Mitigate DDoS attack with effective cost

Nguyễn Chấn Việt

Đơn vị tổ chức:

Đơn vị tài trợ:

The Growth of DDoS Attacks

- Malware
- Exploit

Classification

- Volume Based Attacks –The attacker tries to saturate the bandwidth of the target's website by flooding it with a huge quantity of data. This category includes ICMP floods, UDP floods and other spoofed-packet floods. The magnitude of Volume Based Attacks is measured in bits per second (Bps).

- Protocol Attacks –The attacker's goal is to saturate the target's server resources or those of intermediate communication equipment (e.g., Load balancers) by exploiting network protocol flaws. This category includes SYN floods, Ping of Death, fragmented packet attacks, Smurf DDoS and more. The magnitude of Protocol Attacks is measured in Packets per second.

- Application Layer (Layer 7) Attacks – Designed to exhaust the resource limits of Web services, application layer attacks target specific web applications, flooding them with a huge quantity of HTTP requests that saturate a target's resources. Examples of application layer DDoS attacks include Slowloris, as well as DDoS attacks that target Apache, Windows, or OpenBSD vulnerabilities. The magnitude of application layer attacks is measured in Requests per second.

What we care ?

- Exhausting resources like:
  - CPU
  - Memory/Buffers
  - I/O operations
  - Disk space
  - Network bandwidth

Where to start ?

- Go through all devices on network, from L2 switches to backend servers and identify possible leaks, bottlenecks, attack vectors, applicable DoS attacks, vulnerabilities ... and mitigate or (rate)limit them

Infrastructure

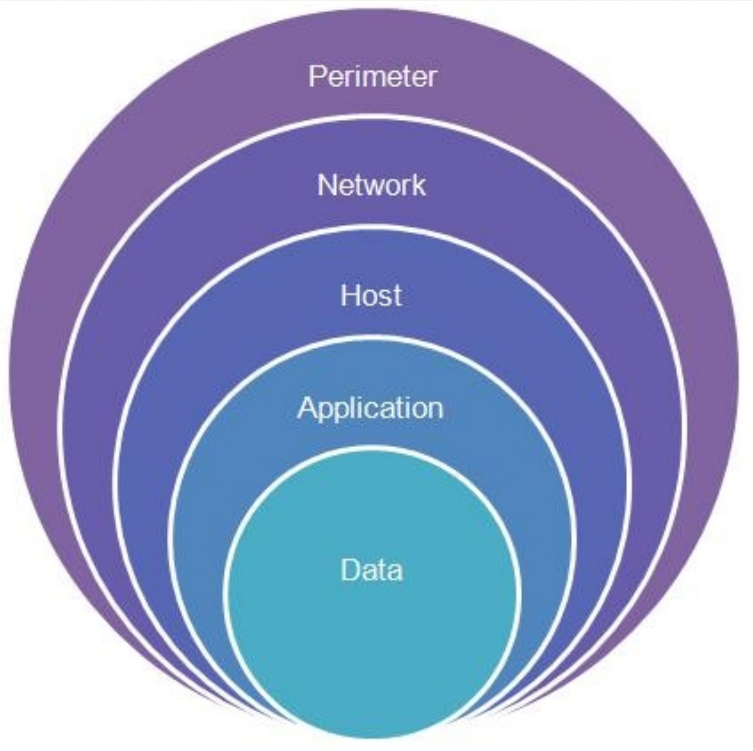
- Hosting and VM is not good idea


Conference &Training
Cần Thơ
SECURITY BOOTCAMP
2013
www.lactien.com

[1]

Architecture

- Rule: Defence in depth (multi-layer)



OS Tuning

- *nix is good choice
- Rule : If not used, turn off

/etc/sysctl.conf tuning

- net.netfilter.nf_conntrack_tcp_timeout_syn_recv = 2
  net.ipv4.tcp_syn_retries = 3
  net.ipv4.tcp_synack_retries = 1
  net.ipv4.tcp_syncookies = 1
  net.ipv4.tcp_max_syn_backlog = 8192
  net.ipv4.tcp_mem = 786432 1048576 1572864
  net.ipv4.tcp_rmem = 4096 87380 1048576
  net.ipv4.tcp_wmem = 4096 16384 1048576
  net.ipv4.tcp_max_orphans = 2048

Layer 3-4

- Stateful Firewall
  - Iptables
  - Tuning connections tracking
- Rule : Deny all, allow selective

Layer 7

- WAF : to filter what firewall missed at IP layer
  - Mod_security
- Why not snort ?

