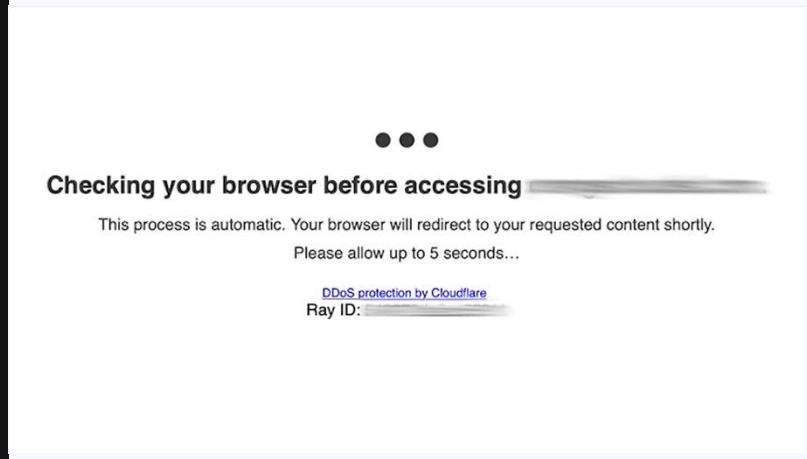
DISTRIBUTED DENIAL OF SERVICE (DDOS) ATTACKS

ARSALAN SEFIDGAR

DoS / DDoS

(Distributed) Denial of Service حملهٔ منع خدمت از سرویس (توزیع شده)



- سناریو های محتمل
  - شبکه مخابرات (تلفن ثابت)
  - سرویس آموزش آنلاین دانشگاه

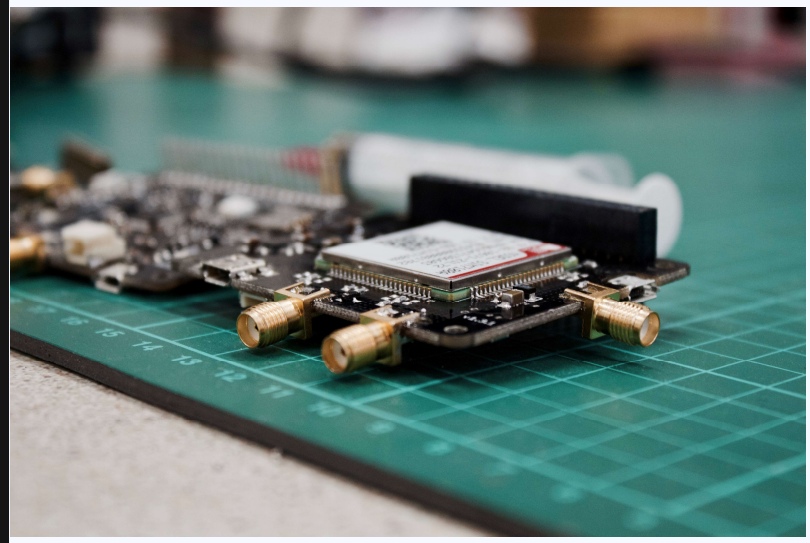
انگیزه هکر

1. منافع متفاوت
2. رقابت
3. اخاذی
4. هکتویست ها
5. حواس پرتی

در سالی که گذشت

1. ابر آروان
2. شرکت زیرساخت کشور
3. اسنپ فود
4. و...

INTERNET OF THINGS



1. میلیون ها دستگاه: دوربین ها، روترها
2. پسورد های از پیش تعیین شده در کارخانه
3. آپدیت نکردن / نقص های امنیتی قدیمی

