Denial of Service - DoS

CATALIN BOJA

CATALIN.BOJA@IE.ASE.RO

Disclaimer

- It is illegal to perform these activities on resources (servers, Web-sites, computers, network services, etc) on which you don’t have permission
- All examples and tools are shown for academic purposes
- The use of any presented software or script is your responsibility

Course

- Terminology & Definitions
- Characteristics
- Common DDoS attacks
- DoS prevention

Resources

- Kaufman, Perlman, and Speciner. *Network Security: Private Communication in a Public World, Second Edition*, Prentice Hall PTR, 2002, ISBN 0130460192.
- Cheswick, Bellovin, and Rubin. *Firewalls and Internet Security: Repelling the Wily Hacker, Second Edition*, Addison-Wesley Professional, 2003, ISBN 020163466X.
- Incapsula online documentation, https://www.incapsula.com/ddos/
- Wikipedia, https://en.wikipedia.org

Characteristics

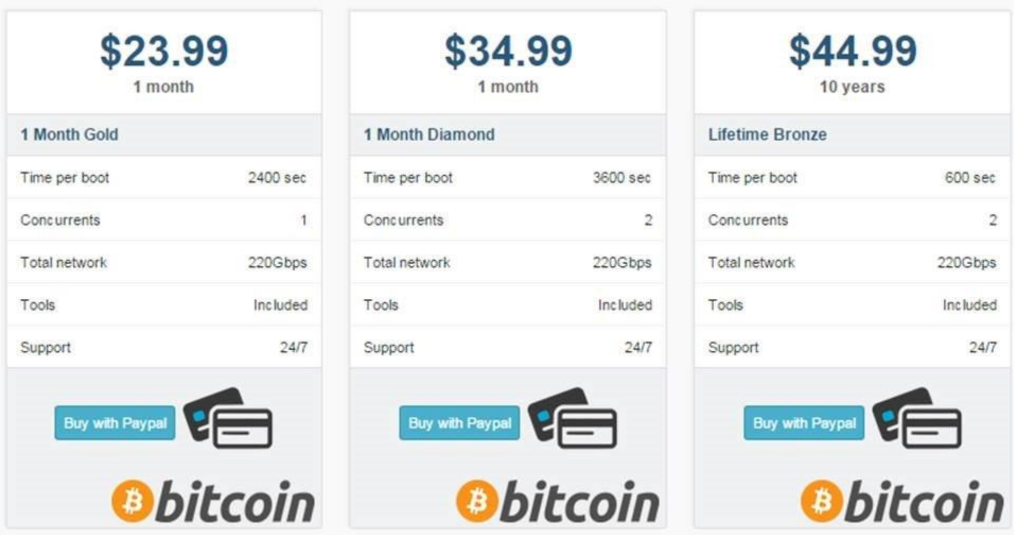
- **Attack vector**: request or use more resources than the service provider can handle
- **Objective**: Affects or disrupts the business or the service as valid users are not able to use it at all or in “normal” conditions
- Usually generates traffic around 100 Gbps limit (near the target) but overall can exceed this limit (since 2016 there are more attacks near or over the limit)
- Uses infected devices or ‘zombie machines’ in coordinated attacks
- Attacker ‘unlimited’ ability to generate requests vs. defender ‘limited’ resources (bandwith, processor power, memory) to respond

Characteristics

- Targeted resources
  - The connection – limited by the maximum bandwidth
  - The processor – limited by the number of messages that it can process
  - The memory – limited
  - Logic resources as number of available connections – limited
- It's cheaper to create and send a message vs processing the message
- The first recorded attack in 1974 – courtesy David Dennis, a 13-year-old student at University High School

Characteristics

- Easy to implement on your home computer
- Requires few technical skills – perfect for script kiddies
- Can be automatized with dedicated software and scripts
- Can be rented as a service - DDoS-for-hire services (booters or stresser)
- Difficult to mitigate



