3. Network Attacks and Their Detection

(D)DoS, Scanning, Brute-Force

Simona Buchovecká, Tomáš Čejka

Faculty of Information Technology, CTU in Prague

simona.buchovecka@fit.cvut.cz, tomas.cejka@fit.cvut.cz

October 18, 2020

Section 1

General Information

Terminology

srcip	Source IP
dstip	Destination IP
srcport	Source port of transport protocol
dstport	Destination port of transport protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Section 2

Scanning

Network Scanning

- Host / Service discovery
- Information gathering
- UDP (connectionless) vs. TCP (connection-oriented)
- ICMP

Scanning Traffic: Packet view

Host discovery by ICMP

ICMP messages with type *echo*, usually one *srcip*, changing *dstip*

TCP SYN

TCP packets, SYN flag, usually one *srcip*, usually one *dstip*, usually many *dstport*, one or more *srcport*

Scanner analyzes response, SYN&ACK for open port.

UDP scan

UDP packets, usually one *srcip*, usually one *dstip*, usually many *dstport*, one or more *srcport*, some payload optional.

Scanner analyzes response, packets are being duplicated, longer timeouts.

Brainstorming: block scan? RST scan? X-mass scan?

Scanning Traffic: Flow view

Host discovery by ICMP

proto = 1, *srcport*= 0, *dstport*= type and code

TCP SYN

Increased number of TCP flow records, mostly with just SYN or SYN&RST flag, with one or more *srcport* and usually many *dstport*.

UDP scan

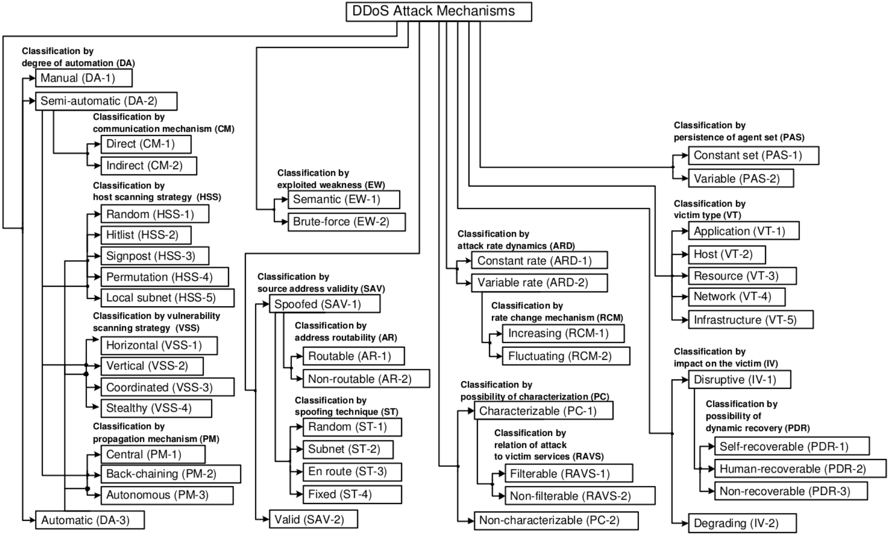
Increased number of UDP flow records, with one or more *srcport* and usually many *dstport*.

Brainstorming: block scan? RST scan? X-mass scan?
Discussion in a particular tutorial.

Section 3

(D)DoS

(Distributed) Denial of Service (DoS)



