KATALÓG SLUŽIEB 2024

NAKIB

ŠKOLENIA PRE SOC SLUŽBY

NÁRODNÁ AKADÉMIA PRE KYBERNETICKÚ
A INFORMAČNÚ BEZPEČNOSŤ

NAKIB.SK

NAKIB

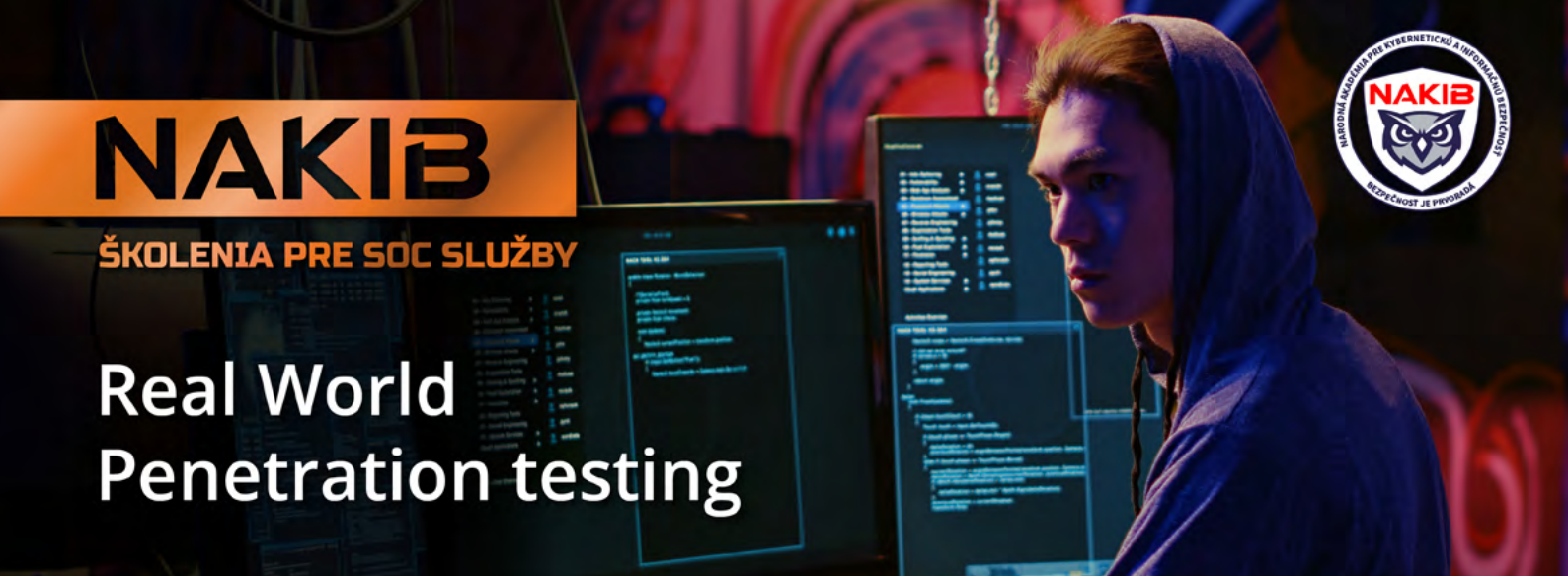
ŠKOLENIA PRE SOC SLUŽBY

Real World Penetration testing

Real World forensics analysis

Real World incident response

NAKIB.SK



ŠKOLENIA NA PRÍPRAVU TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV (SOC) NA KYBERNETICKÚ BEZPEČNOSŤ NA REÁLNE RIEŠENIA INCIDENTOV V ORGANIZÁCII

Čo je?

Vzdelávanie v oblasti Real World Penetration Testing je špecializovaný kurz zameraný na výcvik účastníkov v technikách a metódach používaných na identifikáciu a zneškodnenie zraniteľností v informačných systémoch a sieťových infraštruktúrach. Cieľom je naučiť účastníkov, ako realizovať simulované útoky na systémy s cieľom nájsť a opraviť bezpečnostné slabiny predtým, ako ich využijú skutoční útočníci.
Školenie je rozdelené na 4 časti (rovnako ako samotný proces riešenia incidentov):

- Príprava na riešenie bezpečnostného incidentu
- Detekcia a analýza kybernetického incidentu
- Obmedzenie šírenia bezpečnostného incidentu ,Eradication a Obnova
- Systémové zmeny v bezpečnostnom prostredí organizácie

Prečo?