$23.99 1 month		$34.99 1 month		$44.99 10 years	
1 Month Gold		1 Month Diamond		Lifetime Bronze	
Time per boot	2400 sec	Time per boot	3600 sec	Time per boot	600 sec
Concurrents	1	Concurrents	2	Concurrents	2
Total network	220Gbps	Total network	220Gbps	Total network	220Gbps
Tools	Included	Tools	Included	Tools	Included
Support	24/7	Support	24/7	Support	24/7

https://www.incapsula.com/ddos/booters-stressers-ddosers.html

Characteristics

BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS ©2000 THE CHARLOTTE OBSERVER

http://blogs.it.ox.ac.uk/oxcert/files/2014/05/vandal-hacker.jpg

Characteristics

Based on Akamai research (2015):

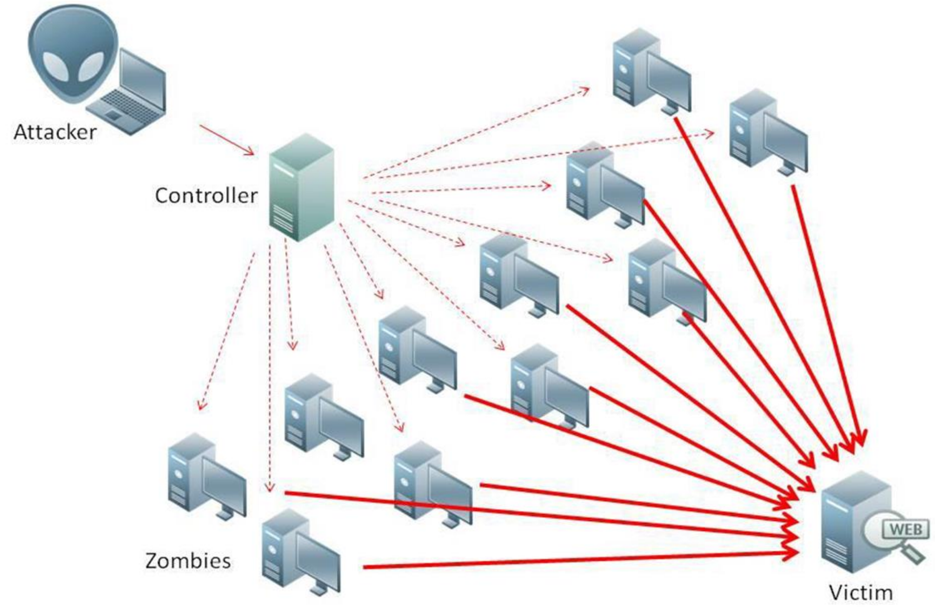
- average DDoS attack duration: 19-22 hours
- Targeted services:
  - 50% gaming industry services (game servers mostly)
  - 25% software and technology companies
  - Less than 5% Telco industry

Terminology & Definitions

- **DoS** – Denial of Service
- **DDoS** – Distributed Denial of Service: a coordinated DoS attack conducted from multiple sources
- **Botnet** – “zombie army”/ a group of hijacked Internet-connected devices
- **Booter/Stresser** – DDoS-for-hire business (not so legal)
- **IP spoofing** – change the source IP value of a network packet

DDoS – Distributed Denial of Service

- Is a DoS attack conducted from multiple devices/machines
  - “zombie army”/botnets infected by malware
  - Legit clients which are forced to connect to the DoS target by exploiting protocols vulnerabilities – **amplify and reflect techniques**
- Requires coordination from a C&C (Command and Control) center
- Can use malware to infect and control the botnets
- Implements a wide range of different DoS attacks

