ON-LINE

Intenzívny kurz

IT SECURITY

PRE KOHO JE KURZ URČENÝ

Kurz je určený pre všetkých, ktorí sa zaujímajú o počítačovú bezpečnosť a chceli by sa jej venovať aj profesne ako technici, sysadmini a začínajúci etickí hackeri.
V prvej časti kurzu sa účastníci oboznámia so základnými konštrukčnými prvkami počítačov, ich diagnostikou, monitorovaním a technickými možnosťami v oblasti počítačovej bezpečnosti.
V druhej časti kurzu účastníci získajú poznatky o všetkých základoch počítačových sietí od kabeláže a topografie až po protokoly a ich možnosti a zraniteľnosti. Taktiež sa zamerajú na konfiguráciu routrov a switchov, WiFi sietí s praktickými cvičeniami cez sieť na vzdialenej sieti.
Tretia časť kurzu bude zameraná na zraniteľnosti a možné prístupy k počítačovej bezpečnosti. Účastníci budú monitorovať a chrániť sieť pred útokmi zvonku aj zvnútra. Bude im vysvetlená problematika konfigurácie firewallu, inštalácie pascí na hackerov a klasifikácie incidentov. Pomocou databáz budú hľadať informácie o vírusoch a malware. Užívatelia budú poučení o nástrojoch sociálneho inžinierstva. Účastníci tiež získajú poznatky o hranici súkromia a bezpečnosti.
Posledná časť kurzu bude venovaná zraniteľnostiam IoT zariadení. Účastníci budú skúmať ich možnosti, nastavenia a kriticky pristupovať k ich konštrukcií či využitiu. Vyhodnotí sa riziko prameniace z ich využitia pre bezpečnosť našej siete a možnosti využitia na nekalé účely.

OBSAHOVÉ ZAMERANIE

PC Hardware
BIOS, BOOT konfigurácia a monitoring. Základné komponenty. Ďalšie komponenty. Virtualizácia, VM, RAID. Sieťové karty a káble. Porty a Protokoly. Bezdrôtové pripojenie. Iné pripojenia. Náradie.
Networking a správa
Základy routerov a prepínačov. Základy topológie siete. Prístup do siete. IP konektivita. IP Služby. IPSec, VPN. Konfigurácia routrov a manažovateľných switchov.
IT Security
Najčastejšie hrozby, útoky a zraniteľnosti. Zero Trust Networks. Fyzická bezpečnosť a šifrovanie. Oprávnenia a ochrana EndPointov. Ochrana pred vírusmi a malware. Firewall a nastavenia. Autentifikácia, kľúče a správa hesiel. Sledovanie siete. Honeypoty a Honeynety. Prevádzka a IR Incident Response. SEC IDS a IPS.
IOT Security
Slabé Heslá. Nezabezpečené sieťové služby. Ecosystem zariadení. Nemožnosť Updatu a patchovania. Použitie nevyhovujúceho a nezabezpečeného hardvéru, Nezabezpečené ukladanie a výmena dát.

PREDPOKLADY

Abstraktné myslenie, základy anglického jazyka.

ROZSAH KURZU

40 hodín (1 hodina = 45 minút)
Večerná forma realizácie| 8 x 5 hodín | vyučovacie dni PON – PIA | v čase 17:00 – 21:00

MIESTO REALIZÁCIE

on-line forma v prostredí aplikácie ZOOM v reálnom čase s lektorom z praxe
Účastník musí mať k dispozícii pripojenie na internet a zariadenie, prostredníctvom ktorého sa pripojí.

TERMÍN

podľa požiadavky

NÁŠ PRÍSTUP KU VZDELÁVANIU

- orientácia na potreby klienta, profesionálna príprava pre potreby praxe,
- vzdelávanie realizované lektorom z praxe, intenzívnou dennou formou s využitím moderných on-line vyučovacích metód, s akcentom na osobný prístup lektora,
- každý účastník získa bezplatný prístup k učebným materiálom, prezentáciám a cvičným úlohám ešte 1 mesiac po skončení kurzu,
- videoarchív – videozáznamy z jednotlivých dní zadarmo na 1 mesiac po skončení kurzu.

TM CONSULTING, s.r.o., Dolnohorská 26, 949 01 Nitra, IČO: 36537551, IČ DPH: SK 2020148625
0907 736 117 ▪ kmihalovicova@tmconsulting.sk