ExploitFarm Project

Analisi di progetto e documentazione

Domingo Dirutigliano

Politecnico di Bari
Software Engineering

Contents

1 Introduzione **2**
- 1.1 Descrizione generale . . . 2
- 1.2 Obiettivi . . . 2
- 1.3 Perchè lo sviluppo di un nuovo attacker/submitter? . . . 2

2 Specifiche **3**
- 2.1 Composizione del progetto . . . 3
  - 2.1.1 Backend . . . 3
  - 2.1.2 Frontend . . . 4
  - 2.1.3 CLI (xfarm) . . . 4
- 2.2 Specifica dei requisiti . . . 4
  - 2.2.1 Setup . . . 4
  - 2.2.2 Gestione Exploit . . . 5
  - 2.2.3 Esecuzione Attacchi . . . 5
  - 2.2.4 Analisi statistiche e visualizzazione . . . 5
  - 2.2.5 Gestione di attacchi distribuiti . . . 5
- 2.3 Specifiche Tecniche . . . 5
  - 2.3.1 Gestione funzionalità backend . . . 5
  - 2.3.2 Funzionalità frontend . . . 5
  - 2.3.3 Strutturazione del client (xfarm) . . . 5
  - 2.3.4 Autobilanciamento del carico sul client per l'esecuzione degli attacchi . . . 5
  - 2.3.5 Gestione e versioning degli exploit . . . 5
  - 2.3.6 Controllo distribuito degli attacchi condivisi . . . 5

3 Modello di Business **5**

4 Analisi SWOT **5**

5 Sviluppi Futuri **5**

1 Introduzione

1.1 Descrizione generale

"Exploitfarm" è un software completamente dedicato alle competizioni CTF Attack/Defence, che si occupa principalmente di gestire la fase di attacco e ti tutto quello che conseguentemente questa fase richiede per essere eseguita correttamente, al fine di semplificare e velocizzare gli attacchi.
In generale Exploitfarm si occupa di attaccare in parallelo una serie di team (attacker) e di raccogliere ed inviare seguendo i criteri e limitazioni indicate per la competizione che si sta svolgendo le flag al gameserver (submitter).

1.2 Obiettivi

- Setup e installazione facile, veloce, personalizzabile e facilmente automizzabile
- Gestione delle risorse per gli attacchi dinamica e reattiva
- Scrittura degli exploit e dei test su questi semplificata
- Interfaccia intuitiva con avvio e configurazione intuitiva e rapida
- Keep track of anything: accumula dati sugli attacchi e ne permette un'analisi veloce ed intuitiva
- Rende semplice la condivisione/collaborazione sugli attacchi e la loro esecuzione
- Leggero da eseguire su qualsiasi piattaforma
- Gestione distribuita degli attacchi

1.3 Perchè lo sviluppo di un nuovo attacker/submitter?

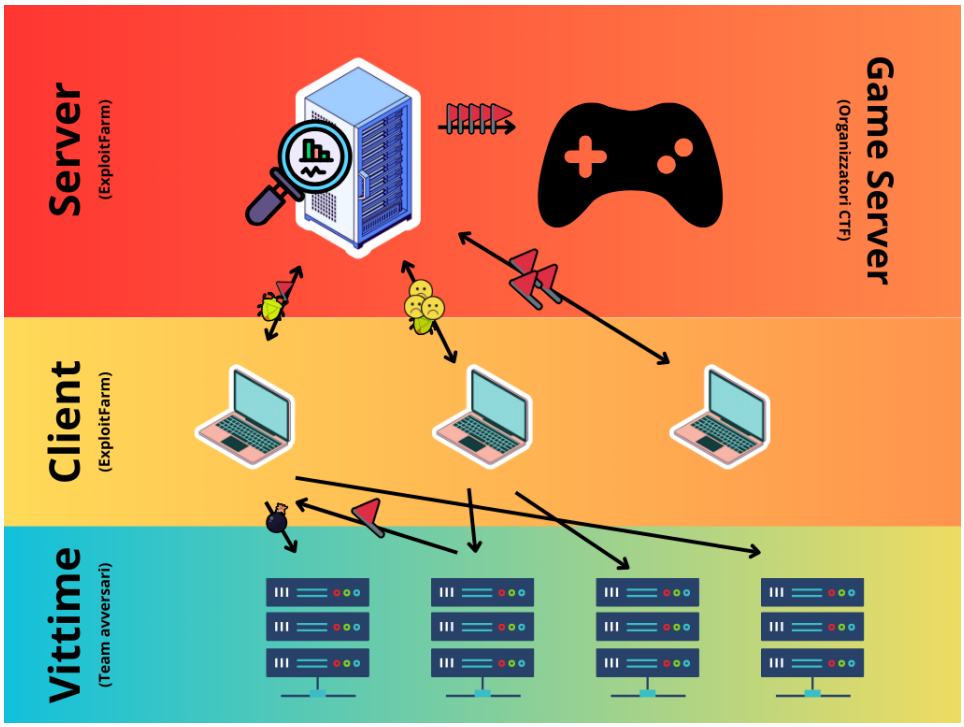
Gli attacker attualmente esistenti sono spesso incompleti, difficili da configurare e da completarne il setup, facilmente inclini ad errori che spesso comportano una perdita di tempo aggiuntiva, non hanno alcun tipo di gestione del carico supportato dalla macchina che esegue gli attacchi, non memorizza o espone alcun dato statistico sull'andamento degli attacchi ed infine non gestisce la condivisione degli exploit stessi.
Date le forti lacune presenti in software simili già esistenti, ho ritenuto opportuno la creazione di un'alternativa agli attacker attualmente esistenti.

