securitylab

Denial of Service

Boris Mutina

boris.mutina@sec-lab.com
boris.mutina@gmail.com
skype: minor.float

Powered by Security Lab

information
security services

zone-h
unrestricted information

Agenda

- DoS and DDOS - what is this about?
  - too much noise for nothing?
  - DoS/DDoS and amplification
    - DoS/DDoS and asymetry

zone-h
unrestricted information

securitylab

• • •


COULD I HAVE A CUP OF COFFEE, PLEASE?
NO
geek and poke
SIMPLY EXPLAINED
PART 1:
DENIAL OF SERVICE

• • •


THE SERVER VIRTUALIZATION PROJECT IS DONE, AND THERE ARE NO TROUBLE TICKETS.
MY RATES MIGHT SEEM STEEP, BUT REMEMBER, THERE ARE NO TROUBLE TICKETS.
OUR ONLINE TROUBLE TICKET SYSTEM IS BROKEN.
www.dilbert.com scottadams@aol.com
© Scott Adams, Inc./Dist. by UFS, Inc.

DoS

Denial of Service - a state when service, componen
or system is not able to perform it's function

affected could be the whole system, service or singl
component

permanent, repeating or temporary

DoS attack

the goal is to disrupt the information source or medi
and avoid usage by the regular users

makes use of the error, standard, asymetry - logic
attack means

...or caused by the physical problem

note: who told only the flooding is the way

DDoS attack

DDoS attac = DoS attack x more sources

in case of DDoS the flooding is mostly in use

flooding by the regular requests seems to be ver
effective way

DDoS make use of asymetry and amplification

DoS or DDoS?

DoS has a single source

DDoS needs necessarily the activity coordination to be effective

DoS attack makes use of the asymetry

DDoS attack creates the asymetry

Attack targets

important infrastructure parts: border gateway mailserver, DNS server...

webserver/webapp/database

end user device or application

note: target might not be the data destinatio
(transit data, backscatter

Too much noise for nothing?

DoS/DDoS damages on the rise, DoS/DDo
execution costs lower

attacks more common also against the relativel
small targets, methods simplier

not working information systems can cause the chai
of other incidents

note: you can buy the insurance in case
of UFO abductions, can you do this for DoS/DDo

... nothing?

If the target are the companies...

...this can happen also to me

If the target are the public sector organizations...

...state services do not work, why paying taxes

If the target are the communication means...

...no connection = no command & control & salvatio

If the target are the end users...

...is on today somebody not important

Network and application flood

SYN flood - very popular and still used w/backscatte

hping -a 10.1.1.1 -p 53 -S 192.168.100.115 -i u

UDP flood - also popular

Teardrop, RUDY, IRC floods, WiFi deauth flood

ICMP flood/Nuke - ...should not work anymore...

Why using flood...

www.cisco.com/warp/public/707/cisco-sa-20111005-asa.shtml

Summary

Cisco ASA 5500 Series Adaptive Security Appliances and Cisco Catalyst 6500 Series ASA Services Module are affected by multiple vulnerabilities as follows:

- MSN Instant Messenger (IM) Inspection Denial of Service vulnerability
- TACACS+ Authentication Bypass vulnerability
- Four SunRPC Inspection Denial of Service vulnerabilities
- Internet Locator Service (ILS) Inspection Denial of Service vulnerability

www.cisco.com/warp/public/707/cisco-sa-20110928-dlsw.shtml

Summary

Cisco IOS Software contains a memory leak vulnerability in the Data-Link Switching (DLSw) feature that could result in a device reload when processing crafted IP Protocol 91 packets.

www.cisco.com/warp/public/707/cisco-sa-20110928-nat.shtml

Summary

The Cisco IOS Software network address translation (NAT) feature contains multiple denial of service (DoS) vulnerabilities in the translation of the following protocols:

- NetMeeting Directory (Lightweight Directory Access Protocol, LDAP)
- Session Initiation Protocol (Multiple vulnerabilities)
- H.323 protocol

zone-h unrestricted information

securitylab

...the result is obvious :)

zone-h unrestricted information

securitylab

Don't forget

IP spoofing is one of the most important aspects fo
DoS and DDoS attacks

request source IP address is changed (if ISP allows)

if random and changing ---> backscatter

if staticaly defined ---> reflected DoS/DDoS

Example: DNS fear in 2008

Dan Kaminsky presented his “Internet killing bug”

```
Dan,

This is another of our clients and you do not have the permission of the =
client to perform this kind of scanning.

You have triggered over 22,000 events for us in this range alone as well =
as caused a few other minor aggravations.

While you may believe you are a researcher and doing good, performing =
your unauthorized testing on live production platforms is a reportable =
offense.

I am going to kindly suggest you seek permission from various targets =
before you continue your &quot;research&quot;.

Please note I am under contractual obligations to report your =
activities, we have recorded your &quot;scans&quot; on over 26 devices globally =
and none of our clients have given you permission to perform these =
&quot;tests&quot;


Thanks

R Grant Leonard=20
Technical Security Specialist
AT&amp;T | Managed Security Services
Threat Management | MIDS | DDoS | Internet Protect | Analysis
rgleonard@att.com &lt;mailto:rgleonard@ems.att.com&gt;  | O 919-474-1147 | C =
919-949-4002
```

zone-h unrestricted information

securitylab

Solution is ...

Dan Kaminsky suggested DNSSEC (!), as a protection means agains the DNS poisoning

but DNSSEC has other issues...

