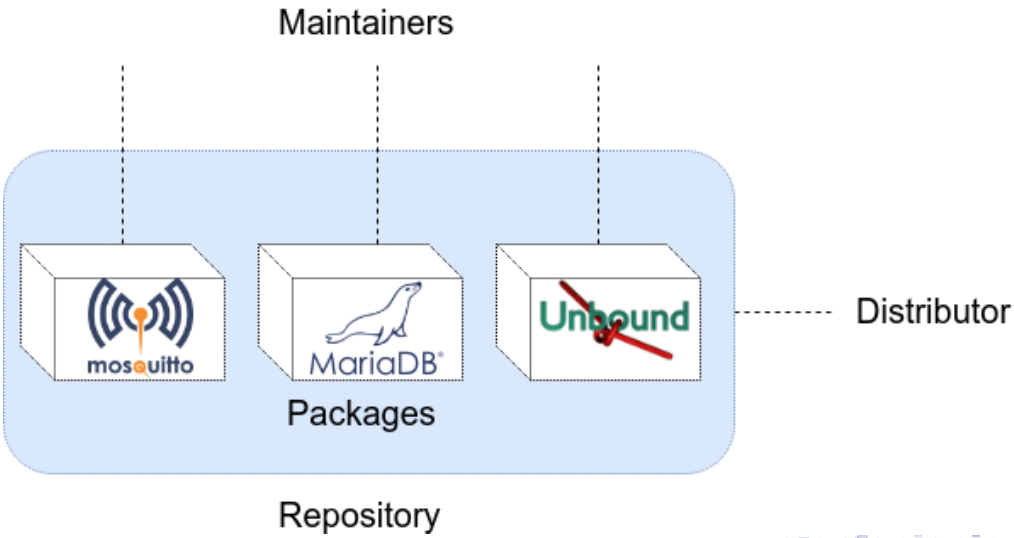
```
# Allow server to accept connections on all interfaces.
#
bind-address=0.0.0.0
#
```

Research Questions

Research Questions

- *What role do distributors play in the quality of default configurations for Internet services?*
- *What is a suitable metric to describe the security posture of default configurations for Internet services?*

Repositories



Methodology

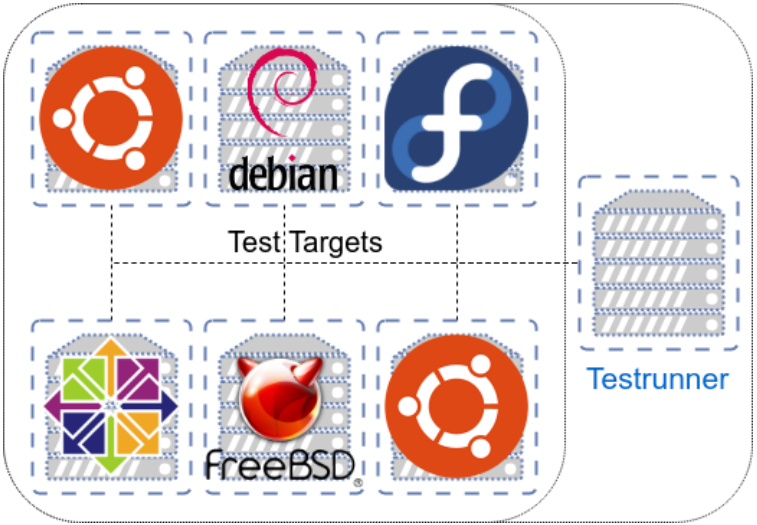
- Install software from repositories on a range of platforms
- Attempt to interact with the services from a remote test host

- Vagrant and Ansible for automated deployment of virtual machines and software
- Shell scripts to conduct tests