NOTA: "ExploitFarm" è liberamente ispirato ad un altro attacker molto famoso chiamato DestructiveFarm, ma ne condivide a livello di codice unicamente delle piccole porzioni del suo client "start_xploit.py" a loro volta modificate ed adattate, in alcune parti riscritte e riprogettate completamente date le netti differenze di requisiti dei progetti.

2 Specifiche

2.1 Composizione del progetto

Il progetto è composto principalmente da un server centrale (nello specifico un web server) che coordinerà una serie di client sia frontend (web) che tramite una CLI. La parte di coordinamento, di submitting e gestione dei dati è affidata al server.



2.1.1 Backend

Il backend sarà il core del progetto poiché conterrà tutta la logica per il coordinamento dei vari client che invieranno il risultato degli attacchi, dovrà

gestire i dati ed elaborarli al fine di renderli facilmente fruibili dai client, inoltre conterrà la logica e si occuperà della gestione del submitting delle flag al gameserver seguendo i requisiti indicati in fase di setup.

2.1.2 Frontend

La visualizzazione avanzata dello stato di ExploitFarm è invece affidata alla parte frontend del webserver che dovrà permettere un facile accesso ai dati presenti sul server, offrendoli tramite strumenti di analisi come grafici che devono essere mirati sulle esigenze decisionali che possono emergere durante una competizione Attack Defence. Inoltre dovrà segnalare e rendere facilmente e tempestivamente nota la presenza di eventuali errori di qualsiasi tipo sull'intera infrastruttura permettendone un'intervento quanto più immediato da parte del team.

2.1.3 CLI (xfarm)

Infine un'ultima parte fondamentale in tutto il progetto è il client che deve essere eseguito preferibilmente su macchine diverse da quella che offre il server, che si occupa dell'esecuzione stessa degli attacchi, della creazione del progetto dell'attacco, del monitoraggio (parziale) dell'attacco stesso. Anche il client stesso dovrà avere un'interfaccia in questo caso TUI intuitiva e veloce da utilizzare che deve rendere immediato e facile l'avvio dell'attacco e l'inserimento dei dati richiesti per l'esecuzione dell'attacco stesso.

2.2 Specifica dei requisiti

2.2.1 Setup

Il setup di ExploitFarm dalla sua installazione alla conclusione della sua configurazione deve essere di facile ed intuitivo utilizzo e di semplice finalizzazione. Al fine di perseguire questo obiettivo[...]

2.2.2 Gestione Exploit

2.2.3 Esecuzione Attacchi

2.2.4 Analisi statistiche e visualizzazione

2.2.5 Gestione di attacchi distribuiti

2.3 Specifiche Tecniche

2.3.1 Gestione funzionalità backend

2.3.2 Funzionalità frontend

2.3.3 Strutturazione del client (xfarm)

2.3.4 Autobilanciamento del carico sul client per l'esecuzione degli attacchi

2.3.5 Gestione e versioning degli exploit

2.3.6 Controllo distribuito degli attacchi condivisi

3 Modello di Business

4 Analisi SWOT

5 Sviluppi Futuri

Server Multipli e Decentralizzati