Report di Valutazione e Utilizzo di TekDefense-Automater

Parte 1: Livelli del Sistema di Valutazione di ThreatConnect

Nel contesto della valutazione delle minacce informatiche, ThreatConnect utilizza un sistema di classificazione basato su sei livelli. Questi livelli aiutano a determinare la gravità e l'affidabilità delle informazioni riguardanti le minacce. Di seguito viene fornita una descrizione dettagliata di ciascun livello:

1. **Confermata (90-100)**
    - **Caratteristiche**: L'informazione è confermata da diverse fonti indipendenti e la minaccia è considerata reale e attuale.
    - **Esempio**: Un attacco di phishing confermato da vari report di sicurezza e analisi forensi, indicando una minaccia concreta e attiva.
2. **Probabile (70-89)**
    - **Caratteristiche**: La minaccia non è completamente confermata, ma ci sono numerosi indizi che suggeriscono una forte probabilità che sia reale.
    - **Esempio**: Rilevazione di attività sospette su più sistemi che suggeriscono un possibile attacco, ma senza prove definitive.
3. **Possibile (50-69)**
    - **Caratteristiche**: Alcune informazioni suggeriscono la possibilità di una minaccia, ma mancano ancora prove concrete per confermarla.
    - **Esempio**: Segnalazioni di comportamenti anomali che potrebbero indicare una vulnerabilità, ma senza evidenze sufficienti per una conferma.
4. **Incerta (30-49)**
    - **Caratteristiche**: La valutazione delle informazioni è possibile, ma sono necessarie ulteriori prove per identificare la minaccia.
    - **Esempio**: Log di sistema che mostrano comportamenti inconsueti, richiedendo ulteriori analisi per determinare la natura della minaccia.
5. **Improbabile (2-29)**
    - **Caratteristiche**: La valutazione delle informazioni è possibile, ma la minaccia è considerata poco probabile a causa di dati discordanti.
    - **Esempio**: Alert generati da falsi positivi noti, che non rappresentano una minaccia reale.
6. **Screditata (1)**
    - **Caratteristiche**: La valutazione ha confermato che la minaccia non è reale.
    - **Esempio**: Indicazioni di minaccia basate su dati errati o interpretazioni sbagliate, successivamente smentite.

Parte 2: Installazione e Utilizzo di TekDefense-Automater su Kali Linux

Per l'analisi del target www.epicode.com, ho utilizzato TekDefense-Automater, uno strumento di raccolta automatizzata di informazioni. Di seguito sono riportati i passaggi dettagliati per l'installazione e l'utilizzo del software su una macchina virtuale Kali Linux.

Preparazione dell'Ambiente

1. **Configurazione di Kali Linux**
    - Mi assicuro che Kali Linux sia installato e connesso a Internet.
    - Utilizzo una macchina virtuale per un ambiente di test sicuro.

Scaricare e Installare TekDefense-Automater

1. **Scarico il software**
    - Clono il repository di TekDefense-Automater dal terminale:

git clone https://github.com/1aN0rmus/TekDefense-Automater.git

2. **Installo le dipendenze**
    - Navigo nella directory del progetto:

cd TekDefense-Automater

    - Mi assicuro di avere Python 2.7 installato (Automater richiede Python 2.7):

sudo apt-get update

sudo apt-get install python2.7

Eseguire TekDefense-Automater

1. **Eseguo il software con il target specificato**
    - Eseguo Automater per analizzare il sito web della scuola di cybersecurity (www.epicode.com):

python2.7 Automater.py www.epicode.com

2. **Esempio di comandi per specificare fonti diverse**
    - Posso specificare le fonti di informazioni che voglio utilizzare:

python2.7 Automater.py -s alienvault,cymon www.epicode.com

3. **Ottenere aiuto e vedere tutte le opzioni**
    - Per visualizzare tutte le opzioni disponibili e ottenere ulteriori dettagli sui comandi:

python2.7 Automater.py -h

Output e Analisi dei Risultati

L'output del comando ha mostrato una serie di informazioni raccolte dal sito target, inclusi:

- Registrazioni DNS
- Informazioni WHOIS
- Dati relativi a malware associati
- Dettagli delle minacce conosciute

Ecco un esempio dei risultati ottenuti dall'analisi di www.epicode.com:

_____ Results found for: www.epicode.com _____

No results found in the FNet URL

No results found in the Un Redirect

[+] IP from URLVoid: No results found

[+] Blacklist from URLVoid: No results found

[+] Domain Age from URLVoid: No results found

[+] Geo Coordinates from URLVoid: No results found

[+] Country from URLVoid: No results found

[+] pDNS data from VirusTotal: No results found

[+] pDNS malicious URLs from VirusTotal: No results found

[+] Malc0de Date: No results found

[+] Malc0de IP: No results found

[+] Malc0de Country: No results found

[+] Malc0de ASN: No results found

[+] Malc0de ASN Name: No results found

[+] Malc0de MD5: No results found

No results found in the THIP

[+] McAfee Web Risk: No results found

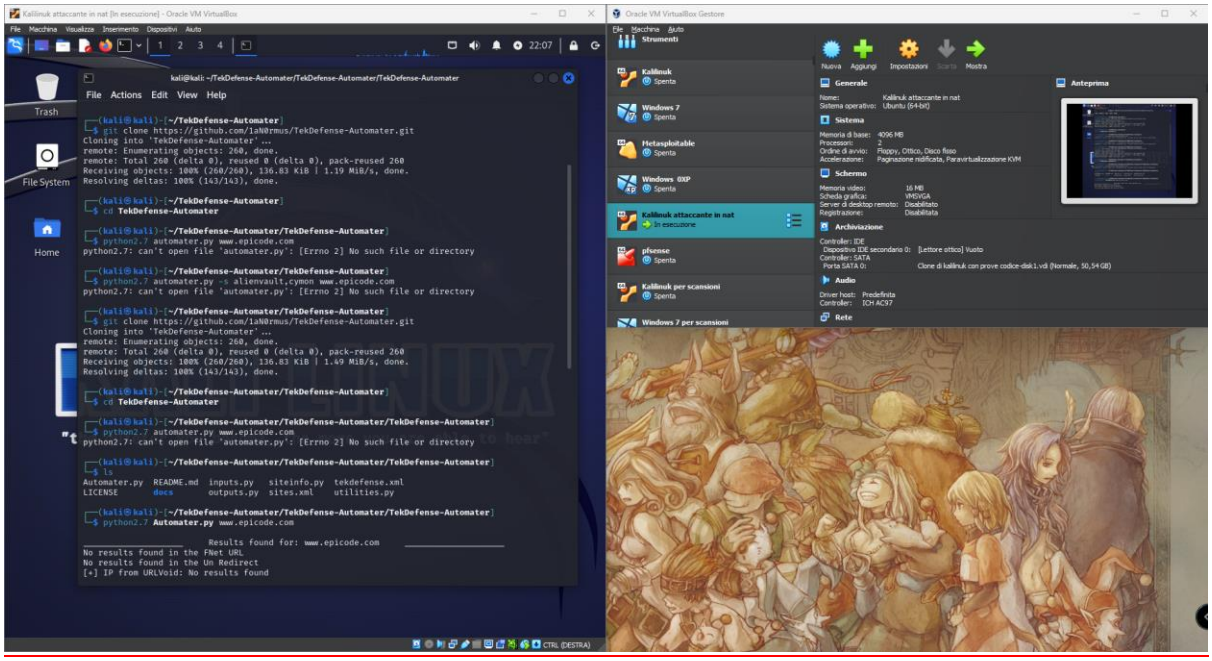
[+] McAfee Web Category: No results found

