**IT SIGURNOST:**

1. **Kako funkcionira "Zaobilaženje kontrole pristupa" i navedite/opišite nekoliko primjera.**

NAC (network access control) je čin držanja neovlaštenih korisnika i uređaja izvan privatne mreže. Zaobilaženje kontrole pristupa funkcionira na način da se izbjegne autentifikacija uređaja ili korisnika. Primjer zaobilaženja je korištenje lažne MAC adrese ili MAC ''spoofing''. VoIP telefon ili printer kojem se uzme MAC adresa te se iskoristi kako bi dobili IP adresu s DHCP poslužitelja. Budući da su ti uređaji na popisu dopuštenih jer ne podržavaju 802.1x autentifikaciju. Putem MAC adrese tog uređaja može se doći do mreže.

1. **Što su keyloggeri i kako rade?**

Keyloggeri su vrsta spyware-a koji prate aktivnost tipkovnice (pritisnute tipke) gdje korisnici nisu svjesni da se njihove radnje prate. Oni bilježe svaku interakciju s tipkovnicom koju korisnik ima, dopuštajući trećoj strani da vidi potpuni zapisnik svake e-pošte, trenutne poruke, upita za pretraživanje, lozinke, korisničkog imena ili drugih sljedova s ​​tipkama koje korisnik upiše. Prikupljene podatke šalje trećoj strani koja je odgovorna za instalaciju software ili hardware keylogger-a.

1. **Koje vrste keyloggera postoje (što bilježe)?**

Postoje software i hardware keyloggers koji se mogu koristiti na više načina.

Software keyloggers putem daljinskog pristupa omogućuju pristup lokalno snimljenim podatcima putem virusa i phishing e-mailova. To su programi koji omogućuju hakerima pristup privatnim podatcima, poslodavcima praćenje aktivnost zaposlenika, dok se neki mogu koristi i kao snimači zaslona.

Hardware keyloggers su dio opreme koji se umeće u već postojeći hardware neprimjetno. Primjeri hardware keyloggera su web kamere koje su postavljene da prate unos na tipkovnici, uređaja postavljenih u bankomate koji kroz tipkovnicu prate unos PIN-a te najmanje korištena metoda, metoda zvuka koja prati zvuk koji napravi svaka tipka prilikom pritiska.

1. **Navedite barem 3 keyloggera?**

WinSpy, Invisible Keylogger, Activity Keylogger.

1. **Kako možemo zaštititi naše računalo od keyloggera?**

Od keyloggera se možemo zaštititi na više načina.

* **Koristeći autentifikaciju u 2 koraka** - za provjeru identiteta potrebno je unijeti pin kod poslan na mobilni telefon putem teksta. Sprječava hakere da pristupe računu čak i ako je u mogućnosti ukrasti vaše korisničko ime i lozinku putem keyloggera.
* **Instalacija ažuriranja software-a** – sprječava ubrizgavanje keyloggera u sustav te uklanja postojeće probleme koje hakeri mogu iskoristiti.
* **Instalacija software-a za šifriranje (Key Encryption Software)** - Softver za šifriranje šifrira tipke koje se pritišću na tipkovnici kako bi spriječili keyloggere da zarobe točne informacije. Keylogger će moći zapisivati ​​samo znakove koji se koriste za šifriranje osjetljivih informacija ne i same informacije.
* **Izbjegavanje preuzimanja Crack software-a** - Crack softver besplatan je software često zaražen zlonamjernim softverom te se može instalirati keylogger prerušen u računalni softver.
* **Instalacija Anti Malware software-a (Instalacija programa protiv zlonamjernog softvera)** - program koji štiti od raznih vrsta zlonamjernog softvera kao što su keyloggeri, ransomware, rootkit i trojan. Skenira datoteke koje ulaze u računalo te tako otkriva i sprječava lažni softver. Također redovito skenira računalo u potrazi za zlonamjernim softverom kako bi zaštitio tvrdi disk od zlonamjernog softvera.
1. **Kako možemo otkriti keylogger na našem računalu?**
* **Putem Task Manager-a (Upravitelj zadataka?)** – prikazuje aktivne aplikacije na računalu. Na popisu aplikacija provjera li sumnjivih datoteka, ako je keylogger aktivan, trebao bi biti vidljiv u Upravitelju zadataka. Potrebno je onemogućiti zlonamjernu aplikaciju.
* **Putem opcije Programi i značajke unutar postavki** – prikazuje popis aplikacija koje su instalirane na računalu. Ako se aplikacija čini sumnjivom kod nepotvrđenog izdavača, potrebno ju je provjeriti putem Google-a. Ako nije potrebna, potrebno ju je deinstalirati.
* **Potpuno skeniranje uređaja Anti Malware software-om** – potrebno izvršiti potpuno skeniranje zlonamjernog softvera na računalu. On će skenirati računalo u potrazi za zlonamjernim softverom. Otkrivene prijetnje biti će prikazane kada se završi proces skeniranja. Pritiskom na ukloni biti će uklonjeni.
1. **Što je tehnika steganografije u hakiranju sustava?**

