### Push to server

pc=”[offtecaw@users.deterlab.net](mailto:offtecaw@users.deterlab.net)”

ssh $pc ‘mkdir ~/ctf1/’ # -t -f

scp -r Desktop/ctf/dataToServer/ $pc:~/ctf1/

### Bootstrap on machines(server+gateway)

# get rid of guagga line (apt won’t install anything otherwise)

sudo cp /var/lib/dpkg/statoverride /var/lib/dpkg/statoverride.bak

sudo grep -E "root" /var/lib/dpkg/statoverride > /tmp/statoverride

sudo cp /tmp/statoverride /var/lib/dpkg/statoverride

sudo apt update && sudo apt install tcpdump wget htop dsniff python3-pip -y sudo apt autoremove -y

pip3 install --no-index --find-links /home/cctf1/backend/packages/ -r /home/cctf1/backend/requirements.txt

# drop all non TCP traffic

sudo iptables -A INPUT -p !tcp -j DROP

# drop high rate

sudo iptables -A INPUT -p tcp --dport 80 -m connlimit --connlimit-above 20 --connlimit-mask 40 -j DROP

# drop fragmented ?

sudo iptables -A INPUT -p tcp -f -j DROP

# allow tcp traffic from clients

sudo iptables -A INPUT -p tcp -s 10.1.2.2/32 --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp -s 10.1.3.2/32 --dport 80 -j ACCEPT

sudo iptables -A INPUT -p tcp -s 10.1.4.2/32 --dport 80 -j ACCEPT

### Bootstrap on server

sudo apt install apache2 -y

sudo modprobe ip\_conntrack

sudo nano /etc/sysctl.conf

sudo sysctl –p

sudo echo “net.ipv4.tcp\_max\_syn\_backlog = 2048 “ >> /etc/

net.ipv4.tcp\_synack\_retries = 3

net.netfilter.nf\_conntrack\_tcp\_timeout\_syn\_recv=30

net.ipv4.tcp\_fin\_timeout = 20

#net.ipv4.conf.all.rp\_filter = 1 # default 0 : not possible to do in this deterlab exercise

# icmp redirect protection

net.ipv4.conf.all.accept\_redirects = 0

net.ipv6.conf.all.accept\_redirects = 0

net.ipv4.conf.all.send\_redirects = 0

net.ipv4.conf.default.accept\_redirects = 0

net.ipv6.conf.default.accept\_redirects = 0

net.ipv4.conf.default.send\_redirects = 0

### Apache hardening

sudo nano /etc/apache2/apache2.conf

ServerTokens Prod

ServerSignature Off

Timeout 40

sudo service apache2 restart

### Web service

date #better to use <https://stackoverflow.com/questions/10087819/convert-date-to-another-timezone-in-javascript>

netstat -natp | tr -s " " #by hand when necessary to check source ip == to pcs allowed

uptime | cut -d' ' -f12,13,14

free -m | grep Mem | tr -s " " | cut -d' ' -f2,3,4,7 #total used free available

ps aux | tr -s " " | sort -nrk 3,3 | head -n 5 | cut -d' ' -f1,2,3,4,11 #user, pid, cpu, ram, command

sudo du -sh /var/log/apache2 | cut -f1 -d$'\t' #multiple size units

### A mano

netstat -at #view all connections in real time and grep for count

sudo tail -f /var/log/apache2/error.log

sudo service apache2 status

sudo service apache2 stop

sudo service apache2 start

sudo service apache2 restart

sudo varnishlog

GET GAME INTERFACE OF SERVER

route -n | grep 10.1.5.0 | tr -s " " | cut -d' ' -f8

### Disaster recovery

interface=$(route -n | grep 10.1.5.0 | tr -s " " | cut -d' ' -f8)

sudo ifconfig $interface down

sudo ifconfig $interface up

### 

### Webservice on Gateway

curl 10.1.5.2 -s -o /dev/null -w "%{time\_total}\n" #Measure performance

### Read Block Size in MB

# ls in MB

ls -l --block-size=M

### Start TCPDUMP

sudo tcpdump -i eth3 -G 60 -w dumpServ-%Y-%m-%d\_%H:%M:%S.pcap

sudo tcpdump -i eth3 -G 60 -w dumpGatw-%Y-%m-%d\_%H:%M:%S.pcap -z "./deleteMoveStat.sh" tcp[tcpflags] != tcp-syn

### Iptables matches count

## IPTABLES MATCHES COUNT

sudo iptables -nvL INPUT --line-numbers

### Iptables MSS

**iptables -A INPUT -p tcp --tcp-flags SYN,ACK,RST SYN -m tcpmss --mss 2000:2500**

<https://homes.di.unimi.it/sisop/qemu/iptables-tutorial.pdf>

-N CLIENTS

-A CLIENTS -p tcp --tcp-option 2 -j ACCEPT

-A CLIENTS -m conntrack --ctstate NEW -m recent --set --name HTTP\_LIMIT --rsource

-A CLIENTS -m conntrack --ctstate NEW -m recent --name HTTP\_LIMIT --update --seconds 15 --hitcount 250 --rsource -j DROP