Server virtualization and security

Overview

- Motivation
- Virtualization
  - Setup process (DigitalOcean)
- Securing a new Ubuntu VM
  - Software patching
  - Access control
  - Firewall setup
  - Monitoring
  - Testing

Health records in Montana hacked, compromises personal data of 1.3 million people

By **Anu Passary**, Tech Times | June 25, 8:36 AM

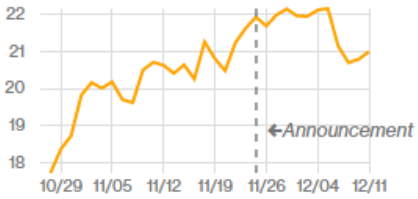
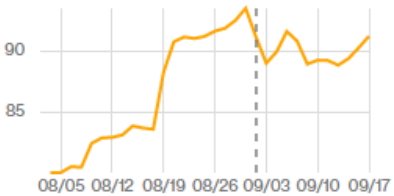
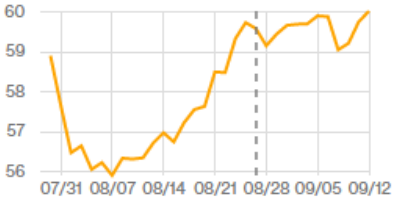
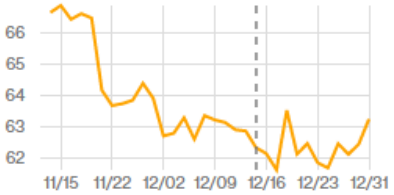
State health department records of 1.3 million people in Montana have been hacked, compromising personal data. The state is offering free credit monitoring and identity-fraud insurance to those affected.
(Photo : Matylda Czarnecka)

Personal data of 1.3 million people have been compromised in Montana as state health department records have been hacked.

The data breach occurred in July 2013, but was discovered in mid-May this year by a computer security contractor who noticed "suspicious activity" on one of the computers in Helena. The state health department acknowledged the data hacking on May 29 this year.

The State of Montana is sending notification letters to the victims of the attack, cautioning them that hackers may have access to their personal details because of the data breach on the state health department's server. Sensitive information that was on the server and has potentially made its way into the hands of hackers includes addresses, names, social security numbers, date of birth, birth/death certificates, prescriptions, insurance and medical records of the residents of Montana.

http://www.techtimes.com/articles/9150/20140625/health-records-in-montana-hacked-compromises-personal-data-of-1-3-million-people.htm

	U.S. STOCK PRICE	RECORDS STOLEN	TYPE
Sony Announced: 11/25/2014 Hackers broke into its network and exposed employment and salary records, documents and embarrassing private emails between Hollywood executives.		47,000	Credit card numbers Social Security numbers **Proprietary information** **Employee details** Email addresses Phone numbers Physical addresses Login credentials
Home Depot Announced: 09/02/2014 The company said 56 million payment cards had been stolen, and later disclosed 53 million e-mail addresses had also been pilfered.		109M	**Credit card numbers** Social Security numbers Proprietary information Employee details **Email addresses** Phone numbers Physical addresses Login credentials
JPMorgan Announced: 08/27/2014 The biggest U.S. bank said a data breach affected 76 million households and 7 million small businesses.		83M	Credit card numbers Social Security numbers Proprietary information Employee details **Email addresses** Phone numbers **Physical addresses** Login credentials
EBay Announced: 05/21/2014 In a massive attack, hackers took customers' personal information, affecting up to 145 million active users.		145M	Credit card numbers Social Security numbers Proprietary information Employee details **Email addresses** Phone numbers **Physical addresses** **Login credentials**
Target Announced: 12/13/2013 Though announced at the end of 2013, the effects of this breach carried into 2014. Target said its U.S. sales were "meaningfully weaker" after the data theft was disclosed.		110M	**Credit card numbers** Social Security numbers Proprietary information Employee details Email addresses Phone numbers Physical addresses Login credentials

http://www.bloomberg.com/graphics/2014-data-breaches/

Linode Manager

[redacted] | my profile | log out

Linodes | NodeBalancers | Longview | DNS Manager | Account | Support | Documentation | Community

Dashboard | Remote Access | Rebuild | Rescue | Resize | Clone | Graphs | Backups | Settings | Extras

Linodes » **linode**[redacted]

Dashboard

Select	Configuration Profiles	Options
◉	My Ubuntu 10.10 Profile (Latest 2.6 (2.6.39.1-linode34))	Edit | Remove

Reboot

Rebuild | Deploy an Image | Create a new Configuration Profile

Disks

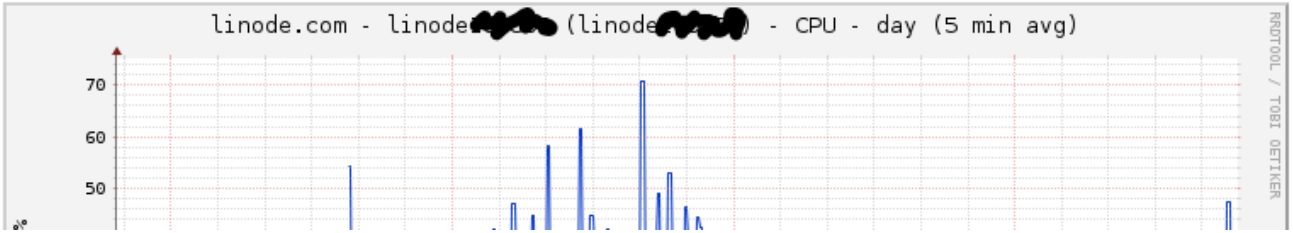
Ubuntu 10.10 Disk Image (48896 MB, ext3)	Edit | Remove
256MB Swap Image (256 MB, swap)	Edit | Remove

Create a new Disk

Host Job Queue (more)

Success	**Lassie initiated boot: My Ubuntu 10.10 Profile**	Entered: 5 months 4 days ago - Took: 15 seconds
Success	**System Boot** - My Ubuntu 10.10 Profile	Entered: 5 months 14 days ago - Took: 17 seconds
Success	**System Shutdown**	Entered: 5 months 14 days ago - Took: 2 minutes, 11 seconds
Success	**Linode Snapshot**	Entered: 7 months 12 days ago - Took: 4 minutes, 0 seconds

Graphs



Server Status

Your Linode is currently

Running

Shut down

157 days uptime

Network

- Transfer/mo: 2000 GB
- Incoming: 45.0 GB
- Outgoing: 16.0 GB
- Total: 61.0 GB

You have used

0%

of your monthly transfer

Storage

- Total: 49152 MB
- Used: 49152 MB
- Free: 0 MB

You have allocated

100%

towards disk images

Backups

Enabled!