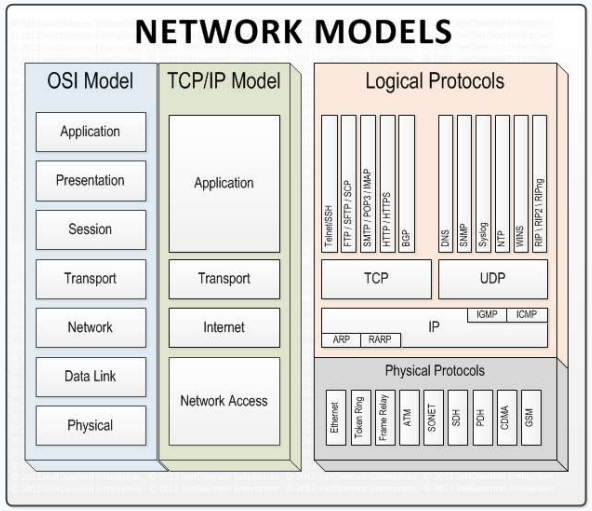
INTERNET OF SHIT

تهدیدات دیگر

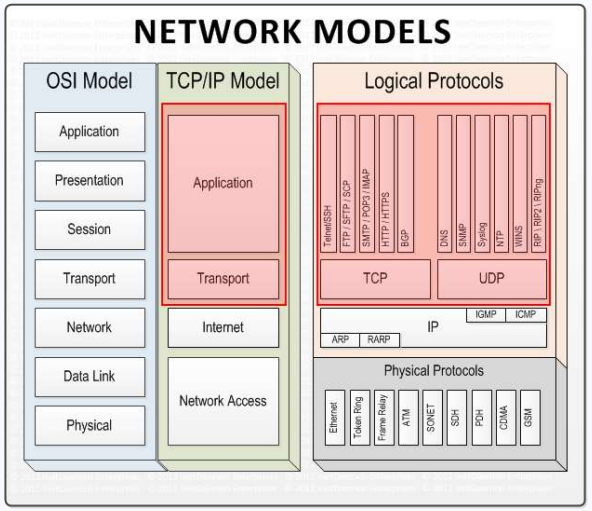
1. میلیون ها سایت مبتنی بر وردپرس با پروتوکل ping-back
2. میلیون ها کامپیوتر، لپ تاپ و سرور در معرض خطر
3. وب اپلیکیشن های در معرض خطر (گذرا)

