Smart**Cyber**Labs

PIANO SCUOLA 4.0

Laboratorio avanzato di **CyberSecurity**

1. Introduzione a SmartCyberLabs

In un mondo sempre più digitalizzato e connesso, la sicurezza informatica è diventata una priorità assoluta per le organizzazioni e gli individui. La crescente domanda di esperti in cybersecurity richiede un'educazione adeguata e tempestiva per preparare la prossima generazione di professionisti del settore. È in questo contesto che Smart**Cyber**Labs di Globsit per le scuole, un ambiente hi-tech all'avanguardia che mira a fornire agli studenti le competenze e le conoscenze necessarie per affrontare le sfide della sicurezza informatica nel mondo reale.

Il laboratorio è composto da due componenti principali: la componente hardware e la componente software. La componente hardware include router, switch, server e access point, che permettono agli studenti di familiarizzare con le diverse tipologie di apparati di rete e di imparare a configurarli in modo sicuro. Grazie a questa componente, i ragazzi avranno l'opportunità di sperimentare direttamente le tecniche e gli strumenti utilizzati dai professionisti del settore per garantire la protezione delle reti informatiche.

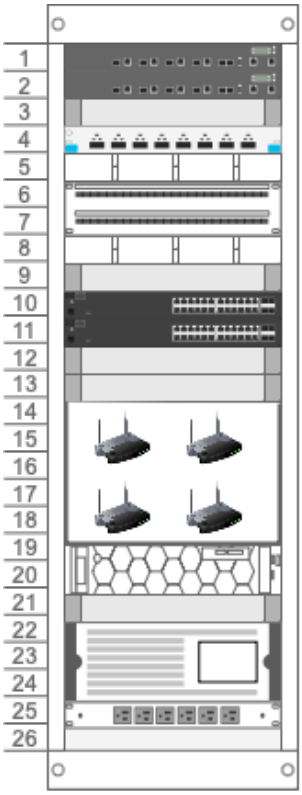
Parallelamente, la componente software del laboratorio offre un sistema di gestione delle immagini di configurazione degli apparati ready-to-go, che consente ai docenti di organizzare lezioni pratiche in scenari realistici e challenge interessanti per gli studenti con pochi click. Questo strumento didattico facilita l'apprendimento degli studenti, permettendo loro di mettere in pratica le teorie apprese in aula e di sviluppare le competenze necessarie per affrontare le minacce informatiche in maniera efficace.

Il focus principale di Smart**Cyber**Labs è, ovviamente, la **cybersecurity** stessa. Gli studenti impareranno a comprendere e identificare le diverse tipologie di attacchi informatici, come prevenirli e come reagire in caso di emergenza. Inoltre, acquisiranno competenze specifiche nel campo della crittografia, dell'autenticazione e delle politiche di sicurezza, elementi fondamentali per garantire la protezione dei dati e delle infrastrutture informatiche.

SmartCyberLabs di Globsit rappresenta per le scuole un'importante opportunità per gli studenti di avvicinarsi al mondo della sicurezza informatica e di acquisire le competenze necessarie per diventare gli esperti del futuro. Grazie all'approccio pratico e all'uso di tecnologie avanzate, i ragazzi potranno imparare in modo efficace e stimolante, preparandosi a intraprendere una carriera di successo nel settore della cybersecurity.

2. Hardware

SmartCyberLabs di Globsit prevede una configurazione flessibile e pronta all'uso, bassata su tecnologia RouterOS di Mikrotik. Gli apparati a brand MikroTik acquistano sempre maggiore popolarità, grazie alla loro estrema flessibilità operativa. Tutto l'hardware è contenuto in un unico armadio rack precablato.



