Let us know what you think

Click ‘engage’ to rate session.
Rate 12 sessions to get the supercool GOTO reward
DOCKER SECURITY

ADRIAN MOUAT

GOTO LONDON

ContainerSolutions
• Chief Scientist @ Container Solutions
• http://www.container-solutions.com
• Writing "Using Docker" for O'Reilly
• @adrianmouat
OVERVIEW

- 5 Round Security Boxing Match
- Container Security Tips & Techniques
CONTAINERS VS VMS!
WHAT WE'RE FIGHTING FOR!
HACKED

I'm In Here Now!

It's Just A Game Sometimes You Win, Sometimes You Lose'

#Sorry Admin
Adobe Hacked: Cyber-Thieves Accessed Credit Card Information Of Nearly 3 Million Customers

Adobe Systems Inc. said a cyberattack on its systems has exposed credit-card information of 2.9 million customers.

The maker of Photoshop and other software said Thursday that the attacker accessed Adobe customer IDs and passwords on its systems. Through that, they were able to remove customer names, encrypted credit and debit card numbers, expiration dates and other information related to the transactions, Adobe said.
Second hack of federal records hit intelligence and military personnel

- OPM hackers linked to China accessed sensitive background information
- News follows revelation records of 14 million federal employees compromised

Associated Press in Washington

Friday 12 June 2015 22.15 BST

The government data breach is believed to be worse than previously admitted.
THE CONTENDERS!
VMS ARE THE HEAVYWEIGHTS WHEN IT COMES TO SECURITY
VMS ARE THE HEAVYWEIGHTS WHEN IT COMES TO SECURITY
CONTAINERS ARE THE UNKNOWN UPSTART
DING DING!
ROUND 1
ISOLATION GUARANTEES
• VMs have hypervisor layer
• VMs have hypervisor layer
• Containers share kernel
<table>
<thead>
<tr>
<th>VM</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9</td>
</tr>
</tbody>
</table>
ROUND 2
ATTACK SURFACE
• Much more going on in a VM
• Emulate devices
  ■ VENOM
  ■ http://venom.crowdstrike.com/
• Much more going on in a VM
• Emulate devices
  ■ VENOM
  ■ http://venom.crowdstrike.com/
• Minimal containers
  ■ Only contain a static binary
<table>
<thead>
<tr>
<th>VM</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>
ROUND 3
CONTROLS
• Both allow limiting access to resources (memory, cpu, disk)
• Both allow limiting access to resources (memory, cpu, disk)
• More controls with containers
  ■ Set filesystem to read-only
  ■ Kernel capabilities
  ■ Seccomp coming!
<table>
<thead>
<tr>
<th>VM</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>
ROUND 4
AUDITING
• More containers than VMs
• More containers than VMs
• VMs longer-lived
  ▪ Diverge from base image
  ▪ CM software used to patch
• More containers than VMs
• VMs longer-lived
  ▪ Diverge from base image
  ▪ CM software used to patch
• Containers are ephemeral
  ▪ Throw them away
  ▪ Don't patch!
• More containers than VMs
• VMs longer-lived
  ■ Diverge from base image
  ■ CM software used to patch
• Containers are ephemeral
  ■ Throw them away
  ■ Don't patch!
• Audit images, not containers
• Docker diff
  ■ Easily verify any differences from base
  ■ Tell if hacked
<table>
<thead>
<tr>
<th>VM</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>
ROUND 5

TRACK RECORD
• VMs have a proven history
• VMs have a proven history
• Containers don't
<table>
<thead>
<tr>
<th>VM</th>
<th>Container</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>VM</td>
<td>Container</td>
</tr>
<tr>
<td>----</td>
<td>-----------</td>
</tr>
<tr>
<td>10</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>47</td>
<td>47</td>
</tr>
</tbody>
</table>
CALL IT A DRAW?
CALL IT A DRAW?

• Beware of the rematch
CALL IT A DRAW?