TYPE OF ATTACKS

OSI STACK



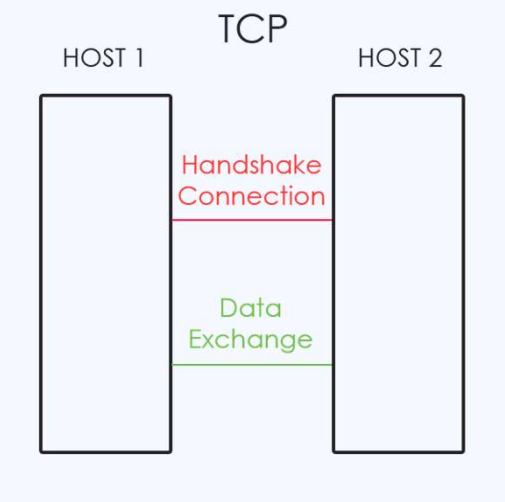
OSI STACK EXPOSURE

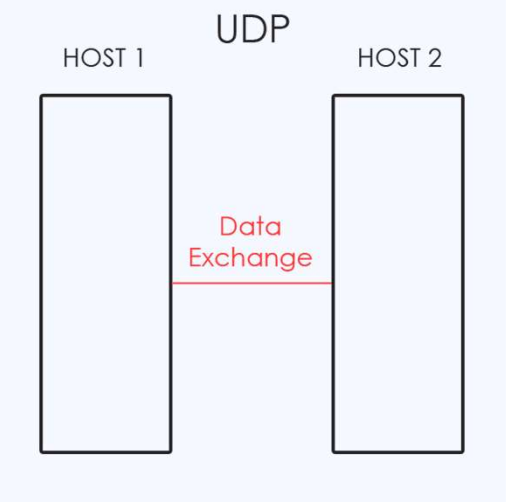


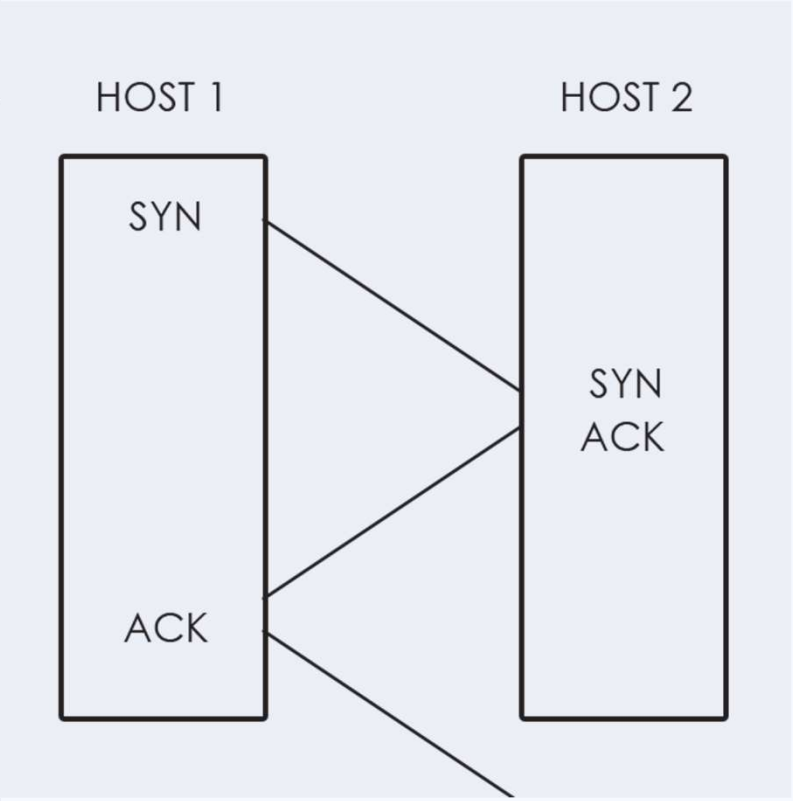
TCP VS UDP

SPOOF ZONE

AUTHENTIC HOSTS





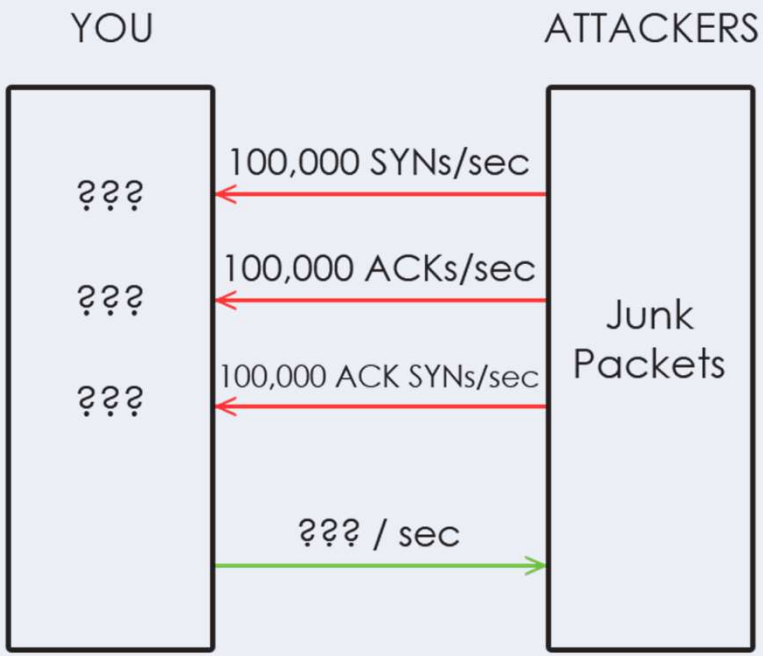


TCP: Attack Transport

TCP Handshake Lifecycle

- Each handshake packet has **its own source IP**
- Source IP **blindly trusted** by both end-points

