Politecnico di Torino

Laurea Magistrale in **Ingegneria Informatica**

Tassonomia dei comportamenti degli attaccanti nelle sfide di Capture The Flag (CTF): un approccio di categorizzazione attraverso l'analisi dei writeup

Relatore
Prof. Cataldo BASILE

Candidato
Francesco LONARDO

Le competizioni di Capture The Flag (CTF) rappresentano un terreno fertile per lo sviluppo e la valutazione delle competenze nel campo della sicurezza informatica. In un'era dove le minacce informatiche sono in costante evoluzione, comprendere il pensiero e le strategie degli attaccanti diventa cruciale.

Obiettivi della Tesi

- **Identificazione e Categorizzazione.** Creare un framework strutturato per identificare e classificare i comportamenti degli attaccanti nelle CTF, superando i limiti dei contesti individuali delle competizioni e prospettando applicazioni teoriche in scenari reali.
- **Contributo Educativo.** Fornire uno strumento didattico per la formazione dei futuri esperti di sicurezza informatica, facilitando la comprensione delle tattiche offensive attraverso l'analisi dei comportamenti nelle competizioni simulate.
- **Innovazione Metodologica.** Impiegare tecnologie avanzate come i modelli di intelligenza artificiale, in particolare GPT di OpenAI, per l'analisi dettagliata dei dati testuali. Questo approccio apre nuove frontiere nella metodologia di ricerca potenziando la capacità di analizzare e interpretare grandi volumi di dati.
- **Supporto alla Ricerca.** Porsi come punto di partenza per un progetto di ricerca più esteso che esplori l'utilizzo dei writeup delle CTF come dati di ricerca, un campo attualmente inesplorato.

Area di Ricerca

La presente ricerca si colloca all'intersezione di vari ambiti cruciali del campo della sicurezza informatica.

- **Competizioni Capture The Flag (CTF).** La ricerca esplora l'importanza educativa delle competizioni CTF come strumenti formativi innovativi per preparare professionisti nel campo della sicurezza informatica.
- **Sicurezza delle Applicazioni Web.** La ricerca si focalizza sui writeup di CTF relativi alla sicurezza delle applicazioni web, analizzando i metodi e le tecniche utilizzate dagli attaccanti per sfruttare le vulnerabilità comuni.
- **Analisi Comportamentale nella Sicurezza Informatica.** La ricerca indaga le tecniche e i comportamenti degli attaccanti nelle CTF, con un'analisi che mira a comprendere le loro metodologie e approcci.
- **Tassonomie nella Sicurezza Informatica.** Si esplora l'utilizzo delle tassonomie per categorizzare comportamenti e attacchi nelle competizioni CTF, con un riferimento a framework come MITRE ATT&CK e D3FEND.
- **Natural Language Processing (NLP).** Si esaminano le applicazioni dei modelli avanzati, come GPT di OpenAI, per una dettagliata interpretazione dei writeup CTF.

Contributi

- **Elaborazione e Normalizzazione dei Writeup CTF.** Utilizzo di GPT per elaborare i writeup CTF, trasformando dati grezzi in informazioni strutturate e analizzabili. Sviluppo di un processo di estrazione e filtraggio del testo utile dai writeup, concentrando l'analisi sulle parti più informative e tecnicamente pertinenti, per facilitare la categorizzazione delle azioni degli attaccanti.
- **Sviluppo di una Tassonomia Dettagliata.** Creazione di una tassonomia basata sui comportamenti osservati nei writeup, che permette un'analisi dettagliata e comprensiva delle strategie degli attaccanti. Utilizzo di approcci semi-automatizzati e supervisionati per la categorizzazione, combinando l'IA con il controllo umano per garantire precisione e rilevanza.
- **Etichettatura e Verifica dei Dati.** Implementazione di un sistema di etichettatura multi-livello per i substep dei writeup, combinando l'uso di GPT con la revisione manuale per la validazione delle etichette, garantendo la pertinenza e l'affidabilità dei dati categorizzati.

Risultati

- **Tassonomia delle Azioni degli Attaccanti.** La creazione di una tassonomia strutturata per classificare le azioni degli attaccanti è stata un risultato chiave. Questa tassonomia ha facilitato la categorizzazione sistematica delle diverse tecniche usate nelle sfide CTF, offrendo un quadro per analizzare e comprendere meglio le loro tattiche e strategie.
- **Contributo alla Formazione in Sicurezza Informatica.** I risultati di questa ricerca hanno notevoli implicazioni educative. La tassonomia e l'analisi degli attaccanti possono essere utilizzate come strumenti didattici efficaci, migliorando la formazione dei professionisti della sicurezza informatica.
- **Innovazione Metodologica.** L'uso dei modelli di intelligenza artificiale GPT-3.5 e GPT-4 per l'analisi dei dati ha mostrato l'efficacia di tali strumenti nell'elaborazione e interpretazione di grandi volumi di dati testuali in ambito di sicurezza informatica.

I risultati di questa tesi aprono la strada a future ricerche e applicazioni nel campo della sicurezza informatica.

Sviluppi Futuri

Progetti futuri potrebbero coinvolgere collaborazioni tra specialisti di sicurezza informatica e sviluppatori di intelligenza artificiale per approfondire la ricerca con nuovi metodi:

- **Analisi del Comportamento degli Attaccanti.** Future analisi potrebbero esplorare l'ordine temporale e le transizioni tra categorie di azioni degli attaccanti, fornendo una comprensione più ricca delle loro strategie e tattiche. L'uso di tecniche come catene di Markov e sequence mining potrebbe rivelare pattern ricorrenti, offrendo nuovi spunti per anticipare le mosse degli attaccanti.
- **Rilevamento di Pattern Comportamentali.** L'impiego di tecniche avanzate come machine learning e deep learning potrebbe trasformare l'analisi dei dati da semplici osservazioni ad intuizioni più profonde sui comportamenti degli attaccanti. Network analysis e data mining potrebbero essere utilizzati per visualizzare relazioni complesse e estrarre tendenze emergenti.

L'ambizione è quella di superare i confini dell'attuale lavoro, aprendo la strada ad indagini che possano utilizzare l'insieme di dati raccolti per decifrare i modelli comportamentali degli attaccanti. Questo percorso di ricerca non solo approfondirebbe la comprensione delle dinamiche attuali, ma potrebbe anche anticipare e prepararsi a sfide future nel campo della sicurezza informatica.