15 - Denial of Service

- Availability si riferisce all'abilità di usare un informazione o servizio desiderato.
- Un Denial of Service attack è il tentativo di rendere quell'informazione non disponibile agli utenti legittimi
- Gli attacchi più comuni sono mirati a internet host, i cui servizi vengono temporaneamente negati

CAPTCHA

- la maggior parte degli umani possono risolverli facilmente
- i computer correnti non sono in grado di risolverli accuratamente
- non si affida al fatto che l'attaccante non ha mai visto questo tipo di CAPTCHA prima
- può essere generato automaticamente ma richiede tecniche di AI per risolverli

reCAPTCHA

200 milioni di CAPTCHA sono risolti da umani ogni giorno
reCAPTCHA cerca di migliorare il processo di digitalizzazione dei libri mandando le parole che non riesce a riconoscere il formato di CAPTCHA per farli decifrare a umani.

noCAPTCHA

é possibile distinguere umani da AI usando tecniche di machine learning che tengono conto di quello che l'utente fa prima e dopo aver cliccato una semplice checkbox

DoS types

Due strategie generiche per gli attacchi:

- crash dei servizi
- flood dei servizi
  Diversi modi di lanciare un attacco
- consumo della banda
- consumo delle risorse host: RAM, disco, CPU
- distruzione di informazioni di stato (TCP sessions)
- distruzione di informazioni in se (cryptolocker)
- distruzione dei componenti fisci della rete (LAN, WAN)

DoS, manifestazioni

US-CERT definisce DoS:

- performance della rete stranamente lente
- impossibilità di provvedere un servizio per accesso remoto (web site)
- impossibilità di accedere a un servizio remoto (web site)
- aumenti del numero di pam email ricevute
- disconnessione da una connessione internet wireless o cablata

Una volita gli attacchi dos venivano fatti da un solo host. Oggi armate di host sono usate per lanciare attacchi molto più efficaci (Distributed DoS, DDoS): botnet of zombies
Con il termine zombie ci si riferisce a computer infettati da malware che vengono usati per effettuare attacchi
Le botnet di zombie vengono controllate dagli attaccanti.

IP Spoofing
Molti DDoS si basano su spoofed source IP address (a vittima crede che il pacchetto sia stato mandato da una macchina diversa da quella che lo ha mandato veramente)
Exploita ip header corrotti
IP spoofing ha applicazioni legittime come simulare traffico e load sulla rete
Può essere abusato per gli attacchi DDoS in quanto:

- rende più difficile tracciare gli attaccanti
- rende più difficile filtrare traffico maligno
- permette errori e floods nel traffico di rete

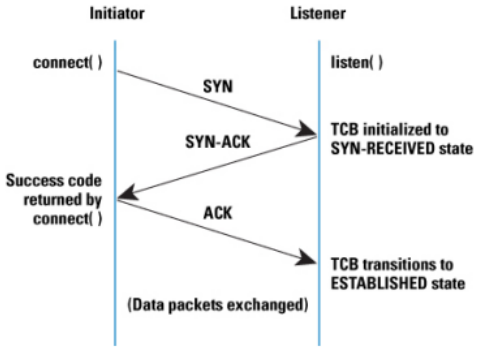
Attacchi conosciuti

- Ping of death
- Teardrop
- SYN Flooding
- Smurf
- Slow HTTP DoS
- altri

Ping of death
L'attaccante crea pacchetti IP che contengono più di 65.536 byte (limite definito dal protocollo ip)
Malformazione del ping ma può essere generalizzato
Exploitava un bug nelle prime implementazioni di TCP/IP durante il riassemblamento dei frammenti dei pacchetti causandone il crash.
Risolto in molti sistemi, è prevenibile con il firewall

Teardrop
Exploita la frammentazione dei pacchetti IP. Ogni frammento di pacchetto identifica un offset che da la possibilità al pacchetto intero di essere riassemblato
L'attaccante manda IP frammenti malformati con payloads sovrapposti e malformati causando il crash della macchina.
Patchato.