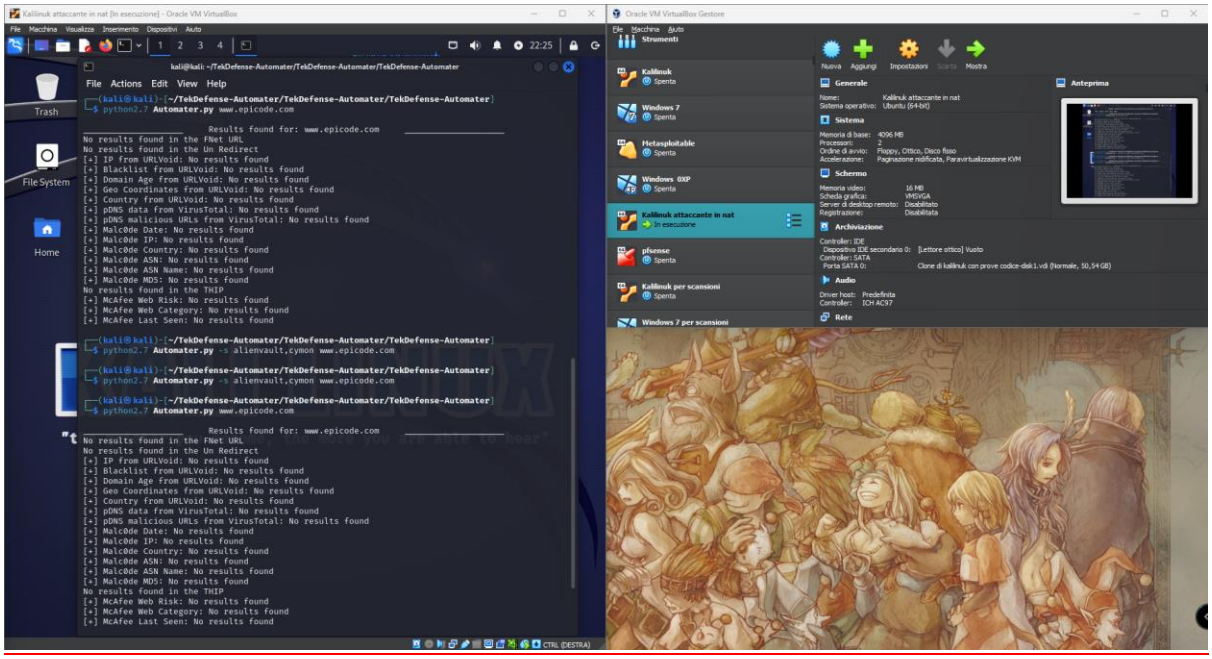
[+] McAfee Last Seen: No results found

Conclusioni

L'analisi eseguita con TekDefense-Automater su www.epicode.com non ha rilevato risultati significativi dalle fonti utilizzate. Questo potrebbe indicare che il sito non è presente nelle liste nere o nei database di minacce pubbliche consultate da Automater. Tuttavia, è sempre consigliabile utilizzare più strumenti di analisi per una valutazione più completa.

Screenshot


Kalilinuk attaccante in nat [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~/TekDefense-Automater/TekDefense-Automater/TekDefense-Automater
File Actions Edit View Help
Trash
File System
Home
Oracle VM VirtualBox Gestore
Strumenti
Kalilinuk
Windows 7
Metasploitable
Windows 8XP
Kalilinuk attaccante in nat
In esecuzione
pfsense
Kalilinuk per scansioni
Windows 7 per scansioni
Nuova
Aggiungi
Impostazioni
Scarta
Mostra
Generale
Anteprima
Sistema
Schermo
Archiviazione
Audio
Rete


Kalilinuk attaccante in nat [In esecuzione] - Oracle VM VirtualBox
File Macchina Visualizza Inserimento Dispositivi Aiuto
kali@kali: ~/TekDefense-Automater/TekDefense-Automater/TekDefense-Automater
File Actions Edit View Help
Trash
File System
Home
Oracle VM VirtualBox Gestore
Strumenti
Kalilinuk
Windows 7
Metasploitable
Windows 8XP
Kalilinuk attaccante in nat
In esecuzione
pfsense
Kalilinuk per scansioni
Windows 7 per scansioni
Nuova
Aggiungi
Impostazioni
Scarta
Mostra
Generale
Anteprima
Sistema
Schermo
Archiviazione
Audio
Rete