Zvýšenie bezpečnostných zručností: Kurz poskytuje hlboké pochopenie bezpečnostných hrozieb, zraniteľností a techník ich odhaľovania a eliminácie. Účastníci sa naučia, ako identifikovať a opraviť slabiny, čím zlepšujú svoje schopnosti ochrany IT infraštruktúry. Prevencia bezpečnostných incidentov: V dnešnej dobe, keď sú kybernetické útoky čoraz sofistikovanejšie, je dôležité byť o krok vpred pred útočníkmi. Penetračné testovanie umožňuje organizáciám identifikovať a riešiť bezpečnostné slabiny skôr, ako ich zneužijú zlomyseľní aktéri. Praktické skúsenosti: Kurzy ako Real World Penetration Testing zahŕňajú praktické laboratórne cvičenia, kde účastníci môžu svoje znalosti aplikovať v reálnych scenároch.

Pre koho?

Školenie Real World Penetration testing je určené pre:
Bezpečnostní profesionáli: Tí, ktorí už pracujú v oblasti informačnej bezpečnosti a chcú rozšíriť svoje znalosti a zručnosti v konkrétnych oblastiach, ako je penetračné testovanie. IT profesionáli: Systémoví a sieťoví administrátori, vývojári softvéru a iní IT odborníci, ktorí chcú získať hlbšie porozumenie bezpečnostných hrozieb a ako ich efektívne riešiť. Personál SOC služieb. Konzultanti a audítori kybernetickej bezpečnosti: Odborníci, ktorí poskytujú rady alebo hodnotenia tretích strán, a potrebujú rozumieť metodikám a technikám penetračného testovania na hlbšej úrovni.

Prínosy?

Absolvovanie školenia prináša nasledovné prínosy:
Zlepšená schopnosť identifikovať zraniteľnosti: Účastníci sa naučia, ako používať rôzne nástroje a techniky na odhalenie slabín v IT infraštruktúre, čo je kľúčové pre zabezpečenie systémov pred útočníkmi. Praktické skúsenosti s penetračnými testami: Kurz poskytuje praktické laboratórne cvičenia, ktoré umožňujú účastníkom aplikovať teoretické znalosti v kontrolovanom prostredí. Toto “učenie sa robením” je neoceniteľné a zvyšuje ich sebadôveru pri vykonávaní skutočných penetračných testov. Pripravenosť na kybernetické hrozby: Kurz pomáha účastníkom rozvíjať schopnosti potrebné na rýchlu reakciu na bezpečnostné incidenty a na efektívne zvládanie potenciálnych hrozieb, čo je nevyhnutné pre udržanie bezpečnosti v dynamickom digitálnom prostredí.

ŠKOLENIE PRIPRAVUJE TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV NA KYBERNETICKÚ BEZPEČNOSŤ NA VYKONANIE FORENZNEJ ANALÝZY PRE POTREBY INCIDENT RESPONSE

Čo je?

Školenie obsahuje:
Základy digitálnej forensics: Úvod do princípov a praktík digitálnej forensics, vrátane právnych a etických aspektov.
Zachovanie dôkazov: Metódy a techniky zabezpečenia a ochrany digitálnych dôkazov aby zostali nezmenené a mohli byť použité v súdnych sporoch.
Analýza dát: Použitie špecializovaných forenzných nástrojov na extrahovanie a analýzu údajov z rôznych zdrojov ako sú pevné disky, mobilné zariadenia, sieťové záznamy atď.
Pokročilé forenzné techniky: Detailné štúdium techník ako Steganografia, kryptografia a analýza malvéru.
Reporting a prezentácia nálezov: Výuka o tom, ako efektívne prezentovať zistenia z forenznej analýzy súdom alebo iným zainteresovaným stranám.
Prípadové štúdie a simulácie: Reálné prípadové štúdie a simulované scenáre, kde môžu účastníci aplikovať svoje znalosti a zručnosti v praxi.

Prečo?

Absolvovanie kurzu Real World Forensics Analysis ponúka množstvo dôležitých prínosov pre jednotlivcov aj organizácie. Tento druh vzdelávania je kľúčový pre rozvoj zručností, ktoré sú nevyhnutné na efektívne zvládanie bezpečnostných incidentov a posilnenie celkovej obranné schopnosti systémov. Kurz naučí účastníkov, ako správne zachytiť, analyzovať a interpretovať digitálne dáta po bezpečnostnom incidente. Tieto zručnosti sú neoceniteľné pri vyšetrovaní a mitigácii škôd spôsobených útokmi.