SYN flooding



Exploita vulnerabilità nell'handshake a tre vie di TCP e IP spoofing:

- L'attaccante (tramite botnet) inizia diverse richieste di connessioni TCP mandando SYNs all host vittima
- La vittima inizializza la connessione nel Transmission Control Block (TBC), invia SYN-ACKs a attende per ACKs prima di dichiarare ogni connessione ESTABLISHED
- Visto che le connessioni iniziali sono spoofed i messaggi SYN-ACK sono persi quindi gli ACKs non arriveranno mai.
- La coda di connessioni in arrivo al TCB si riempie e TCB non è più in grado di accettare richieste.

Reflector
Variazione del SYN flood attack usando l'handshake a tre vie di TCP e IP spoofing:

- l'attaccante (tramite botnet) inizia tante connessioni TCP con tanti host dove la source address (spoofed) è quella della vittima
- Ogni reflector manda il il messaggio di SYN-ACK alla vittima, floodandola

Smurf
Exploita le vulnerabilità del ICMP, Ip spoofing e errori nella configurazione del network broadcast

- l'attaccante manda pacchetti di ICMP echo-request sull'indirizzo di broadcast della rete
- Questi pacchetti contengono IP address spoofed impostati a quello della vittima e vengono mandati in broadcast a a tutti gli host della sottorete
- ogni host risponde inviando un sacco di pacchetti ICMP echo-reply alla vittima.

Slow HTTP
Exploita una vulnerabilità nei thread-based web servers (es. apache) che attendono la ricezione di tutti gli header HTTP prima di stabilire la connessione
benchè i server tipicamente fanno uso di timeout per concludere le richieste HTTP non complete (default a 300 sec) il timer si resetta ogni volta che il client manda dati aggiuntivi

Tenendo le richieste HTTP aperte e mandando dati ogni volta che il timer sta per finire le connessioni HTTP rimangono aperte
Se un attaccante riesce a occupare tutte le connessioni HTTP disponibili blocca l'accesso al server agli utenti legittimi.

Difese

Gli attacchi DoS non possono essere prevenuti o contrastati al 100%
Perchè:

- è molto difficile distinguere traffico legittimo e traffico non legittimo
  - filtrare il traffico in entrata potrebbe rifiutare richieste legittime
- Indirizzi IP spoofed rendono difficile il tracciamento dell'attaccante
- eterogeneità dei software e piattaforme
  Tre difese principali:
- prevenzione attacco
- detection dell'attacco e filtering
- tracciamento dell'origine dell'attacco e identificazione

prevenzione

- riduce la possibilità di essere uno zombie
- installa patch di sicurezza, antivirus e intrusion detection system
- mantenere i protocolli e OS up-to-date
- installare firewalls e configurare le reti per filtrare traffico in input/output
- Configurare risorse disponibili
  - path di rete alternati
  - load balancing
  - server addizionali

Detection
Cercare di rilevare un attacco il prima possibile e rispondere

- identificare pattern statistici di DDoS attacks e compararli con il traffico live
  - per attacchi conosciuti si possono usare tecniche di machine learning
  - ricerca firme da un database di attacchi
  - funziona con gli attacchi vecchi
- identificazioni di deviazioni da comportamenti standard dei clienti nel traffico normale della rete
  - comparare parametri correnti con quelli passati
  - funziona con gli attacchi nuovi

FIltering
Una volta rilevato traffico malevolo, esso può essere bloccato applicando filtri

- dove:
  - più vicino all'attaccante più è efficace
  - la cosa migliore sarebbe applicare filtri nelle macchine zombie (molto difficile, improbabile)
  Criteri di filtraggio
- source address
  - funziona se l'attaccante è conosciuto (IP può essere spoofato)
  - service/port
    - funziona se il meccanismo di attacco è conosciuto (UDP, TCP)
    - non funziona se l'attaccante usa una porta o servizio comune
  - Destination address
    - funziona se la vittima è conosciuta
    - traffico legittimo potrebbe essere rigettato
    - utile per limitare conseguenze di un attacco ad altri host serviti dallo stesso ISP