DDoS e IDS:
Attacchi DoS→ sono attacchi che impediscono l'utilizzo autorizzato di una risorsa esaurendola.

Classificazione dei DoS:

1. Banda di rete→ è il più comune. L'attaccante satura la capacità dei collegamenti
2. Risorse di sistema→ mandare pacchetti di rete che esauriranno il software di gestione della rete (e.g. memoria)
3. Risorse applicative→ tentativo di esaurire la memoria relativa ad una specifica applicazione

Se lo scopo di un attaccante è il DoS è semplice conoscere l'indirizzo dell'attaccante.
Una delle tecniche usate dagli attaccanti è lo spoofing dell'indirizzo sorgente, così da realizzare l'attacco senza essere tracciati.
Associato al concetto di "reflection".
Ciò che ogni ISP dovrebbe fare è filtrare gli indirizzi IP "spoofed": se si prova ad inviare un pacchetto ad un indirizzo "spoofed" il pacchetto resta nella LAN, non raggiunge la rete.

SYN spoofing→ è un attacco comune verso le risorse di sistema. Il SYN inizia una connessione TCP; il server alloca della memoria per ogni SYN perché si aspetta una connessione. L'attaccante manda un SYN con un indirizzo sorgente "spoofed"; il server risponde all'indirizzo sorgente, se è valido si otterrà un "RESET", perchè il client non aveva inviato la richiesta, se non esiste ritrasmetterà ed aspetterà (per un certo tempo definito da un t.o.) questo è il caso peggiore perchè per un certo periodo di tempo il server manterrà allocata la memoria.
Quando la tabella TCP è piena non si possono più accettare richieste, quindi quelle legittime verranno scartate.

Attacchi HTTP:
Due tipo:

1. Flooding di richieste HTTP ad un web server. E' un "amplification attack" perchè a pochi bytes di richiesta corrispondono molti bytes di risposta per caricare la pagina web
2. "Slowloris" per monopolizzare il server http. Consiste nell'inviare delle richieste HTTP che non si completano mai; si mandano pochi bytes in ogni richiesta e si consuma banda. Questi attacchi sono mitigati dalle signatures, che permettono di capire se il traffico in entrata è un attacco slowloris o meno.

Reflection attack→ utilizzano delle "middlebox" per riflettere un attacco. Si possono portare avanti dei grandi DoS senza avere bisogno di molta capacità, si sfrutta la capacità dei server esistenti.
La reflection ha bisogno di "source address spoofing".

Amplification attack→ non ha bisogno di source address spoofing, usa fattori di amplificazione, come quelli che abbiamo visto per DNSsec: mandare pochi bytes risulta in un quantitativo di bytes amplificato.
La mitigazione migliore è bloccare i pacchetti in entrata "spoofed".

Attacchi a DNS:
DNS si basa su UDP, quindi protocollo non basato sul concetto di connessione.
Si può fare reflection e amplification.
Amplification→ la richiesta di un record è di circa 10 B; se mando una richiesta con tipo "ANY" la risposta contiene tutti i record nel NS, quindi molto più grande. Il target è inondato di risposte.

Gli attacchi memcached sono attacchi di reflection ed amplification.

DDoS:
Sta per "distributed denial of service"; sono coinvolti diversi sistemi che contribuiscono all'attacco.
L'attaccante usa dei controller per controllare delle macchine "zombie", che sono macchine infette.

Mitigazione: non possono prevenirlo interamente; il problema è la distribuzione geografica delle macchine infette. E' difficile accorgersi di questo attacco, perché in alcuni momenti posso avere più traffico che in altri per un certo indirizzo, quindi risulta complicato distinguere traffico legittimo da sw malevolo.
La forma ed il contenuto dei pacchetti possono dare qualche indizio.

Prevenzione:
1. Bloccare gli indirizzi ip "spoofed"
2. Ci sono tecniche specifiche per determinate applicazioni, ad esempio i "SYN cookies" (numeri di sequenza cifrati, difficili da calcolare se non si ha la chiave) per prevenire i SYN spoofing attacks
3. Usare server replicati
4. Usare servizi cloud, come Cloudflare, che sono eseprti nell'accorgersi di attcchi DDoS. Controlla che tu sia un essere umano che vuole effettivamente completare la connessione.

Attack detection e filtering→ durante l'attacco, si può avere protezione su singolo IP o su intera sottorete.

Botnets:
Sono dispositivi connessi a internet su cui è in esecuzione del sw malevolo.
Vengono utilizzati per DDoS, spam, fishing, rubare dati,...
I proprietari li controllano tramite software "Command and control".
I bot tradizionali comunicano con il controller tramite struttura client-server; oggi non è più così, i nuovi botnet comunicano tramite reti P2P, hanno stesse funzionalità del modello client-server, ma non necessitano di un controllo centralizzato.

Modello client-server→ IRC (internet relay chat) a cui ci si può iscrivere ad un canale e si possono distribuire informazioni mandando comandi sullo specifico canale, i, client esegue il comando ricevuto e manda indietro sul canale il rosultato ottenuto.
P2P→ permette a tutti i bot di lavorare sia come client che come server; se un server si guasta non ci sono problemi nella coordinazione.

I bot più comuni utilizzano alcuni meccanismi di discovery per unirsi ad una botnet: si contattano indirizzi IP randomici, quando si contatta un bot risponderà con il comando giusto da eseguire.

Componenti principali:

1. bot master: è l'iniziatore. Controlla la botnet tramite: IRC, ssh, telnet, pagine web, twitter, Fast Flux
2. Macchine zombies: macchine compromesse; la maggiorparte di esse non è a conoscenza del fatto che vengono utilizzate in questo modo.
   Il fatto che si usino le risorse di queste macchine si dice "scrumping".

Detection di botnets:
Da un punto di vista di sistema bisogna accorgersi del sw malevolo (e.g. antivirus).
Dal punto di vista delle rete ci si deve accorgere di attività inusuali (e.g. sistemi di monitoraggio delle intrusioni).

Fast Flux botnets:
Single fast flux→ il client infettato da mw deve contattare il server C&C. Un host infetto contatta gli agenti FF tramite risoluzione di un nome di dominio fissato. L'attaccante usa DNS per cambiare rapidamente gli indirizzi IP degli agenti da contattare. Non si vogliono mostrare gli indirizzi IP del sw C&C, quindi gli agenti FF si comportano come proxy, poi sono loro a contattare il server C&C.
Il problema sono i nameserver autoritativi per FF, che sono fissi e possono essere chiusi dalle autorità.

Double fast flux→ cambia anche il NS autoritativo. Il client infetto manda una richiesta al TLD, che risponderà con l'IP del NS autoritativo e farà da proxy per l'inoltro della query; in questo modo anche l'indirizzo del NS autoritativo cambia rapidamente.
Problema: il domain name per i domini FF è ancora fisso.

Questo problema ci porta a parlare di **algoritmi per la generazione di un dominio.**
Gli host infetti e i server C&C generano randomicamente i nomi dei domini. A partire dallo stesso seme si avrà la stessa sequenza, quindi il client inizia a generare nomi finché non riceve una risposta.

Sistemi di rilevamento delle intrusioni:
Sono funzioni HW o SW che analizzano le infromazioni da dicversi utenti per identificare le intrusioni.
Si possono avere:

1. Host-based IDS
2. Network-based IDS→ hanno sensori nella rete
3. IDS ibridi

Sono leggermente diversi dai firewall, vanno più a fondo nei pacchetti e usano tecniche più avanzate.

Due approcci:

1. Anomaly detection: statistiche basate sulla raccolta di dati relativi al comportamento di utenti legittimi, “knoledge based”, che usano sistemi esperti che identificano comportamenti legittimi e approcci di ML.
2. Signature/heuristic detection: le signatures si basano su una serie di pattern, che si cercano nei pacchetti per bloccarli.Ciò può essere applicato anche al traffico cifrato; le euristiche invece sono una serie di regole che vengono definite per identificare comportamenti sospetti.

Honeypots:
Per venire a conoscenza di possibili attacchi.
Sono sistemi fatti a posta per attirare attacchi.
Non hanno indirizzi IP, non ci sono informazioni sensibili. Si registra il traffico e si ottengono informazioni riguardo i tipi di attacchi, in modo da poter poi prevenire questi tipi di attacchi.
Si usano particolarmente nel campo della ricerca.

Snort:
Snort è il principale Sistema di Prevenzione delle Intrusioni (IPS) Open Source al mondo.
Utilizza una serie di regole che aiutano a definire attività di rete dannose e utilizza tali regole per trovare pacchetti che corrispondono ad esse e genera allarmi per gli utenti.
Può essere implementato anche “inline” per bloccare questo tipo di pacchetti.
Tre utilizzi principali:
❏ come sniffer di pacchetti come tcpdump
❏ come logger di pacchetti, utile per il debug del traffico di rete
❏ oppure può essere utilizzato come un sistema completo di prevenzione delle intrusioni di rete.

Le regole degli IPS possono essere create in base a euristiche, ma solitamente si scarica un set di regole predefinite, che vengono aggiornate in base a nuovi attacchi scoperti.