Last backup was 9 hours ago

Host

dallas[redacted] — online

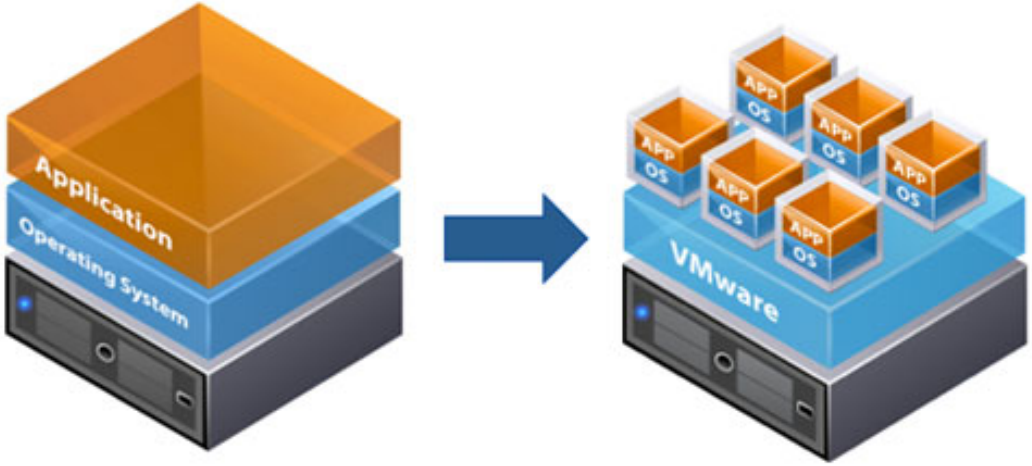
idle — Load

```
Jan 13 07:53:57 topi sshd[4410]: Failed password for invalid user root from 87.106.47.213 port 34830 ssh2
Jan 13 07:53:58 topi sshd[4413]: Invalid user admin from 87.106.47.213
Jan 13 07:53:58 topi sshd[4413]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 07:53:58 topi sshd[4413]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=s15381625.onlinehome-server.info
Jan 13 07:54:00 topi sshd[4413]: Failed password for invalid user admin from 87.106.47.213 port 34873 ssh2
Jan 13 07:57:12 topi sshd[4423]: Invalid user PlcmSpIp from 58.215.188.65
Jan 13 07:57:12 topi sshd[4423]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 07:57:12 topi sshd[4423]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=58.215.188.65
Jan 13 07:57:14 topi sshd[4423]: Failed password for invalid user PlcmSpIp from 58.215.188.65 port 7176 ssh2
Jan 13 07:59:44 topi sshd[4426]: Invalid user aaron from 58.215.188.65
Jan 13 07:59:44 topi sshd[4426]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 07:59:44 topi sshd[4426]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=58.215.188.65
Jan 13 07:59:46 topi sshd[4426]: Failed password for invalid user aaron from 58.215.188.65 port 42001 ssh2
Jan 13 08:27:56 topi sshd[4594]: Invalid user default from 58.215.188.65
Jan 13 08:27:56 topi sshd[4594]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 08:27:56 topi sshd[4594]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=58.215.188.65
Jan 13 08:27:58 topi sshd[4594]: Failed password for invalid user default from 58.215.188.65 port 56402 ssh2
Jan 13 08:27:58 topi sshd[4594]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 08:28:00 topi sshd[4594]: Failed password for invalid user default from 58.215.188.65 port 56402 ssh2
Jan 13 08:28:01 topi sshd[4594]: PAM 1 more authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=58.215.18
8.65
Jan 13 08:29:10 topi sshd[4611]: User root from thomasw.de not allowed because not listed in AllowUsers
Jan 13 08:29:10 topi sshd[4611]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=thomasw.de  user=root
Jan 13 08:29:12 topi sshd[4611]: Failed password for invalid user root from 87.106.50.214 port 48502 ssh2
Jan 13 08:29:13 topi sshd[4614]: Invalid user admin from 87.106.50.214
Jan 13 08:29:13 topi sshd[4614]: pam_unix(sshd:auth): check pass; user unknown
Jan 13 08:29:13 topi sshd[4614]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=thomasw.de
Jan 13 08:29:15 topi sshd[4614]: Failed password for invalid user admin from 87.106.50.214 port 49145 ssh2
Jan 13 09:25:47 topi sshd[4831]: User root from 62-210-180-180.rev.poneytelecom.eu not allowed because not listed in All
owUsers
Jan 13 09:25:47 topi sshd[4831]: Failed none for invalid user root from 62.210.180.180 port 47919 ssh2
Jan 13 09:25:47 topi sshd[4831]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=62-210-180-180.rev.poneytelecom.eu  user=root
Jan 13 09:25:49 topi sshd[4831]: Failed password for invalid user root from 62.210.180.180 port 47919 ssh2
Jan 13 09:25:53 topi sshd[4831]: last message repeated 2 times
Jan 13 09:25:53 topi sshd[4831]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=62-210-1
80-180.rev.poneytelecom.eu  user=root
Jan 13 09:25:54 topi sshd[4834]: User root from 62-210-180-180.rev.poneytelecom.eu not allowed because not listed in All
owUsers
Jan 13 09:25:54 topi sshd[4834]: Failed none for invalid user root from 62.210.180.180 port 33950 ssh2
Jan 13 09:25:54 topi sshd[4834]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost
=62-210-180-180.rev.poneytelecom.eu  user=root
Jan 13 09:25:56 topi sshd[4834]: Failed password for invalid user root from 62.210.180.180 port 33950 ssh2
Jan 13 11:38:38 topi su[5411]: pam_authenticate: Authentication failure
root@topi:/var/log#
```

```
2015-01-12 16:39:07,619 fail2ban.actions: WARNING [ssh] Unban 222.186.34.161
2015-01-12 19:05:57,904 fail2ban.actions: WARNING [ssh] Ban 186.119.139.130
2015-01-12 19:25:58,331 fail2ban.actions: WARNING [ssh] Unban 186.119.139.130
2015-01-12 19:34:27,932 fail2ban.actions: WARNING [ssh] Ban 186.119.139.130
2015-01-12 19:54:28,373 fail2ban.actions: WARNING [ssh] Unban 186.119.139.130
2015-01-12 20:53:13,448 fail2ban.actions: WARNING [ssh] Ban 79.168.80.100
2015-01-12 21:03:29,190 fail2ban.actions: WARNING [ssh] Ban 122.225.103.73
2015-01-12 21:03:30,851 fail2ban.actions: WARNING [fail2ban] Ban 122.225.103.73
2015-01-12 21:13:13,911 fail2ban.actions: WARNING [ssh] Unban 79.168.80.100
2015-01-12 21:23:29,644 fail2ban.actions: WARNING [ssh] Unban 122.225.103.73
2015-01-12 21:47:25,334 fail2ban.actions: WARNING [ssh] Ban 62.210.180.72
2015-01-12 22:07:25,722 fail2ban.actions: WARNING [ssh] Unban 62.210.180.72
2015-01-13 00:05:29,908 fail2ban.actions: WARNING [ssh] Ban 68.178.128.177
2015-01-13 00:15:27,619 fail2ban.actions: WARNING [ssh] Ban 122.225.97.67
2015-01-13 00:15:28,645 fail2ban.actions: WARNING [fail2ban] Ban 122.225.97.67
2015-01-13 00:25:30,366 fail2ban.actions: WARNING [ssh] Unban 68.178.128.177
2015-01-13 00:27:51,562 fail2ban.actions: WARNING [ssh] Ban 68.178.128.177
2015-01-13 00:35:28,131 fail2ban.actions: WARNING [ssh] Unban 122.225.97.67
2015-01-13 00:47:52,038 fail2ban.actions: WARNING [ssh] Unban 68.178.128.177
2015-01-13 00:50:22,227 fail2ban.actions: WARNING [ssh] Ban 68.178.128.177
2015-01-13 00:50:22,932 fail2ban.actions: WARNING [fail2ban] Ban 68.178.128.177
2015-01-13 01:10:22,638 fail2ban.actions: WARNING [ssh] Unban 68.178.128.177
2015-01-13 01:35:45,505 fail2ban.actions: WARNING [ssh] Ban 180.210.234.87
2015-01-13 01:35:46,134 fail2ban.actions: WARNING [fail2ban] Ban 180.210.234.87
2015-01-13 01:55:45,932 fail2ban.actions: WARNING [ssh] Unban 180.210.234.87
2015-01-13 03:44:29,648 fail2ban.actions: WARNING [ssh] Ban 61.174.51.220
2015-01-13 03:44:29,942 fail2ban.actions: WARNING [fail2ban] 61.174.51.220 already banned
2015-01-13 04:04:30,068 fail2ban.actions: WARNING [ssh] Unban 61.174.51.220
2015-01-13 04:06:10,198 fail2ban.actions: WARNING [ssh] Ban 213.165.91.120
2015-01-13 04:26:10,584 fail2ban.actions: WARNING [ssh] Unban 213.165.91.120
2015-01-13 04:33:22,106 fail2ban.actions: WARNING [ssh] Ban 213.165.91.120
2015-01-13 04:33:22,383 fail2ban.actions: WARNING [fail2ban] Ban 213.165.91.120
2015-01-13 04:37:27,409 fail2ban.actions: WARNING [ssh] Ban 222.73.226.7
2015-01-13 04:53:22,539 fail2ban.actions: WARNING [ssh] Unban 213.165.91.120
2015-01-13 04:57:27,842 fail2ban.actions: WARNING [ssh] Unban 222.73.226.7
2015-01-13 05:02:27,205 fail2ban.actions: WARNING [ssh] Ban 222.73.226.7
2015-01-13 05:02:28,115 fail2ban.actions: WARNING [fail2ban] Ban 222.73.226.7
2015-01-13 05:22:27,627 fail2ban.actions: WARNING [ssh] Unban 222.73.226.7
2015-01-13 06:00:46,293 fail2ban.actions: WARNING [ssh] Ban 50.62.161.74
2015-01-13 06:20:46,710 fail2ban.actions: WARNING [ssh] Unban 50.62.161.74
2015-01-13 07:53:59,135 fail2ban.actions: WARNING [ssh] Ban 87.106.47.213
2015-01-13 07:59:44,574 fail2ban.actions: WARNING [ssh] Ban 58.215.188.65
2015-01-13 08:13:59,589 fail2ban.actions: WARNING [ssh] Unban 87.106.47.213
2015-01-13 08:19:45,010 fail2ban.actions: WARNING [ssh] Unban 58.215.188.65
2015-01-13 08:28:01,588 fail2ban.actions: WARNING [ssh] Ban 58.215.188.65
2015-01-13 08:28:03,406 fail2ban.actions: WARNING [fail2ban] Ban 58.215.188.65
2015-01-13 08:29:14,705 fail2ban.actions: WARNING [ssh] Ban 87.106.50.214
2015-01-13 08:48:02,036 fail2ban.actions: WARNING [ssh] Unban 58.215.188.65
2015-01-13 08:49:15,141 fail2ban.actions: WARNING [ssh] Unban 87.106.50.214
2015-01-13 09:25:55,678 fail2ban.actions: WARNING [ssh] Ban 62.210.180.180
2015-01-13 09:45:56,068 fail2ban.actions: WARNING [ssh] Unban 62.210.180.180
root@topi:/var/log#
```