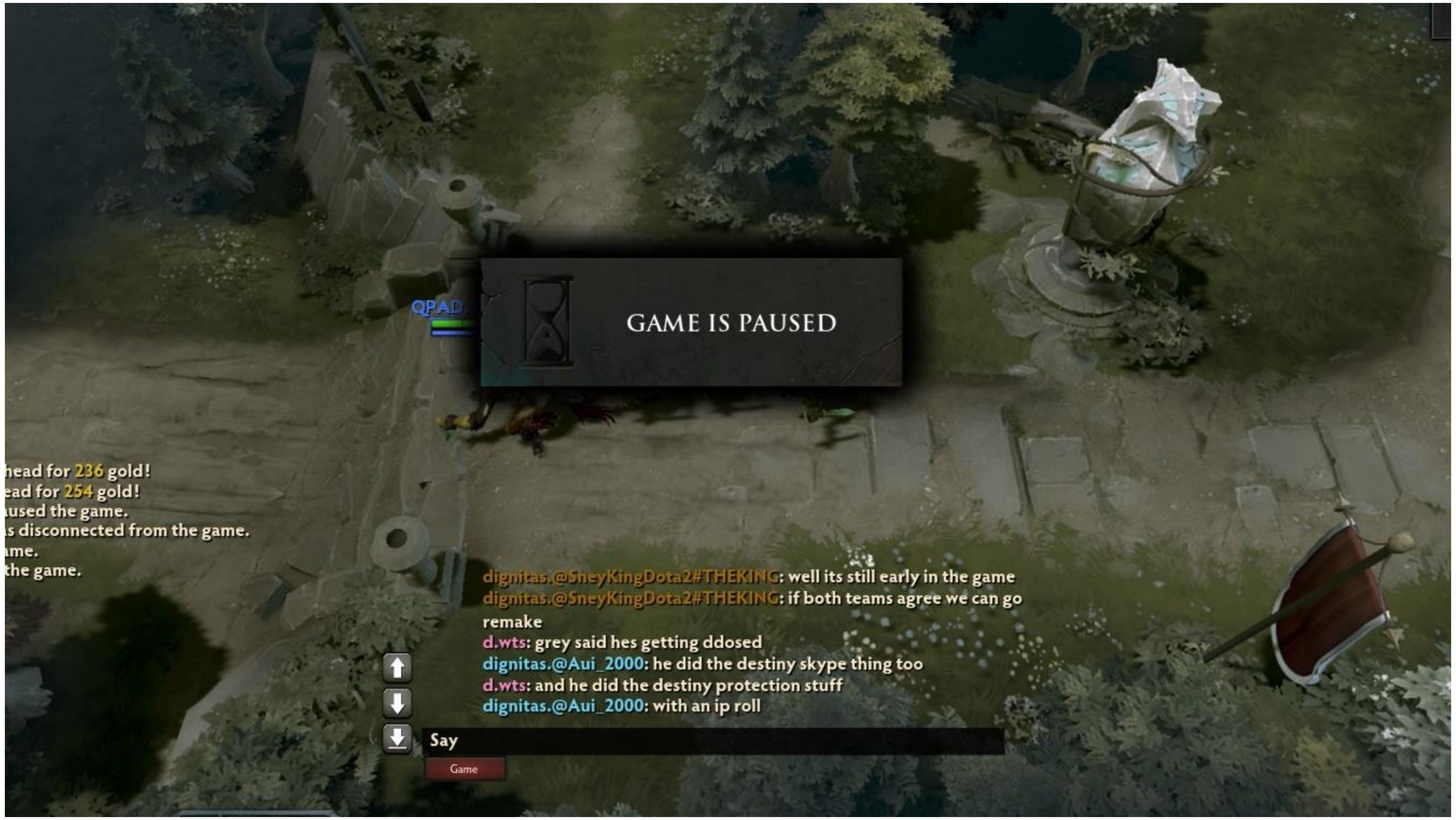


Source: https://www.realnets.com/our-blog/massive-ddos-attacks-lizardstresser/

Scope

- **Hacktivism** – to make a public statement
- **Cyber vandalism** – mostly script-kiddies
- **Extortion** – for the money
- **Business competition** – to disrupt competition services
- **Personal rivalry** – just personal (mostly gamers stuff)
- **Cyberwarfare** – state backed attacks

Scope



GAME IS PAUSED

```
head for 236 gold!
ead for 254 gold!
used the game.
s disconnected from the game.
me.
the game.
```

```
dignitas.@SneyKingDota2#THEKING: well its still early in the game
dignitas.@SneyKingDota2#THEKING: if both teams agree we can go
remake
d.wts: grey said hes getting ddosed
dignitas.@Aui_2000: he did the destiny skype thing too
d.wts: and he did the destiny protection stuff
dignitas.@Aui_2000: with an ip roll
```

