Seznam zkušebních okruhů pro SZZ v bakalářském oboru Aplikovaná informatika

Předmět: Kriminalisticko-technická činnost v IT

1. Základní pojmy bezpečnosti informačních systém ů a tím spojené kriminalisticko-technické činnosti.
   a) Nebezpečí (hrozby), která hrozí výpočetním systémům. Druhy útoků na počítačové systémy
   b) Uveďte základní principy zajišťování důkazního materiálu pro účely trestního řízení
   c) Řešení – dokumentace kriminalistických stop v souvislosti s napadením systému

2. Příprava domovní prohlídky, prohlídky jiných prostor
   a) Na jaké informace se soustředíte při přípravě na domovní prohlídku, prohlídku jiných prostor (rozdíl mezi nimi, jaký je postup vyžadování orgány činnými v trestním řízení)
   b) Na co si je nutné dávat pozor při řešení jednotlivých druhů tr. činnosti (nejen informační kriminality)
   c) Jaké informace byste si měli zjistit před úkonem

3. Základní pojmy dokumentace digitálních dat pro účely důkazního řízení
   a) Jaké jsou pravidla při zajišťování důkazního materiálu, dat?
   b) Jaký je rozdíl mezi forenzní zálohou dat a uživatelskou zálohou, vysvětlete hlavní odlišnost jednotlivých prostředků
   c) Jaké prostředky použijete pro dokumentaci dat pro účely důkazního řízení a svůj postup zdůvodněte
   d) V jakých případech je nutné provést dokumentaci operační paměti

4. Jak budete postupovat v případě podezření napadení informačních systémů a jejich následnému zneužití k útoku na další systémy
   a) Jak budete postupovat v prostředí firemní sítě
   b) Jak případně ustanovíte konkrétní počítač v počítačové síti
   c) Jak budete postupovat v případě napadení domácího počítače

5. Jakým způsobem provedete dokumentaci dat pro účely důkazního řízení
   a) Jaké informace budete dokumentovat a jaká data vám vzniknou
   b) Jak zadokumentujete předložená data tak, aby byla využitelná pro důkazní řízení
   c) Jaké informace musí obsahovat dokument o zajištění digitální techniky a dat

6. Jaké zákonné normy jsou využívány při řešení informační kriminality a kriminality, kde je využit o telekomunikační techniky
   a) Jakými zákony se orgány činné v trestním řízení musí řídit při řešení kriminality za využití telekomunikační technologie – jaká technika se spadá
   - Podobněji se zaměřte na zákon o kybernetické bezpečnosti
   b) Jak dlouhá je zákonná lhůta, kdy orgány činné v trestním řízení mohou vyžadovat údaje o telekomunikačním provozu, kdy se jedná o telekomunikační provoz, jaký je postup orgánů činných v trestním řízení
   c) Kde naleznete a jaký je postup při vyžadování informací o telekomunikačním provozu, jaká jsou další zákonná omezení (schvalování, upravující zákonná norma)

7. Jaká jsou pravidla při zajišťování telekomunikační technik y, tablety apod.
   a) Jak budete zajišťovat telekomunikační techniku (mobilní telefony, tablety apod.)
   b) Jaká, zde hrozí rizika.
   c) Jaké druhy zkoumání jsou možná (fyzická, logická, souborový systém), jaké mají výsledky a jaké kriminalisticko-technická pravidla v těchto jednotlivých případech nelze dodržet a proč.

8. Základní pojmy a standardy ve forenzní praxi
   a) Jaká je zásada při forenzním zkoumání digitálních dat a s jakými situacemi se můžeme setkat, oproti obecné kriminalisticko-technické činnosti
   b) Jaké druhy bitových kopií znáte a jaké jsou mezi nimi rozdíly (pohled uživatelský a forenzní)
   c) Jaký je rozdíl mezi běžnými uživatelskými prostředky a forenzními prostředky
   d) Jaké úrovně smazaných informací znáte a jak se s tím jednotlivé druhy software vypořádají, viz předchozí bod
   e) Z jakého důvodu není vhodné využívat byť nazývané forenzní prostředky typu freeware, popř. vyhodnoťte tyto prostředky z pohledu zákona, účelně vynaložených prostředků

9. Jak pracují forenzní nástroje pro vyhodnocování digitální h dat
   a) Jak pracují běžné prostředky při identifikaci jednotlivých dat a jak pracují a vyhodnocují data forenzní nástroje
   b) Kde naleznete smazané informace – uveďte jednotlivé stupně smazaných dat
   c) O jaká data se jedná, když nám forenzní nástroj je vyhodnotí jako tzv. Carved data, jaké tyto data mají omezení ve vztahu k jejich identifikaci a dokumentaci a jaké informace mohou obsahovat, princip získání, identifikace forenzními prostředky
   d) Co jsou Slack data a jaké informace v těchto můžeme nalézt (příklady, jejich velikost)
   e) Jakým způsobem naleznete údaje obsažené ve slacku.

