Piattaforma per esercitazioni sulla sicurezza di sistemi SCADA

User Requirements Document

DIBRIS – Università di Genova. Scuola Politecnica, Corso di Ingegneria del Software 80154

DATA – 23/03/2018

VERSION: 1.1

Autori

Fabio Cassinelli

REVISION HISTORY

Versione	Data	Autori	Note
1.0	14/03/2018	FC	Inizio
1.1	23/03/2018	FC	Revisione

Indice dei Contenuti

1 Introduzione

1.1 Scopo del Documento

Questo documento riguarda il progetto con ID 29 del corso di SE dell'Università di Genova. Lo scopo del documento è di descrivere le funzionalità di una piattaforma dedicata alle esercitazioni sulla sicurezza di sistemi SCADA.

1.2 Ambito Applicativo del Documento

Il documento è utile a chi vuole conoscere il contesto, le motivazioni e i requisiti che dovrà avere il progetto 29 di SE.

1.3 Definizioni e Acronimi

Acronimo-Nome	**Definizione**
FC	Fabio Cassinelli
SE	Software Engineering
CTF	Capture The Flag
RT	Red Team
BT	Blue Team
WT	White Team
IT	Information Technology
OT	Operational Technology

1.4 Bibliografia

1.5 Overview del documento

Il documento è organizzato come segue: la prima parte del documento contiene una breve descrizione del problema che si vuole affrontare e una possibile soluzione; la seconda parte elenca le funzionalità aspettate dal sistema e la loro priorità di implementazione.

2 Descrizione Generale del Sistema

La piattaforma sviluppata consente di simulare attacchi e difese ad impianti di automazione industriale con l'obiettivo di poter valutare la sicurezza dell'infrastruttura simulata. Un "**White Team**" (WT) predispone l'esercitazione, configurando l'impianto e mettendolo a disposizione degli altri due team. La piattaforma simula l'interfaccia che un operatore deve usare per controllare da remoto l'impianto industriale. Gli attacchi vengono effettuati da un "**Red Team**" (RT), mentre le difese sono affidate ad un "**Blue Team**" (BT). Al termine della simulazione il WT raccoglie i risultati dell'esercitazione e, in base a quali attacchi sono andati a buon fine e quali invece hanno fallito, deduce i punti deboli dell'infrastruttura così configurata, in modo tale da identificare in quali parti di essa bisogna andare ad investire per incrementare la sicurezza globale del sistema.

2.1 Contesto e Motivazioni

Gli impianti di automazione industriale, pur nascendo per loro natura isolati dal resto dell'infrastruttura informatica, stanno diventando sempre più esposti ad attacchi informatici che ne vanno minare il corretto funzionamento. Questo accade perché in ambito industriale vi è una sempre maggiore esigenza di **remotizzare** la supervisione e il controllo degli impianti, affidando così delicate operazioni di gestione dei comandi alla rete, e quindi spesso a canali di comunicazione vulnerabili o facilmente attaccabili. Per testare la reale sicurezza degli impianti e della relativa infrastruttura informatica che sta loro attorno, si è pensato di applicare ed estendere lo stesso paradigma che si usa in ambito IT, ovvero quello delle **esercitazioni**. Esistono infatti delle piattaforme che già forniscono la possibilità di svolgere delle CTF in un contesto IT, in cui un RT svolge il ruolo degli hacker e tenta degli attacchi informatici alla piattaforma, che può simulare ad esempio un **server** che fornisce dei servizi. Nel contempo un BT cerca di sventare tali attacchi del RT con le difese che ha a disposizione, mentre un WT predispone l'esercitazione, ne osserva lo svolgimento e al termine di esso deduce i punti deboli del sistema, in modo tale da capire dove esso è più vulnerabile.

2.2 Obiettivo del progetto

Il progetto si propone di estendere una piattaforma esistente per la costruzione di esercitazioni per la cyber-security in ambito IT **(Information Technology**) ad un ambito ibrido IT/OT (**Operational Technology**). Agli utenti del sistema è fornito un accesso alla piattaforma attraverso cui potranno esercitarsi a compiere attacchi a sistemi SCADA simulati o a difendere questi sistemi da tali attacchi. La piattaforma non simula quindi un server che mette a disposizione dei servizi, ma l'interfaccia che un operatore deve usare per controllare da remoto un impianto industriale, come ad esempio un **depuratore**, di cui è possibile gestire tramite la rete i setpoint e i parametri di sistema. Queste esercitazioni servono agli utenti per acquisire le conoscenze necessarie a permettere loro di proteggere meglio le infrastrutture critiche su cui operano.

2.3 Utenti

Gli utenti del sistema sono 3: il White Team, il Red Team e il Blue Team, ovvero 3 gruppi di persone con obiettivi diversi. Il White-Team si occupa di predisporre l'esercitazione e di mostrare agli altri utenti quali impianti sono presenti nella simulazione e come essi siano collegati fra di loro. Al termine dell'esercitazione ha anche il compito di fare un bilancio per determinare i punti deboli dell'impianto e della sua infrastruttura informatica. Il Red Team riveste il ruolo degli hacker, ovvero svolge una Capture The Flag, cercando di 'bucare' il sistema con degli attacchi mirati. Essendo in un contesto OT, le conseguenze di un attacco su sistemi critici del genere possono essere anche molto gravi. Il Blue Team invece cerca di impedire al Red Team di portare a termine con successo la Capture The Flag, difendendo il sistema.

3 User Requirement

In questa sezione descriveremo i requisiti della piattaforma per esercitazioni sulla sicurezza di sistemi SCADA. In particolare ad ogni requisito daremo un id unico e una priorità seguendo la seguente tabella:

M Mandatory. Requisito Obbligatorio.

D Desiderable. Requisito che dovrebbe essere inserito nel sistema, a meno che il costo per implementarla non sia troppo alto.

O Optional. Una funzionalità marcata con O può essere inserita nel sistema, a discrezione del manager del progetto. Ad esempio se il tempo di sviluppo è minore di quello previsto oppure se il costo per implementarla non è troppo alto.

E future Enhancement. Questo requisito viene lasciato per la prossima release.

ID	DESCRIZIONE	PRIORITA'
1	Al White Team deve essere permesso di predisporre l'esercitazione e di mostrare agli altri utenti quali impianti sono presenti nella simulazione e come essi siano collegati fra di loro.	M
2	Il sistema deve mettere a disposizione un'interfaccia reale per l'utente "benevolo", cioè l'operatore che opera sugli impianti industriali. Egli deve potersi autenticare e poter controllare l'impianto da remoto, ovvero poter inviare i parametri al sistema attraverso la rete.	M
3	Il sistema deve poter riconoscere quali parametri del sistema simulato provengono dall'esterno, ovvero quali possono essere stati manomessi dal Red Team.	M
4	Il sistema deve essere in grado di fornire la risposta dell'impianto, ovvero come esso reagisce ai controlli inviatigli dall'esterno, sulla base dei parametri che gli arrivano, sia che essi siano mandati da un utente "benevolo", cioè l'operatore autenticato, sia da uno "malevolo", cioè il Red Team.	M
