Seznam zkušebních okruhů pro SZZ v bakalářském oboru Aplikovaná informatika

Předmět: Bezpečnost a sítě

1. Základní pojmy bezpečnosti informačních systémů.
    a) Nebezpečí (hrozby), která hrozí výpočetním systémům.
    b) Zabezpečení klienta a serveru: Uveďte oblasti, kterým je nutno věnovat pozornost, při zabezpečení počítače.

2. Možnosti zabezpečení systémů.
    a) Jak je možné snížit pravděpodobnost zneužití spuštěných služeb na serveru?
    b) Jak je možné zvýšit zabezpečení počítače na úrovni síťových protokolů?
    c) Jakými způsoby je možné snížit pravděpodobnost napadení klienta virem nebo trojským koněm?
    d) Jakým způsobem lze ověřit zabezpečení výpočetního systému? Jaká jsou pravidla pro vytvoření a zabezpečení silného hesla a silného autentizačního mechanizmu?

3. Monitorování a detekce útoků.
    a) Prostředky, které slouží k monitorování a detekci útoků, na výpočetní systémy.
    b) Vysvětlete pojem a principy fungování IDS.
    c) Vysvětlete pojem a principy fungování honeypotu/honeynetu.

4. Reakce na incident.
    a) Základní body metodologie reakce na incidenty a forenzní analýzy.
    b) Jaká by měla být počáteční reakce na incident? Uveďte základní postupy řešení incidentu.

5. Penetrační test a příslušné metodologie.
    a) Vysvětlete pojem a základní cíle auditu/penetračního testu a uveďte hlavní metodologie, které lze k testování použít.
    b) Metody získávání informací o testované síti.

6. Metody testování webových aplikací.
    a) Jaké jsou metody testování webových aplikací?
    b) Jaké jsou metody identifikace webových aplikací na serveru, adresářů web serveru a vstupních stránek aplikací?

7. 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?

8. 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.

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

10. Zabezpečené internetové protokoly.
    a) Protokol TLS (bezpečný web).
    b) Asymetrická kryptografie.

11. Základní právní předpisy ČR související s problematikou počítačové kriminality.
    a) Uveďte základní metody zneužití výpočetní techniky.
    b) Uveďte základní skupiny trestných činů souvisejících se zneužitím výpočetní techniky.
    c) Uveďte příklady souvisejících trestných činů.

12. Zabezpečení webového serveru.
    a) Popište základní nedostatky konfigurace webových serverů.
    b) Uveďte základní bezpečnostní nedostatky web aplikací.

13. 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.

14. Bezpečnost sítí - odposlech (snifování) provozu.
    a) Jaká data lze při přenosu sítí odposlechnout? Popište základní vlastnosti ethernetu v souvislosti s možnostmi odposlechu dat. Odposlech IEEE 802.11
    b) Jaké jsou možnosti obrany proti odposlechu? Jaký je rozdíl mezi hubem a přepínačem v souvislosti s možnostmi odposlechu dat v lokální síti?
    c) Jaké jsou možnosti odposlechu dat na přepínači? Jaké existují metody odposlechu dat v IP sítích?
    d) Popište metody útoků na WIFI sítě. Uveďte bezpečnostní prvky doporučení WPA, WPA2 a 802.11i.

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

16. 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?

17. 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.

18. Základní pojmy (link agregace, redundance, load balancing, hierarchický model, port mirroring atd.).

19. Úloha přepínače v designu sítě (přepínací tabulka, port security, DHCP ochrana, VLAN ID, VLAN routing, Trunk). Smyčka na L2 (Broadcast storm, STP, TRILL).

20. Základy směrování (popis, princip, TTL, gateway, rozhodování směrovače, směrovací tabulka, statické vs dynamické směrování, redundance brány, objects tracking).

21. Bezdrátová bezpečnost (SSID, WEP, WPA(2), IEEE 802.1x).

22. Firewally (popis, blokace, DMZ, zone-based, ACL, (tvorba, rozdělení a aplikace), Proxy, DPI, IDS/IPS, Honeypot VPN)