Virtualization

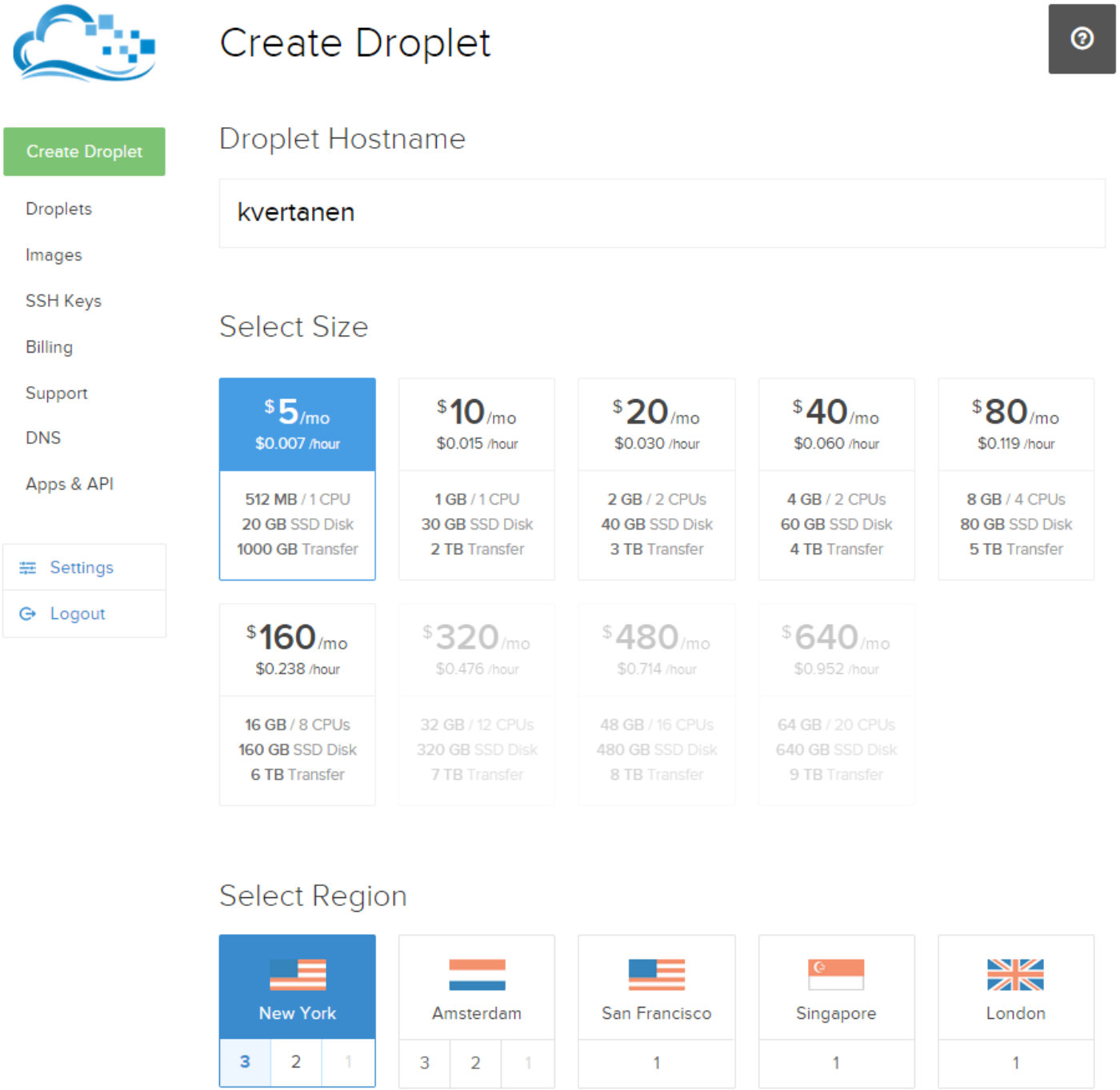
- Virtual machine (VM)
  - Isolated software container with OS and app
  - Separate and independent
  - Many can run simultaneously on a single computer