Platforms & Software

Platform	Version	MySQL	Unbound	Bind	NTP	MQTT	Postfix	Sendmail
Ubuntu	18.04	10.1.29-6	1.6.7	9.11.3	4.2.8p10	1.4.15-2	3.3.0	8.15.2-10
	16.04	10.0.34	1.5.8	9.10.3	4.2.8p4	1.4.8	3.1.0	8.15.2-3
	14.04	5.5.59	1.4.22	9.9.5	4.2.6p5	0.15	2.11.0	8.14.4-4
Debian	Stretch	10.1.26	1.6.0	9.10.3	4.2.8p10	1.4.10-3	3.1.8	8.15.2-8
	Jessie	10.0.35	1.4.22	9.9.5	4.2.6p5	1.3.4-2	2.11.3	8.14.4-8
CentOS	7	5.5.56	1.6.6	9.9.4	4.2.6p5	1.4.15	2.10.1	8.14.7
	6	5.1.73	1.4.20	9.8.2	4.2.6p5	N/A	2.6.6	8.14.4
Fedora	28	10.2.15	1.7.2	9.11.3	4.2.8p11	1.5	3.2.5	8.15.2
	27	10.2.15	1.7.2	9.11.3	4.2.8p11	1.5	3.2.5	8.15.2
FreeBSD	11.1	5.5.60	1.7.3	9.12.1	4.2.8p11	1.4.14_2	3.3.1,1	8.15.2
	10.4	5.5.60	1.7.3	9.12.1	4.2.8p11	1.4.14_2	3.3.1,1	8.15.2

Methodology



Results

Platform	MySQL	DNS: Bind	DNS: Unbound	NTP
Ubuntu 18.04	Bound to localhost	Open resolver	Bound to localhost	Queries blocked
Ubuntu 16.04	Bound to localhost	Open resolver	Bound to localhost	Queries blocked
Ubuntu 14.04	Bound to localhost	Open resolver	Bound to localhost	Queries blocked
Debian Stretch	Bound to localhost	Open resolver	Bound to localhost	Queries blocked
Debian Jessie	Bound to localhost	Open resolver	Bound to localhost	Queries blocked
CentOS 7	User ACL	Bound to localhost	Bound to localhost	Queries blocked
CentOS 6	User ACL	Bound to localhost	Bound to localhost	Queries blocked
Fedora 28	User ACL	Bound to localhost	Bound to localhost	Queries blocked
Fedora 27	User ACL	Bound to localhost	Bound to localhost	Queries blocked
FreeBSD 11.1	User ACL	Bound to localhost	Bound to localhost	Queries blocked
FreeBSD 10.4	User ACL	Bound to localhost	Bound to localhost	Queries blocked

Table: Overview of test results, green for secure defaults, yellow for problematic choices, red for dangerous defaults

Results

Platform	MQTT	Postfix	Sendmail
Ubuntu 18.04	Public read and write	Relay access denied	Bound to localhost
Ubuntu 16.04	Public read and write	Relay access denied	Bound to localhost
Ubuntu 14.04	Public read and write	Relay access denied	Bound to localhost
Debian Stretch	Public read and write	Relay access denied	Bound to localhost
Debian Jessie	Public read and write	Relay access denied	Bound to localhost
CentOS 7	Public read and write	Bound to localhost	Bound to localhost
CentOS 6	N/A	Bound to localhost	Bound to localhost
Fedora 28	Public read and write	Bound to localhost	Bound to localhost
Fedora 27	Public read and write	Bound to localhost	Bound to localhost
FreeBSD 11.1	Public read and write	Relay access denied	Relay access denied
FreeBSD 10.4	Public read and write	Relay access denied	Relay access denied

Table: Overview of test results, (dark)green for secure defaults, yellow for problematic choices, red for dangerous defaults

Results

- Notable differences between platforms: FreeBSD/CentOS/Fedora - Debian/Ubuntu
  - Different security policies
- NTP secure by default nowadays
- Upstream default configuration may be ignored entirely

Conclusion

Research Question

- *What is a suitable metric to describe the security posture of default configurations for Internet services?*

- Security posture can be expressed in the number of defence layers
  - On-host tests or configuration required to determine number of layers

Conclusion

Research Question

- *What role do distributors play in the quality of default configurations for Internet services?*

- Distributors have security policies
  - Enforcing different levels of security
  - Default security is influenced by no-setting defaults

Future Work

- Test more platforms and software
- Embedded devices
- Tutorial configurations
- Test Docker images
- Old installations
  - Old defaults may persist in current installations

Recap

- Installing the same software on different platforms can have different results
- As a developer, sane no-setting defaults is the most secure
  - NTP, Unbound
- Distributor has final say and responsibility for enforcing sane defaults