TCP Handshake Lifecycle Floods

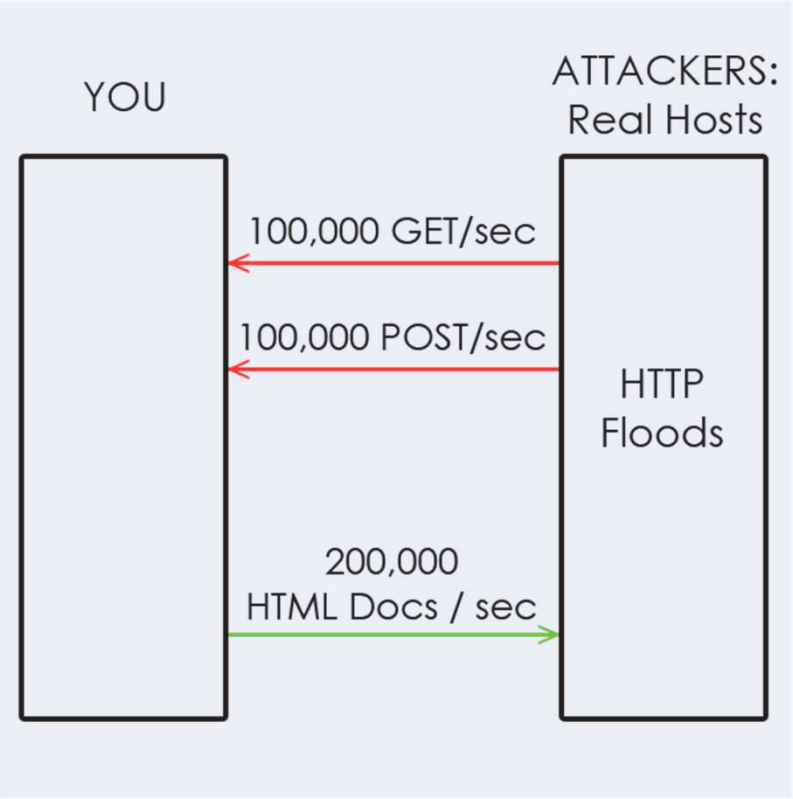


Real hosts

Fake hosts aka “spoofed”

- CPU
- MEMORY

TCP: Attack Application (HTTP)



Hundreds of Infected machines

- CPU
- MEMORY
- Bandwidth

Beyond:

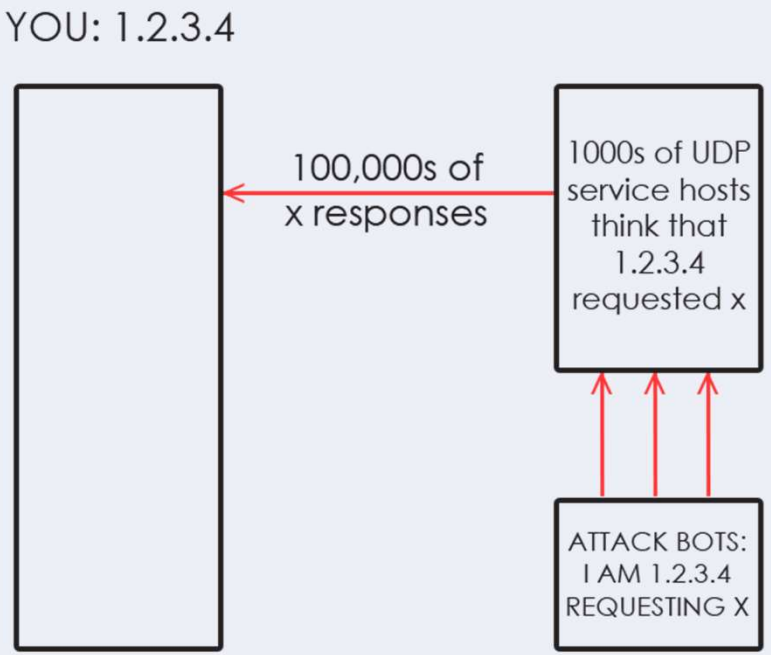
*Default ulimit is 1024 connection sockets