DDoS Attack Mechanisms

- Classification by degree of automation (DA)
  - Manual (DA-1)
  - Semi-automatic (DA-2)
    - Classification by communication mechanism (CM)
      - Direct (CM-1)
      - Indirect (CM-2)
    - Classification by host scanning strategy (HSS)
      - Random (HSS-1)
      - Hitlist (HSS-2)
      - Signpost (HSS-3)
      - Permutation (HSS-4)
      - Local subnet (HSS-5)
    - Classification by vulnerability scanning strategy (VSS)
      - Horizontal (VSS-1)
      - Vertical (VSS-2)
      - Coordinated (VSS-3)
      - Stealthy (VSS-4)
    - Classification by propagation mechanism (PM)
      - Central (PM-1)
      - Back-chaining (PM-2)
      - Autonomous (PM-3)
  - Automatic (DA-3)
- Classification by exploited weakness (EW)
  - Semantic (EW-1)
  - Brute-force (EW-2)
- Classification by source address validity (SAV)
  - Spoofed (SAV-1)
    - Classification by address routability (AR)
      - Routable (AR-1)
      - Non-routable (AR-2)
    - Classification by spoofing technique (ST)
      - Random (ST-1)
      - Subnet (ST-2)
      - En route (ST-3)
      - Fixed (ST-4)
  - Valid (SAV-2)
- Classification by attack rate dynamics (ARD)
  - Constant rate (ARD-1)
  - Variable rate (ARD-2)
    - Classification by rate change mechanism (RCM)
      - Increasing (RCM-1)
      - Fluctuating (RCM-2)
- Classification by possibility of characterization (PC)
  - Characterizable (PC-1)
    - Classification by relation of attack to victim services (RAVS)
      - Filterable (RAVS-1)
      - Non-filterable (RAVS-2)
  - Non-characterizable (PC-2)
- Classification by persistence of agent set (PAS)
  - Constant set (PAS-1)
  - Variable (PAS-2)
- Classification by victim type (VT)
  - Application (VT-1)
  - Host (VT-2)
  - Resource (VT-3)
  - Network (VT-4)
  - Infrastructure (VT-5)
- Classification by impact on the victim (IV)
  - Disruptive (IV-1)
    - Classification by possibility of dynamic recovery (PDR)
      - Self-recoverable (PDR-1)
      - Human-recoverable (PDR-2)
      - Non-recoverable (PDR-3)
  - Degrading (IV-2)

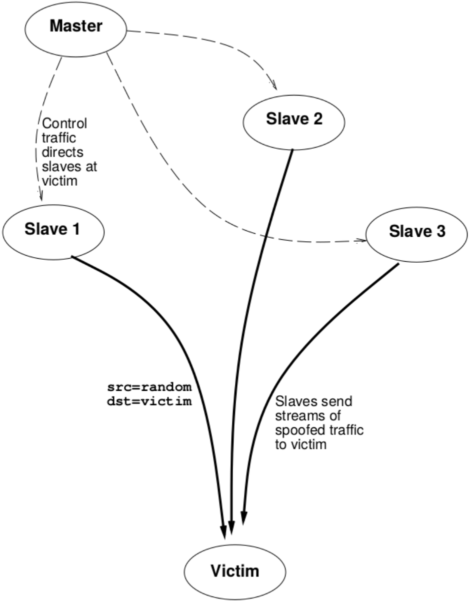
About DoS

- Making system slow/unusable by overloading its resources (with a little computing work)
- Availability attack
- Generally: unsophisticated attack, attackers do not gain any information from the target system, BUT they can learn its defense
- There are (unfortunately) many vulnerabilities in current software/hardware
- Basically, any error that ends with crash can cause DoS
- Depletion of victim's resources can cause DoS
- Deadlocks can cause DoS
- Infinite loops can cause DoS
- Bad configuration of network infrastructure can cause DoS
- See database of Common Vulnerabilities and Exposures (CVE) `https://cve.mitre.org/`, `https://www.exploit-db.com/`

“Bombs”

- Well-known fork bombs (https://en.wikipedia.org/wiki/Fork_bomb), possible even in shell
- Attacks against parsers:
  - XDoS attack (XML) (consuming expansion: https://en.wikipedia.org/wiki/Billion_laughs_attack)
  - Multiple signatures (consuming verification)
  - Regular expression DoS (ReDoS) (consuming evaluation: https://en.wikipedia.org/wiki/ReDoS)
  - (zip) archive that is too large after extraction

Distributed DoS (DDoS)


Master
Slave 2
Control traffic directs slaves at victim
Slave 1
Slave 3
src=random
dst=victim
Slaves send streams of spoofed traffic to victim
Victim

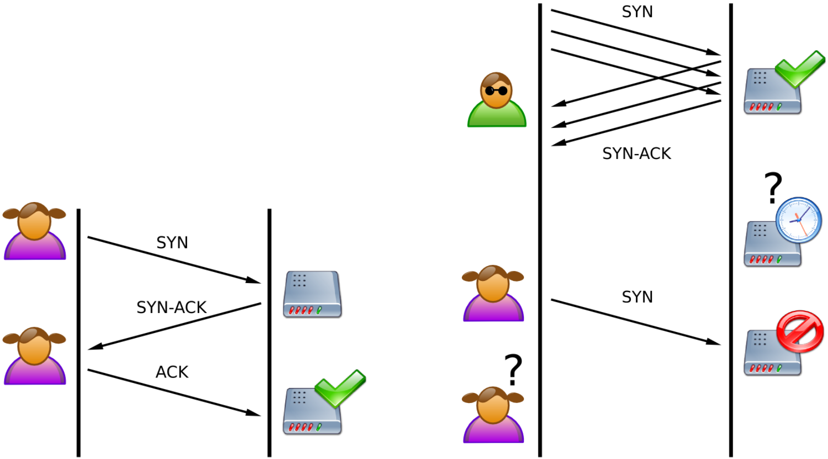
Distributed DoS (DDoS)