Traditional Architecture Virtual Architecture

http://www.vmware.com/virtualization/virtualization-basics/how-virtualization-works

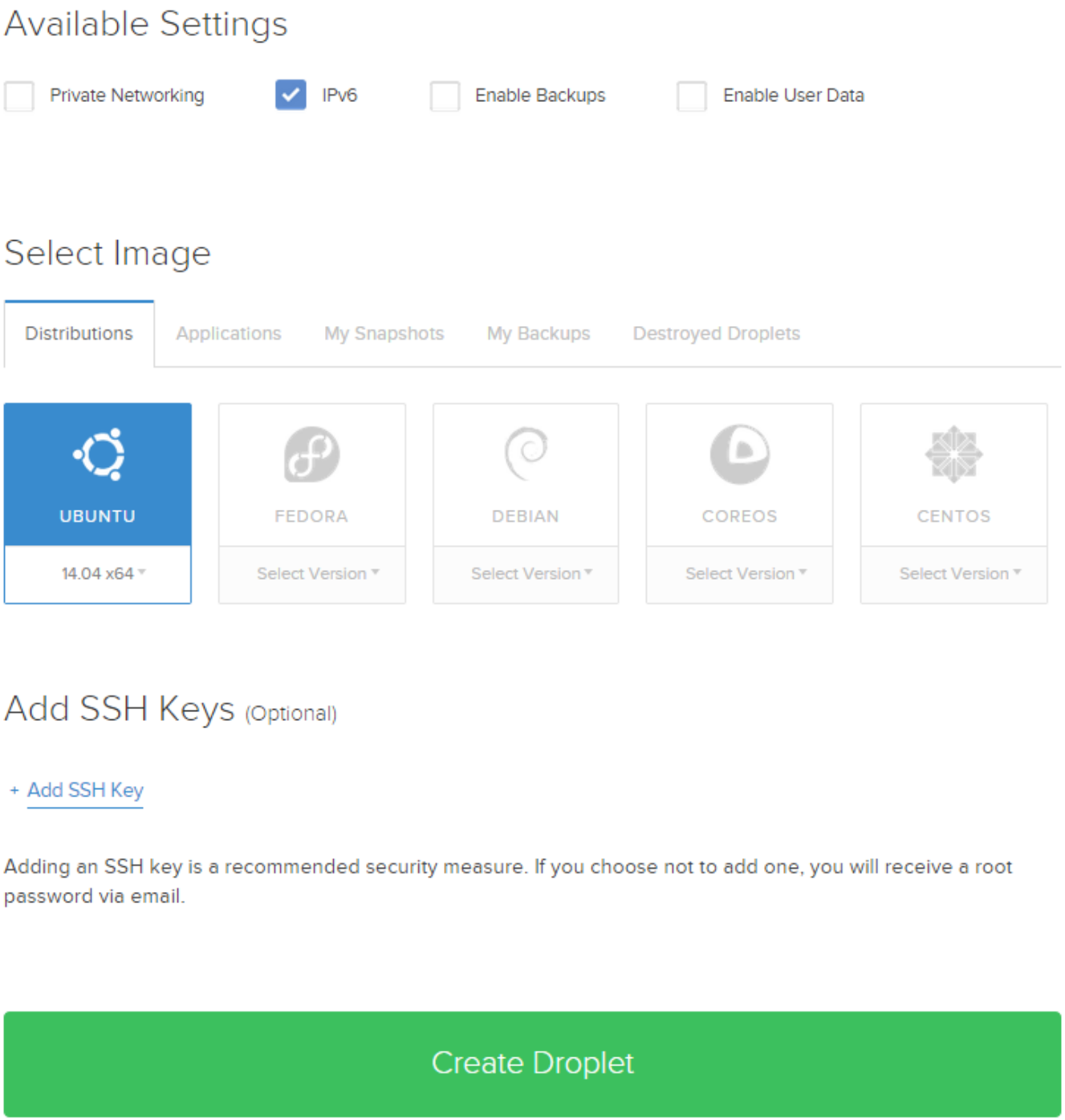
Creating VM



<u>Step 1:</u>
Signup, verify email, credit card details

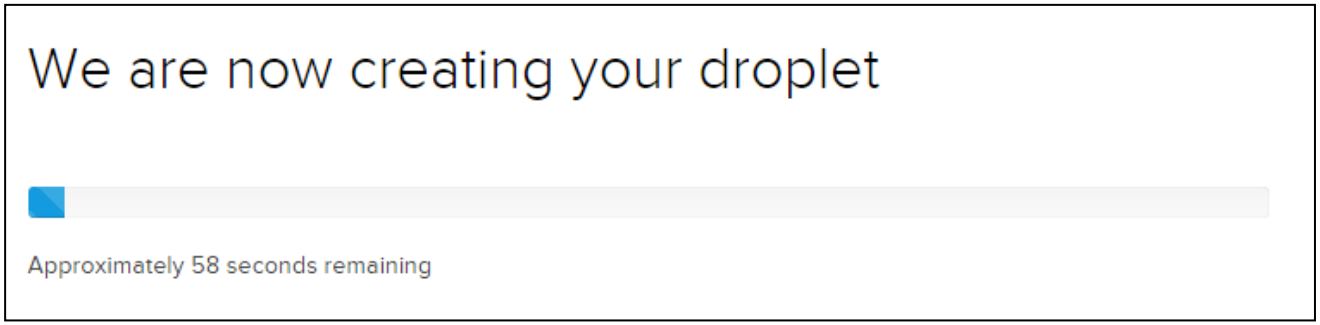
<u>Step 2:</u> Configure desired resources, physical location, features, initial account access