Recent history of DDoS attacks

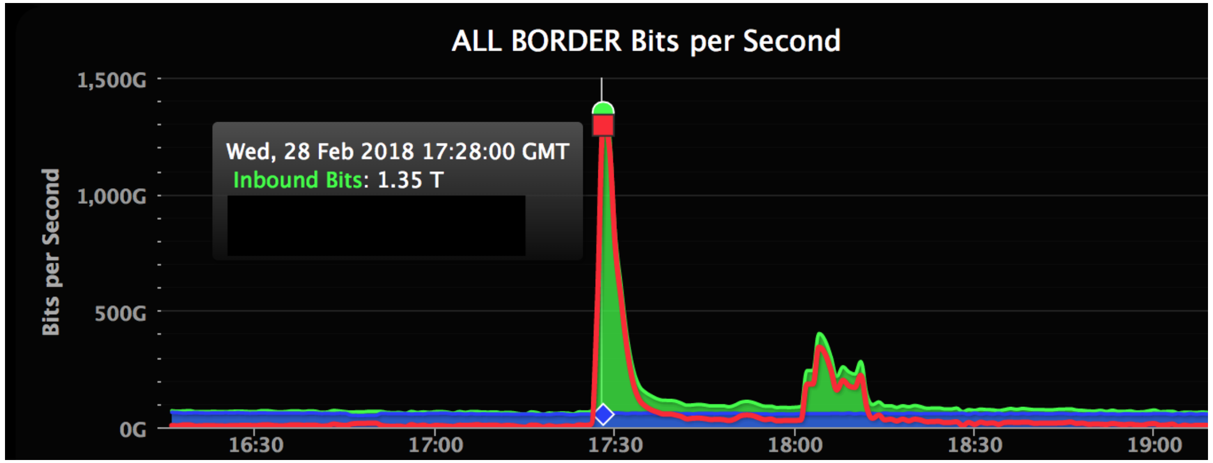
- 2013 – Largest DDoS attack that exceeded the 100 Gbps limit
  - hit the CloudFlare network, which hosts SpamHaus.org
  - Upstream providers have seen traffic > 350 Gbps
  - Affected Internet connections in Europe
  - Until then a common DDoS were peaking around 20 – 40 Gbps

Recent history of DDoS attacks

- 2016 Mirai botnet DDoS
  - the Mirai malware infected Internet of Things (IoT) devices – between 100,000 - 150,000 devices, mostly CCTV and IP Cameras (which were using default admin accounts)
  - generated more than 500 Gbps on the target
  - targeted DNS provider Dyn – affecting Twitter, GitHub, Amazon, Netflix, Pinterest, Etsy, Reddit, PayPal, and AirBnb services
  - hit French Internet service and hosting provider OVH - traffic peaked at 1.1 Tbps
  - were able to isolate Liberia from the rest of the Internet (they have only 1 underwater cable connection)
  - https://thehackernews.com/2016/09/ddos-attack-iot.html
  - Why and how it started https://www.wired.com/story/mirai-botnet-minecraft-scam-brought-down-the-internet/
  - https://github.com/jgamblin/Mirai-Source-Code

Recent history of DDoS attacks

- March 2018 GitHub DDoS
  - The largest recorded DDoS with a peak of 1.35Tbps ~ 126.9 million requests per second (RPS)
  - https://githubengineering.com/ddos-incident-report/
  - Uses a new Memcached UDP Reflection and Amplification attack
  - https://blog.cloudflare.com/memcrashed-major-amplification-attacks-from-port-11211/