Layer 7

- Choosing webserver
  - Nginx is the best
- Tuning webserver
  - Improve Apache with mod_reqtimeout
- Caching is very important
  - Static cache
  - memcached

Patching

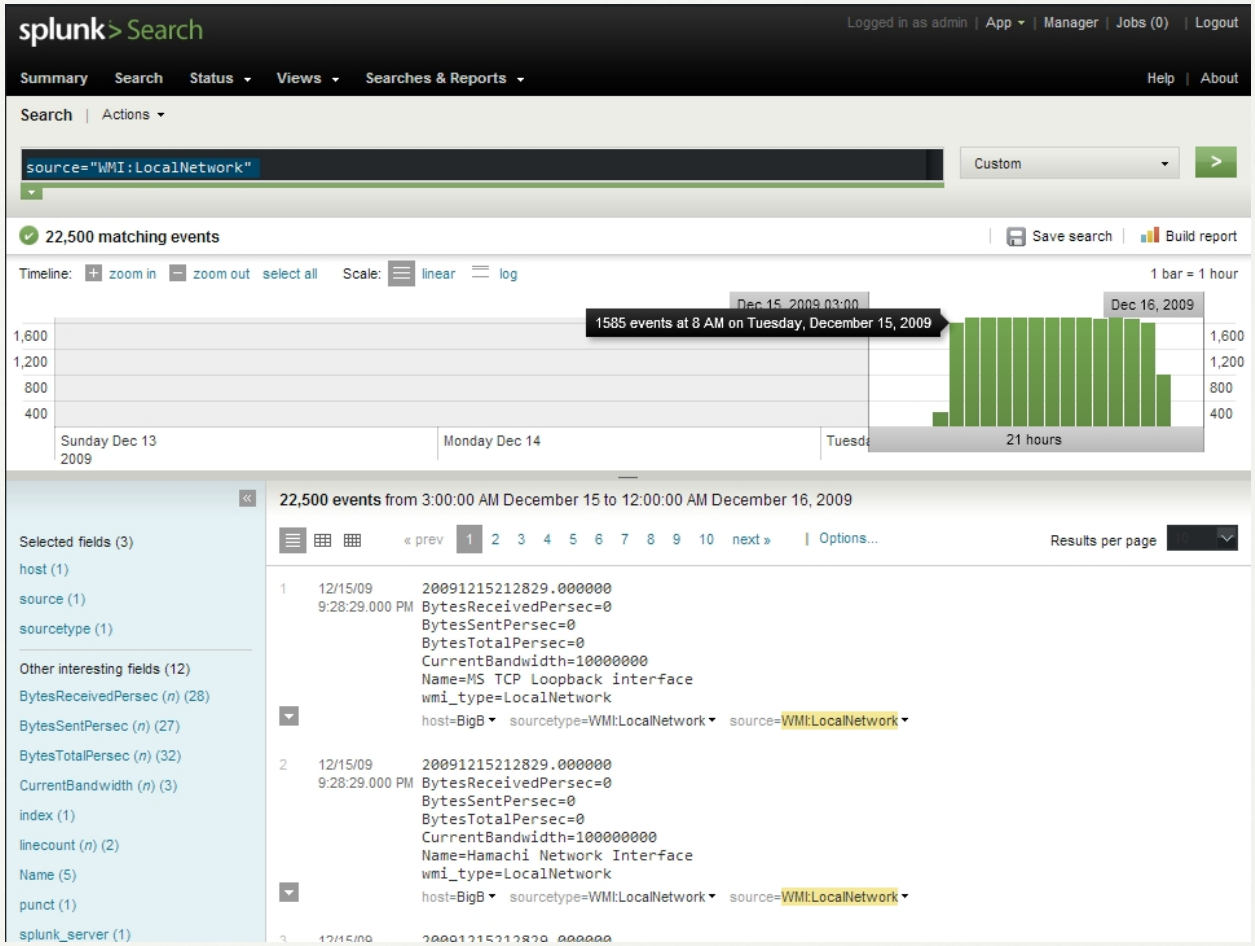
- Keep Your System Up-to-date
- Example :
  - Slowloris : based on missing CRLF
  - Slow Read attack : based on TCP persist timer exploit
  - Apache Range Header attack

Proactive with NSM

- Logs is very important
- My suggestion : Syslog-ng + Splunk

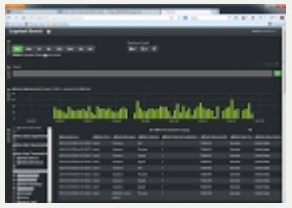
Proactive with NSM

Proactive with NSM



Proactive with NSM

- Alternative :

