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. Antimalwarové desatero – aneb jak se bezpečně chovat v kyberprostoru.
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. Závislost malware na OS, hardware, souborovém systému. Reverzní kompatibilita a křížová infekce.
10. Základní obranné strategie malware. Skenování paměti, emulace kódu, obfuskace, šifrování dat, antiemulační a antiheuristické techniky.
11. Rezidentní virus, vysvětlete a zobrazte schematické principy, stealth virus, schematicky princip, techniky stealth.
12. Retroviry. 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. Kryptoměny 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. Desatero kybernetické bezpečnosti.
21. Blockchain technologie a její využití v oblasti počítačové bezpečnosti.
22. Penetrační testování softwarových aplikací, penetrate and patch model, popis výhod a nevýhod. Testování přístupem white box, black box a grey box.
23. Preskriptivní a deskriptivní přístup v procesu penetračního testování a vývoje software. Pro každý přístup uveďte a popište konkrétní příklad rámce nebo standardu.

24. Skriptovací útoky a možnosti obrany proti těmto útokům (PowerShell skripty, JavaScript skripty). Specifika spojená se skriptovacími útoky, vektory infekce, persistentní a nepersistentní útoky.
25. Problém validace vstupů a útoky metodou injection (SQL injection, XPATH injection, OS command injection).
26. Útoky za použití metody znepřístupnění služby (DOS, DDOS), typy útoků a možnosti obrany.
27. Správa citlivých dat aplikace (např. práce s konfiguračními hodnotami, použití výjimek a způsob jejich zobrazení, atp.), logování dat pro potřeby analýzy počítačových útoků.
28. Sociální inženýrství, možné způsoby využití, phishing, popis techniky a příklady využití.
29. Analýza a řízení bezpečnostních rizik. Bezpečnostní audit.
30. Správa identit a přístupu, monitoring.
31. Datová centra: typické komponenty a standardy pro jejich návrh a provoz.
32. Zabezpečení síťové infrastruktury a SAN sítí datových center.

Informační a komunikační technologie

1. Symetrická kryptografie. Principy a příklady algoritmů.
2. Asymetrická kryptografie. Principy a příklady algoritmů.
3. Distribuce klíčů s využitím principů kvantové mechaniky.
4. Zabezpečení komunikace pomocí SSL/TLS, IPsec a využití ve VPN.
5. Bezpečnost bezdrátových sítí - WiFi, Bluetooth, Zigbee a mobilních sítí.
6. Firewall - základní rozdělení, metody filtrování síťové a transportní vrstvy, stavová inspekce, IPtables.
7. Hashovací funkce - principy funkce, zásady bezpečné hashovací funkce, příklady užití, možné bezpečnostní slabiny.
8. Public Key Infrastructure (PKI) - možnosti distribuce klíčů - DH algoritmus, princip centralizované a decentralizované důvěry (CA, PGP), certifikáty dle X.509, digitální podpis.
9. Intrusivní detekční a protekční systémy - princip funkce, nasazení v síťové topologii, rozdíly využití IDS a IPS, příklady implementace.
10. Secure Shell - transportní a autentizační protokol SSH, verze, využití, příklady implementace.
11. Penetrační testování - princip a účel penetračních testů, příklady nástrojů a systémů.
12. Vývoj kryptografie, principy a příklady historických šifer. Steganografie.
13. Protokoly pro zabezpečení multimediálního obsahu - SRTP a ZRTP.
14. Protokol SIP a jeho zabezpečení na úrovni SIP TLS a DTLS.
15. Manipulace s obsahem videa a audia, mixování obsahu, manipulace se SIP signalizací (registrace, redirekce a záměrné ukončování relací).
16. Odhalování zdrojů útoků pomocí honeypotů.
17. Technologie WebRTC a WebSockets z pohledu bezpečnosti v multimédiích - způsoby přenosu signalizace a médií, způsob výměny klíčů, zabezpečení na úrovni vrstev ISO/OSI.
18. Skenování a monitoring v IP telefonii - princip odhalování IP telefonních prvků, možnosti skenování a jejich detekce.
19. Denial of service útoky v IP telefonii - rozdělení DoS, princip funkce a

možnosti protiopatření.

20. Man in the Middle v multimediích - možnosti tvorby a nasazení Man in the Middle, rizika zachycení signalizace a médií, detekce a obrana MitM.
21. Steganografie v IP telefonii - principy aplikace steganografických metod v singalizaci a médiích, vyuižtí v reálném provozu, způsoby detekce.
22. Sociální útoky ve VoIP - Spam v IP telefonii - principy, metody, využití, Wangiri - princip, metody, využití.
23. Generátory SIP a RTP provozu – principy, metody a způsoby nasazení, možnosti tvorby scénářů, implementace.
24. Autentizace v protokolu SIP – SIP žádost a odpověd při vyžadované autentizaci, využívané metody autentizace, předávané autentizační pole a skladba kontrolního řetězce.

Verze okruhů k SZZ z 17.2.2020