Steganografija je proces skrivanja podataka u drugim vrstama podataka kao što su slike ili tekstualne datoteke. Najpopularnija metoda skrivanja podataka u datotekama je korištenje slika kao skrovišta. Haker može sakriti bilo koji tekst koji se može zamisliti u slici. Čak i nakon dodavanja bajtova podataka, nema povećanja veličine slike. Učitava i sprema u datoteke i stoga može zaobići većinu ''sniffera'' e-pošte.

1. **Što je napad "brute sile" (brute force)?**

Koristi metodu pokušaja i pogreške da pogodi podatke za prijavu, ključeve za šifriranje ili pronađe skrivenu web stranicu. Hakeri prolaze kroz sve moguće kombinacije nadajući se da će točno pogoditi. Ovi napadi se izvode "grubom silom" što znači da koriste pretjerane nasilne pokušaje da pokušaju "nasilno" ući u privatne račune. Brute force napad je jednostavan za implementaciju, te ovisno o snazi zaporke može trajati kratko ili nekoliko tjedana.

1. **Kako funkcionira napad "Brute force"?**

Jednostavni brute force napadi sastoje se od toga da haker pokušava logičkim slijedom pogoditi podatke za prijavu - potpuno bez pomoći softverskih alata ili drugih sredstava. Oni mogu otkriti vrlo jednostavne lozinke i PIN-ove. Npr. lozinka koja je postavljena kao "gost12345". Brute force napadi (poput Dictionary napada) koriste metodu provale u računalo, mrežu ili drugi IT resurs zaštićeno lozinkom sustavnim unošenjem svake riječi u rječniku kao lozinke dodajući po potrebi specijalne znakove. Također (uz mnoge druge) postoje i hibridni brute force napadi koji koriste jednostavni napad + dictionary napad.

1. **Kako se zaštititi od "Brute force" napada?**

Postoji nekoliko osnovnih metoda zaštite od ovakvih napada. One uključuju slijedeće korake:

• ograničenje broja neuspješnih pokušaja pristupa sustavu

• zabranu pristupa s IP adrese s koje su došli neuspjeli pokušaji pristupa

• redovito traženje zapisa o neuspješnim pokušajima pristupa u dnevničkim zapisima

• zatvaranje korisničkih računa za tzv. "gost" korisnike jer će oni biti prva točka upada
 za potencijalne napadače

• kreiranje samo jednog korisničkog računa s najvišim ovlastima.

1. **Što je "napad pogađanja lozinke" i kako se možemo zaštititi od njega?**

Pogađanje lozinki je proces koji uključuje pokušaj dobivanja neautoriziranog pristupa nad

zaštićenim objektima pogađanjem lozinke.

Jačina lozinke je mjera učinkovitosti odupiranja određene lozinke metodama koje se koriste za pogađanje iste. Određuje je nekoliko faktora:

• Dužina – Ima li lozinka dovoljno znakova?
• Kompleksnost – Da li je lozinka kombinacija različitih znakova (slova, brojevi, simboli)?
• Nepredvidljivost – Može li napadač pogoditi lozinku koristeći informacije koje je prikupio o meti?

1. **Što je napad ubrizgavanjem hasha?**

Tehnika u kojoj napadač hvata hash lozinke (za razliku od znakova lozinke) i zatim ga jednostavno prosljeđuje za autentifikaciju i potencijalno pristup drugim umreženim sustavima.

1. **Što je "Man in the Middle attack" i opišite primjer takvog napada kada se spojite na bežičnu pristupnu točku?**

Man in the middle attack je cybernapad u kojem napadač tajno prenosi i eventualno mijenja komunikaciju između dviju strana koje vjeruju da međusobno izravno komuniciraju, budući da se napadač ubacio između dvije strane. Na primjer, lažna bankarska web stranica može se koristiti za prikupljanje financijskih podataka za prijavu. Lažna stranica je "u sredini" između korisnika i stvarne web stranice banke.
2. **Što je "Rainbow table napad" i koja je razlika u odnosu na "Brute force" napad?**

Metoda razbijanja lozinki koja koristi posebnu tablicu ("tablica duge/rainbow table") za probijanje hashova lozinki u bazi podataka. Aplikacije ne pohranjuju lozinke u plaintextu, već umjesto toga šifriraju lozinke pomoću hashova. Nakon što korisnik unese svoju lozinku za prijavu, ona se pretvara u hasheve, a rezultat se uspoređuje sa pohranjenim hashovima na poslužitelju kako bi se tražilo podudaranje. Ako se podudaraju, korisnik je autentificiran i može se prijaviti na aplikaciju. Rainbow table napad se koristi za napad na hashiranu lozinku u obrnutom smjeru dok se brute force napad odnosi na pogađanje lozinke putem znakova.