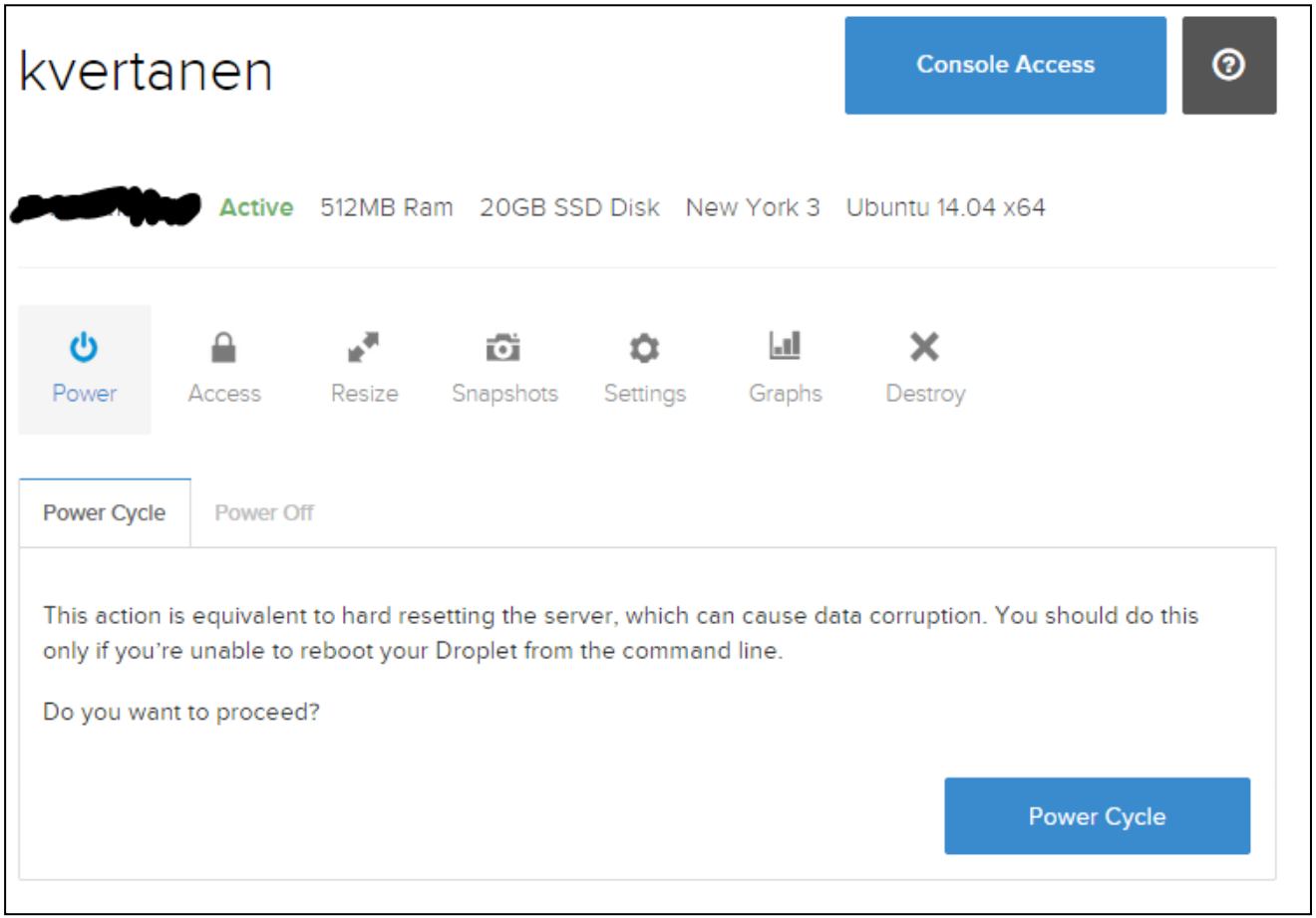
Creating VM



<u>Step 1:</u>
Signup, verify email, credit card details

<u>Step 2:</u> Configure desired resources, physical location, features, initial account access





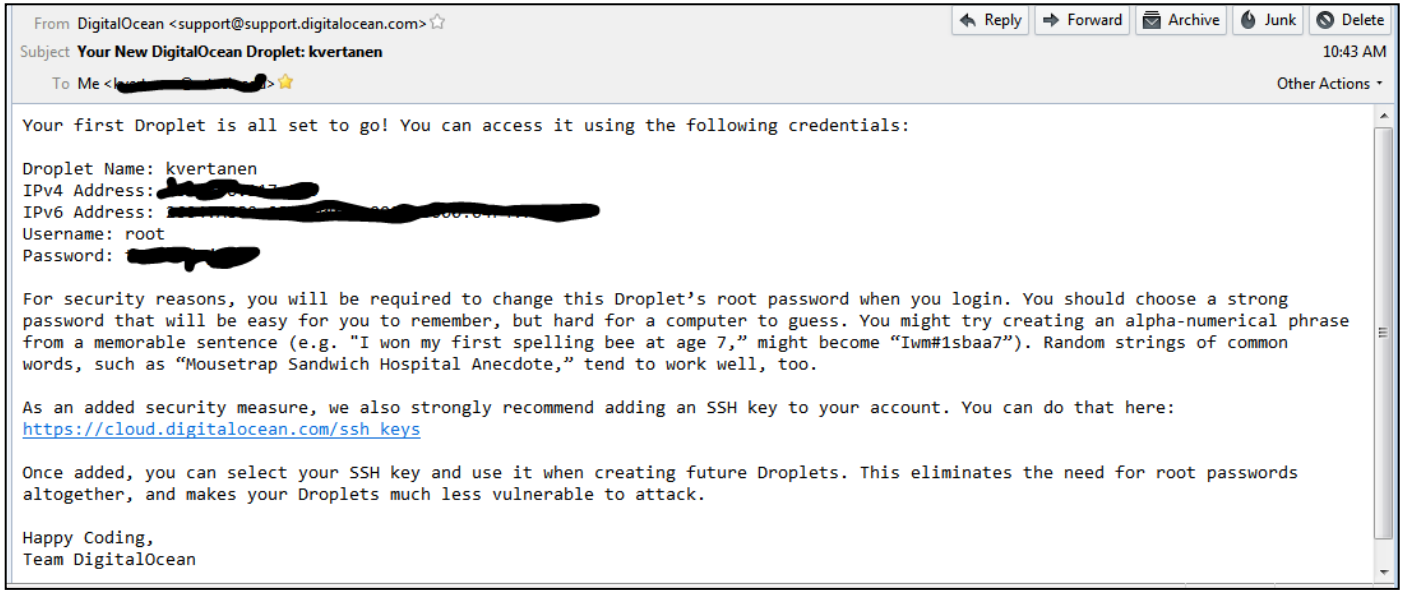
Creating VM

Step 1:
Signup, verify email, credit card details

Step 2: Configure desired resources, physical location, features, initial account access