...DNSSEC zone walking
...implementation weaknesse
...amplification for Do

Example: amplification w/ DNSSEC

attacker sends the request to the DNSSEC server with a spoofed IP address

DNSSEC server responds with more than 30x bigger data than the request was

if attacker manages to send the 10Mbps flood against DNSSEC server, it responds with about 300Mbps (against the spoofed IP address) :):)

Dan Bernstein, http://cr.yp.to/talks/2010.12.28/slides.p

Asymetry

Internet is very asymetric environmet, allows also the strong to be attacked by the weak

data processing is mostly on the server side and the networking components

DDoS attacks outballance this asymetry

DoS attacks make use of

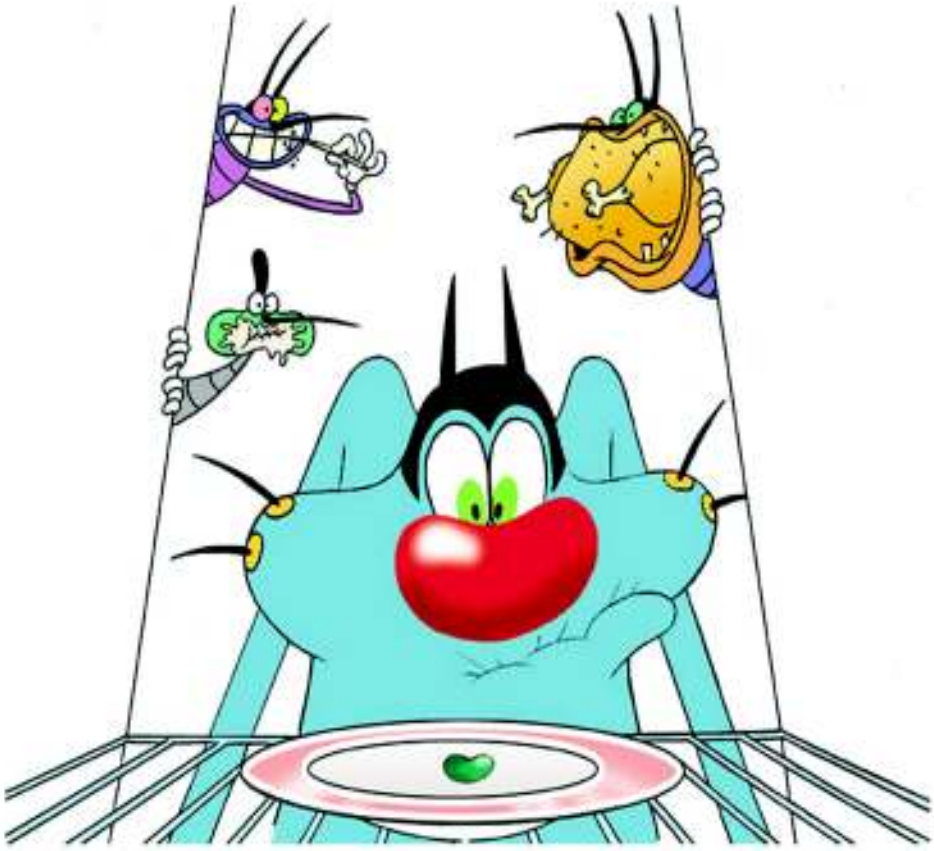
Asymetry and DDoS attacks

one attacker cannot disrupt one server

group of attackers can handle more servers

botnet concept

botnet build of servers?



Asymetry and DoS attacks

servers handle a big ammount of requests

find the weakest point...

...the right data...

...and here we are!

Example: Asymetry w/SSL

after the SSL renegotiation fear there is an old nev
SSL fear

common server handles about 300 SSL handshake
per second

common client can request more than 300 SS
negotiations per second

asymetry result: one atatcker crashes one server

Example:Asymetry with SSL

not only web servers w/HTTPS

is not a real flood but exhausting the system resources

SSL akcelerator can solve this but what if DoS becomes DDoS

tool freely available

DoS on network backbone?

75-year old copper miner found the optic fibre

www.bbc.co.uk/news/world-europe-12985082

Pensioner in Georgia cuts Armenia off from internet

An elderly woman in Georgia is facing a prison sentence after reportedly causing internet services in neighbouring Armenia to crash.

The country found itself offline for hours on 28 March after cables linking Georgia to Armenia were damaged.

A Georgian interior ministry spokesman said a 75-year-old woman had admitted damaging fibre-optic cables while scavenging for copper.

Fibre-optic cables carry services via Georgia to Armenia

She has been charged and reportedly faces up to three years in prison.

zone-h unrestricted information

securitylab

DoS a-la digg-deeper

something is wrong here... :)

Bagrista překopl optický kabel

České Velenice – Na 121 tisíc korun se odhaduje škoda, kterou způsobil řidič pracovního stroje při výkopových pracích.

22.11.2009 4:41

Lžící bagru na začátku října přerušil optický kabel, čímž vyřadil z provozu pevné linky, ale i bankomaty a podobně.

Podle sděleného obvinění nedodržel

zone-h unrestricted information

securitylab

Short end

think about “what if”...

disaster recovery, plan B

prevention better than therapy

...the most impossible thing reverts to be enough dangerous

Q&A

Thank you for listening!

500 Internal Server Error

Sorry, something went wrong.

A team of highly trained monkeys has been dispatched to deal with this situation.

Also, please include the following information in your error report:

```
UgGBfkcPPhkqcIB7SONKKIOcOZ143BB3PMJP1bbfRpqwIHfywzb5YIy-uT6g
qg8s4OVima1L_131GwZBWlKm4bt2gSqZETKcNpffenMi6kMDI_PO9yNfDb41
HFO6x6joyrMrpWEnwpg9J1TxC9mP14s4DoDdDTwwC4A2UHPnODZrMJxFbTks
8wd4q8HeqQvvopbx5v4Lw7ai5AzYmELOBOZ21HNVWqLN61SO7kBbOUQGn lt
```

zone-h unrestricted information

securitylab