1. **Koje su prednosti i nedostaci "Rainbow table napada"?**

**PREDNOSTI:**

1. Za razliku od brute force-a, izvođenje hash funkcije nije problem (jer je sve unaprijed izračunato) jer sa već izračunatim vrijednostima, pojednostavljeno je na jednostavnu operaciju pretraživanja i usporedbe na tablici.

2. Nije potrebno znati točan niz lozinke. Ako se hash podudara, nije važno ako niz nije sama lozinka, biti će autentificirana.

**NEDOSTATCI:**

1. Potrebno je velika količina prostora za pohranu.
2. Sa svim već izračunatim vrijednostima, pojednostavljeno je na jednostavnu operaciju pretraživanja i usporedbe na tablici (prednost je i nedostatak također).
3. **Što je DNK napad objasniti kako funkcionira?**

Novi pristup oporavku datoteka zaštićenih lozinkom. U prošlosti, oporavak je bio ograničen na procesorsku snagu jednog stroja. Distributed Network Attack (DNA) koristi snagu strojeva diljem mreže ili diljem svijeta za dešifriranje lozinki. DNA Manager koordinira napad, dodjeljujući male dijelove pretraživanja ključeva strojevima raspoređenim po cijeloj mreži. DNA klijent će raditi u pozadini, oduzimajući samo neiskorišteno vrijeme procesora.
4. **Što je "Rootkit" - objasniti?**
Rootkit je paket zlonamjernog softvera dizajniran za neovlašteni pristup računalu ili drugom softveru. Rootkite je teško otkriti i mogu prikriti svoju prisutnost unutar zaraženog sustava. Hakeri koriste rootkit zlonamjerni softver za daljinski pristup vašem računalu, manipuliranje njime i krađu podataka.
5. **Što je "Zero day" exploit-objašnjenje?**

Eksploatacija nula dana (0 dana) je cyber napad usmjeren na ranjivost softvera koja je nepoznata dobavljaču softvera ili dobavljačima antivirusnih programa. Napadač uoči ranjivost softvera prije nego bilo koja strana zainteresirana za njezino ublažavanje, brzo stvori exploit i koristi ga za napad.

1. **Odaberite antivirusni softver na Internetu i objasnite zašto ste odabrali baš taj softver?**

Pogledajte pitanje 20. i 21. i birajte :D

1. **Navedite 3 glavne funkcionalnosti antivirusnog softvera koje smatrate korisnima za vas i opišite kako rade?**

 Individualno za svakog ali ću stavit dosta opcija pa si izaberite neke (da nemamo svi isto).

Prevencija, detekcija, sposobnost stavljanja datoteke u karantenu umjesto brisanja, zaštita podataka, analiza sustava, dark web monitoring, alati za roditeljsku zaštitu, zaštita u real time-u, skener ''junk'' datoteka, praćenje cookies-a te čistač istih, VPN…

1. **Koja je optimalna cijena koju možete postići za antivirusno rješenje po vašem izboru (mogućnost licenciranja istraživanja i plaćanja)?**

Mislim da pitanje nije bitno pa neću ni odgovarat naširoko ali ima puno – npr. Windows Defender koji je ugrađen i free. Ima Bitdefender koji je za 3 uređaja na 1 godinu 300kn, Norton koji je 1 uređaj na 1 godinu za 60$ …

1. **Što je CIA trianga?**

Povjerljivost, integritet i dostupnost, također poznat kao CIA trijada, model je osmišljen da vodi politike za informacijsku sigurnost unutar organizacije. Model se također ponekad naziva AIC trijada (dostupnost, integritet i povjerljivost) kako bi se izbjegla zabuna sa Središnjom obavještajnom agencijom. Iako su elementi trijade tri najosnovnije i najvažnije potrebe kibernetičke sigurnosti, stručnjaci vjeruju da je trijada CIA-e potrebna nadogradnja kako bi ostala učinkovita.

1. **Što je definicija kibernetičke sigurnosti?**

Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi.

1. **Osmislite lozinku (koju nećete koristiti-samo za vježbu) koristeći „najbolje prakse“**

Osmislite – primjer: Ze1enaJ4buk487!

1. **Koje su faze kibernetičkog napada?**

1.RECONNAISSANCE (hrv. izvidnica)
2.SCANNING (hrv. skeniranje)
3.GAINING ACCESS (hrv. dobivanje pristupa)
4.MAINTAINING ACCESS (hrv. održavanje pristupa)
5.COVERING TRACKS (hrv. prikrivanje tragova)