Source: https://githubengineering.com/ddos-incident-report/

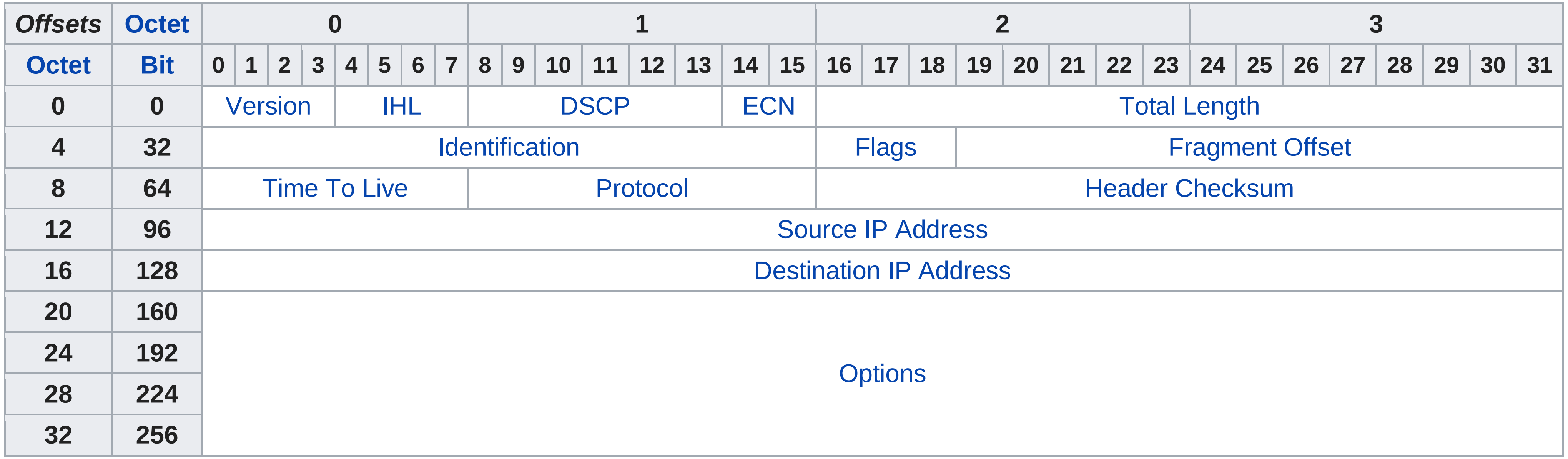
Classification

- **Volume-based attacks**
  - generate too much traffic than the server/service can process
- **Protocol/Network attacks**
  - exploits server resources and protocol vulnerabilities
  - *Ping of Death* or *Sync Flood*
- **Application attacks**
  - targets the disruption of a particular application (mostly Web applications) and not the entire host
  - *HTTP Flood*
- **Multi-Vector attacks**
  - a combination of tools and strategies

Spoofing

- **To spoof** - *to fool by a hoax; play a trick on, especially one intended to deceive (http://www.dictionary.com/browse/spoofing)*
- Technique used to impersonate a user or device
- **DNS server spoofing** – control DNS response to redirect clients to other addresses.
- **ARP spoofing** – associate the attacker device MAC to the target IP by manipulating ARP packets
- **IP address spoofing** – change the source IP address to hide the attacker identity or to conduct reflect attacks

IP Spoofing



Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset												
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options																															
24	192																																
28	224																																
32	256																																