- Huge (synchronized) traffic (/many requests) from many sources against a victim
- Usage of botnets, many existing, many available, famous one `https://github.com/jgamblin/Mirai-Source-Code` in 2016
- Responding honeypots

Multiple hosts affected — usually compromised

- primary victim — service under attack
- secondary victims — compromised systems launching the attack, zombies/bots (botnet)

SYN Flood Attack



SYN Flood Traffic

Packets

TCP packets with SYN flag, Usually one or more *srcip*, one *dstip*, usually many *srcport*, one *dstport*.

Flows

Increased number of TCP flow records with SYN flag, see the Packets description.

UDP Flood Attack

- Sending large number of UDP packets to random ports
- Victim will reply with ICMP Destination unreachable packet for every UDP request to the closed ports
- Processing and sending big amount of ICMP packets may make system unresponsive for legitimate requests

Ping of Death

- Typical size of IPv4 packet: 64 bytes
- Maximum size may be up to 65 535 bytes
- Many systems were not designed to properly process such big packets
- ICMP echo request (ping) with maximum packet size may cause buffer overflow, system instability... or other problems on the receiving/victim system

WiFi DoS Attacks

De-authentication attack

- IEEE 802.11 defines *deauthentication* frame (management frames are being sent unencrypted)
- AP can send the *deauthentication* frame to a station
- Attacker can send a *deauthentication* frame with a spoofed address to a victim

Signal interference

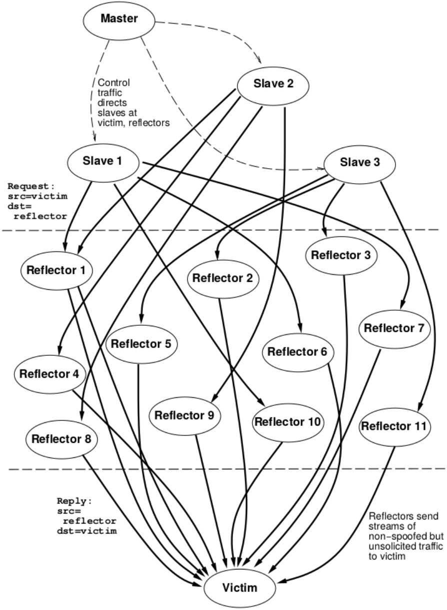
- Jamming
- WiFi jammer generates a noise on WiFi channels, making the frequencies unusable

Application Layer (L7) DDoS

Example: HTTP

- HTTP GET request flooding
- Volumetric attack, using a botnet to perform HTTP GET requests that pretend to be valid
- HTTP POST
- Valid POST request sent at very low rate – preventing the connection to be properly completed
- HTTP slow read
- Read the HTTP response "slowly" = set up small window (maximum amount of received data) size
- HTTP Malformed attacks
- Trying malformed/intentionally invalid requests; goal: unstable system

Distributed Reflection DoS (DRDoS)


Master
Control traffic directs slaves at victim, reflectors
Slave 2
Slave 1
Slave 3
Request: src=victim dst= reflector
Reflector 1
Reflector 2
Reflector 3
Reflector 7
Reflector 5
Reflector 6
Reflector 4
Reflector 9
Reflector 10
Reflector 11
Reflector 8
Reply: src= reflector dst=victim
Reflectors send streams of non−spoofed but unsolicited traffic to victim
Victim

DRDoS

- Amplification often employed
  - small number of packets (bytes) from source
  - generating bigger number of packets (bytes) against destination (attack target)
- Asymmetric attack (low resources, large consequences)
- Primary victim — service under attack
- Secondary victims — compromised systems launching the attack, zombies/bots (botnet)
- Reflectors/amplifiers (e.g. open DNS resolvers)

Smurf Attack

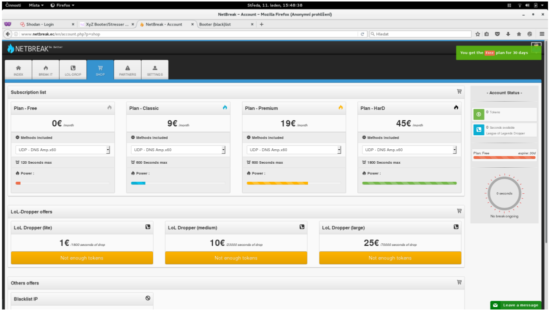
- reflected attack
- ICMP packets, broadcast address
- ICMP with spoofed *srcip* (victim's)

