http2-app-flood

Part A:

Metric/Property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	Unresponsive	Unresponsive * varies with attack parameters
CPU consumption	docker stats	400-500%	Attacker: 5%< Victim:90-100%
Mem usage	docker stats	50.08MiB / 554.9MiB (9.03%)	Attacker: 100+ MB Victim: 50+ MB
Network I/O	docker stats	11.6MB / 992kB	Attacker: 1-1000 KB Victim: 1-10 MB
Number of established connections	docker exec *-victim-server sh -c "awk 'NR>1 && \$4==\"01\" {count++} END {print count+0}' /proc/net/tcp"	Fully established	- Fully established - Match the attacker script

Part B:

Metric/Property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	Basic attacker: Unsresponsive Advanced attacker: Unresponsive	Basic attacker: Unresponsive * varies with attack parameters
CPU consumption	docker stats	806.59%	Basic attacker: 50%<
			Victim:100-400%
Mem usage	docker stats	170.2MiB / 554.9MiB 30.68%	Basic attacker: 250+- MB
			Victim: 300+- MB
Network I/O	docker stats	4.8MB / 288kB	Basic attacker: 1-2MB / 4-5MB
			Victim: 3-4MB / 1-2MB
Number of established connections	docker exec *-victim-server sh -c "awk 'NR>1 && \$4==\"01\" {count++} END {print count+0}' /proc/net/tcp"	Fully established	- Fully established - Match the attacker script

—--

Flow-control

Zero Window:

metric/property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	Unresponsive	Unresponsive
CPU consumption	Via docker –stats	0.2% - 1.2%	Attacker: 1-5%
			Victim: 0-1% (does not handle requests)
Mem usage	Via docker –stats	108.9MiB	Attacker: 52.88MiB
			Victim: 137.6MiB
Network I/O	Via docker –stats	1.2MB / 747kB	Attacker: 1.09MB / 1.53MB
			Victim: 2.76MB / 2.47MB
Number of established connections	docker exec *-victim-server sh -c "netstat -an | grep :8080 | grep ESTABLISHED | wc -l"	Up to ~325	- Fully established - Will match attacker script

<u>Slow Incremental:</u>

metric/property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	unresponsive	Unresponsive
CPU consumption	Via docker –stats	~5%	Attacker: 20% Victim: Around 5%
Mem usage	Via docker –stats	~112 MB	Attacker: ~50 MB Victim: ~180MB
Network I/O	Via docker –stats	~22MB	Attacker: 31.4MB / 56.7MB Victim: 54.9MB / 30.8MB
Number of established connections	docker exec *-victim-server sh -c "netstat -an | grep :8080 | grep ESTABLISHED | wc -l"	- Fully established, not maintained. ~290 has been observed to be sufficient to choke the server	- Fully established and maintained ~400 has been observed to be sufficient to choke the server

Adaptive Slow:

- Attack designed for cloud deployment

metric/property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	unresponsive	NAN
CPU consumption	Via docker –stats	~ 5%	NAN
Mem usage	Via docker –stats	~108MB	NAN
Network I/O	Via docker –stats	~24MB	NAN
Number of established connections	docker exec *-victim-server sh -c "netstat -an | grep :8080 | grep ESTABLISHED | wc -l"	- Fully established and maintained. ~290 has been observed to be sufficient to choke the server	NAN

—--

Slowloris

Old Apache Server (httpd:2.2.34)

Release data: July 11, 2017

- We launch this part only locally

metric/property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	NAN	Unresponsive (quickly)
CPU consumption	Via docker –stats	NAN	Attacker:0.00%
			Victim:0.01%
Mem usage	Via docker –stats	NAN	Attacker:9 MiB
			Victim: 192.8MiB
Network I/O	Via docker –stats	NAN	Attacker: 290kB / 389kB
			Victim: 354kB / 259kB
Number of established connections	docker exec *-victim-server sh -c "netstat -an | grep :8080 | grep ESTABLISHED | wc -l"	NAN	- Exhausted - ~250 connections

Latest Apache Image:

metric/property	CLI	Cloud	Local
Response time	"curl -o /dev/null -s -w "Time: %{time_total}\n" $TARGET_URL"	Advanced attacker: unresponsive	Unresponsive
		Cloud attacker:	
CPU consumption	Via docker –stats	Advanced Attacker: 10-20%	Advanced attacker: 10-20%
		Cloud Attacker: 10-20%	
		Victim: ~1-5%	Victim:0-5%
Mem usage	Via docker –stats	Advanced attacker: ~70MB	Advanced attacker: 120MB
		Cloud Attacker: ~70 MB	
		Victim ~100MB	Victim: 70MB
Network I/O	Via docker –stats	Advanced attacker:1.2MB/1.57MB	Advanced attacker: 5.91MB / 18.3MB
		Cloud Attacker ~2MB/3MB:	
		Victim: 19MB	Victim: 78.1MB / 37.1MB
Number of established connections	docker exec *-victim-server sh -c "netstat -an | grep :8080 | grep ESTABLISHED | wc -l"	- choked with 907 connections (both attacks). The server drops connections and the attack keeps increasing it. Cloud attack preserve connections for more time, and thus chocks the server for longer.	- choked with maximized 910 connections maintained during the attack