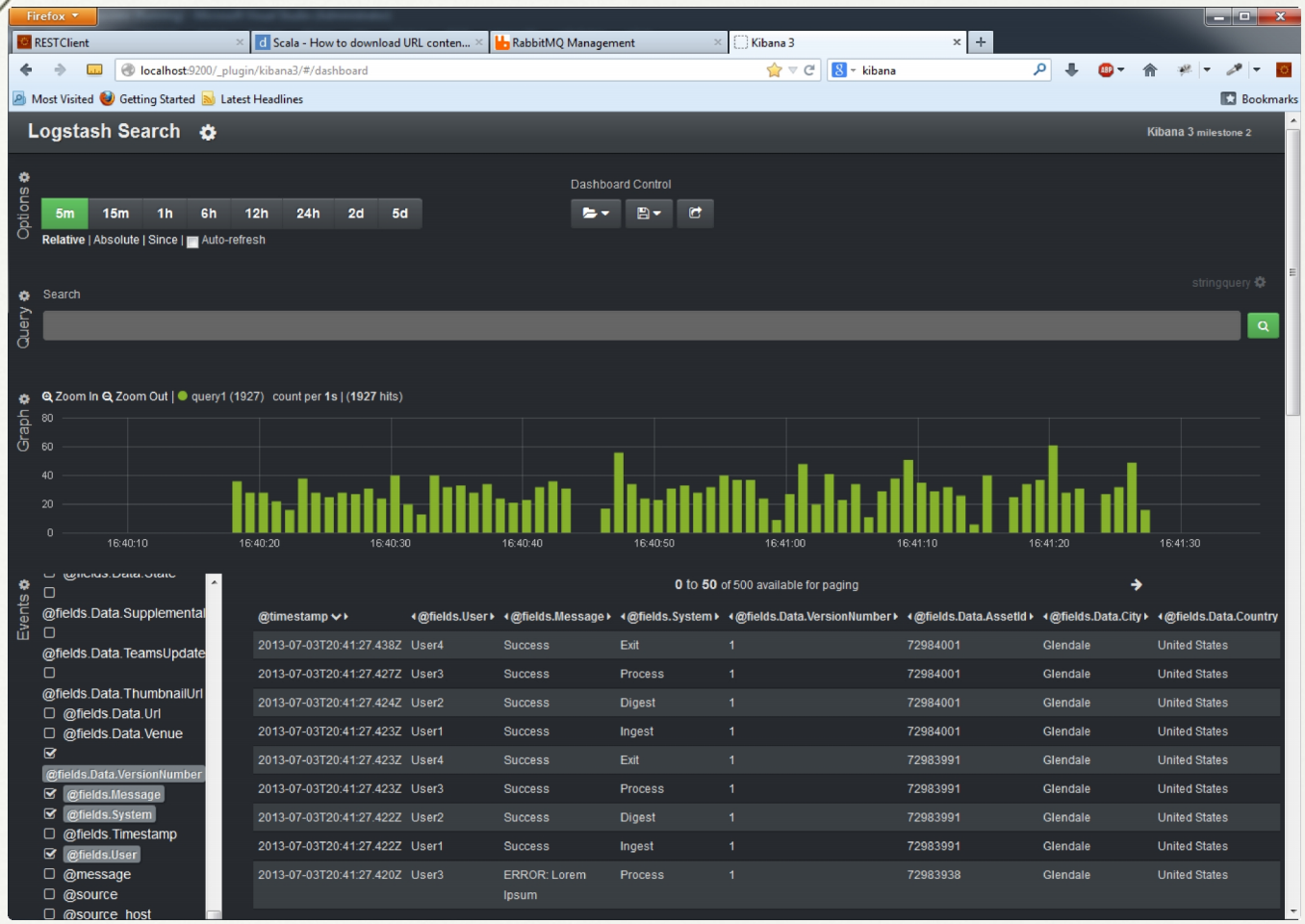


Logstash is a free tool for managing events and logs. It has three primary components, an Input module for collecting logs from various sources

ElasticSearch is this awesome distributable, RESTful, free Lucene powered search engine/server. Unlike SOLR, ES is very simple to use and maintain and similar to SOLR, indexing is near realtime.

Kibana is a presentation layer that sits on top of Elasticsearch to analyze and make sense of logs that logstash throws into Elastic search; Kibana is a highly scalable interface for Logstash and ElasticSearch that allows you to efficiently search, graph, analyze and otherwise make sense of a mountain of logs.