https://en.wikipedia.org/wiki/IPv4

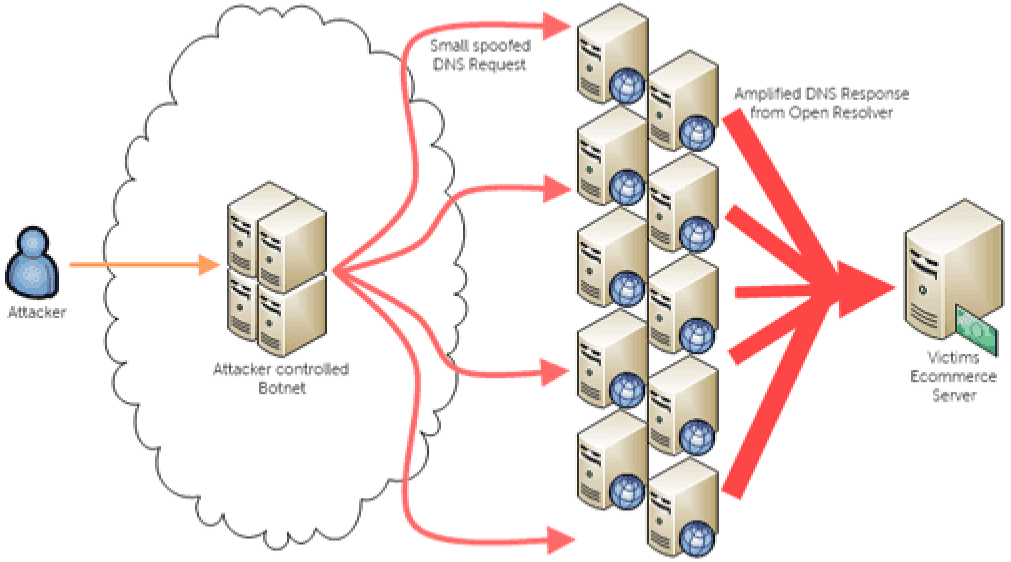
IP Spoofing

Used in DDoS to:

- Hide the attacker identity
- Amplify and reflect the attack
- Conceal botnet devices
- Avoid mitigation measures based on blacklisting IP addresses

DoS attacks – Amplify & Reflect

- A technique that exploits protocols vulnerabilities
- Tricks legit client to connect in the same time to the DoS target
- A single broadcast message generates an amplified response (the amplification factor = no of clients that get the request)
- Changes different protocol packages (SNMP, ICMP) by spoofing the target IP
- Examples: Smurf, SNMP reflection/amplification, DNS Amplification, SNMP reflection


Small spoofed DNS Request
Amplified DNS Response from Open Resolver
Attacker
Attacker controlled Botnet
Victims Ecommerce Server

https://blog.sflow.com/2013/10/dns-amplification-attacks.html

DoS attacks – Amplify

- A technique that exploits protocols vulnerabilities
- Tricks legit client to connect in the same time to the DoS target
- A single request message triggers a response with a bigger size (amplification factor)
- Examples: DNS amplification, Memcache amplification

DoS attacks – Reflect

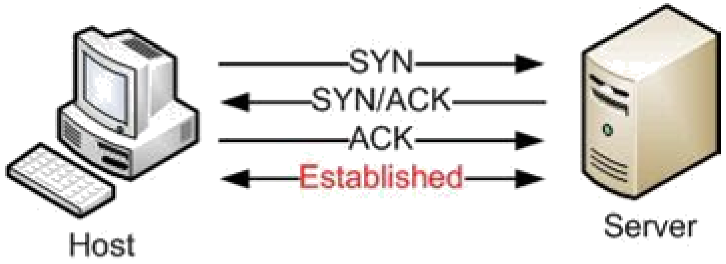
- Tricks legit clients to connect in the same time to the DoS target by forging the request source identity – spoofing
- Changes different protocol packages (SNMP, ICMP) by spoofing the target IP
- A single broadcast message generates an amplified response (the amplification factor = no of clients that get the request)
- Examples: Smurf, SNMP reflection, UDP Spoofing, IP Spoofing
- Can exploit applications vulnerabilities - *P2P File-sharing in Hell: Exploiting BitTorrent Vulnerabilities to Launch Distributed Reflective DoS Attacks*

DoS attacks

- SYN Flood
- UDP Flood
- HTTP Flood
- Ping of Death
- Smurf Attack
- Amplify & Reflect Attack
- Nuke
- DNS or NTP Amplification
- Slowloris
- Advanced Persistent DoS (APDos)
- Zero-Day DDoS attacks

DoS attacks – SYN Flood

- exploits the TCP "three-way handshake" protocol (https://support.microsoft.com/en-us/help/172983/explanation-of-the-three-way-handshake-via-tcp-ip)
- Opens multiple valid TCP connections without closing them – connections are closed only after the time-out expires
- The server resources are exhausted because a lot of connections are opened but not used (eats up memory and processor)



DoS attacks – HTTP Flood

- Floods the Web server with valid POST and GET requests
- Can replay real requests
- Efficient from the bandwidth volume values – can be conducted from low speed networks
- Forces the Web server to process the requests – it will generate processor and memory spikes

