Safeticc

Mallette expérimentale et kit à intégrer pour un apprentissage concret de la cybersécurité

SAFETICC est un ensemble d'expérimentation de la cybersécurité dont l'élément central est un firewall certifié ANSSI*.
Le concept se décline en deux équipements parfaitement distincts : une mallette expérimentale permettant de simuler un système automatisé soumis à une cyberattaque et doté d'une protection par pare-feu, et une mallette de composants pour le déploiement de la solution de cybersécurité sur divers systèmes du plateau technique.
Les deux solutions intègrent un générateur d'attaques qui assure les scénarios de mise en défaut.

**Agence Nationale de la Sécurité des Systèmes d'Information*

A l'image d'un système réel, la mallette expérimentale *SAFETICC* comprend une section OT *(Operation Technology)* et une section IT *(Information Technology)*.
L'OT présente le cœur d'un système automatisé classique avec API, IHM, balise d'état et switch Ethernet. L'IT concerne la couche numérique d'échange entre l'OT et le monde extérieur. Il intègre le dispositif de cyberattaque et le pare-feu de protection du système.
Tous ces constituants sont accompagnés de câbles réseaux requis pour la communication.
Une partie opérative peut se raccorder à la mallette qui devient alors un véritable système automatisé.
Le kit regroupe le générateur d'attaque et les composants de protection par le pare-feu.

Activités pédagogiques :
- Principes de la cybersécurité,
- Mise en place d'un LAN et raccordements des éléments d'une chaîne d'information numérique,
- Mise en œuvre d'un scénario de cyberattaque,
- Analyse de trames numériques avant et après une attaque,
- Programmation de pare-feu.

Principales filières concernées :
- Systèmes numériques (Bac, BTS et BUT)
- Maintenance industrielle (partie Amélioration d'un bien),

Rév. D – 21 mai 2024

ASTRIANE
1884, avenue Saint Maurice
04100 MANOSQUE
FRANCE
Téléphone : +33 (0)4 92 75 87 80
Fax : +33 (0)4 92 74 08 20
www.didact.fr

Safeticc

Mallette expérimentale et kit à intégrer pour un apprentissage concret de la cybersécurité

Au regard des attaques qui visent tous les champs économiques des sociétés industrielles, la protection des données numériques est devenue un terrain d'amélioration prioritaire dans de nombreuses entreprises.
Le déploiement de "firewalls" s'étend aux ateliers dont les machines restent souvent un maillon faible de la sécurité digitale.
Notre gamme, riche de plusieurs lignes de production, se prête particulièrement bien à l'implantation d'une solution de protection numérique.

Présentation de l'équipement

L'équipement ***SAFETICC*** se décline en 2 solutions :
- une mallette expérimentale destinée à la compréhension d'un dispositif « firewall » industriel, son paramétrage et son fonctionnement,
- un kit qui rassemble tous les éléments techniques requis pour implanter le « firewall » industriel sur les équipements existants de la gamme.

Les deux solutions intègrent un générateur d'attaques qui assure des mises en défaut par DoS (Deny of Service) et provoque la saturation de la communication normale par des requêtes incessantes.
La technique "Man-in-the-Middle" définit une cyberattaque consécutive à une phase d'observation des échanges numériques. Un code défectueux se substitue alors au code sain des programmes des machines.
Ce cas est mis en scène sur des systèmes de notre gamme.

fonctionnelles

SAFETICC intègre une interface permettant d'avoir un menu personnalisé pour chaque application :
Un mode universel, permet la personnalisation des cibles (typiquement Automate / IHM /module E/S) et des variables à perturber.
Des modes « SAVONICC » et « RECYCLICC », avec les automates de la ligne préconfigurés, ainsi que les consignes qui peuvent être perturbées (consignes de température, consigne de coupe, etc)

Systèmes associés

La gamme ASTRIANE offre plusieurs systèmes rendus compatibles avec le scénario de cybersécurité. C'est le cas des lignes de production SAVONICC et RECYCLICC.

Une application plus simple est également proposée. Elle met en œuvre un convoyeur à bande motorisé pour le tri de pièces dont le fonctionnement est mis en péril par la cyberattaque. Cette PO inclut notamment un jeu de capteurs et un variateur de vitesse de la bande transporteuse.

Illustration de la PO 100% électrique convoyeur de tri

Exploitation pédagogique

- Mise en place du LAN : utilisation de Machine Expert, paramétrage de l'IHM et paramétrage des périphériques déportés.
- Analyse de la trame Ethernet avec Wireshark,
- Attaques DoS et effets sur le système automatisé,
- Analyse de trame lors d'une attaque DoS : principe du déni de service,
- Attaque de perturbation ou forçage de sortie : effets sur le système,
- Mise en place du pare-feu et vérification du fonctionnement face aux différents types d'attaque,
- Analyse des trames en amont et en aval du pare-feu lors d'une attaque DoS.
- Application "Man in the middle" (niveau avancé) :
  a) Mode « Espion » avec surveillance des trames échangées entre 2 équipements.
  b) Sortie d'un journal exploitable sur Wireshark pour identifier les trames intéressantes pour une attaque.
  c) Passage de l'application "Man in the middle" en mode "Espion" au mode "Modification" des trames identifiées.
- Paramétrage des règles de pare-feu (niveau avancé).

Caractéristiques générales

Mallette expérimentale :
- Lxlxh = 400x500x300 mm
- Masse : 18 kg
- Energies : 230V - 50Hz
- P consommée = max 500W

Partie opérative :
- Lxlxh = 500x450x135 mm
- Masse : 9 kg
- Energies électrique : 230V-50Hz
- P consommée : 100 W

ASTRIANE
1884, avenue Saint Maurice
04100 MANOSQUE
FRANCE
Téléphone : +33 (0)4 92 75 87 80
Fax : +33 (0)4 92 74 08 20
www.didact.fr