- Beware of the rematch
- Lots of work to speed up VMs
- Lots of work to secure containers
USE CONTAINERS AND VMS

- Use VMs to segregate groups of containers
- Use containers to add another layer of security
  - (plus all the nice stuff containers give you)
CONTAINER SECURITY
SECURITY PARADIGMS

- Defence-In-Depth
  - Multiple layers of security
SECURITY PARADIGMS

• Defence-In-Depth
  ■ Multiple layers of security
• Least Privilege
  ■ Only access data and resources essential to function
  ■ "Need to Know"
  ■ "Least Privilege Microservices" by Nathan McCauley and Diogo Mónica
TIPS
Users are not namespaced

- Root in container is root on host
SET A USER

- Create a user in your Dockerfile
- Change to the user via USER or su/sudo/gosu

```
RUN groupadd -r user && useradd -r -g user user
USER user
```
SET CONTAINER FS TO READ-ONLY

$ docker run --read-only debian touch x
touch: cannot touch 'x': Read-only file system
SET VOLUMES TO READ-ONLY

$ docker run -v $(pwd)/secrets:/secrets:ro \
   debian touch /secrets/x
touch: cannot touch '/secrets/x': Read-only file system
DROP CAPABILITIES

$ docker run --cap-drop SETUID --cap-drop SETGID myimage
$ docker run --cap-drop ALL --cap-add ...
SET CPUSHARES

$ docker run -d myimage
$ docker run -d -c 512 myimage
$ docker run -d -c 512 myimage
SET MEMORY LIMITS

$ docker run -m 512m myimage
DEFANG SETUID/SETGID BINARIES

- Applications probably don't need them
- So don't run them in production
TO FIND THEM

$ docker run debian \
        find / -perm +6000 -type f -exec ls -ld {} \; 2> /dev/null
-rwsr-xr-x 1 root root 10248 Apr 15 00:02 /usr/lib/pt_chown
-rwxr-sr-x 1 root shadow 62272 Nov 20 2014 /usr/bin/chage
-rwsr-xr-x 1 root root 75376 Nov 20 2014 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 53616 Nov 20 2014 /usr/bin/chfn
...
FROM debian:wheezy
RUN find / -perm +6000 -type f -exec chmod a-s {} \; \\ || true
$ docker build -t defanged-debian .
...
Successfully built 526744cf1bc1
$ docker run --rm defanged-debian \
  find / -perm +6000 -type f -exec ls -ld {} \; \
  2> /dev/null | wc -l
  
  0
  $
TURN OFF INTER-CONTAINER COMMUNICATION

$ docker daemon --icc=false
NOW CONTAINERS CAN'T ATTACK EACH OTHER
PEACE :)
BUT A BIT USELESS
ALLOW LINKED CONTAINERS TO COMMUNICATE

$ docker daemon --icc=false --iptables
SHARING SECRETS
BAKE IT INTO THE IMAGE
ENVIRONMENT VARIABLES

$ docker run -e API_TOKEN=MY_SECRET myimage

- Suggested by 12 factor apps
ENVIRONMENT VARIABLES

$ docker run -e API_TOKEN=MY_SECRET myimage

- Suggested by 12 factor apps
- Can be seen too many places
ENVIRONMENT VARIABLES

$ docker run -e API_TOKEN=MY_SECRET myimage

- Suggested by 12 factor apps
- Can be seen too many places
  - linked containers, inspect
ENVIRONMENT VARIABLES

$ docker run -e API_TOKEN=MY_SECRET myimage

- Suggested by 12 factor apps
- Can be seen too many places
  - linked containers, inspect
- Can't be deleted
ENVIRONMENT VARIABLES

$ docker run -e API_TOKEN=MY_SECRET myimage

- Suggested by 12 factor apps
- Can be seen too many places
  - linked containers, inspect
- Can't be deleted
- Get included in reports
MOUNTED VOLUMES OR DATA VOLUME CONTAINERS

$ docker run -v /secretdir/keyfile:/keyfile:ro myimage
$ docker run --volumes-from my-secret-container myimage
MOUNTED VOLUMES OR DATA VOLUME CONTAINERS

$ docker run -v /secretdir/keyfile:/keyfile:ro myimage
$ docker run --volumes-from my-secret-container myimage

- Works, but icky
- Files can get checked in by accident
SECURED KEY-VALUE STORE

- vault
  - https://hashicorp.com/blog/vault.html
- keywhiz
  - https://github.com/square/keywhiz/
- Can control leases, store encrypted
- Still requires some sort of authentication
CONCLUSION

- Containers add security
- Use with VMs if concerned
- Think Defence-In-Depth
  - Multiple layers of security
- Least privilege
  - Need to know
Please remember to rate this session. Thank you!
• Chief Scientist @ Container Solutions
• http://www.container-solutions.com
• Writing "Using Docker" for O'Reilly
• @adrianmouat