Tematické okruhy k magisterské státní zkoušce z povinných předmětů IKB

Informační a komunikační bezpečnost

1. Historie malware a nejznámější ukázky malware. Nebezpečnost malware, příklady. Turingův stroj a Von Neumannovy autoreprodukční automaty. Rekurzivní funkce a funkčnost virů.
2. Kybernetická válka a kybernetická zbraň. Pilíře válečné zóny - vysvětlete postavení a roli malware.
3. Formální definice viru, struktura, operace a fáze. Chování a vlastnosti viru. 7 rozdílů - podobností mezi počítačovými a biologickými viry, stavební bloky viru a jejich funkční pořadí.
4. Statistiky a sledování informací o škodlivých aktivitách malware.
5. Infekce virem. Metody. Oligomorfismus, polymorfismus a metamorfismus, dekryptor, EPO. jeho funkčnost a použití. Zobrazit příklady.
6. Generátor virů, netradiční metody syntézy a mutace virového kódu.
7. Reverzní inženýrství viru, technologie a prostředky.
8. Kryptografické metody a jejich využití v malware (ransomware, ...)
9. Antimalwarové desatero.
10. Závislost malware na OS, hardware, souborovém systému. Reverzní kompatibilita a křížová infekce.
11. Základní obranné strategie malware. Skenování paměti, emulace kódu, obfuskace, šifrování dat, antiemulační a antiheuristické techniky. Rezidentní virus, vysvětlete a zobrazte schematické principy, stealth virus, schematicky princip, techniky stealth.
12. Retrovity. Technologie a principy.
13. Generická struktura počítačového červa. Šíření infekce. Aktualizace červa, interakce mezi rozdílnými typy malware. Červ a mobilní zařízení.
14. Payload. Destruktivní vs nedestruktivní payload. Příklady.
15. Zálohování a obnovení. Frekvence zálohování. Typy zálohovacích technologií a sw. Základní zásady zálohování.
16. Tři úrovně webu, vysvětlete. Prohlížeče, vyhledávače, TOR, DuckDuckGo. Temný vs hluboký web. Silk road a wikipedie temného webu. Bitcoin a temný web. Kyberkriminalita a temný web.
17. Cyberspace. Definice. Počítačový zločin a bezpečnost. 5 pilířů kybernetické bezpečnosti.
18. Rozdíl mezi počítačovou bezpečností a “cybersafety”.
19. Vektor a fáze kybernetického útoku. Malware a útok – CnC, DDoS, Botnet. Zranitelnost.
20. Jaké jsou pokročilé politiky ochrany před hrozbami.
21. Desatero kybernetické bezpečnosti.
22. Penetrační testování softwarových aplikací, penetrate and patch model, popis výhod a nevýhod. Uveďte alternativní přístup, white box, black box a grey box testování
23. Preskriptivní a deskriptivní přístup v procesu vývoje software (z hlediska počítačové bezpečnosti)
24. Cross-site scripting útoky, Útoky typu Cross Site Request Forgery (CSRF)
25. Útoky metodou injection (SQL injection, XPATH injection, OS injection)
26. Útoky za použití metody znepřístupnění služby (DOS, DDOS)
27. Hashovací funkce
28. Správa citlivých dat aplikace (např. práce s konfiguračníma hodnotama, použití vyjímek a způsob jejich zobrazení, etc.), logování dat pro potřeby analýzy počítačových útoků

29. Získání hesla uživatele. Popište možné techniky útoku a obrany proti ukradení hesla
30. Sociální inženýrství, možné způsoby využití, phishing, popis techniky a příklady využití
31. Ukradení sezení (Session hijacking)