DoS attacks – UDP Flood

- Floods the target with valid UDP packets on different ports
- Efficient from the attacker needed resources perspective: fire and forget (UDP is a sessionless protocol)
- Can use broadcast UDP packets to flood the entire network (in closed environments)
- Forces the target to check if there are applications listening on those ports

DoS attacks – Ping of Death

- Floods the target with a high number of pings (IP protocol)
- Send ping packets larger than the maximum byte size (for IPv4 is 65,535 bytes)
- It is possible because large ping packets are divided by default in fragments and reassembled at the destination; at the destination the huge packet can generate errors (buffer-overflow) and force the server to crash
- Popular at the beginning of DoS but now is ineffective (routers and servers can be configured to drop ping packets)

DoS attacks – Ping of Death

- Just for academic purpose. On Windows you can use the command line **ping** utility with some options
  - -l size for buffer size
  - -w for waiting time
  - -n for number of echoes to send
- You can create a bash file (test.bat)

```
:loop
ping <IP Address> -l 65500 -w 1 -n 1
goto :loop
```

DoS attacks – Slowloris

- a complex tool used to generate DoS attack
- Reduces greatly the resources needed by the attacker by reducing requests size and increase the time the connection is kept up
- Generates a large number of HTTP connections which are kept opened for a long time
- Used in the 2009 Iranian presidential election DoS
- Difficult to mitigate
- https://github.com/llaera/slowloris.pl

DoS attacks – Others

- Zero-Day DoS attack
  - an attack method that to date has no patches
- Advanced Persistent DoS (APDos)
  - Uses multiple attack techniques
  - Very complex
  - Difficult to mitigate
- DNS or NTP Amplification
  - Exploits Network Time Protocol (NTP) or Domain Name Servers (DNS) servers by tricking them to send large responses (for small requests) to the target (using IP Spoofing)

DoS protection

- Reserve bandwidth for spikes
- Implement technical measures that can partially mitigate the effect of an attack (in early stages)
- Stay close to your ISP or Hosting Provider
- use a specialist DDoS mitigation company (if you are a large company) – they have the infrastructure to reroute and dissipate the DDoS attack; Akamai, CloudFlare, Incapsula, etc.
- …. or disconnect from the network ☺

DoS protection

- Overprovisioning – reserve more bandwidth and processing power, expecting the worst (DDoS)
- Black–hole routing – disconnect the target in order to save the others
- Filter anomalies – drop packets based on filters (most DoS packets are 'strange')
- Replication – replicate resources to multiple nodes and switch between them when one is attacked
- Pushback – recursively go upstream and instruct nodes to reduce the rate at which they route intended for the DoS target

You can't hide something connected to the Internet

DoS Tools

Scripts:

- **HTTP Unbearable Load King (HULK)** - http://www.sectorix.com/2012/05/17/hulk-web-server-dos-tool/
- **R.U.D.Y. (R-U-Dead-Yet?)** - https://github.com/loganhasson/r-u-dead-yet
- **Slowloris** - https://github.com/llaera/slowloris.pl
- High Orbit Ion Cannon (HOIC)
- Low Orbit Ion Cannon (LOIC)

Toolkits:

- Complex tools used to create and control botnets for DDoS

These tools are meant for educational purposes only, and should not be used for malicious activity of any kind.

DoS Tools

- hping 3 Linux tool
  - https://tools.kali.org/information-gathering/hping3
  - Can be used to simulate different flood attacks
  - `hping3 –i u100 –S –p <IP address>`
    - 100 packets per second
    - SYN flag
- nmap
  - https://nmap.org/nsedoc/categories/dos.html
  - `nmap --script http-slowloris --max-parallelism 400 <IP address> -vv`

More DoS

- Major problem for the Internet as we know it (and will be)
- Not a simple problem – for now mitigation solutions are based on filtering and on re-routing the DDoS traffic
- IoT development (around 7-8 billion devices) will fuel up more DDoS attacks
- DDoS and crypto currencies DDoSCoin - https://www.usenix.org/conference/woot16/workshop-program/presentation/wustrow
- Still an undeveloped area in matter of protection