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).

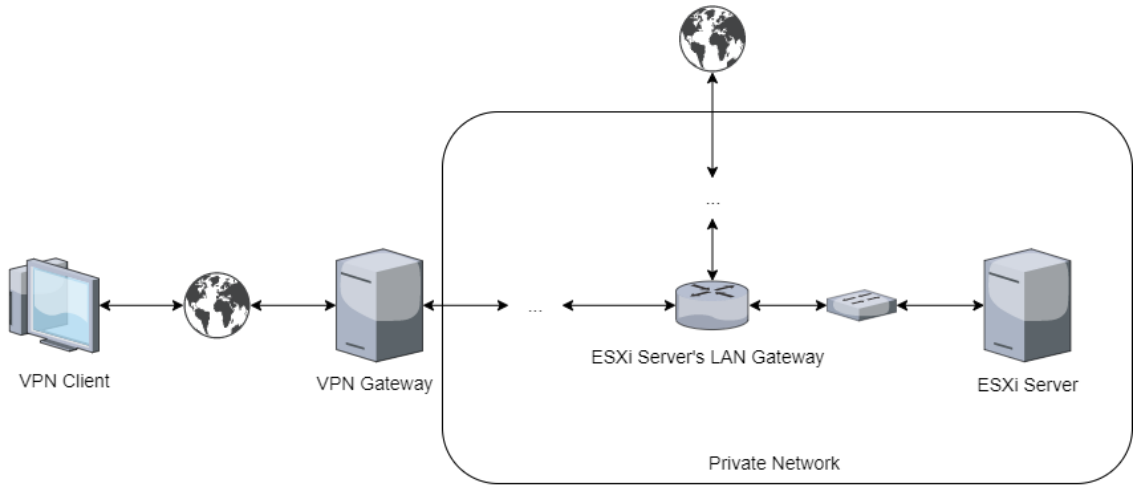
Definita da:

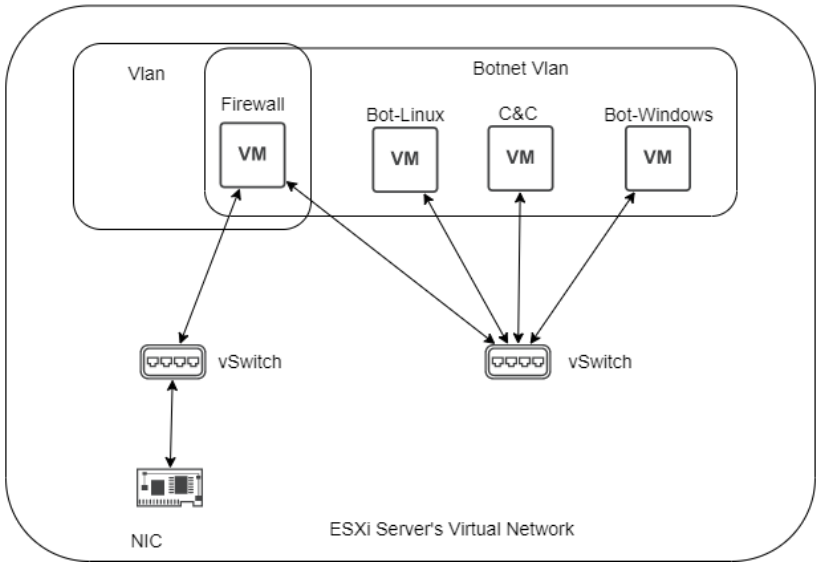
- Schema comunicazionale:
  - propagazione
    - ★ attiva
    - ★ passiva
  - operazione
- Topologia
  - Centralizzata
  - Decentralizzata (P2P)
  - Ibrida
- Tecniche di occultamento/offuscamento
  - Crittografia
  - Fast-flux network
  - Protocol Encapsulation
  - Stepping stones
  - Rootkit
  - Etc.
- Protocolli utilizzati
  - HTTP, IRC, SMTP, etc.

Realizzazione dell'infrastruttura di testing

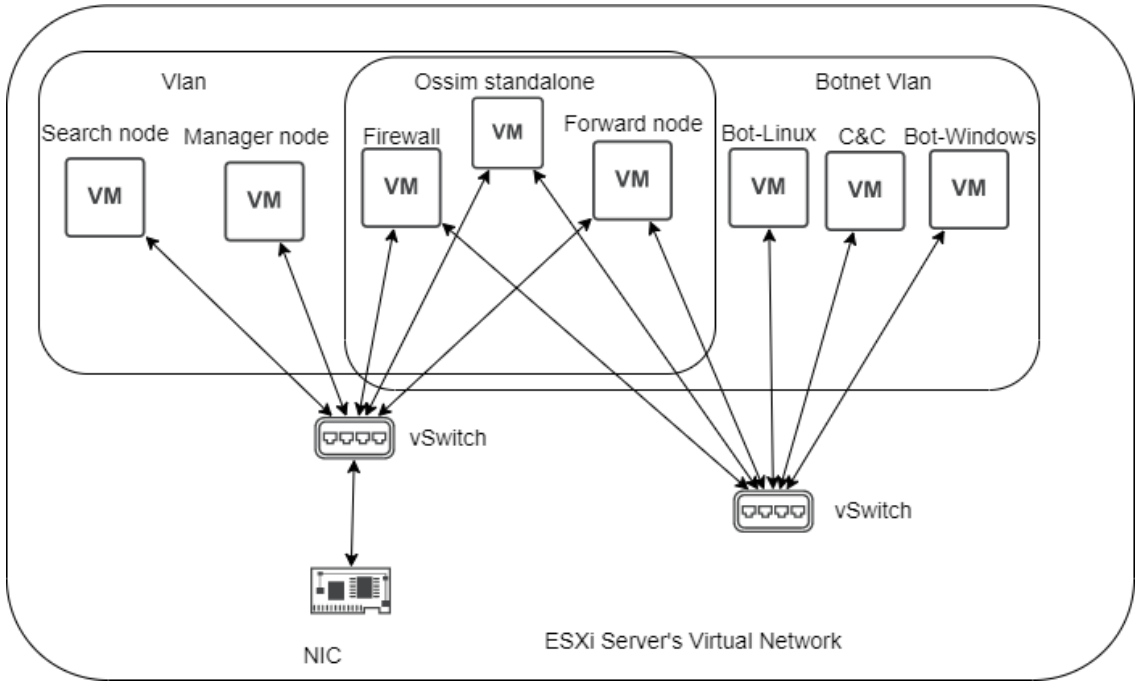
Tecnologie analizzate:

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





Intrusion Detection System (IDS)



Categorizzabili in:

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

oppure in:

- Network based (NIDS)
- Host based (HIDS)

Analizzati e utilizzati:

- Security Onion
- Ossim

Dettagli implementativi

Security Onion

- SaltStack
- Docker
- ElasticStack
- Vasta gamma di componenti software utilizzabili o integrabili per l'analisi di traffico di rete e di host.

Ossim

- Vulnerability assessment attraverso scansioni
- Intrusion detection attaverso tool NIDS, HIDS, e File Integrity Monitoring
- Behavioral Monitoring e capacità di availability monitoring
- Integrazione con OTX

Security Onion installato con architettura distribuita mentre Ossim installato in standalone.

Studio della prima botnet - Byob

Caratteristiche:

- Topologia Centralizzata
- Push based
- Propagazione passiva
- Scitto in Python
- Diversi post exploitation module
- Zero dipendenze
- Multi-stage infection

Rilevazioni con NIDS:

- Download di Stager e Payload
- Download di eseguibile generico
- Download di Miner (malware)
- Rilevazioni minori

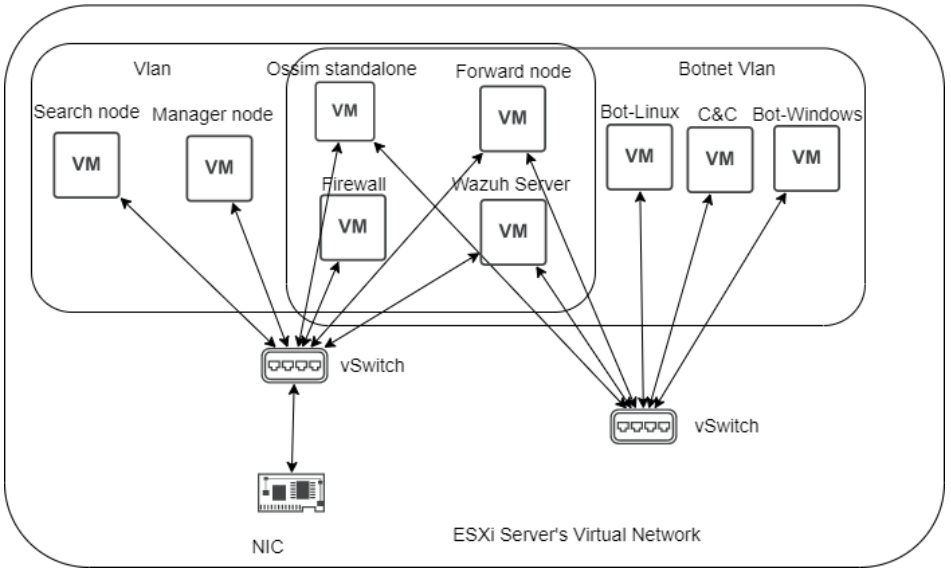
Non rilevati:

- Moduli Python ad-hoc
- Comandi della reverse shell (crittografati con AES)

Agent-based HIDS: Wazuh

Capacità:

- Intrusion detection
- Analisi dei log
- File integrity monitoring
- Vulnerability detection
- Configuration assessment
- Incident response



Installato in standalone con Docker e integrato con Sysmon.

Studio della seconda botnet - Uboat

Caratteristiche:

- Topologia centralizzata con possibilità di C&C di fall-back
- Pull based
- Scritto in C++
- Propagazione passiva
- Zero dipendenze
- Diverse capacità operazionali

Rilevazioni con NIDS:

- Possibilità di identificazione seppur mitigabile con comunicazioni crittografate, fast-flux network, etc.

Rilevazioni con HIDS:

- Identificazione di tutte le attività della botnet attraverso fingerprint appositamente create.

Altri approcci SIDS analizzati

- Yara rules
- Integrazioni con virus engine
- API hooking

Realizzazione di prototipo basilare con l'intento di monitorare pattern di API call:

- DLL injection
- API hooking
- Generazione evento (Windows Event Log System)
- Collezione evento via agent
- Ulteriori analisi

Conclusioni

Analisi approccio signature based a seguito dei test:

Pro:

- Molto efficiente nel rilevare minacce note

Contro:

- Incapace di rilevare minacce Zero Day
- Tipicamente rumoroso
- Versioning del malware e teniche di detection evasion possono rendere inefficace l'approccio

Estensioni:

- Approcci behavior based
- Automazione del deploy dell'infrastruttura

Grazie per l'attenzione