Informační a komunikační technologie

1. Symetrické, Asymetrické šifrování - rozdíly, princip použití, příklady algoritmů.
2. Zabezpečení komunikace pomocí SSL/TLS, IPsec a využití ve VPN.
3. Bezpečnost bezdrátových sítí - WiFi, Bluetooth, Zigbee a mobilních sítí.
4. Firewall - základní rozdělení, metody filtrování síťové a transportní vrstvy, stavová inspekce, IPtables.
5. Hashovací funkce - principy funkce, zásady bezpečné hashovací funkce, příklady užití, možné bezpečnostní slabiny.
6. Public Key Infrastructure (PKI) - možnosti distribuce klíčů - DH algoritmus, princip centralizované a decentralizované důvěry (CA, PGP), certifikáty dle X.509, digitální podpis.
7. Intrusivní detekční a protekční systémy - princip funkce, nasazení v síťové topologii, rozdíly využití IDS a IPS, příklady implementace.
8. Secure Shell - transportní a autentizační protokol SSH, verze, využití, příklady implementace.
9. Penetrační testování - princip a účel penetračních testů, příklady nástrojů a systémů.
10. Vývoj kryptografie - transpoziční a substituční šifry, steganografie, příklady známých šifrovacích algoritmů a jejich principů.
11. Protokoly pro zabezpečení multimediálního obsahu - SRTP a ZRTP.
12. Protokol SIP a jeho zabezpečení na úrovni SIP TLS a DTLS.
13. Manipulace s obsahem videa a audia, mixování obsahu, manipulace se SIP signalizací (registrace, redirekce a záměrné ukončování relací).
14. Odhalování zdrojů útoků pomocí honeypotů, penetrační a výkonnostní testování VoIP infrastruktury.
15. Technologie WebRTC a WebSockets z pohledu bezpečnosti v multimédiích - způsoby přenosu signalizace a médií, způsob výměny klíčů, zabezpečení na úrovni vrstev ISO/OSI.
16. Skenování a monitoring v IP telefonii - princip odhalování IP telefonních prvků, možnosti skenování a jejich detekce.
17. Denial of service útoky v IP telefonii - rozdělení DoS, princip funkce a možnosti protiopatření.
18. Man in the Middle v multimediích - možnosti tvorby a nasazení Man in the Middle, rizika zachycení signalizace a médií, detekce a obrana MitM.
19. Steganografie v IP telefonii - principy aplikace steganografických metod v singalizaci a médiích, využití v reálném provozu, způsoby detekce.
20. Sociální útoky ve VoIP - Spam v IP telefonii - principy, metody, využití, Wangiri - princip, metody, využití.
21. Architektura mikroprocesorů v mobilních a embedded zařízeních (ARM, MIPS, x86 - srovnání, instrukční sady, registry), typické integrované periférie, funkce MMU (překlad adres, fyzická/virtuální adresa), mechanismy úspory elektrické energie, možnosti použití.
22. Struktura OS (funkce a vrstvy) a jeho návaznost na hardwarové vybavení zařízení. Vlastnosti monolitického jádra a mikrojádra, jejich srovnání. Systémová volání, jejich význam, implementace a příklady. Real-time operační systémy (RTOS), charakteristika, typy a dělení.
23. Protokolová rodina TCP/IP (Model TCP/IP a jeho vztah k ISO-OSI modelu, fragmentace, IPv4 a IPv6 a jejich zásadní odlišnosti, protokoly a entity transportní vrstvy, ICMP, ARP).

24. Metody sdíleného přístupu ke společnému kanálu (Deterministické vs. pravděpodobnostní, popis mechanismů, konkrétní metody: Přidělení na výzvu, bitmapy, Token Passing, binární vyhledávání, ALOHA, CSMA, CSMA/CD, CSMA/CA).
25. Problémy směrování v počítačových sítích (Směrovač, směrovací tabulka, směrovací vs. směrovaný protokol. Dynamické vs. statické směrování, hierarchické směrování, distance vector vs. link state, typické problémy u distance vector a jejich řešení). Adresování v IP, překlad adres (podoba a reprezentace IP adres, dynamický a statický NAT, PAT).