Slowloris: open connection, and keep it opened

TLS Exhaustion

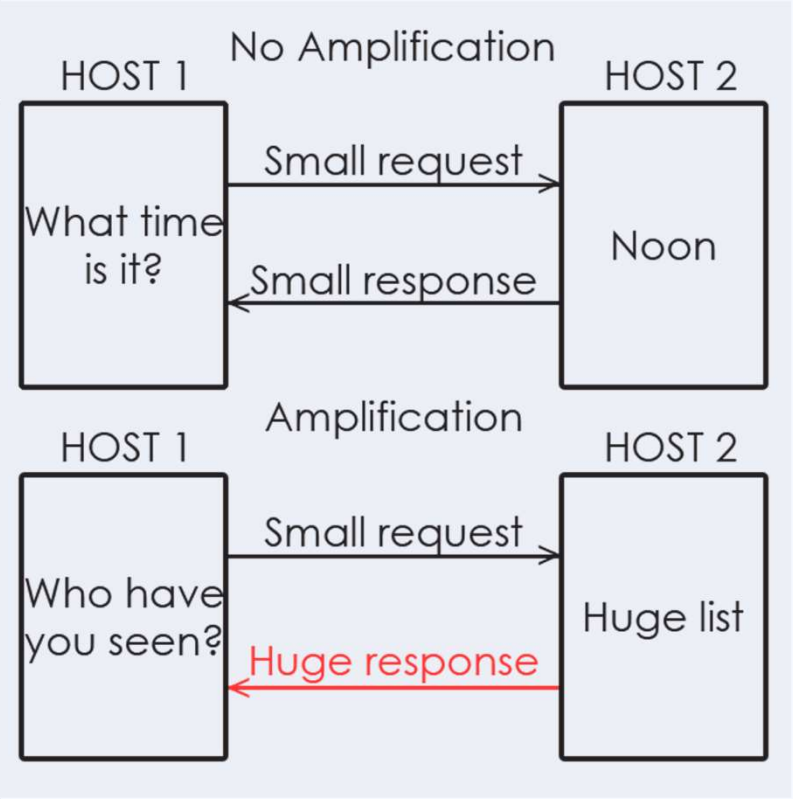
HashDoS: kill CPU with a few requests

UDP: NO TRANSPORT TO ATTACK



UDP Reflection

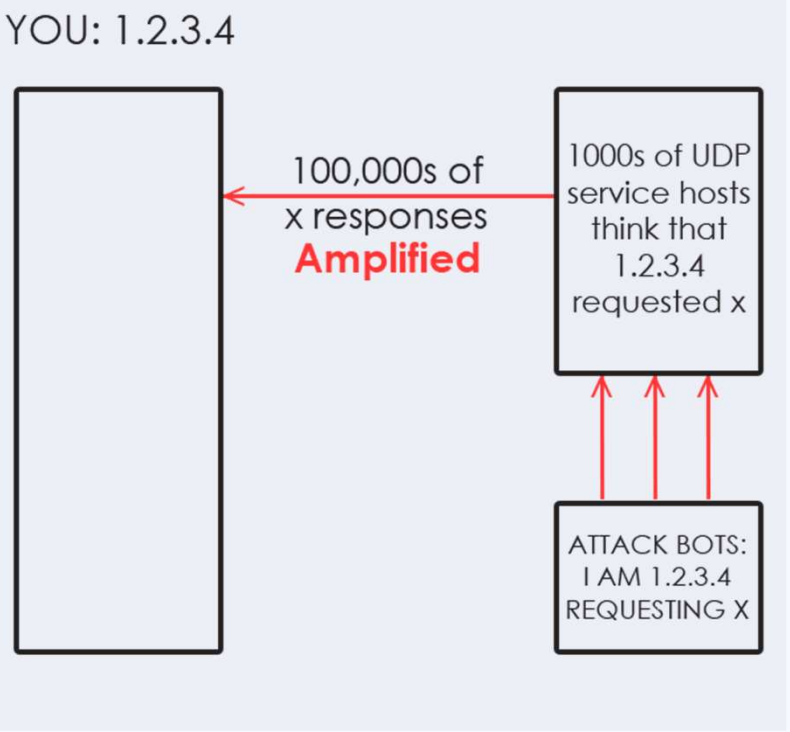
*Bandwidth



UDP: NO TRANSPORT TO ATTACK

UDP Amplification

UDP: NO TRANSPORT TO ATTACK

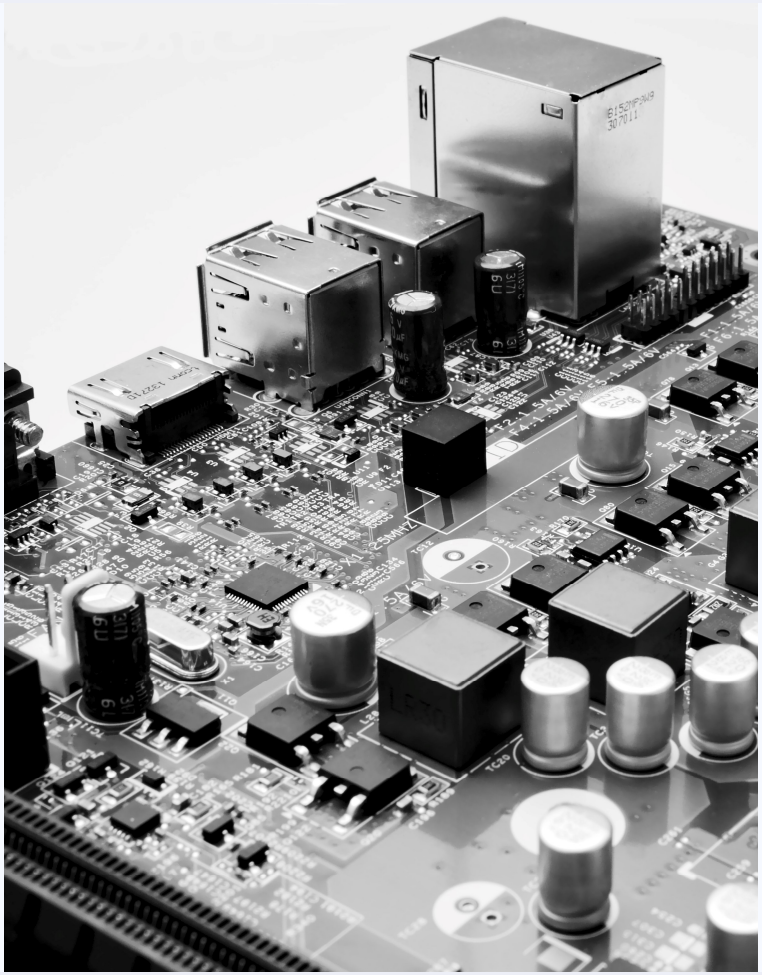


UDP Reflection + Amplification

*Bandwidth

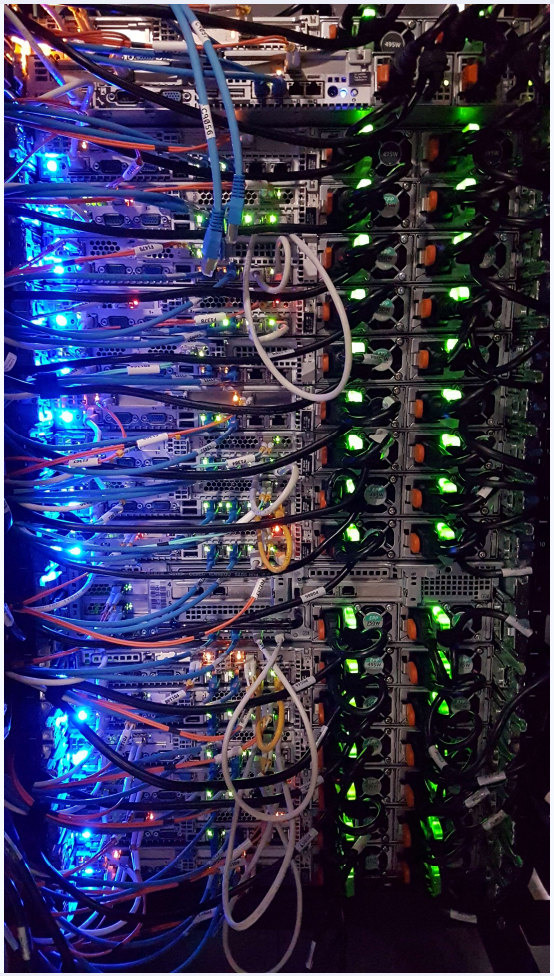
FIX IOT

- MUD: Manufacturer Usage Descriptions
  - Manufacturer Usage Descriptions (MUD) is meant to defend against. MUD works by providing a formal language and mechanism for manufacturers to specify which systems a device is designed to connect with. The converse, therefore, is that the network can prevent the device from both being attacked and attacking others. The key to all of this are manufacturer and their willingness to describe these devices.