10. Analýza komunikačních prostředků – např. Skype , ICQ, Facebook, atd.
    a) Jaké jsou z pohledu forenzní analýzy rozdíly u jednotlivých komunikačních prostředků
    b) Jaké informace můžeme zjistit z jednotlivých dat komunikačních prostředků, je možno identifikovat protistranu? Jakým způsobem.
    c) Jaké prostředky použijete a proč.

11. Analýza emailové komunikace
    a) Jaké informace můžeme získat z emailové komunikace
    b) Jak zjistíme, zda email nebyl podvržen
    c) Jaké informace lze v rámci emailové komunikace podvrhnout
    d) Kde ověříme místo odeslání
    e) Jak budeme analyzovat email, v jakém formátu ho musíme mít

12. Ochrana osobních údajů – základní pojmy.
    a) Co jsou osobní údaje? Jak jsou definovány citlivé údaje?
    b) Operace s osobními údaji, které spadají po pojem „zpracování".
    c) Čím se vyznačuje tzv. nepřímá identifikace fyzické osoby?
    d) Vyjmenujte základní principy ochrany osobních údajů.
    e) Jaké náležitosti musí mít souhlas se zpracováním osobních údajů? Čím se vyznačuje „informovaný souhlas" a čím „výslovný souhlas"?
    f) Co je „povinnost mlčenlivosti", kdo (co) ji ukládá, jaké jsou důsledky porušení této povinnosti? Která instituce v ČR vykonává dozor nad dodržováním zákona o ochraně osobních údajů?

13. Ochrana utajovaných informací – základní pojmy
    a) Základní pojmy ochrany utajovaných informací (legislativa týkající se ochrany utajovaných informací, systém opatření k zjišťování a ověřování podmínek pro přístup a nakládání s utajovanými informacemi).
    b) Utajovaná informace (stupně utajení, funkce bezpečnostního ředitele, poučení, přístup k utajovaným informacím stupně Důvěrné ve firmě).
    c) Podmínky pro získání osvědčení na stupeň utajení Důvěrné a vyšší.
    d) Administrativa ochrany utajovaných informací: Jednací protokol, označování utajovaných dokumentů, přeprava utajovaných informací. stupně Důvěrné.

14. Systémy PKI.
    a) Certifikát.
    b) Žádost o certifikát.
    c) CRL.
    d) Časové razítko.
    e) Certifikační autorita.
    f) Archivace elektronických dokumentů.

15. Zabezpečení webového serveru.
    a) Metody získávání informací o webovém serveru a aplikacích, které jsou na webovém serveru provozovány.
    b) Popište základní nedostatky konfigurace webových serverů a aplikací.

16. Bezpečnost webových aplikací.
    a) Popište základní nedostatky a možné útoky na autentizační mechanizmy webových aplikací. Jak je možné obejít autorizační schéma systému?
    b) Popište, co to je management relace webové aplikace a jaké jsou možnosti jeho zneužití a testování.
    c) Popište problematiku kontroly vstupů webových aplikací a základní útoky, které lze pomocí nedostatečně kontrolovaných vstupů provést.

17. Bezpečnost sítí - odposlech provozu.
    a) Jaká data lze při přenosu sítí odposlechnout? Popište základní vlastnosti ethernetu
        1. souvislosti s možnostmi odposlechu dat.
        2. Jaké jsou možnosti obrany proti odposlechu? Jaký je rozdíl mezi hubem přepínačem v souvislosti s možnostmi odposlechu dat v lokální síti?
        3. Jaké jsou možnosti odposlechu dat na přepínači? Jaké existují metody odposlechu dat v IP sítích?
        4. Popište metody útoků na WIFI sítě. Uveďte bezpečnostní prvky doporučení WPA, WPA2 a 802.11.

18. Škodlivý kód, ochranné strategie.
    a) Škodlivý kód: Uveďte a popište základní kategorie škodlivého kódu. Uveďte příklady prostředí, pomocí kterých se škodlivý kód šíří a obranné strategie, které používá proti odhalení. Popište základní moduly počítačového červa.
    b) Vysvětlete pojem Botnet a možnosti použití botnetu k nelegálním činnostem.

19. Anonymní přístup k Internetu.
    a) Anonymní přístup k Internetu: Popište možnosti identifikace útočníka v IP síti (IP adresa, E-mail).
    b) Jak je možné zůstat anonymní pomocí běžných prostředků? Jaké existují možnosti anonymizace uživatele (IP adresy, E-mail adresy) v Internetu?
    c) Objasněte pojem datová stopa.

20. Sociální inženýrství.
    a) Vysvětlete pojem sociální inženýrství a popište jak se bránit útokům, které jsou na něm založeny. Uveďte příklady útoků založených na metodách sociálního inženýrství.
    b) Problematika poplašných a podvodných zpráv, problematika řetězových e-mailů.

21. Základní pojmy z oblasti bezpečnosti počítačových sítí (Princip sdíleného media, CD vs CA, port mirroring, IDS/IPS).

22. Typy síťových útoků (min 5) a obrana před nimi.

23. Zabezpečení WiFi – vše (od open přes hidden, podvržení SSID, Rogue AP, WEP/WPA/WPA2)

24. Firewally a proxy (popis, blokace, příklad pravidla, DMZ, zone&time based, logování).