Studio delle Botnet per mezzo di IDS

Presentazione di tesi di Laurea

Manuel Luzietti

Università di Bologna

26/05/2023

Introduzione alle Botnet

Definition (Botnet)

Rete di host compromessi chiamati bot, che eseguono istruzioni impartite da host detto botmaster, attraverso l'ausilio di un server che funge da tramite, detto Command And Control Server (C&C).

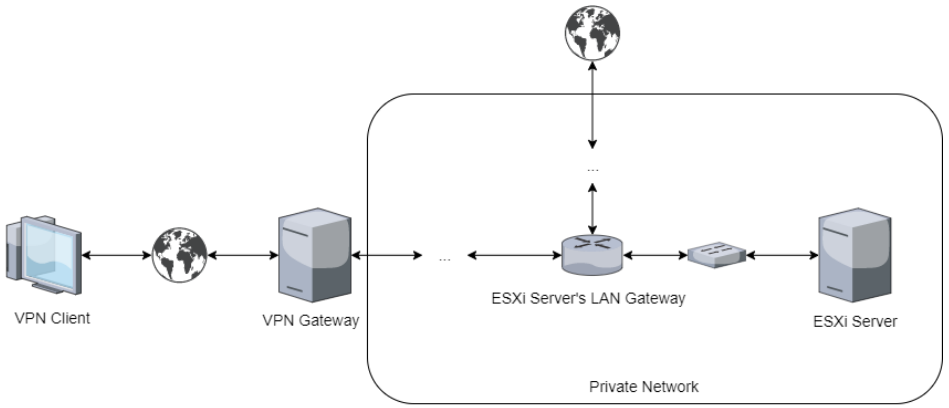
Definita da:

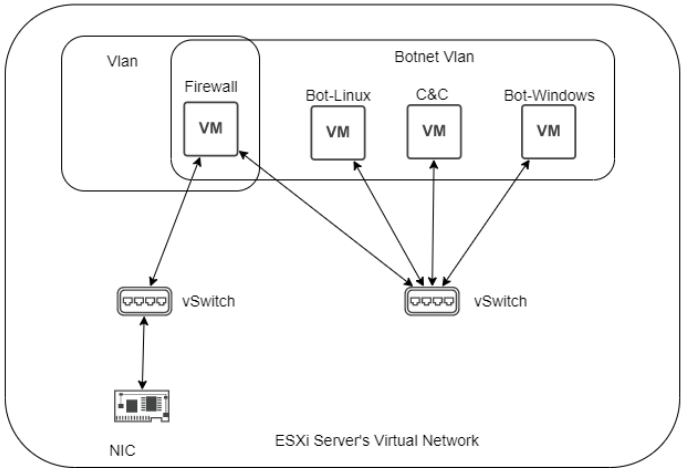
- Topologia
  - Centralizzata
  - Decentralizzata (P2P)
  - Ibrida
- Schema comunicazionale:
  - propagazione
    - ★ attiva
    - ★ passiva
  - operazione
- Protocolli utilizzati
- Tecniche di occultamento/offuscamento

Realizzazione dell'infrastruttura di testing

Principali tecnologie analizzate:

- Server VMWare ESXi
- Firewall
  - Netfilter
  - Iptables
  - NFtables
  - Firewalld
- Docker





Intrusion Detection System (IDS)

Categorizzabili in:

- Signature based (SIDS)
- Anomaly based (AIDS)

In particolare sono stati approfonditi ed utilizzati:

- Security Onion
- Ossim

Utilizzati principalmente come NIDS.