DNS Amplification

- Amplification through DNS
- typically transmitted over UDP, i.e., *srcip* can be spoofed
- size(Response) $>$ size(query)
- Problem: open DNS resolvers (respond to any query by any *srcip*)
  - *srcip* spoofed with victim's address
  - small query send by attacker
  - victim will receive much larger response

Booters Phenomenon

- Stress-test / DDoS-for-hire / DDoS-on-Demand
- Cheap attacks/stress-tests available for everyone! (It makes it more dangerous)



You get the Free plan for 30 days

Subscription list

Plan - Free
0€ /month
Methods included
UDP - DNS Amp.x60
120 Seconds max
Power :

Plan - Classic
9€ /month
Methods included
UDP - DNS Amp.x60
600 Seconds max
Power :

Plan - Premium
19€ /month
Methods included
UDP - DNS Amp.x60
600 Seconds max
Power :

Plan - HarD
45€ /month
Methods included
UDP - DNS Amp.x60
1800 Seconds max
Power :

- Account Status -

0 Tokens

0 Seconds available
League of Legends Dropper

Plan: Free expire: 30d

0 seconds
No break ongoing

LoL-Dropper offers

LoL Dropper (lite)
1€ /1800 seconds of drop
Not enough tokens

LoL Dropper (medium)
10€ /23000 seconds of drop
Not enough tokens

LoL Dropper (large)
25€ /70000 seconds of drop
Not enough tokens

Others offers

Blacklist IP

Additional Reading:

J. J. Santanna et al., "Booters — An analysis of DDoS-as-a-service attacks," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015, pp. 243-251, doi: 10.1109/INM.2015.7140298.

Slashdot / FlashCrowd effect

- It is not an intended attack (false positives?),
- but effects are the same as for real attacks.
- Popular news spread very quickly
- Social media help information spreading (twitter, facebook, ...)

Section 4

Brute-Force

Brute-Force Attacks / Scans

- Motivation: gain access
- Guessing username or password / scanning hosts
- Dictionary / Enumerated attempts
- Against any protocol or service
- The aim is to gain access (or) steal identity / gather information

Section 5

Defense

Scanning Defense

- Let open only necessary ports
- Drop instead of Reject (politeness vs scanner slowdown?)
- Decoy/Honeypot?

SYN Flood Defense

- SYN cookies
- allocate system resources only after TCP handshake is completed
- RST cookies
- after received SYN, server sends invalid SYN ACK
- RST should be received from client – in this case the client is valid
- Micro blocks
- only small memory space allocated for incoming SYN requests (e.g. 16 bytes)
- Stack tweaking
- selectively dropping incoming connections
- reducing the timeout when the memory allocated for the connection is freed up

SYN cookies

- Transmission Control Block (TCB): data structure which holds the connection state information
- Cookie = calculated TCP sequence number

Smurf attack Defense

- Endpoints should not respond to broadcasted ICMP requests
- Routers should drop the broadcasted ICMP requests

(D(R))DoS Defense

- Difficult
- Most effective: ISP providing countermeasures
- SYN proxy (until ACK, connection request not forwarded)
- Connection limits (prioritize existing connection, limit per IP etc.)
- Aging (how long can the connection be idle? → TCP RST), timeouts
- Anomaly recognition (malformed headers, protocol state etc.)
- Dark address prevention (address not assigned by IANA most probably spoofed)
- Bandwidth over-subscription
- Blackholing / RTBH
- Load-balancing
- System hardening, tuning (profiling)

DDoS Defense: Main Issues

- Victim can do completely nothing when the network is under attack. **The only hope is contacting ISP (or peering network operator).**
- Victim can easily see the attack X Source network can easily drop the traffic (`http://www.bcp38.info`)
- Lets drop evil packets... **Well, which packets are evil?** This kind of recognition is The Question that can make us rich!
- **Dropping/blocking all means successful attack** — system/service is down or disconnected.
- **World is bigger than we are.**
  There are many devices out there that can be used by attackers, we always have significantly less resources.
- **Spoofed addresses** make harder to find origins of the traffic.

Brute-Force Attack Defense

- fail2ban
- limited number of login attempts
- good passwords
- key vs password
- unpredictable username (if possible)

Section 6

Closing Words

Questions?