Učebné osnovy
CISCO CCNA Cybersecurity 200-201

1. Kapitola - Úvod do kybernetickej bezpečnosti a počítačových sietí

Spoznáš základy kybernetickej bezpečnosti, najčastejšie digitálne hrozby a motiváciu kybernetických útočníkov. Pochopíš fungovanie bezpečnostného operačného centra (SOC), princípy počítačových sietí a základy IP adresovania, ktoré tvoria nevyhnutný základ pre prácu v oblasti kybernetickej bezpečnosti.

Prax: Prevody medzi číselnými sústavami, tvorba podsietí a rovnomerné aj nerovnomerné rozdeľovanie IP sietí.

Témy:
- Úvod do kybernetickej bezpečnosti
- Aktéri digitálnej kriminality
- Centrum bezpečnostných operácií (SoC)
- Číselné sústavy
- Základy počítačových sietí

2. Kapitola - Princípy komunikácie v počítačových sieťach

Odhalíš, ako medzi sebou komunikujú zariadenia a ako sa prenášajú dáta v počítačových sieťach. Naučíš sa rozumieť protokolom Ethernet, IP, ARP a TCP, fungovaniu sieťových služieb a spôsobom diagnostiky sieťových problémov. Spoznáš nástroje využívané pri analýze sieťovej prevádzky a identifikácii podozrivej komunikácie.

Prax: Diagnostika siete pomocou ping a traceroute, analýza komunikácie v nástroji Wireshark, skúmanie TCP Three-Way Handshake a práca s nástrojom Nmap.

Témy:
- Protokol, protokolová sada
- Ethernet a IP
- Overenie sieťovej konektivity
- ARP
- Sieťové služby
- Transportná vrstva

3. Kapitola - Operačný systém Windows

Oboznámiš sa s fungovaním operačného systému Windows z pohľadu administrátora a bezpečnostného analytika. Spoznáš jeho architektúru, súborový systém, správu používateľských oprávnení a bezpečnostné mechanizmy. Naučíš sa monitorovať systémové procesy, identifikovať neštandardné správanie a efektívne spravovať systém.

Prax: Správa procesov, vlákien a registrov, konfigurácia používateľských účtov a oprávnení, práca s PowerShellom, Správcom úloh a monitorovaním systémových zdrojov.

Témy:
- Architektúra
- Súborový systém
- Konfigurácia a monitorovanie
- Bezpečnosť

4. Kapitola - Operačný systém Linux

Osvojíš si prácu s Linuxom, ktorý tvorí základ mnohých serverových a bezpečnostných riešení. Naučíš sa ovládať príkazový riadok, spravovať súborový systém, používateľské oprávnenia a základné serverové služby. Spoznáš postupy monitorovania systému a vyhľadávania bezpečnostne významných záznamov.

Prax: Práca s Linux Shell, správa textových súborov, navigácia v adresároch, vyhľadávanie systémových logov a nastavovanie prístupových oprávnení.

Témy:
- Práca so shellom
- Linux server a klient
- Administrácia servera
- Súborový systém
- Práca s GUI

5. Kapitola - Prvky prenosu a bezpečnostná infraštruktúra počítačových sietí

Preskúmaš kľúčové technológie a zariadenia zabezpečujúce komunikáciu v počítačových sieťach. Pochopíš význam sieťovej infraštruktúry, princípy jej fungovania a úlohu bezpečnostných prvkov pri ochrane firemných systémov a prenášaných dát.

Témy:
- Prvky sieťovej komunikácie
- Bezpečnostná infraštruktúra počítačových sietí

6. Kapitola - Morfológia kybernetických útokov a hrozieb

Nahliadneš do sveta kybernetických útočníkov a spoznáš techniky, ktorými napádajú počítačové siete, servery a databázy. Naučíš sa rozpoznávať prejavy škodlivého softvéru, analyzovať podozrivú sieťovú komunikáciu a porozumieť princípom ochrany pred kybernetickými útokmi.

Prax: Analýza malvéru, skúmanie DNS prevádzky, rozbor útoku na SQL databázu a identifikácia podozrivých udalostí v serverových logoch.

Témy:

- Vývoj digitálnej kriminality
- Výzbroj kyberútočníkov
- Monitorovanie sietí
- Jadro siete pod útokom
- Sieťové služby pod útokom
- Princípy kybernetickej obrany

7. Kapitola - Piliere kybernetickej bezpečnosti

Získaš prehľad o základných princípoch kybernetickej obrany, riadení prístupu a bezpečnostnom spravodajstve (Cyber Threat Intelligence). Naučíš sa pracovať s bezpečnostnými informáciami, vyhodnocovať systémové udalosti a identifikovať potenciálne riziká v sieťovej prevádzke.

Prax: Interpretácia bezpečnostných logov, analýza sieťovej komunikácie a spracovanie bezpečnostných dát.

Témy:

- Princípy kybernetickej obrany
- Riadenie prístupu
- Kybernetické spravodajstvo

8. Kapitola - Kryptografia, VPN a ochrana koncových zariadení

Objavíš technológie, ktoré chránia citlivé údaje a zabezpečujú digitálnu komunikáciu. Spoznáš princípy šifrovania, hašovania, digitálnych certifikátov a virtuálnych privátnych sietí (VPN). Naučíš sa rozumieť bezpečnostným zraniteľnostiam koncových zariadení a možnostiam ich ochrany.

Prax: Hašovacie algoritmy, šifrovanie a dešifrovanie pomocou OpenSSL a bezpečnostných nástrojov, správa digitálnych certifikátov.

Témy:

- Kryptografia
- Ochrana koncových zariadení
- Posudzovanie zraniteľností koncových zariadení
- Virtual Private Networks (VPN)

9. Kapitola - Technológie bezpečnosti a sieťových protokolov

Prehĺbiš si znalosti o technológiách a protokoloch využívaných na zabezpečenie počítačových sietí. Pochopíš význam bezpečnostných údajov, ich využitie pri monitorovaní sieťovej prevádzky a úlohu pri identifikácii potenciálnych kybernetických hrozieb.

Témy:

- Technológie a protokoly
- Bezpečnostné údaje siete

10. Kapitola - Digitálna forenzná analýza

Vstúpiš do sveta digitálneho vyšetrovania a naučíš sa odhaľovať stopy kybernetických útokov. Spoznáš postupy vyhodnocovania bezpečnostných výstrah, analýzy sieťových dát a identifikácie napadnutých zariadení. Získaš praktické skúsenosti s nástrojmi a postupmi využívanými pri vyšetrovaní bezpečnostných incidentov.

Prax: Práca s nástrojom Snort a pravidlami firewallu, spracovanie bezpečnostných dát, regulárne výrazy, analýza PCAP súborov, protokolov HTTP a DNS, identifikácia kompromitovaných zariadení a vyšetrovanie malvérových útokov na systémy Windows.

Témy:

- Vyhodnocovanie výstrah
- Práca s dátami sieťovej bezpečnosti
- Digitálna forenzná analýza