Step 3: Wait 1 minute

Creating VM



From DigitalOcean <support@support.digitalocean.com>
Subject **Your New DigitalOcean Droplet: kvertanen**
To Me <[redacted]>

Reply | Forward | Archive | Junk | Delete
10:43 AM
Other Actions

Your first Droplet is all set to go! You can access it using the following credentials:

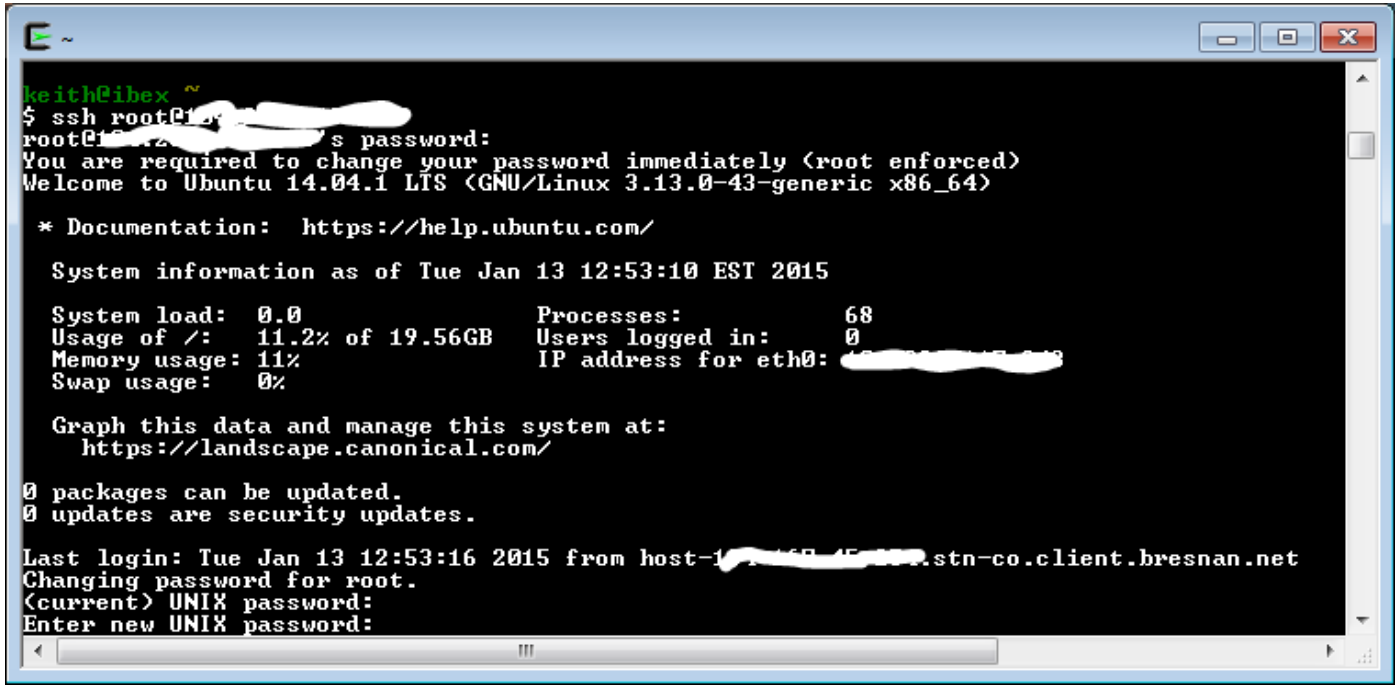
Droplet Name: kvertanen
IPv4 Address: [redacted]
IPv6 Address: [redacted]
Username: root
Password: [redacted]

For security reasons, you will be required to change this Droplet's root password when you login. You should choose a strong password that will be easy for you to remember, but hard for a computer to guess. You might try creating an alpha-numerical phrase from a memorable sentence (e.g. "I won my first spelling bee at age 7," might become "Iwm#1sbaa7"). Random strings of common words, such as "Mousetrap Sandwich Hospital Anecdote," tend to work well, too.

As an added security measure, we also strongly recommend adding an SSH key to your account. You can do that here:
https://cloud.digitalocean.com/ssh_keys

Once added, you can select your SSH key and use it when creating future Droplets. This eliminates the need for root passwords altogether, and makes your Droplets much less vulnerable to attack.

Happy Coding,
Team DigitalOcean



```
keith@ibex ~
$ ssh root@[redacted]
root@[redacted]'s password:
You are required to change your password immediately (root enforced)
Welcome to Ubuntu 14.04.1 LTS (GNU/Linux 3.13.0-43-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Jan 13 12:53:10 EST 2015

  System load:  0.0                Processes:           68
  Usage of /:   11.2% of 19.56GB   Users logged in:     0
  Memory usage: 11%                IP address for eth0: [redacted]
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/

0 packages can be updated.
0 updates are security updates.

Last login: Tue Jan 13 12:53:16 2015 from host-[redacted].stn-co.client.bresnan.net
Changing password for root.
(current) UNIX password:
Enter new UNIX password:
```

Step 1:
Signup, verify email, credit card details

Step 2: Configure desired resources, physical location, features, initial account access

Step 3: Wait 1 minute

Step 4: Change emailed root password to something hard to guess

Grab lunch, and then…

```
% more /var/log/auth.log
Jan 13 12:44:47 kvertanen sshd[1002]: Server listening on 0.0.0.0 port 22.
...
Jan 13 13:49:32 kvertanen sshd[1371]: reverse mapping checking getaddrinfo for huzhou.ctc.mx.fund123.cn
[122.225.97.84] failed - POSSIBLE BREAK-IN ATTEMPT!
Jan 13 13:49:33 kvertanen sshd[1371]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=122.225.97.84  user=root
Jan 13 13:49:35 kvertanen sshd[1371]: Failed password for root from 122.225.97.84 port 15186 ssh2
Jan 13 13:49:46 kvertanen sshd[1371]: message repeated 5 times: [ Failed password for root from 122.225.97.84
port 15186 ssh2]
Jan 13 13:49:46 kvertanen sshd[1371]: Disconnecting: Too many authentication failures for root [preauth]
Jan 13 13:49:46 kvertanen sshd[1371]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=122.225.97.84  user=root
Jan 13 13:49:46 kvertanen sshd[1371]: PAM service(sshd) ignoring max retries; 6 > 3
Jan 13 13:49:47 kvertanen sshd[1373]: error: Could not load host key: /etc/ssh/ssh_host_ed25519_key
Jan 13 13:49:48 kvertanen sshd[1373]: reverse mapping checking getaddrinfo for huzhou.ctc.mx.fund123.cn
[122.225.97.84] failed - POSSIBLE BREAK-IN ATTEMPT!
Jan 13 13:49:49 kvertanen sshd[1373]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=122.225.97.84  user=root
Jan 13 13:49:51 kvertanen sshd[1373]: Failed password for root from 122.225.97.84 port 16507 ssh2
Jan 13 13:49:53 kvertanen sshd[1375]: error: Could not load host key: /etc/ssh/ssh_host_ed25519_key
Jan 13 13:50:03 kvertanen sshd[1373]: message repeated 5 times: [ Failed password for root from 122.225.97.84
port 16507 ssh2]
Jan 13 13:50:03 kvertanen sshd[1373]: Disconnecting: Too many authentication failures for root [preauth]
Jan 13 13:50:03 kvertanen sshd[1373]: PAM 5 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser=
rhost=122.225.97.84  user=root
Jan 13 13:50:03 kvertanen sshd[1373]: PAM service(sshd) ignoring max retries; 6 > 3
Jan 13 13:50:03 kvertanen sshd[1377]: error: Could not load host key: /etc/ssh/ssh_host_ed25519_key
Jan 13 13:50:05 kvertanen sshd[1377]: reverse mapping checking getaddrinfo for huzhou.ctc.mx.fund123.cn
[122.225.97.84] failed - POSSIBLE BREAK-IN ATTEMPT!
Jan 13 13:50:05 kvertanen sshd[1377]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=122.225.97.84  user=root
Jan 13 13:50:07 kvertanen sshd[1377]: Failed password for root from 122.225.97.84 port 20165 ssh2
Jan 13 13:50:11 kvertanen sshd[1375]: reverse mapping checking getaddrinfo for huzhou.ctc.mx.fund123.cn
[122.225.97.84] failed - POSSIBLE BREAK-IN ATTEMPT!
Jan 13 13:50:11 kvertanen sshd[1375]: pam_unix(sshd:auth): authentication failure; logname= uid=0 eu
```

0: Initial vulnerability testing

```
% sudo nmap 123.123.123.123

Starting Nmap 6.40 ( http://nmap.org ) at 2015-01-13 11:50
MST
Nmap scan report for 123.123.123.123
Host is up (0.094s latency).
Not shown: 995 closed ports
PORT     STATE    SERVICE
22/tcp   open     ssh
135/tcp  filtered msrpc
139/tcp  filtered netbios-ssn
445/tcp  filtered microsoft-ds
593/tcp  filtered http-rpc-epmap

Nmap done: 1 IP address (1 host up) scanned in 322.51
seconds
```

Run `nmap` to scan for open ports on the VM

```
% apt-get update
Ign http://mirrors.digitalocean.com trusty InRelease
...
Fetched 2,533 kB in 4s (625 kB/s)
Reading package lists... Done

% apt-get install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
...
The following NEW packages will be installed:
  fail2ban python-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 3 not
upgraded.
Need to get 184 kB of archives.
After this operation, 927 kB of additional disk space will
be used.
Do you want to continue? [Y/n] Y
...

% more /var/log/fail2ban.log
2015-01-13 14:33:46,613 fail2ban.jail   : INFO   Jail 'ssh'
started
2015-01-13 15:09:40,229 fail2ban.actions: WARNING [ssh] Ban
122.225.109.195
2015-01-13 15:19:40,969 fail2ban.actions: WARNING [ssh]
Unban 122.225.109.195
```

1: Securing SSH

Threat:
Unauthorized logins

Mitigation:
Install `fail2ban`

Create non-obvious username with sudo privileges

Only allow login from non-obvious username

Disable root login

Move SSH from port 22 to another port below 1024

Switch to public/private key authentication

```
% adduser kvertanen
Adding user `kvertanen' ...
Adding new group `kvertanen' (1000) ...
Adding new user `kvertanen' (1000) with group
`kvertanen' ...
Creating home directory `/home/kvertanen' ...
Copying files from `/etc/skel' ...
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
Changing the user information for kvertanen
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
% visudo
```

Add new user by duplicating root reference:

```
root      ALL=(ALL:ALL) ALL
kvertanen ALL=(ALL:ALL) ALL
```

1: Securing SSH

Threat:
Unauthorized logins

Mitigation:
Install `fail2ban`

Create non-obvious username with sudo privileges

Only allow login from non-obvious username

Disable root login

Move SSH from port 22 to another port below 1024

Switch to public/private key authentication

```
% nano /etc/ssh/sshd_config
```

Restrict to given user (optionally, specific IP address using @):

```
AllowUsers kvertanen
```

Disable login using root username:

```
PermitRootLogin no
```

Move to different port, e.g. 587 (but below 1024 so as to require root privileges to start):

```
Port 587
```

Restart SSH server:

```
% service ssh restart
```

Test in new terminal window:

```
% ssh -p 587kvertanen@123.123.123.123
kvertanen@123.123.123.123's password:
Welcome to Ubuntu
...
% ssh -p 587root@123.123.123.123
kvertanen@123.123.123.123's password:
Permission denied, please try again.
% ssh kvertanen@123.123.123.123
ssh: connect to host 104.236.117.243 port 22: Connection
refused
```

1: Securing SSH

Threat:
Unauthorized logins

Mitigation:
Install `fail2ban`

Create non-obvious username with sudo privileges

Only allow login from non-obvious username

Disable root login

Move SSH from port 22 to another port below 1024

Switch to public/private key authentication

1: Securing SSH

Prepare location on VM for public keys (as the non-root user):

```
% ssh -p 587 kvertanen@123.123.123.123
kvertanen@123.123.123.123's password:
Welcome to Ubuntu
...
% mkdir /home/kvertanen/.ssh
% chmod 700 /home/kvertanen/.ssh
```

Create a public/private key pair on local client (e.g. on katie):

```
% ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/staff/
vertanen/.ssh/id_rsa): id_digital
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in id_digital.
Your public key has been saved in id_digital.pub.
...
% ls -l id_digital*
-rw------- 1 vertanen staff 1675 Jan 13 13:34 id_digital
-rw-r--r-- 1 vertanen staff  396 Jan 13 13:34 id_digital.pub
```

id_digital = your private RSA key (keep somewhere safe)
id_digital.pub = your public RSA key (goes on server in ~/.ssh/authorized_keys)

Threat:
Unauthorized logins

Mitigation:
Install `fail2ban`

Create non-obvious username with sudo privileges

Only allow login from non-obvious username

Disable root login

Move SSH from port 22 to another port below 1024

Switch to public/private key authentication

1: Securing SSH

Copy public key from client onto VM:

```
% cat ./id_digital.pub | ssh -p 587kvertanen@123.123.123.123
"cat >> ~/.ssh/authorized_keys"
kvertanen@123.123.123.123's password:
```

Test out logging in using private key:

```
% ssh -p 587 -i id_digital kvertanen@123.123.123.123
Welcome to Ubuntu
...
```

Prevent password-based logins:

```
% nano /etc/ssh/sshd_config
```

```
PasswordAuthentication No
```

Restart SSH server:

```
% service ssh restart
```

Threat:
Unauthorized logins

Mitigation:
Install `fail2ban`

Create non-obvious username with sudo privileges

Only allow login from non-obvious username

Disable root login

Move SSH from port 22 to another port below 1024

Switch to public/private key authentication

```
% apt-get update
Ign http://mirrors.digitalocean.com trusty InRelease
...
Get:18 http://security.ubuntu.com trusty-security/main
Translation-en [97.0 kB]
Hit http://security.ubuntu.com trusty-security/universe
Translation-en
Fetched 2,533 kB in 4s (625 kB/s)
Reading package lists... Done

% apt-get upgrade
Reading package lists... Done
...
5 upgraded, 0 newly installed, 0 to remove and 3 not
upgraded.
Need to get 1,538 kB of archives.
After this operation, 8,192 B disk space will be freed.
Do you want to continue? [Y/n] Y
Get:1 http://mirrors.digitalocean.com/ubuntu/ trusty-
updates/main libssl1.0.0 amd64 1.0.1f-1ubuntu2.
8 [826 kB]
...
Fetched 1,538 kB in 0s (3,314 kB/s)
Preconfiguring packages ...
(Reading database ... 146178 files and directories
currently installed.)
Unpacking libssl1.0.0:amd64 (1.0.1f-1ubuntu2.8) over
(1.0.1f-1ubuntu2.7) ...
...
```

2: Securing software

Threat:
Exploit of known software vulnerabilities

Mitigation:
Make sure you are starting with up-to-date software

Configure automatic security updates

Verify automatic updates are working

```
% apt-get install unattended-upgrades
```

Edit `/etc/apt/apt.conf.d/50unattended-upgrades`
Change to include unattended-upgrades:

```
Unattended-Upgrade::Allowed-Origins {
     "Ubuntu precise-security";
     // "Ubuntu precise-updates";
  };
```

Edit `/etc/apt/apt.conf.d/10periodic`
Change to:

```
APT::Periodic::Update-Package-Lists "1";
APT::Periodic::Download-Upgradeable-Packages "1";
APT::Periodic::AutocleanInterval "7";
APT::Periodic::Unattended-Upgrade "1";
```

2: Securing software

Threat:
Exploit of known software vulnerabilities

Mitigation:
Make sure you are starting with up-to-date software

Configure automatic security updates

Verify automatic updates are working (after a day)

```
% more /var/log/unattended-upgrades/unattended-upgrades.log
```

```
2015-01-12 07:57:40,315 INFO Initial blacklisted packages:
2015-01-12 07:57:40,315 INFO Starting unattended upgrades script
2015-01-12 07:57:40,315 INFO Allowed origins are: ['o=Ubuntu,a=trusty-
security']
2015-01-12 07:57:49,592 INFO Packages that will be upgraded:
liboxideqt-qmlplugin linux-generic linux-headers-generic li
nux-image-generic oxideqt-codecs-extra
2015-01-12 07:57:49,592 INFO Writing dpkg log to '/var/log/unattended-
upgrades/unattended-upgrades-dpkg_2015-01-12_07:57
:49.592511.log'
2015-01-12 07:58:44,956 INFO All upgrades installed
2015-01-13 07:54:41,448 INFO Initial blacklisted packages:
2015-01-13 07:54:41,449 INFO Starting unattended upgrades script
2015-01-13 07:54:41,449 INFO Allowed origins are: ['o=Ubuntu,a=trusty-
security']
2015-01-13 07:54:53,582 INFO Packages that will be upgraded:
libssl1.0.0 linux-generic linux-generic-lts-saucy linux-gen
eric-lts-trusty linux-headers-generic linux-headers-generic-lts-saucy
linux-headers-generic-lts-trusty linux-image-gener
ic linux-image-generic-lts-saucy linux-image-generic-lts-trusty linux-
libc-dev openssl
2015-01-13 07:54:53,583 INFO Writing dpkg log to '/var/log/unattended-
upgrades/unattended-upgrades-dpkg_2015-01-13_07:54
:53.583043.log'
2015-01-13 07:55:50,474 INFO All upgrades installed
```

2: Securing software

Threat:
Exploit of known software vulnerabilities

Mitigation:
Make sure you are starting with up-to-date software

Configure automatic security updates

Verify automatic updates are working (after a day)

3: Securing network

Add needed ports (at a minimum port that SSH is on):

```
% ufw allow 587
% ufw enable
Command may disrupt existing ssh connections. Proceed with
operation (y|n)? y
Firewall is active and enabled on system startup

% ufw status
Status: active

To                         Action      From
--                         ------      ----
587                        ALLOW       Anywhere
587 (v6)                   ALLOW       Anywhere (v6)
```

Verify ports are closed using Nmap:

```
% sudo nmap 123.123.123.123
Starting Nmap 6.40 ( http://nmap.org )
Nmap scan report for 123.123.123.123
Host is up (0.55s latency).
Not shown: 999 filtered ports
PORT    STATE SERVICE
587/tcp open  fw1-secureremote

Nmap done: 1 IP address (1 host up) scanned in 47.73 seconds
```

Threat:
Exploits on other (unneeded) network services

Mitigation:
Use a software firewall, open only needed ports

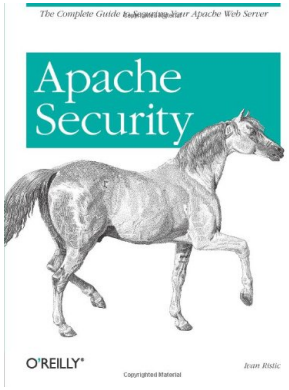
Further securing

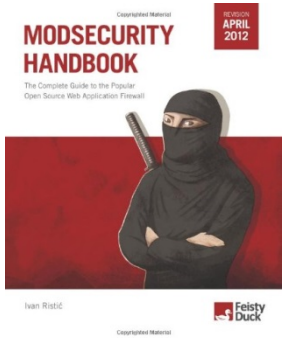
- Intrusion Detection System (IDS)
  - Monitors for suspicious activities
  - Network-based
    - Packets on the network
  - Host-based
    - Monitor logs, files
  - Send out warnings via email, etc.

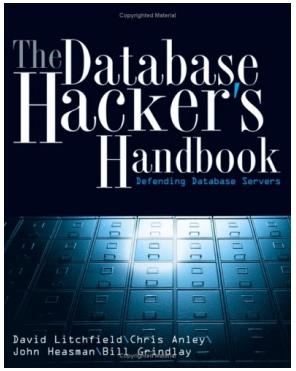
tripwire™

Further securing

- Hardening specific applications:
  - Apache (web server)
  - PHP (server-side scripting)
  - MySQL (database)
  - …







Summary

- Virtualization
  - Your own server in 60 seconds
- Securing a new VM:
  - Lock down ability to login
  - Keep software up to date
  - Use a firewall
  - Install intrusion detection system(s)
  - Harden installed apps (e.g. Apache, MySQL)