Pre koho?

Kurz Real World Forensics Analysis je určený pre odborníkov, ktorí chcú rozvíjať svoje znalosti a zručnosti v oblasti digitálnej forensics ako sú bezpečnostní profesionáli, členovia SOC tímov, právnici a právni poradcovia, vládni vyšetrovatelia a zamestnanci bezpečnostných agentúr, nezávislí konzultanti a bezpečnostní audítori.

Prínosy?

Rozšírené forenzné zručnosti: Účastníci získajú hlboké pochopenie o tom, ako zachytiť, analyzovať a interpretovať digitálne dáta v súvislosti s bezpečnostnými incidentmi. Tieto zručnosti sú neoceniteľné pri určovaní príčin a rozsahu kybernetických útokov a iných bezpečnostných porušení.
Lepšia schopnosť reagovať na incidenty. Kurz poskytuje prístup k najnovším technológiam a metodikám v digitálnej forensics, čo umožňuje účastníkom zostať na čele v rýchlo sa meniacom poli kybernetickej bezpečnosti.

ŠKOLENIE JE PRIPRAVÍ TECHNICKÝCH ŠPECIALISTOV A ODBORNÍKOV NA REÁLNE RIEŠENIE KYBERNETICKÝCH BEZPEČNOSTNÝCH INCIDENTOV V ORGANIZÁCII

Čo je?

Školenie je rozdelené na 4 časti (rovnako ako samotný proces riešenia incidentov):
• Príprava na riešenie bezpečnostného incidentu
• Detekcia a analýza kybernetického incidentu
• Obmedzenie šírenia bezpečnostného incidentu ,Eradication a Obnova
• Systémové zmeny v bezpečnostnom prostredí organizácie
Každá časť je postavená na reálnych prípadoch a zostavená tak, aby účastníkovi školenia dala poznatky a „hands-on“ pri jednotlivých krokoch riešenia bezpečnostného incidentu.
Scenár incidentu, ktorý sa bude počas školenia riešiť je postavený na reálnom prípade APT útoku na nadnárodnú organizáciu.

Prečo?

Kurz poskytuje účastníkom znalosti a zručnosti potrebné na rýchle a efektívne reagovanie na bezpečnostné incidenty. Toto je kriticky dôležité v dnešnej dobe, keď sú kybernetické útoky čoraz častejšie a sofistikovanejšie.
Minimalizácia škôd a nákladov: Správna reakcia na incidenty môže výrazne znížiť výšku škôd spôsobených útokmi a tým obmedziť finančné a reputačné straty pre organizáciu.
Zlepšenie bezpečnostných postupov: Kurz poskytuje podrobné informácie o najlepších praktikách a stratégiách, ktoré pomáhajú organizáciám zlepšiť ich celkové bezpečnostné postupy a politiky.
Kurz zahŕňa scenáre a simulácie, ktoré účastníkom umožňujú prakticky si vyskúšať a zdokonaliť naučené metódy v kontrolovanom prostredí.

Pre koho?

Školenie Real World incident respons je určené pre:
Bezpečnostní odborníci: Tí, ktorí už pracujú v oblasti kybernetickej bezpečnosti a chcú rozšíriť svoje zručnosti v riadení incidentov. Členovia SOC tímov. IT profesionáli: Systémoví a sieťoví administrátori, ktorí potrebujú zvládať a riešiť bezpečnostné incidenty vo svojich sieťach a systémoch. Incident Response Teams (IRT): Členovia tímov reagujúcich na incidenty, ktorí sa špecializujú na rýchlu a efektívnu reakciu na bezpečnostné incidenty v reálnom čase.

Prínosy?

Zlepšené schopnosti detekcie a reakcie: Účastníci sa naučia, ako efektívne identifikovať a reagovať na bezpečnostné incidenty. Získané znalosti pomáhajú rýchlejšie rozpoznať hrozby a adekvátne na ne reagovať, čo je kľúčové pre minimalizáciu škôd a obnovu normálnej prevádzky.
Zníženie nákladov spojených s incidentmi: Efektívna reakcia na incidenty môže výrazne znížiť náklady spojené s narušením operácií, stratou dát a následnými právnymi alebo regulačnými sankciami. Účastníci sa naučia, ako znižovať tieto náklady prostredníctvom rýchlej a organizovanej reakcie.
Komplexné zvládnutie incident response procesu: