Informačná bezpečnosť a hackovanie

1. Vysvetlite základné pojmy:
    - Dôvernosť - k inform8ciam majú prístup iba osoby oprávnené k informáciam pristupovať
    - Integrita - informácie sa menia iba s vedomím oprávnených osôb
    - Dostupnosť - informácie by mali byť kedikoľvek dostupné
    - Autentickosť - informácie, ktoré odišli zo zdroja sú rovnaké ako tie čo došli do ciela
    - Súkromnosť - citlivé informácie by mali byť súkromné, to znamená, že k nim má prístup iba ich vlastník
    - Nepopretie pôvodu - dôkaz o odoslaní informácie zo zdroja
    - Nepopretie prijatia - dôkaz o obdržaní informácie v cieli
    - Identita - súhrn všetkých znakov nejakej entity, človeka, ktoré ho jednoznačne oddelujú od ostatných
    - Autentifikácia - overenie identity, heslo
    - Autorizácia - overenie prístupu, login
    - Anonymita - utajenie identity, napríklad nahradenie mena číslom
    - Pseudonymita - nickname, nahradenie nejakého znaku iným
    - Bezpečnostný incident - spojenie útoku, hrozby a zraniteľnosti, znamná, že došlo k ukradnutiu alebo poškodeniu informácií
    - Hrozba - potenciálny útok, snaha získať citlivé informácie, prírodné katastrofy
    - Zraniteľnosť - slabé miesto v systéme
    - Informačná bezpečnosť - snaha zabezpečiť informácie pred poškodením alebo ukradnutím
2. Popíšte typy hackrov:
    - black hat - prcuje nelegálne so zlými úmyslami

- gray hat - pracuje nelegálne, ale svoje znalosti nezneužíva na zlé úmysly
- white hat - pracuje legálne, etický hacker
- teroristi
- script kidies
- hacktivisti
- fanatici
- sebevražední hackeri

3. Vymenujte fázy hackovania:
    - obhliadka
    - skenovanie
    - získanie prístupu
    - udržiavanie prístupu
    - čistenie stôp
4. Aké problémy musí riešiť etický hacker a ake musí mať zručnosti ?
    - pracuje ako normálny hacker
    - snaží sa nájsť slabé miesta informačného systému
5. Čo je informačná vojna a popíšte dva druhy informačnej vojny:
    - vojna, v ktorej hlavným cieľom je získať čo najviac informácií o konkurentovi, súperovi
    - útočná sa zameriava na získanie týchto informácií
    - obranná sa zameriava na ochranu informácií a opatreniam proti neoprávnenému získaniu informácií
6. Popíšte Zónoovanie sieťovej bezpečnosti:
    - internetová - nekontrolovaná
    - demilitarizovaná - kontrolovaná, rozhranie medzi intra a inter
    - produkčná - obmedzená, kontrolovaná
    - intranetová - kontrolovaná bez prísnych opatrení
    - zóna riadenia - zabezpečená zóna s obmedzeným prístupom

7. Definujte politiku informačnej bezpečnosti a popíšte typy bezpečnostných politík:
    - je to súhrn pravidiel informačnej bezpečnosti, ktoré musia zamestnanci organizácie dodržiavať, “zákony” organizácie týkajúce sa informácií
    - promiskuitna
    - prístupná
    - obozretná
    - paranoidná
8. Uveďte 5 príkladov bezpečnostnej politiky:
    - pravidlá vzdialeného prístupu, VPN
    - zásady sieťového pripojenia
    - pravidlá týkajúce sa hesiel
    - GDPR
    - obmedzenie prístupu k istým stránkam na internete
9. Popíšte kontrolu fyzickej bezpečnosti budovy:
    - vrátnica
    - kamery
    - požiarný systém
    - plot
    - bmedzenie prístupu do areálu
    - alarm
    - zamknuté miestnosti s citlivými informáciami a zariadeniami
    - žiadne vstupné a výstupné zariadenia v serverovni
    - serverovňa v suteréne a správne chladená
    - záložný elektrický zdroj
10. Čo je hodnotenie zraniteľnosti a popíšte druhy hodnotenia zraniteľností:
    - preskúmanie odolnosti systému a jeho schopnosti odolávať útokom
    - zisťuje aké chyby a zraniteľné miesta má daný systém
    - aktívne - používa sa sieťovaý skener

- pasívne - odchytávanie packetov, z ktorých sa následne získavajú informácie
- hostiteľské - hodnotenie konkrétneho, jedného zariadenia
- sieťové - kontrola siete
- hodnotenie bezdrôtovej siete
- interné - skenovanie vnútornej infraštruktúry
- externé - hodnotenie systému zvonku, z pohľadu hackera

11. Čo je penetračné testovanie a popíšte druhy penetračného testovania:
    - je to snaha neoprávnene vniknúť do informačného systému, hack, avšak so súhlasom firmy
    - slúži ako simulácia útoku, nájdenie slabých miest
    - čierna skrinka - žiadne info na začiatku útoku
    - biela skrinka - prístup ku všetkým informáciami organizácie
    - šedá skrinka - obmedzený prístup k info
12. Popíšte fázy penetračného testovania:
    - plánovanie a príprava - získavanie informácií o cieli, prieskum
    - návrh metodiky - vymyslenie nejakého plánu útoku, ako to celé bude postupovať
    - zhromažďovanie informácií o sieti - skenovanie siete a hladanie slabých miest
    - získavanie cieľa - nájdenie slabého miesta a preniknutie do systému
    - stupňovanie privilégií - získavanie prístupu k stále viac a viac informáiam, aj tým, ku ktorým majú prístup len isté osoby z organizácie
    - implementácia, stiahnutie - vloženie výrúsu, spyweru, stiahnutie dôležitých informácií
    - podávanie správ - informovať hackera o stave útoku
    - vyčistenie stôp - aby sa neprišlo n to kto to spravil
    - zničenie artefaktu - zničenie dôkazov o tom, že systém niekto vôbec hackol

13. Vymenujte a popíste 10 techník sledovania, pomocou ktorých môžeme robiť prieskum na internete:
    - sledovanie emailov
    - sledovanie dns
    - sledovanie na sociálnych sieťach
    - sociálne inžinierstvo
    - WHOIS
    - sledovanie informácií z konkurenčných organizácií
    - sledovanie siete
    - sledovanie webových stránok
    - sledovanie pomocou rozšíreného vyhladávania google
    - všeobecné sledovanie na internete - získavanie informácií napríkad s máp
14. Uveďte aké protiopatrenia by ste urobili proti sledovaniu:
    - obmedzenie prístupu zamestnancov k sociálnym sieťam
    - dobrý firewall na perifériach intranetu aby sa útočník nedostal k informáciam o vnútornej sieti
    - nezverejňovať dôležité a citlivé informácie na internete
    - obmedzenie prístupu na podozrivé stránky z vnútra organizácie
    - dohoda o mlčanlivosti
    - vychovávať zamestnancov
    - šifrovanie informácií a ochrana heslom