#	Apparato
1	RouterBoard RB5009UG+S+IN SFP+
2	RouterBoard RB5009UG+S+IN SFP+
4	Patch Fibra Ottica
6-7	Patch Rame
10	CloudSwitch Dual Boot CRS328-24P-4S+RM SFP+
11	CloudSwitch Dual Boot CRS328-24P-4S+RM SFP+
14-18	WiFi 6 Area – 4x AccessPoint hAP ax^2
19-20	Configuration Server
22-24	UPS
	*i codici prodotto sono indicativi, e possono essere sostituiti con apparati di pari performance a secondo della disponibilità attualizzata al momento dell'ordine

Il sistema hardware viene fornito pronto all'uso, dotato di cavetteria, patch in rame, patch in fibra e ricetrasmettitori MiniGbic per ogni porta in fibra disponibile sui dispositivi installati.

2. Formazione

Smart**Cyber**Labs di Globsit si pone come obiettivo la formazione pratica degli studenti nell'ambito della sicurezza informatica, attraverso un percorso formativo innovativo strutturato secondo le esigenze del mercato del lavoro contemporaneo. A Smart**Cyber**Labs è associato un percorso di formazione per consentire ai docenti di acquisire le competenze necessarie per utilizzare al meglio l'hardware del laboratorio e i sistemi di autoconfigurazione dei vari scenari disponibili. In questo modo, i docenti saranno in grado di trasmettere ai propri studenti le conoscenze indispensabili per affrontare le sfide del mondo del lavoro nel settore della cybersecurity.

Il corso di formazione proposto si articola in diverse fasi, che prevedono sia una parte teorica che una parte pratica. Durante la parte teorica, verrà fornita una panoramica delle esercitazioni standard disponibili nel laboratorio, fornendo ai docenti gli strumenti necessari per comprendere le diverse tematiche affrontate e per selezionare ed implementare gli esercizi più adatti alle esigenze dei propri studenti.

Successivamente, nella parte pratica del corso, i docenti avranno la possibilità di familiarizzare con l'hardware del laboratorio e con i sistemi di autoconfigurazione dei vari scenari. Questo permetterà loro di padroneggiare le diverse funzionalità offerte dal laboratorio e di saperle utilizzare in maniera efficace e sicura.

Inoltre, il corso prevede anche una formazione specifica **sulla creazione e gestione di nuovi scenari**, in modo che i docenti possano adattare il percorso formativo alle esigenze dei propri studenti e alle specificità del

contesto in cui operano. Grazie a questa formazione, i docenti saranno in grado di progettare e realizzare nuovi esercizi, ampliando così l'offerta formativa del laboratorio e rendendola sempre più ricca e stimolante.

La formazione offerta da SmartCyberLabs è indispensabile per sfruttare al meglio le potenzialità del laboratorio e per trasformarlo in un polo formativo d'eccellenza. Infatti, solo attraverso una formazione adeguata e aggiornata, i docenti potranno trasmettere ai propri studenti le competenze necessarie per inserirsi nel mondo del lavoro in modo competitivo e consapevole. Inoltre, la formazione continua dei docenti è fondamentale per garantire che il laboratorio possa mantenere elevati standard qualitativi e aggiornarsi costantemente alle nuove sfide e alle evoluzioni del mondo della cybersecurity.

La formazione associata a SmartCyberLabs è una risorsa preziosa per le scuole che intendono creare un ambiente innovativo che sia davvero utile al percorso di vita degli studenti, offrendo un'opportunità di crescita professionale e personale.

3. Implementazioni operative

A seguire un elenco non esaustivo degli scenari operativi inclusi con SmartCyberLabs.

NETWORKING CHALLENGES

- 10 GB Fiber Link configuration
- Secure WiFi Mesh configuration
- OpenVPN configuration
- Wireguard VPN configuration
- WiFi centralized management (CAPsMAN)
- WiFi 6 configuration
- WiFi Custom Capture Portal
- IPSec VPN configuration
- RouterOS Hardening configuration
- GNS3 Virtual Networking

- OSPF configuration
- Firewall configuration
- Hardcoded route configuration
- Loop free switching
- Network Automation with Python
- VLAN configuration
- VRRP for Load-Balancing and Failover

CYBERSEC CHALLENGES

- Spot the misconfiguration (100 scenaries)
- Capture the Flag games
- Spot the web vulnerabilities (PHP/MySQL package)
- Spot the web vulnerabilities (JavaScript package)
- PenTest Lab
- Exploit Exercises
- Wargames
- Criptography challenges
- Forensic challenges

4. Sbocchi professionali

Le competenze nel campo del networking e della cybersecurity sono sempre più richieste nel mondo del lavoro, poiché le aziende, le istituzioni e le organizzazioni internazionali stanno investendo ingenti risorse per garantire la sicurezza dei loro sistemi informatici e delle loro reti. Tra i principali sbocchi lavorativi in questi ambiti, possiamo citare:

1. Esperto di sicurezza informatica (Cybersecurity Specialist): figura professionale che si occupa di proteggere i sistemi informatici e le reti aziendali da attacchi informatici e violazioni della sicurezza. Questi professionisti sono in grado di progettare, implementare e monitorare piani di sicurezza informatica, nonché di rispondere a eventuali incidenti di sicurezza.

2. Network Engineer: esperto nella progettazione, installazione, gestione e manutenzione delle infrastrutture di rete aziendali. Questi professionisti sono responsabili della configurazione e dell'ottimizzazione delle reti, garantendo la loro sicurezza e il loro corretto funzionamento.

3. Penetration Tester: figura professionale che si occupa di verificare e valutare la sicurezza delle reti e dei sistemi informatici attraverso test di intrusione e analisi delle vulnerabilità. Il loro obiettivo è individuare eventuali debolezze e proporre soluzioni per migliorare la sicurezza.

4. Security Analyst: professionista che monitora e analizza costantemente la sicurezza delle reti e dei sistemi informatici, rilevando eventuali anomalie e attività sospette. Il loro compito è identificare potenziali minacce e rischi, e collaborare con gli altri esperti per mitigarli.

5. Responsabile della sicurezza delle informazioni (CISO): figura dirigenziale che si occupa di definire e coordinare le strategie di sicurezza informatica a livello aziendale. Il CISO è responsabile dell'implementazione delle politiche e delle procedure di sicurezza e deve garantire la conformità alle normative e agli standard internazionali.

Per prepararsi adeguatamente a questi lavori del futuro, è fondamentale investire nella formazione e nello sviluppo delle competenze tecniche e trasversali. La scuola, in particolare, deve adattarsi all'evoluzione tecnologica e offrire percorsi formativi in grado di fornire ai ragazzi le competenze necessarie per lavorare nel settore del networking e della cybersecurity. Tra le principali aree di formazione, è possibile citare:

- Informatica e programmazione: la conoscenza dei principali linguaggi di programmazione e delle architetture dei sistemi informatici è fondamentale per comprendere il funzionamento delle reti e delle applicazioni.

- **Networking e sistemi operativi:** la padronanza delle principali tecnologie di rete (come TCP/IP, Ethernet, Wi-Fi) e dei sistemi operativi (Windows, Linux, macOS) è essenziale per lavorare nel settore.

- **Sicurezza informatica e cybersecurity:** la formazione specifica in materia di sicurezza informatica e protezione delle reti è indispensabile per acquisire le competenze necessarie per prevenire e contrastare gli attacchi informatici.

- **Legislazione e normative:** la conoscenza delle leggi e delle normative relative alla protezione dei dati e alla sicurezza informatica è fondamentale per operare nel rispetto della legalità e garantire la conformità delle soluzioni adottate.

- **Soft skills:** la capacità di lavorare in team, la comunicazione, la gestione del tempo e la capacità di adattarsi alle novità sono alcune delle competenze trasversali che possono fare la differenza nel mondo del lavoro.