REDUCE REFLECTION & AMPLIFICATION

- Close-Down Open DNS Resolvers
- Use a Secure NTP Template
  - Network Time Protocol

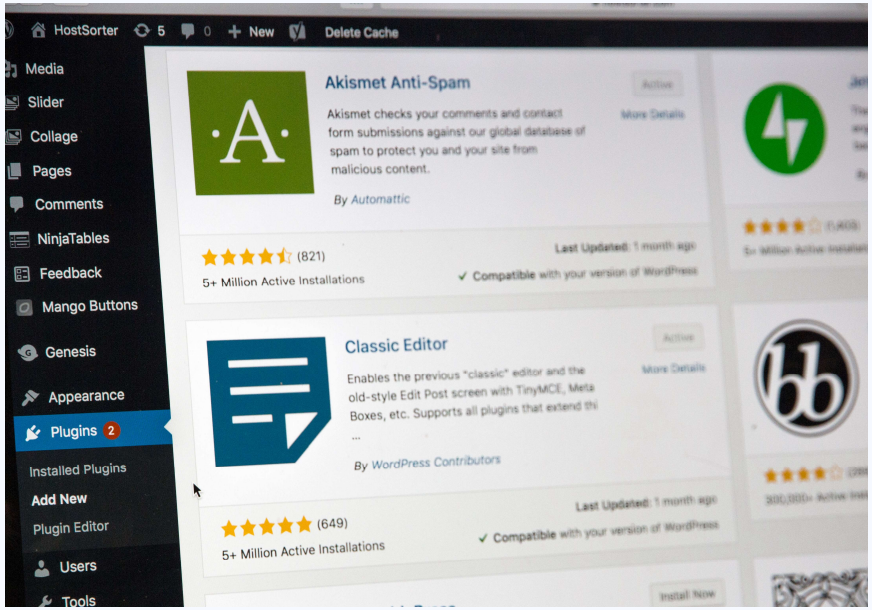


FIX SPOOFING

- Stop spoofing
  - RFC 2267: Ratified in 1998, Now BCP38
  - RFC 3704: Ratified in 2004, Now BCP84

FIX WORDPRESS

- WordPress ping-back verification protocol
  - Exposed and Exploited since 2014
  - The World's easiest Botnet
  - Millions of WordPress sites



ATTACK SURFACE: REDUCE

I. Before
   I. UDP services: NTP, DNS, RTP
   II. TCP services: HTTP, SSH, FTP, SIP

II. After
   I. NMAP
   II. TCP services: HTTP(S)

ATTACK SURFACE: DIVERSIFY

I. Use Dedicated Host Names or even Domains
   I. API: api.yoursite.com, yoursiteapi.com
   II. Content / Marketing: www.yoursite.com
   III. Commerce: shop.yoursite.com
   IV. SaaS: app.yoursite.com

DNS: PERFORMANCE & AVAILABILITY

I. pingdom.com or statuscake.com to monitor

II. Keep Tabs on DNS Performance & Availability

WEB APPLICATION PERFORMANCE

I. Tune NGINX for High-Throughput Levels
II. Configure gzip / deflate compression carefully
III. Reduce number of DB queries per request
IV. RDBMS backed by SSDs
V. PHP: Ensure OpCache Properly Configured

WEB APPLICATION SCALABILITY

I. Redis Data Caches
II. Web Servers: NGINX
III. Content Caching Servers: Varnish
IV. CDN for Static Resources

MONITOR: PERFORMANCE & AVAILABILITY

I. Profile Application, Fix Bottlenecks with newrelic.com or appdynamics.com
II. zabbix.org
III. Conduct Load-Tests: loader.io

CONTACT ME

LINKEDIN
ARSALANSE

TWITTER
@ARSALANSE

EMAIL
ASEFIDGAR@BIRJAND.AC.IR

PHONE
0914-773-4436

LINKS

1. Github
2. Arvancloud
3. RFC 2267
4. BCP38