Proactive with NSM




Conference &Training
Cần Thơ
SECURITY BOOTCAMP
2013
www.lactien.com

[2] Case Study

Our suggestion

- Diagram

Our suggestion

- Router with high throughput
- reverse proxy servers :
  - 32Gb RAM, 10Gb NIC, Quad Core I7, SSD disk (for internal I/O better)
  - Linux OS, running IPTables + apache (worker MPM) + mod_security

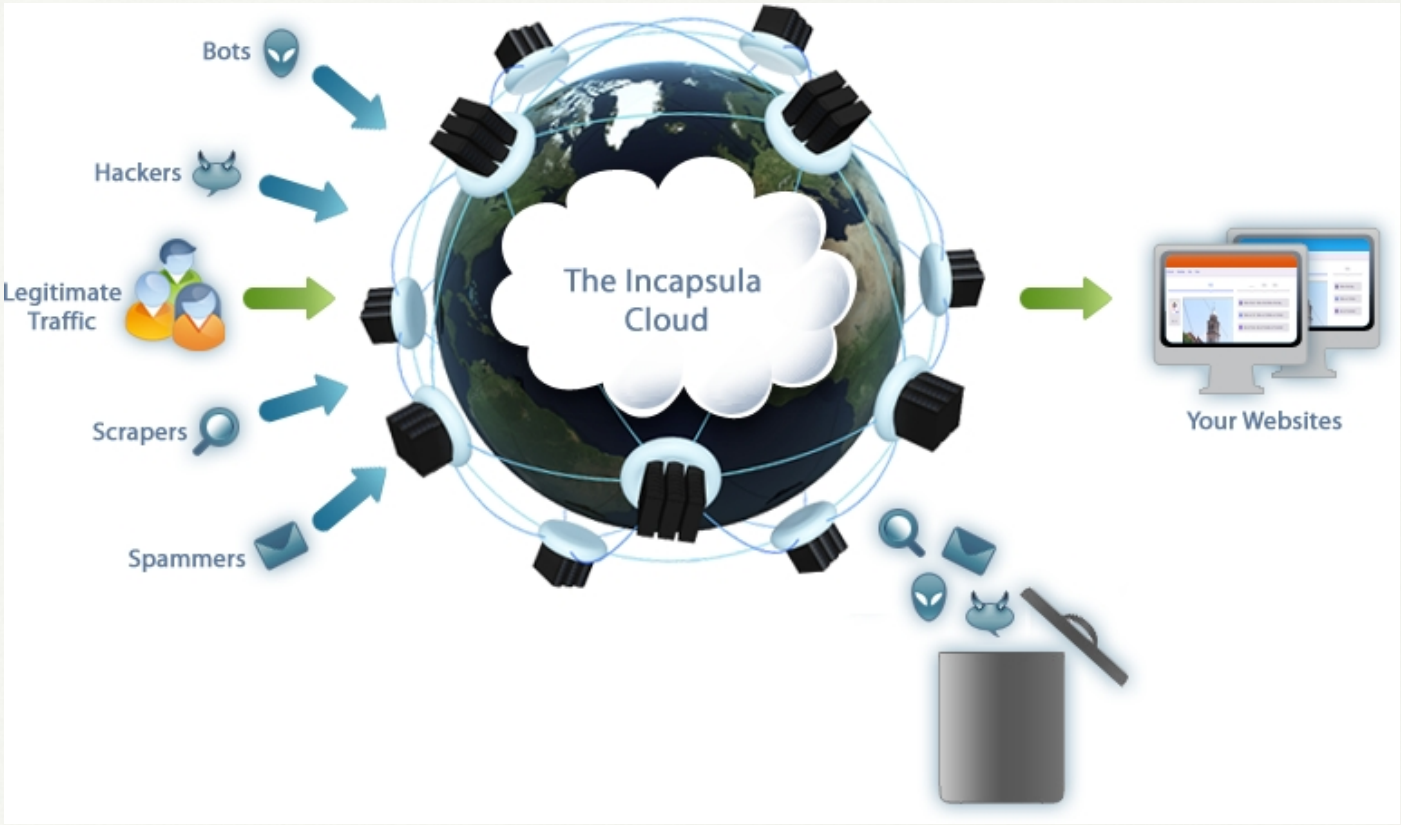
Our suggestion

- cache servers :
  - Using SSD Disk
  - Application cache (ex : xcache/APC for PHP, …)
  - Generic cache : Apache Traffic Server

Cloud-based Solutions

- For large DDoS attack (e.g Spamhaus was DDoS by 300Gb/s of traffic), we need a third-party :
  - Incapsula
  - CloudFlare

Cloud-based Solutions



Simple but effective

- If you can determine C&C servers, just null route them

Testing

- Test your network and devices by simulating real DoS attack (LOIC/HOIC, hping, slowhttptest, thc-ssl-dos, pktgen, ...)

Conclusion

- This approach is not “silver bullet” for preventing DDoS attacks
- There isn’t “a technique” for mitigrating DDoS
  - DDoS Mitigation = Hardened System + Money


Conference &Training
Cần Thơ
SECURITY BOOTCAMP
2013
www.lactien.com

Thank you !